

ALDERMERE SYSTEMS

SAFE • LAWFUL • EVIDENCE-LED OSINT

OSINT Bible

A Practical, Safe, Evidence-Led Guide to Open-Source
Intelligence

Complete Edition / Six Volumes / Sixty Chapters

v23 Premium Typeset Edition / 2026-06-07

ALDERMERE SYSTEMS

OSINT Bible

A practical, safe, evidence-led guide to open-source intelligence

v23 Premium Typeset Edition

Table of Contents

Volume One - Foundations

- Chapter 1: What OSINT Is and Is Not
- Chapter 2: Ethics, Law, Consent, and Harm Reduction
- Chapter 3: The OSINT Mindset
- Chapter 4: Building Your Workspace
- Chapter 5: Notes, Evidence, and Source Control
- Chapter 6: Search Fundamentals
- Chapter 7: Source Reliability and Bias
- Chapter 8: Identity, Entities, and Attribution Basics
- Chapter 9: Building a Safe Investigation Plan
- Chapter 10: First Complete Mini-Investigation

Volume Two - Search and Sources

- Chapter 11: Search Operators and Query Building
- Chapter 12: News, Archives, and Cached Material
- Chapter 13: Government, Public Records, and Registries
- Chapter 14: Academic, Technical, and Specialist Sources
- Chapter 15: Company and Domain Research
- Chapter 16: Social Platform Search Basics
- Chapter 17: Forums, Marketplaces, and Community Sources
- Chapter 18: Alerts, Monitoring, and Change Detection
- Chapter 19: Building Source Lists
- Chapter 20: Search Workflow Case Study

Volume Three - People, Companies, and Communities

- Chapter 21: Person-of-Interest Research, Safely and Lawfully
- Chapter 22: Username and Profile Correlation
- Chapter 23: Email and Contact Clue Analysis
- Chapter 24: Organisation Mapping
- Chapter 25: Company Ownership and Directorships
- Chapter 26: Job Posts, Leaks of Process, and Public Footprints
- Chapter 27: Community and Network Mapping
- Chapter 28: Reputation, Scams, and Fraud Indicators
- Chapter 29: Handling Ambiguous Identity Matches
- Chapter 30: Entity Investigation Case Study

Volume Four - Images, Maps, and Geolocation

- Chapter 31: Image Search and Reverse Image Search
- Chapter 32: Metadata and File Clues
- Chapter 33: Visual Geolocation Basics

Chapter 34: Maps, Satellite View, and Street-Level Clues
Chapter 35: Weather, Sun, Shadow, and Time Clues
Chapter 36: Transport, Buildings, Signs, and Language Clues
Chapter 37: Video Verification
Chapter 38: Event Verification
Chapter 39: Geolocation Reporting
Chapter 40: Geolocation Case Study

Volume Five - Analysis, Workflows, and Reporting

Chapter 41: Turning Clues into Findings
Chapter 42: Link Analysis and Entity Graphs
Chapter 43: Timeline Building
Chapter 44: Confidence Levels and Analytical Language
Chapter 45: Contradictions and Alternative Explanations
Chapter 46: Report Structure and Evidence Packs
Chapter 47: Redaction and Privacy Protection
Chapter 48: Automation Without Losing Control
Chapter 49: Quality Control Checklist
Chapter 50: Full Investigation Report Case Study

Volume Six - Defensive OSINT and Professional Practice

Chapter 51: Personal Digital Footprint Audit
Chapter 52: Family and Small-Business Exposure Review
Chapter 53: Scam, Fraud, and Impersonation Checks
Chapter 54: Brand and Domain Monitoring
Chapter 55: Incident Support and Evidence Preservation
Chapter 56: Working With Clients or Teams
Chapter 57: Legal Boundaries and Escalation
Chapter 58: Tooling, Maintenance, and Updates
Chapter 59: Building Your OSINT Playbook
Chapter 60: Capstone: Defensive OSINT Operation

Reference Section - Appendices

Appendix A - Glossary
Appendix B - Safe Investigation Checklist
Appendix C - Source Reliability Rubric
Appendix D - Confidence Language Guide
Appendix E - Redaction Checklist
Appendix F - OSINT Report Template
Appendix G - Tool Category Index
Appendix H - Visual Index
Appendix I - Final QC Checklist

Copyright Page

OSINT Bible - Complete Rebuild Edition A Practical, Safe, Evidence-Led Guide to Open-Source Intelligence

Copyright © 2026 Aldermere Systems. All rights reserved.

No part of this publication may be reproduced, distributed, sold, or transmitted in any form without prior written permission from the copyright holder, except for short quotations used for review, education, or lawful commentary.

This publication is provided for education, defensive research, professional development, and lawful public-source intelligence work. It does not grant permission to access private systems, evade security controls, harass individuals, bypass terms of service, impersonate others, collect data unlawfully, or conduct surveillance without appropriate authority.

Aldermere Systems is not a law firm. Nothing in this book is legal advice. Readers are responsible for understanding and obeying the laws, platform rules, employment rules, contract terms, and professional standards that apply in their own jurisdiction and operating context.

Version: Production Structure v23 Build date: 2026-06-07

Safe-Use Disclaimer

This book teaches lawful, ethical, evidence-led OSINT practice using public information, careful documentation, and proportionate investigation methods.

It must not be used for stalking, harassment, doxxing, coercion, blackmail, unlawful profiling, discrimination, unauthorised access, credential attacks, evasion, impersonation, or targeting private individuals beyond a legitimate and lawful purpose.

Before starting any investigation, the reader should confirm:

- There is a legitimate purpose.
- The scope is clearly defined.
- The work is necessary and proportionate.
- The sources are lawful to access.
- Personal information is handled carefully.
- Sensitive information is redacted where appropriate.
- Escalation routes are known before evidence is collected.

Where the work involves clients, employers, safeguarding, fraud, security incidents, legal disputes, journalists, vulnerable people, children, or personal data, obtain appropriate professional guidance before acting.

The safest OSINT operator is not the one who gathers the most. It is the one who gathers only what is necessary, records it accurately, protects it properly, and knows when to stop.

Foreword

Open-source intelligence is often misunderstood. It is not magic, hacking, or guesswork. Done properly, it is disciplined public-source research supported by careful documentation, proportionate scope, and honest reporting.

The purpose of this book is to give the reader a structured way to think, search, verify, record, and report. It is deliberately built around safety, legality, evidence handling, and restraint. Those limits are not obstacles to good OSINT. They are what make OSINT useful, credible, and defensible.

The reader should approach every chapter with the same guiding principle: never turn a clue into a conclusion too early. Treat every finding as something that must be checked, sourced, and explained in plain language.

This rebuild edition is arranged as a practical working manual. It begins with foundations, moves through search and source discovery, handles people and organisations carefully, introduces images and geolocation, then closes with analysis, reporting, defensive checks, and professional practice.

Introduction

The OSINT Bible is designed as a practical guide for people who need to make sense of public information without losing discipline, ethics, or legal boundaries.

It is suitable for defensive researchers, small-business owners, investigators, journalists, safety teams, fraud-awareness work, reputation checks, incident support, training, and personal digital-footprint review. It is not a manual for intrusion, harassment, covert targeting, or bypassing protected systems.

The book is divided into six volumes:

1. **Foundations** - ethics, scope, evidence handling, source discipline, and safe investigation setup.
2. **Search and Sources** - query building, archives, public records, specialist sources, monitoring, and source lists.
3. **People, Companies, and Communities** - careful entity handling, company research, identity ambiguity, and lawful community mapping.
4. **Images, Maps, and Geolocation** - visual clues, metadata, maps, weather, video, event verification, and reporting.
5. **Analysis, Workflows, and Reporting** - turning clues into findings, timelines, confidence language, evidence packs, redaction, automation control, and quality control.
6. **Defensive OSINT and Professional Practice** - personal and business exposure reviews, fraud checks, monitoring, incident preservation, legal escalation, maintenance, playbooks, and the capstone operation.

The aim is not to produce a person who knows every tool. Tools change. The aim is to produce a reader who can think clearly, work safely, preserve evidence, and explain findings honestly.

How to Use This Book

Read the book in order the first time. The early chapters build the discipline that makes the later chapters safe and useful.

For training, each chapter can be treated as a lesson:

1. Read the concept section.
2. Complete the practical exercise.
3. Fill in the relevant worksheet.
4. Check the safe-use notes.
5. Record what was found, what was not found, and what remains uncertain.

For field use, the appendices and worksheets can be printed or copied into a case folder. The most useful recurring documents are the investigation plan, source log, evidence card, entity table, timeline sheet, redaction checklist, and final report template.

For client, workplace, or public-facing use, do not skip the disclaimer, scope statement, redaction process, and quality-control checklist.

Recommended reading paths:

- **Beginner path:** Chapters 1-10, then 41-50.
- **Search path:** Chapters 6, 11-20, 41, 46, and 49.
- **Entity research path:** Chapters 8, 21-30, 42, 44, and 47.
- **Image/geolocation path:** Chapters 31-40, 43, 44, and 49.
- **Defensive review path:** Chapters 1, 5, 9, 51-60.

Volume 1 - Foundations

- Chapter 1 - What OSINT Is and Is Not
- Chapter 2 - Ethics, Law, Consent, and Harm Reduction
- Chapter 3 - The OSINT Mindset
- Chapter 4 - Building Your Workspace
- Chapter 5 - Notes, Evidence, and Source Control
- Chapter 6 - Search Fundamentals
- Chapter 7 - Source Reliability and Bias
- Chapter 8 - Identity, Entities, and Attribution Basics
- Chapter 9 - Building a Safe Investigation Plan
- Chapter 10 - First Complete Mini-Investigation

Volume 2 - Search and Sources

- Chapter 11 - Search Operators and Query Building
- Chapter 12 - News, Archives, and Cached Material
- Chapter 13 - Government, Public Records, and Registries
- Chapter 14 - Academic, Technical, and Specialist Sources
- Chapter 15 - Company and Domain Research

- Chapter 16 - Social Platform Search Basics
- Chapter 17 - Forums, Marketplaces, and Community Sources
- Chapter 18 - Alerts, Monitoring, and Change Detection
- Chapter 19 - Building Source Lists
- Chapter 20 - Search Workflow Case Study

Volume 3 - People, Companies, and Communities

- Chapter 21 - Person-of-Interest Research, Safely and Lawfully
- Chapter 22 - Username and Profile Correlation
- Chapter 23 - Email and Contact Clue Analysis
- Chapter 24 - Organisation Mapping
- Chapter 25 - Company Ownership and Directorships
- Chapter 26 - Job Posts, Leaks of Process, and Public Footprints
- Chapter 27 - Community and Network Mapping
- Chapter 28 - Reputation, Scams, and Fraud Indicators
- Chapter 29 - Handling Ambiguous Identity Matches
- Chapter 30 - Entity Investigation Case Study

Volume 4 - Images, Maps, and Geolocation

- Chapter 31 - Image Search and Reverse Image Search
- Chapter 32 - Metadata and File Clues
- Chapter 33 - Visual Geolocation Basics
- Chapter 34 - Maps, Satellite View, and Street-Level Clues
- Chapter 35 - Weather, Sun, Shadow, and Time Clues
- Chapter 36 - Transport, Buildings, Signs, and Language Clues
- Chapter 37 - Video Verification
- Chapter 38 - Event Verification
- Chapter 39 - Geolocation Reporting
- Chapter 40 - Geolocation Case Study

Volume 5 - Analysis, Workflows, and Reporting

- Chapter 41 - Turning Clues into Findings
- Chapter 42 - Link Analysis and Entity Graphs
- Chapter 43 - Timeline Building
- Chapter 44 - Confidence Levels and Analytical Language
- Chapter 45 - Contradictions and Alternative Explanations
- Chapter 46 - Report Structure and Evidence Packs
- Chapter 47 - Redaction and Privacy Protection
- Chapter 48 - Automation Without Losing Control
- Chapter 49 - Quality Control Checklist
- Chapter 50 - Full Investigation Report Case Study

VOLUME ONE

Foundations

Principles, scope, evidence discipline, and safe investigation setup.

CHAPTERS 1-10



SAFE INVESTIGATION PLANNING BOARD

Plan before you collect

<div></div> <div>1. QUESTION What are you trying to find out?</div> <div></div>	<div></div> <div>2. SCOPE What's in scope? What's the context?</div> <div></div>	<div></div> <div>3. EXCLUSIONS What is out of scope? What will you not pursue?</div> <div></div>	<div> START WITH</div> <div> The objective</div> <div> Key entities</div> <div> Timeframe</div> <div> Public sources</div> <div> Expected output</div>	
<div></div> <div>4. LEGAL/ETHICAL CHECK Is it legal, ethical, and necessary?</div> <div></div>	<div></div> <div>5. SOURCES Which public sources will you use?</div> <div></div>	<div></div> <div>6. COLLECTION RULES How will you collect, store, and document?</div> <div></div>		<div> CONTROL SCOPE CREEP</div> <div><ul style="list-style-type: none">• Define exclusions• Record new leads separately• Re-check necessity• Pause before expansion</div>
<div></div> <div>7. RISKS What are the risks and mitigations?</div> <div></div>	<div></div> <div>8. STOP POINTS When will you pause or stop?</div> <div></div>	<div></div> <div>9. OUTPUT What will you produce and how will it be used?</div> <div></div>		<div> STOP CONDITIONS</div> <div><ul style="list-style-type: none">• Objective met• Insufficient public evidence• Safety concern• Legal concern• Relevance lost</div> <div><ul style="list-style-type: none">• Keep a journal• State assumptions• Prioritize sources• Note uncertainty• Review proportionality</div>



Plan lawful, proportionate, and necessary research only.



Chapter 1 - What OSINT Is and Is Not

***Safety and lawful-use note:** This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.*

Purpose

This chapter gives the reader a clean, beginner-friendly understanding of OSINT. It explains what open-source intelligence is, what it is useful for, and where the boundaries are. The aim is to build confidence without making OSINT sound mysterious, illegal, or only suitable for specialists.

Plain-English Explanation

OSINT means using information that is openly available, lawfully accessible, or provided with permission, then turning that information into useful intelligence.

The important word is not just “open”. The important word is “intelligence”. A random screenshot, web page, post, company record, map view, or news article is not intelligence by itself. It becomes intelligence when it is collected for a reason, checked, compared with other sources, placed in context, and explained clearly.

OSINT is not hacking. It is not breaking into accounts. It is not stealing private data. It is not tricking people into giving you information. It is not harassment, doxxing, stalking, or revenge research. Good OSINT is controlled, documented, lawful, and proportionate.

What Counts as OSINT

OSINT may include information from:

- Search engines.
- News websites.
- Public company records.
- Government registers.
- Maps and satellite imagery.
- Public social media posts.
- Public forums and communities.
- Academic papers and technical reports.
- Domain and website registration clues.
- Publicly released images, videos, and documents.
- Archives and historical snapshots.

The key point is that the material must be legally accessible and used responsibly.

What OSINT Is Used For

OSINT can support many lawful and useful tasks, including:

- Checking whether a story or claim is true.
- Verifying images, videos, or locations.
- Researching a company before doing business with it.

- Detecting scams, impersonation, or fraud indicators.
- Understanding public risk around a brand, domain, or organisation.
- Supporting journalism, academic research, security awareness, or due diligence.
- Reviewing your own digital footprint so you can reduce exposure.

In professional settings, OSINT is often used to answer a defined question. For example:

- “Is this company real and active?”
- “Does this image show the place claimed?”
- “Is this account likely connected to that organisation?”
- “What public information about this domain could expose a business risk?”

A good OSINT question is specific. A bad OSINT question is vague, emotional, or unlimited.

What OSINT Is Not

OSINT is not an excuse to invade privacy. It does not include:

- Guessing passwords.
- Accessing private accounts.
- Bypassing paywalls or login systems.
- Using leaked private data irresponsibly.
- Harassing or exposing private individuals.
- Creating fake identities to manipulate people.
- Installing spyware or tracking tools.
- Attempting to exploit systems or accounts.

A simple rule: if the method requires deception, unauthorised access, intimidation, or technical bypassing, it is not normal OSINT and should be avoided.

The Difference Between Information and Intelligence

Information is raw material.

Intelligence is information that has been checked, organised, and interpreted.

Example:

Raw information: “A public company record shows a business was incorporated in 2022.”

Better intelligence: “The company appears to be legally registered and active, but the available records are limited. This supports existence, but does not by itself prove trading history, financial health, or trustworthiness.”

That second version is more useful because it explains what the evidence does and does not prove.

The OSINT Lifecycle

A safe OSINT workflow usually follows this pattern:

1. Define the question.
2. Set the scope and boundaries.
3. Collect public information.
4. Record where each item came from.
5. Verify with more than one source where possible.
6. Analyse what the evidence means.

7. Report findings clearly.
8. State limitations and confidence level.

This lifecycle prevents messy research. It also protects the researcher from jumping to conclusions.

Why Scope Matters

Scope means the agreed limit of the work.

For example, a safe scope might be:

“Check whether this charity website is genuine by reviewing public records, website clues, domain information, and official references.”

An unsafe or badly scoped version would be:

“Find everything about the person who runs this charity.”

The first version is focused and proportionate. The second version is too broad and risks becoming invasive.

Confidence Levels

OSINT findings should not be written as absolute truth unless the evidence is strong.

Useful confidence language includes:

- Confirmed: supported by strong primary or official evidence.
- Likely: supported by several consistent sources.
- Possible: supported by limited clues but not enough to rely on alone.
- Unclear: evidence is mixed or insufficient.
- Unsupported: the claim is not backed by reliable evidence found during the research.

This protects the reader and keeps the report honest.

Common Beginner Mistakes

New OSINT learners often make the same mistakes:

- Starting with tools instead of questions.
- Saving screenshots without recording where they came from.
- Trusting the first result they find.
- Confusing a name match with an identity match.
- Treating social media claims as facts.
- Ignoring dates.
- Forgetting that old information may no longer be accurate.
- Going beyond the original purpose of the research.

Good OSINT is not about collecting the most information. It is about collecting the right information and explaining it properly.

Safe Practical Exercise

Choose a public organisation, such as a museum, local council service, registered charity, or known business. Do not choose a private individual.

Answer these questions:

1. What is the official website?
2. What public record confirms the organisation exists?

3. What address or contact details are listed officially?
4. Are the website details consistent with the official record?
5. What is one thing you still cannot prove from public information alone?

Write the result in five sentences. Include at least two sources and a confidence level.

Chapter Checklist

By the end of this chapter, the reader should understand that:

- OSINT uses lawful, open, or permission-based information.
- Intelligence is checked and interpreted information, not random data collection.
- OSINT is not hacking, stalking, doxxing, or private account access.
- Good OSINT starts with a clear question and defined scope.
- Findings should include confidence levels and limitations.

Chapter 2 - Ethics, Law, Consent, and Harm Reduction

***Safety and lawful-use note:** This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.*

Purpose

This chapter sets the operating rules for responsible OSINT. It explains why ethical boundaries matter, why legal access is not always the same as responsible use, and how to reduce harm while still doing useful research.

Plain-English Explanation

OSINT often deals with real people, real organisations, and real consequences. Just because something can be found online does not always mean it should be collected, stored, shared, or published.

Responsible OSINT means asking four questions before and during the work:

1. Is this lawful?
2. Is this necessary?
3. Is this proportionate?
4. Could this cause avoidable harm?

If the answer is uncomfortable, the work needs to be narrowed, paused, or escalated to someone qualified.

Legal Is Not Always Ethical

A piece of information may be publicly visible but still sensitive. For example, a person may have accidentally exposed a phone number, home address, family detail, medical clue, or location pattern. Repeating or amplifying that information may create risk.

Good OSINT avoids unnecessary exposure. The aim is to answer the research question, not to collect everything possible.

Consent-Based OSINT

Consent-based OSINT is research performed with permission from the person or organisation being reviewed. Examples include:

- A small business asking for a public footprint audit.
- A family asking what personal details are visible online.
- A charity checking whether scammers are impersonating it.
- A professional checking their own public profile before a job change.

Consent makes the work cleaner, safer, and easier to report.

Proportionality

Proportionality means the depth of research should match the purpose.

A public scam warning may justify collecting website, domain, company, and payment clues. It does not automatically justify publishing private personal details of a suspected individual.

A company due-diligence check may justify reviewing official records and public statements. It does not justify trying to access staff accounts or personal lives.

Data Minimisation

Collect only what is needed.

A good OSINT note should include:

- The finding.
- The source.
- The capture date.
- Why it matters.
- Confidence level.

It should not include unnecessary private details, gossip, or irrelevant personal material.

Redaction

Redaction means hiding or removing sensitive details before sharing a report. Redact information that is not needed for the reader to understand the finding.

Common items to redact include:

- Personal phone numbers.
- Home addresses.
- Email addresses, unless directly relevant.
- Names of family members.
- Full dates of birth.
- Account recovery clues.
- Faces of uninvolved people.
- Vehicle registration numbers, unless relevant and lawful.

The report should prove the point without creating extra risk.

Avoiding Harm

Before sharing OSINT findings, ask:

- Could this help someone harass a person?
- Could this expose a vulnerable person?
- Could this wrongly accuse someone?
- Could this damage a reputation without strong evidence?
- Could this reveal security weaknesses before they are fixed?

If yes, reduce detail, delay publication, anonymise the subject, or escalate responsibly.

Handling Uncertainty

Never dress up weak evidence as certainty. If evidence is unclear, say so.

Bad wording: “This person is definitely behind the scam.”

Better wording: “The same username appears on two public profiles, but there is not enough evidence to confirm both accounts belong to the same person.”

Careful language protects everyone.

Safe Practical Workflow

1. Define the exact purpose of the research.
2. Write down what is out of scope.
3. Use lawful public or permission-based sources only.
4. Collect only relevant evidence.
5. Record source links and capture dates.
6. Mark confidence level.
7. Redact unnecessary personal details.
8. Share only with the correct audience.

Common Mistakes

- Thinking “public” means “free to misuse”.
- Researching people when the question is actually about a company, website, or claim.
- Collecting sensitive personal details without a clear need.
- Publishing findings before checking them.
- Forgetting to redact.
- Allowing curiosity to expand the scope.

Mini Exercise

Take this research question:

“Is this online shop likely to be legitimate?”

Write a safe scope for the investigation. Include:

- What you will check.
- What you will not check.
- What personal information you will avoid collecting.
- What would make you stop and escalate.

Chapter Checklist

By the end of this chapter, the reader should understand that:

- Lawful access and ethical use are not identical.
- OSINT should be necessary and proportionate.
- Consent-based research is safest where possible.
- Sensitive details should be minimised and redacted.
- Uncertainty must be reported honestly.

Chapter 3 - The OSINT Mindset

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Volume: 1 - Foundations **Status:** Rebuilt draft **Purpose:** Teach the mental habits that make OSINT useful, safe, repeatable, and defensible.

3.1 Why Mindset Matters More Than Tools

Good OSINT is not about owning the largest list of tools. It is about asking the right question, controlling assumptions, collecting responsibly, and explaining what the evidence actually supports.

A beginner often thinks OSINT means searching harder. A better investigator learns to search more clearly.

The strongest OSINT work usually comes from simple habits repeated well:

- define the question before collecting anything;
- separate facts from guesses;
- record where information came from;
- check whether a source is original or repeated;
- protect people from unnecessary exposure;
- state confidence honestly;
- stop when the objective has been answered.

The mindset is the operating system. Tools are only accessories.

3.2 Start With the Question

Every investigation should begin with a clear question. Without one, research becomes wandering. Wandering creates bloated notes, weak conclusions, and avoidable privacy risk.

A poor starting question is broad:

“Find everything about this person/company/event.”

A better starting question is controlled:

“What public evidence confirms whether this company operated under this name before March 2024?”

“Can this image be linked to a real location using visible, non-invasive clues?”

“Which public sources support or contradict this claim?”

A good OSINT question should contain:

1. **The target of research** - person, organisation, domain, image, event, claim, or location.
2. **The purpose** - verification, context, risk review, defensive audit, reporting, or education.
3. **The boundary** - what will not be checked, collected, or exposed.
4. **The output** - note, timeline, short answer, evidence pack, report, or visual map.

Before collecting, write one sentence:

“The purpose of this research is to establish _____ using lawful, public, proportionate sources only.”

That sentence keeps the investigation under control.

3.3 Curiosity With Discipline

Curiosity drives OSINT. Discipline makes it safe.

The internet rewards rabbit holes. Every clue can produce five more clues. A name leads to a profile. A profile leads to a photograph. A photograph leads to a location. A location leads to family, workplace, routines, and private life. That does not mean every clue should be followed.

The disciplined OSINT mindset asks:

- Does this answer the original question?
- Is this proportionate to the purpose?
- Is this information genuinely public and lawful to use?
- Could recording or sharing this cause unnecessary harm?
- Am I collecting because it is useful, or because it is interesting?

A professional researcher knows when to stop. Stopping is not weakness. It is evidence control.

3.4 Facts, Clues, Assumptions, and Conclusions

OSINT work becomes unreliable when different types of information are mixed together. Keep them separate.

Fact

A fact is directly supported by a source.

Example:

A company registry page lists “Example Trading Ltd” as incorporated on a specific date.

Clue

A clue is a piece of information that may point toward something but does not prove it alone.

Example:

A username appears on two platforms with the same avatar.

Assumption

An assumption is something believed but not yet proven.

Example:

The same username and avatar probably belong to the same person.

Conclusion

A conclusion is the reasoned answer reached after checking evidence.

Example:

The two accounts are likely linked, but the evidence is not strong enough to identify the user as a named individual.

Good OSINT writing labels these clearly. Bad OSINT presents clues as facts.

3.5 The Three-Column Note Habit

A simple way to stay honest is to keep notes in three columns:

Evidence	What it may mean	Confidence
Source, date, link/reference, captured detail	Interpretation or possible relevance	Low / Medium / High

This prevents premature certainty.

For example:

Evidence	What it may mean	Confidence
Same business address appears on two public company profiles	Companies may be connected, or may only share a registered office provider	Low
Official registry shows same director name and date of birth month/year	Stronger indication of organisational connection	Medium
Company website links directly to the second brand	Direct public connection between entities	High

This habit also makes the final report easier to write because the logic is already visible.

3.6 Think in Layers, Not Leaps

Weak OSINT jumps from one clue to a dramatic answer. Strong OSINT builds layers.

A layered approach might look like this:

1. **Identify the claim** - what exactly is being tested?
2. **Find the original source** - who first said or published it?
3. **Check official or primary records** - registries, original documents, direct publications.
4. **Compare reputable secondary sources** - established reporting, specialist databases, archives.
5. **Look for contradictions** - dates, names, locations, missing context.
6. **Assess confidence** - what is proven, likely, possible, or unsupported?
7. **Report only what is necessary** - avoid dumping unrelated personal detail.

This keeps the investigation grounded.

3.7 The “Could I Explain This?” Test

Before accepting a finding, ask:

“Could I explain how I got here to someone else, step by step, without relying on guesswork?”

If the answer is no, the finding is not ready.

A good OSINT finding should be explainable in plain English:

- what was searched;
- what was found;
- where it was found;
- when it was captured;
- why the source matters;
- what the evidence supports;
- what the evidence does not support.

If a conclusion depends on a hidden leap, the work needs more checking.

3.8 Avoid Confirmation Bias

Confirmation bias is the habit of noticing information that supports the answer you already expect and ignoring information that weakens it.

In OSINT, this is dangerous. It can damage reputations, misidentify people, or turn weak clues into false certainty.

Use these countermeasures:

- Search for evidence that would disprove your current theory.
- Keep a section in your notes called “Alternative explanations.”
- Record contradictions instead of deleting them.
- Do not treat repeated copies of the same claim as independent confirmation.
- Be cautious with usernames, profile pictures, common names, and shared addresses.
- Prefer primary sources over screenshots or reposts.

A useful phrase is:

“What else could explain this?”

That single question improves almost every investigation.

3.9 Do Not Mistake Volume for Truth

Ten websites repeating the same claim may still be one weak source echoed ten times.

This is common with news aggregation, social posts, forum rumours, copied biographies, scam allegations, and product claims. The same wording may appear in multiple places because everyone copied the same original text.

When checking a claim, ask:

- Who is the earliest source I can find?
- Is this source original, or is it quoting someone else?
- Do independent sources confirm the same point separately?
- Are dates consistent?
- Has the claim been corrected, updated, or withdrawn?

OSINT is not a vote-counting exercise. It is source tracing.

3.10 Proportionate Collection

Just because information is public does not mean it should be collected, stored, or shared.

Proportionate collection means gathering only what is needed for the stated purpose.

For example, if the question is whether a business website is legitimate, you may need public company registration details, domain age, contact consistency, trading history, reviews, and payment-risk indicators. You probably do not need unrelated details about staff family members, home addresses, social posts, or private routines.

Proportionate OSINT reduces harm and improves quality. It keeps the report focused.

Use this rule:

Collect the minimum information needed to answer the question responsibly.

3.11 The Safety Pause

Before saving, sharing, or publishing OSINT findings, pause and ask:

1. Does this contain personal information that is not necessary?

2. Could this expose someone to harassment, embarrassment, or physical risk?
3. Have I included private details merely because they were easy to find?
4. Have I separated evidence from opinion?
5. Have I stated confidence honestly?
6. Would redaction make the output safer without weakening the finding?

The safety pause is especially important when dealing with private individuals, children, vulnerable people, victims, witnesses, activists, journalists, or ordinary members of the public who have been pulled into a story.

3.12 The Difference Between Investigation and Intrusion

The OSINT mindset respects boundaries.

OSINT uses lawful, public, permission-based, or otherwise authorised information. It does not require tricking people, bypassing access controls, breaking into accounts, scraping private areas, impersonating others, or pressuring people for information.

A useful boundary test is:

“Would this still be acceptable if I had to describe the method in the final report?”

If the method would need to be hidden because it is deceptive, invasive, or unlawful, it does not belong in this book’s OSINT workflow.

3.13 Calm Language Wins

Good OSINT reporting avoids dramatic language. The job is not to sound impressive. The job is to be accurate.

Instead of:

“This proves the account is fake.”

Write:

“The account shows several indicators consistent with inauthentic activity, including recent creation, reused profile imagery, and repeated promotional text. These indicators are not conclusive on their own.”

Instead of:

“This person is definitely connected to the company.”

Write:

“Public records show a person with the same name listed as a director of both companies. Additional identifiers would be needed before treating this as a confirmed same-person match.”

Calm language protects the researcher and the subject. It also makes the work more credible.

3.14 A Repeatable OSINT Thinking Loop

Use this loop throughout the book:

1. **Question** - What am I trying to answer?
2. **Scope** - What is allowed, relevant, and proportionate?
3. **Collect** - What public sources can answer this?
4. **Record** - Where did each item come from?
5. **Verify** - Is there independent or primary support?
6. **Analyse** - What does the evidence mean, and what else could it mean?
7. **Report** - What can be stated safely and honestly?

8. **Review** - What should be redacted, corrected, or left out?

This loop is simple enough for beginners and strong enough for professional work.

3.15 Mini Exercise: Turning a Messy Question Into a Safe One

Messy question:

“Find out everything about this online seller.”

Safer OSINT question:

“Assess whether this online seller appears legitimate using public business records, website information, marketplace history, review patterns, and contact consistency. Do not collect unrelated personal details.”

Messy question:

“Who is behind this username?”

Safer OSINT question:

“Identify whether this username appears across public platforms and assess whether the accounts are likely connected. Do not attempt to expose a private person’s offline identity unless there is a lawful, proportionate reason.”

Messy question:

“Where was this photo taken?”

Safer OSINT question:

“Use visible public clues in the image to identify a likely location, recording confidence and avoiding any private residential exposure unless directly relevant and safe to report.”

3.16 Chapter Checklist

By the end of this chapter, you should be able to:

- define a clear OSINT question before collecting information;
- separate facts, clues, assumptions, and conclusions;
- avoid mistaking repeated claims for independent confirmation;
- use proportionate collection;
- pause before sharing sensitive findings;
- explain a finding step by step;
- use calm, confidence-based language;
- stop when the question has been answered.

3.17 Key Takeaways

The OSINT mindset is built on disciplined curiosity.

The best investigator is not the person who collects the most. It is the person who asks the clearest question, records evidence carefully, checks alternatives, respects boundaries, and reports only what the evidence supports.

In the next chapter, we turn this mindset into a practical working environment: folders, notes, browser setup, evidence storage, and safe repeatable workspace habits.

Visual Brief for Chapter 3

Visual ID: V01-A **Title:** The OSINT Thinking Loop **Format:** Dark technical workbook diagram with gold/amber accents. **Elements:** Circular loop with eight stages: Question → Scope → Collect → Record → Verify → Analyse → Report → Review. **Style Notes:** Clean, premium, non-aggressive. Avoid hacker imagery, skulls, masks, red warning graphics, or law-enforcement styling. **Caption:** “Good OSINT is not random searching. It is a repeatable thinking loop.”

Chapter 4 - Building Your Workspace

***Safety and lawful-use note:** This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.*

Volume: 1 - Foundations **Status:** Rebuilt draft **Purpose:** Set up a clean, repeatable, low-risk OSINT workspace for lawful research, note-taking, source capture, and report building.

4.1 Why the Workspace Matters

A good OSINT workspace does three things:

1. It keeps research organised.
2. It protects the integrity of evidence.
3. It reduces the chance of accidental harm.

Many poor investigations fail not because the researcher could not find information, but because they could not prove where the information came from, when it was seen, why it mattered, or how it supported the conclusion.

The workspace is the difference between casual searching and controlled research.

For this guide, a workspace does not mean a secretive or aggressive setup. It means a safe, clean, documented environment where lawful public research can be carried out without mixing projects, losing sources, exposing unrelated personal information, or turning a simple question into an uncontrolled rabbit hole.

The rule is simple:

If you cannot retrace your work, you cannot defend your findings.

4.2 The Safe Workspace Principle

A safe OSINT workspace should be:

- **lawful** - only public, authorised, or consent-based material is used;
- **proportionate** - only collect what is needed for the stated purpose;
- **organised** - every project has its own folder and notes;
- **repeatable** - another person could understand the steps taken;
- **separated** - personal browsing, business work, and investigations are not mixed;
- **privacy-aware** - unnecessary personal data is not stored or shared;
- **evidence-aware** - sources are recorded clearly and consistently.

The aim is not to hide wrongdoing or bypass restrictions. The aim is to avoid contamination, confusion, accidental exposure, and sloppy reporting.

4.3 Recommended Folder Structure

Every investigation should have a dedicated folder. Do not scatter screenshots, notes, downloads, and reports across the desktop.

A simple structure is enough:

```
PROJECT_NAME
■
■■■ 00_Admin
■■■ 01_Research_Questions
■■■ 02_Notes
■■■ 03_Sources
■■■ 04_Screenshots
■■■ 05_Downloaded_Public_Documents
■■■ 06_Timelines
■■■ 07_Entity_Maps
■■■ 08_Drafts
■■■ 09_Final_Report
■■■ 99_Archive
```

00_Admin

Use this for the project brief, scope, permissions, client request, or personal reason for the research.

For a defensive personal audit, this might simply be a text file saying:

```
Purpose: Review my own public digital footprint.
Scope: Public search results, public profiles, domain records, and public business listings.
Exclusions: No private accounts, no login bypassing, no contact with third parties.
Output: Short exposure summary and cleanup checklist.
```

01_Research_Questions

This folder holds the questions being answered.

Good questions keep the work controlled:

```
Question 1: What public profiles are linked to this username?
Question 2: Are any old business addresses still visible online?
Question 3: Do public search results expose a personal phone number?
```

Avoid uncontrolled questions such as:

```
Find everything about this person.
```

That is too broad, too risky, and usually unnecessary.

02_Notes

Use this for working notes. Keep notes factual and separate from interpretation.

A useful note format is:

```
Date checked:
Source:
Link or reference:
What was observed:
Why it may matter:
Confidence:
Follow-up needed:
```

03_Sources

Use this for source lists, URLs, archive references, and citations.

A source list should include:

- title or description;
- URL or database reference;
- date and time accessed;
- what the source supports;
- reliability rating;
- whether the source is primary, secondary, copied, or uncertain.

04_Screenshots

Screenshots should be named clearly. Do not leave them as random filenames.

Recommended naming format:

```
YYYY-MM-DD_source-short-description.png
```

Example:

2026-06-07_company-registry_director-listing.png
2026-06-07_search-result_old-address-visible.png
2026-06-07_public-profile_username-match.png

05_Downloaded_Public_Documents

Only store public documents that are necessary for the research.

Examples:

- public company filings;
- published reports;
- official notices;
- publicly available PDFs;
- archived pages saved for citation.

Do not hoard unrelated personal documents. Collection should always match the purpose.

06_Timelines

Use this when dates matter.

A timeline helps when checking:

- whether an event happened before or after another event;
- whether a claim is current or outdated;
- whether a profile changed over time;
- whether a company name, address, or ownership changed;
- whether news articles are repeating old information.

07_Entity_Maps

Use this for relationship diagrams.

Entities can include:

- people;
- companies;
- domains;
- email addresses;
- usernames;
- phone numbers;
- places;
- documents;
- events.

Entity maps should show confidence. A confirmed link and a possible link are not the same thing.

08_Drafts

Use this for draft reports. Keep drafts separate from final outputs.

09_Final_Report

Only final reviewed material belongs here.

99_Archive

Use this when a project is complete. The archive should preserve the final report, source list, and necessary evidence, but avoid retaining unrelated material.

4.4 File Naming Rules

Good file names save time and reduce mistakes.

Use names that explain what the file is without opening it.

Poor file names:

```
screenshot1.png
notes.txt
final.docx
newfinal2.docx
stuff.zip
```

Better file names:

```
2026-06-07_notes_public-profile-review.md
2026-06-07_source-list_company-registry.csv
2026-06-07_screenshot_search-result-old-address.png
2026-06-07_draft_exposure-review-v01.md
2026-06-07_report_exposure-review-final.pdf
```

Recommended pattern:

```
YYYY-MM-DD_type_subject_version.extension
```

Examples:

```
2026-06-07_notes_username-correlation-v01.md
2026-06-07_timeline_company-history-v02.xlsx
2026-06-07_report_brand-monitoring-final.pdf
```

Do not rely on memory. File names are part of evidence discipline.

4.5 Separate Browser Profiles

A basic OSINT workspace should use a separate browser profile for research.

This helps prevent:

- personal bookmarks mixing with research bookmarks;
- personal accounts accidentally appearing in research activity;
- irrelevant browsing history contaminating the project;
- saved passwords or autofill details appearing in the wrong context;
- confusion between personal searches and project searches.

A separate browser profile is not a licence to behave deceptively. It is simply a clean workspace.

Recommended profiles:

```
Personal browsing
Business/admin browsing
OSINT training and research
Client/project-specific research, if needed
```

Do not log in to personal accounts inside a research profile unless the project specifically requires it and the access is lawful and authorised.

4.6 Bookmarks and Source Lists

Browser bookmarks are useful, but they are not enough. A bookmark records where something is. It does not explain why it matters.

Use two layers:

1. **Bookmarks** for quick access.
2. **Source list** for evidence and reporting.

A source list can be a spreadsheet, Markdown table, or notes database.

Minimum fields:

Field	Purpose
Source ID	Short reference code, such as S001
Title	Page, document, or source name
URL/reference	Where it was found
Date accessed	When it was checked
Source type	Official, primary, secondary, social, archive, unknown
Supports	What claim or finding it supports
Reliability	Low, medium, high
Notes	Context, limitations, contradictions

Example:

Source ID	Title	Date accessed	Source type	Supports	Reliability
S001	Official company registry record	2026-06-07	Official/primary	Confirms company name and incorporation date	High
S002	Archived website homepage	2026-06-07	Archive	Shows brand name used in 2023	Medium
S003	Forum comment repeating allegation	2026-06-07	Social/claim	Indicates allegation exists, not that it is true	Low

The key is to record what a source actually supports. A source may prove that a claim was made, but not that the claim is true.

4.7 Screenshots and Capture Discipline

Screenshots are useful because online material can change. However, screenshots are not magic evidence. They must be handled carefully.

A good screenshot should capture:

- the relevant content;
- the page title or context where possible;
- the date and time captured in your notes;
- the URL in a separate source list;
- enough surrounding page detail to understand the content.

Do not rely on cropped fragments alone. A cropped fragment may be useful in a report, but the project folder should retain a fuller capture where possible.

For every screenshot, record:

Screenshot filename:
Source URL/reference:
Date/time captured:
What it shows:
Why it matters:
Limitations:

Limitations are important. A screenshot may show that a page displayed certain information at the time you saw it. It may not prove who created the content, whether it is accurate, or whether it was later corrected.

4.8 Note-Taking Systems

The best note system is the one you will actually use consistently.

Suitable options include:

- plain Markdown files;
- a local notes app;
- a spreadsheet;
- a document editor;
- a case-management notebook;
- a private local knowledge base.

For beginners, Markdown is excellent because it is simple, portable, and easy to back up.

A basic Markdown note can look like this:

```
# Project Notes – Example Research

## Research Question
What public sources confirm whether Example Ltd changed its trading name in 2024?

## Sources Checked
- S001 – Official registry page – confirms legal company name.
- S002 – Archived website – shows previous brand name.
- S003 – News article – mentions rebrand but does not provide documents.

## Findings
- The legal company name did not change according to S001.
- The public-facing trading style appears to have changed according to S002 and S003.

## Confidence
Medium. Official registry confirms legal status, but the trading-name change is supported by secondary and archived web pages.

## Alternative Explanations
- The company may use multiple trading styles at the same time.
- The archived page may represent a temporary campaign rather than a formal rebrand.
```

This kind of note is far stronger than a pile of links.

4.9 Evidence Log Template

Every project should include an evidence log. This can be a spreadsheet or a Markdown table.

Template:

Evidence ID	Date captured	Source	Location/reference	Observation	Supports	Confidence	Notes
E001	YYYY-MM-DD	Source name	URL/ref	What was seen	Which finding it supports	Low/Medium/High	Limitations

Example:

Evidence ID	Date captured	Source	Location/reference	Observation	Supports	Confidence	Notes
E001	2026-06-07	Official registry	Registry record	Company incorporated in 2021	Company existed before 2024	High	Official record
E002	2026-06-07	Archived website	Archive URL	Homepage displayed old trading name	Brand was publicly used before rebrand	Medium	Archive may not show full site context
E003	2026-06-07	Social post	Public post URL	User claimed company closed in 2023	Shows claim existed	Low	Does not prove closure

The evidence log keeps conclusions tied to sources.

4.10 Confidence Labels

Use confidence labels consistently.

High confidence

Use when the finding is supported by strong, direct, reliable evidence.

Example:

High confidence: The official registry lists the company as incorporated on the stated date.

Medium confidence

Use when evidence is credible but incomplete, indirect, or not fully primary.

Example:

Medium confidence: Archived webpages and news coverage indicate the brand was active during this period, but no official announcement was found.

Low confidence

Use when evidence is weak, ambiguous, single-source, or based on clues rather than confirmation.

Example:

Low confidence: The same username appears on two platforms, but there is not enough evidence to confirm both accounts belong to the same person.

Avoid pretending certainty. Honest confidence language makes the work more credible.

4.11 Handling Personal Information

OSINT can easily touch personal information. Handle it carefully.

Before saving personal details, ask:

- Is this detail necessary for the research question?
- Is it lawful and proportionate to collect it?
- Could this expose someone to unnecessary harm?
- Can the finding be reported without including the detail?
- Should the detail be redacted in the final report?

For example, if you are reviewing whether a small business has exposed an old home address online, the final report may not need to print the full address repeatedly. It may be enough to say:

A previous residential address is visible in two public business directory listings. Full details are retained in the private evidence log and should be removed from public listings where possible.

The goal is to solve the problem, not spread the exposure further.

4.12 Redaction Folder

Create a redaction workflow before producing reports.

Suggested folders:

08_Drafts



■■■ Unredacted_Internal_Draft

■■■ Redacted_Sharing_Draft

The unredacted internal draft should be handled carefully and shared only where appropriate. The redacted version should remove unnecessary personal information, sensitive details, and unrelated material.

Common items to redact:

- home addresses;
- personal phone numbers;
- personal email addresses;
- names of unrelated family members;
- dates of birth;
- account recovery clues;
- private identifiers;
- material about minors;
- irrelevant photographs;
- unrelated social profiles.

Redaction is not about hiding the truth. It is about limiting harm and keeping the report proportionate.

4.13 Backups and Version Control

A project is not safe if it exists in only one place.

Use a simple backup rule:

```
Working copy
Local backup
External or cloud backup, if appropriate
```

For sensitive work, consider whether cloud backup is suitable. Some projects should remain local only. Others may benefit from encrypted backup.

Version important files:

```
report-v01.md
report-v02.md
report-v03-reviewed.md
report-final.md
```

Avoid overwriting major drafts. If a conclusion changes, the older draft may explain why.

4.14 Tool List Discipline

Beginners often collect huge lists of OSINT tools. This can become a distraction.

For each tool, record:

- what it is used for;
- whether it is free, paid, local, or cloud-based;
- what data it sends away;
- whether it requires an account or API key;
- whether it is still maintained;
- what risks or limitations it has;
- what kind of output it produces.

A controlled tool register might look like this:

Tool	Purpose	Local/cloud	Account needed	Risk/limitation	Notes
Search engine	General discovery	Cloud	No/optional	Results vary by location and time	Record date searched
Archive service	Historical web pages	Cloud	Usually no	Archive may be incomplete	Good for timeline checks
Spreadsheet	Evidence log	Local	No	Manual discipline needed	Simple and reliable
Diagram tool	Entity maps	Local/cloud	Depends	Can become messy	Label confidence levels

Do not add tools simply because they sound powerful. Add them because they solve a defined problem safely.

4.15 The Workspace Start Checklist

Before starting a project, complete this checklist:

- ☐ Project folder created
- ☐ Scope written
- ☐ Research question written
- ☐ Exclusions written
- ☐ Source list created
- ☐ Evidence log created
- ☐ Screenshot folder created
- ☐ Browser profile selected
- ☐ Personal accounts separated
- ☐ Redaction plan noted
- ☐ Backup location chosen

This may feel slow at first. It saves time later.

4.16 The Workspace End Checklist

Before closing a project, complete this checklist:

- ☐ Final answer matches the original question
- ☐ Findings are linked to evidence IDs
- ☐ Source list is complete
- ☐ Screenshots are named clearly
- ☐ Confidence levels are stated
- ☐ Contradictions are recorded
- ☐ Unnecessary personal data is removed from the report
- ☐ Draft and final versions are separated
- ☐ Backup completed
- ☐ Project archived

A project should end cleanly. Do not leave loose screenshots, half-written notes, and uncategorised downloads scattered across the computer.

4.17 Common Workspace Mistakes

Mistake 1: Searching before defining the question

This creates noise and privacy risk.

Fix:

Write the research question first.

Mistake 2: Saving links without context

A link alone does not explain why it matters.

Fix:

Record what the source supports.

Mistake 3: Mixing personal browsing with research

This causes confusion and accidental exposure.

Fix:

Use a separate browser profile.

Mistake 4: Treating screenshots as full proof

A screenshot may show that something appeared, but not that it was true.

Fix:

Pair screenshots with source notes and confidence labels.

Mistake 5: Over-collecting personal information

Collecting unnecessary personal detail increases harm and liability.

Fix:

Collect only what is needed and redact where possible.

Mistake 6: Using too many tools too early

Too many tools can create messy, unverifiable output.

Fix:

Start with manual source control and add tools only when needed.

4.18 Practical Exercise: Build a Blank OSINT Case Folder

Create a blank practice folder called:

Practice_01_Public_Claim_Check

Inside it, create:

00_Admin
01_Research_Questions
02_Notes
03_Sources
04_Screenshots
05_Downloaded_Public_Documents
06_Timelines
07_Entity_Maps
08_Drafts
09_Final_Report
99_Archive

Then create three files:

01_Research_Questions/research-question.md
03_Sources/source-list.md
02_Notes/evidence-log.md

In `research-question.md`, write:

Research Question

What public evidence supports or contradicts the claim being tested?

Scope

Public web sources only.

Exclusions

No private accounts, no contact with individuals, no bypassing access controls.

Output

Short finding with source list and confidence rating.

In `source-list.md`, write:

Source List

| Source ID | Title | URL/reference | Date accessed | Source type | Supports | Reliability | Notes |

```
|---|---|---|---|---|---|---|
| S001 | | | | | | | |
```

In `evidence-log.md`, write:

```
# Evidence Log

| Evidence ID | Date captured | Source ID | Observation | Supports | Confidence | Notes |
|---|---|---|---|---|---|---|
| E001 | | | | | | |
```

This blank folder becomes the base for future practice investigations.

4.19 Visual Brief - Clean OSINT Workspace

Visual title: Clean OSINT Workspace Layout **Purpose:** Show the difference between messy searching and structured research. **Style:** Dark workbook design, black/charcoal background, amber/gold highlights, clean folder-tree diagram. **Elements:**

- left side: messy desktop with random files, unnamed screenshots, loose links;
- right side: clean project folder with Admin, Questions, Notes, Sources, Screenshots, Timelines, Reports, Archive;
- central arrow labelled “workspace discipline”;
- small footer note: “Clean structure protects evidence, privacy, and repeatability.”

Safety note: Do not include hacker imagery, masks, police badges, surveillance screens, or illegal-access symbolism.

4.20 Chapter Summary

A professional OSINT workspace does not need to be complicated. It needs to be consistent.

The key habits are:

- create a project folder before searching;
- define the question and scope;
- separate sources, notes, screenshots, and reports;
- record dates and source references;
- use confidence labels;
- collect only what is necessary;
- redact unnecessary personal information;
- back up and archive properly.

A clean workspace makes later chapters easier. Search operators, public records, username research, image analysis, timelines, and reports all depend on the same foundation: controlled notes, clear sources, and disciplined evidence handling.

In the next chapter, we build the evidence discipline further by focusing on notes, source control, reliability, and how to keep findings tied to proof.

Chapter 5 - Notes, Evidence, and Source Control

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Volume: 1 - Foundations **Status:** Rebuilt draft **Purpose:** Build disciplined note-taking, evidence capture, citation, version control, and source-management habits so OSINT findings can be checked, explained, corrected, and defended.

5.1 Why Notes Matter

OSINT work can quickly become messy. One search leads to another search. A username leads to a profile. A profile leads to a company page. A company page leads to an old PDF. An old PDF leads to a name, an address, a date, or a contradiction.

Without controlled notes, the researcher can easily forget:

- where a clue came from;
- when it was captured;
- whether it was verified;
- whether it was current or outdated;
- whether it was fact, interpretation, or suspicion;
- whether it was even relevant to the original question.

Good notes are not decoration. They are the backbone of the work.

A weak OSINT result says:

I found this online.

A professional OSINT result says:

This was observed at this source, on this date, using this method, and it supports this specific finding with this confidence level.

The difference is evidence discipline.

5.2 The Core Rule

The core rule for OSINT note-taking is:

Separate observation, interpretation, and conclusion.

These three things must not be mixed together.

Observation

An observation is what was directly seen.

Example:

A public profile using the username example_user_73 displayed the name A. Carter and listed Manchester, UK as the location.

Interpretation

An interpretation explains what the observation might mean.

Example:

This may be relevant because the same username appears on another public platform connected to a Manchester-based photography business.

Conclusion

A conclusion states what can reasonably be said after checking the evidence.

Example:

The two profiles may belong to the same person, but this is not confirmed. More evidence is required before treating the two as a confirmed same-person match.

A common beginner mistake is to jump straight from observation to conclusion: Same username, same person. That is not evidence discipline. It is an assumption.

5.3 The OSINT Case Journal

Every investigation should have a case journal. This can be a Markdown file, text file, spreadsheet, note database, or paper notebook. The format matters less than consistency.

A case journal records the work as it happens.

Recommended journal format:

Date:
Time:
Researcher:
Case or project name:
Research question:
Action taken:
Search terms or source checked:
Result observed:
Evidence captured:
Follow-up required:
Confidence:
Notes:

Example entry:

Date: 2026-06-07
Time: 10:15 BST
Researcher: Billy
Case: Example defensive footprint review
Research question: Is the old business phone number still publicly visible?
Action taken: Searched exact phone number in a search engine using quotation marks.
Search terms or source checked: "01234 567890"
Result observed: One old directory listing appeared in search results.
Evidence captured: Screenshot saved as 2026-06-07_search-result_old-phone-number.png
Follow-up required: Check whether the directory listing page itself is still live.

Notes: Search result snippet may be cached or outdated; must verify from the original page before reporting as a live exposure.

The journal should be written in plain language. It is not there to impress anyone. It is there to make the work retraceable.

5.4 Evidence Cards

An evidence card is a small structured note for one useful piece of evidence. It prevents screenshots and links from becoming meaningless later.

Use this template:

Evidence ID:
Short title:
Source type:
Source name:
URL or reference:
Date/time accessed:
Captured by:
What it shows:
Why it matters:
Reliability:
Limitations:
Related evidence:

Storage location:

Example:

Evidence ID: EVID-0007
Short title: Old public directory listing showing business phone number
Source type: Public web directory
Source name: Example Local Directory
URL or reference: [URL recorded in source list]
Date/time accessed: 2026-06-07 10:22 BST
Captured by: Billy
What it shows: The page displays the business name and an old phone number.
Why it matters: The number may still be exposed publicly after the business stopped using it.
Reliability: Medium
Limitations: Directory pages may be outdated, scraped, or abandoned.
Related evidence: EVID-0006 search-result screenshot
Storage location: 04_Screenshots/2026-06-07_directory_old-phone-number.png

Evidence cards are especially useful when a case grows. They allow you to build a final report from small, checked blocks instead of relying on memory.

5.5 Source Lists

A source list is not the same as a pile of bookmarks.

A bookmark says:

Here is a page.

A source list says:

Here is a page, here is when it was checked, here is what it supports, and here is how reliable it appears to be.

Recommended source-list fields:

Source ID
Title or description
URL or reference
Source type
Date/time accessed
What it supports
Reliability rating
Limitations
Evidence files linked
Follow-up status

Example:

SRC-001
Public company registry profile for Example Ltd
Official registry page
Official public registry
2026-06-07 10:40 BST
Supports company existence, registered name, company number, and filing history
High for registry facts; not proof of current trading activity
May not show all operational details
EVID-0010, EVID-0011
Checked

A source can be reliable for one fact but weak for another.

For example, an official company registry may be strong evidence for a company number, registered office, and filing dates. It may not prove what the company actually does day to day, whether a website is controlled by the same people, or whether a named person personally operates a social account.

5.6 Naming Evidence Files

Evidence files should be named so they make sense without opening them.

Recommended format:

YYYY-MM-DD_EVID-ID_source-short-description.ext

Examples:

2026-06-07_EVID-0001_search_exact-username-results.png
2026-06-07_EVID-0002_public-profile_about-page.png

2026-06-07_EVID-0003_company-registry_filing-history.pdf
2026-06-07_EVID-0004_archive_old-homepage-snapshot.png

Avoid names like:

image.png
screenshot new.png
proof.png
john_stuff.png
important!!!!.png

Poor file names create confusion later. They also make it harder to remove unnecessary personal data at the end of the project.

5.7 Screenshot Discipline

Screenshots are useful, but they are not magic proof. They need context.

A useful screenshot should normally include:

- the visible page content;
- the page title or recognisable header;
- the date/time if available;
- enough surrounding context to understand what is being shown;
- a matching source-list entry;
- a matching evidence-card entry.

A screenshot by itself can be misleading. It may be cropped, old, edited, out of context, or taken from a copied page.

When possible, preserve:

Screenshot + URL/reference + date accessed + note explaining why it matters

Do not edit original screenshots except to create a separate redacted copy for sharing. Keep the original evidence file untouched.

A safe workflow is:

Original screenshot saved in evidence folder
Redacted copy saved separately for reports or sharing
Source entry recorded in source list
Evidence card completed
Journal entry updated

5.8 Original, Working, and Redacted Copies

A disciplined evidence folder separates original material from working and redacted material.

Recommended structure:

04_Screenshots
■
■■■ Originals
■■■ Working_Copies
■■■ Redacted_For_Report

Originals

Originals are kept unchanged. Do not crop, annotate, overwrite, rename repeatedly, or draw on them.

Working Copies

Working copies can be cropped, marked, highlighted, or annotated while analysing.

Redacted Copies

Redacted copies are used in reports, presentations, or client packs. They remove unnecessary personal information.

Redaction should hide information that is not needed, such as:

- private addresses;
- unrelated phone numbers;
- unrelated usernames;
- children's information;
- health details;
- passwords, tokens, private keys, or account identifiers;
- personal details of bystanders or unrelated people.

The aim of OSINT reporting is to explain the finding, not expose everyone connected to the page.

5.9 Version Control for Notes and Reports

Source control means keeping track of changes.

For simple projects, a plain version naming system is enough:

```
report_v01_draft.md
report_v02_reviewed.md
report_v03_redacted.md
report_v04_final.md
```

For larger projects, a local Git repository can be useful for text notes, Markdown files, templates, and reports. Git is not required for beginners, and it should be used carefully because it can preserve sensitive text in history.

Safe beginner rule:

Use Git for templates, indexes, and non-sensitive working documents. Be careful before adding evidence files or personal data.

If using Git locally, keep the repository private and local unless there is a clear reason to share it.

Do not upload case evidence to public repositories.

Do not upload private personal data to public cloud tools by accident.

Do not use version control as a dumping ground for everything.

5.10 The Change Log

Every serious OSINT project benefits from a change log.

A change log records important changes to the project, not every tiny note.

Example:

```
# Change Log

## 2026-06-07
- Created project folder.
- Defined scope: defensive review of public exposure only.
- Added first source list.
- Captured EVID-0001 to EVID-0004.
- Removed unrelated screenshot from evidence folder after review.

## 2026-06-08
- Verified old directory listing is still live.
- Added redacted report copy.
- Updated finding confidence from Medium to High.
```

The change log is useful when returning to a project later. It also helps another reviewer understand what happened and when.

5.11 Confidence Levels

Notes should record confidence. Not all findings are equal.

A simple confidence scale:

High – supported by strong, direct, current evidence.
Medium – supported by useful evidence, but with some limitations.
Low – possible clue only; needs more verification.
Unknown – recorded but not assessed yet.
False / discounted – checked and found not to support the finding.

Examples:

High: Official registry confirms company number and registered name.
Medium: Two public profiles share a username and location, but no direct link confirms same owner.
Low: A forum mention may refer to the same person, but the name is common.
False: Search result snippet looked relevant, but the live page showed a different person.

Confidence is not a guess about whether the researcher feels certain. It is a statement about how strong the evidence is.

5.12 Recording Contradictions

Contradictions are not failures. They are useful.

A contradiction may show that:

- one source is outdated;
- one source copied another source incorrectly;
- two people share the same name;
- a company changed address;
- a profile was reused or renamed;
- a claim is exaggerated;
- a timeline is wrong.

Do not hide contradictions. Record them.

Contradiction note template:

Contradiction ID:
Finding affected:
Source A says:
Source B says:
Date of Source A:
Date of Source B:
Possible explanation:
Current confidence:
Follow-up required:

Example:

Contradiction ID: CON-003
Finding affected: Current business address
Source A says: Address is 10 High Street
Source B says: Address is 24 Station Road
Date of Source A: 2021 archived listing
Date of Source B: 2026 official registry
Possible explanation: Business moved; old directory not updated
Current confidence: High confidence in official registry for registered address; low confidence in old directory for current address
Follow-up required: Check company website contact page

This prevents the report from becoming overconfident.

5.13 Avoiding Evidence Hoarding

Good OSINT does not mean collecting everything.

Evidence hoarding creates problems:

- it increases privacy risk;
- it makes review harder;
- it fills storage;

- it mixes relevant and irrelevant material;
- it makes deletion and redaction more difficult;
- it may create unnecessary exposure for unrelated people.

Before saving something, ask:

Does this directly support the research question?
 Is it lawful and proportionate to keep?
 Could I describe the finding without storing this personal detail?
 Can I redact unnecessary information?
 How long does this need to be retained?

A professional researcher collects enough to support the finding, not enough to overwhelm the folder.

5.14 Audit Trail

An audit trail is the path from question to conclusion.

Research question → search/source checked → observation → evidence captured → analysis note → confidence rating → final finding.

If one link in that chain is missing, the finding becomes weaker.

Example:

Question: Is the old phone number still public?
 Source checked: Exact phone-number search and live directory page
 Observation: Directory page displays old phone number
 Evidence: Screenshot and source entry saved
 Analysis: Directory appears live but may be outdated
 Confidence: Medium for public exposure; low for current business use
 Finding: Old number remains publicly visible on at least one directory page
 Report citation: EVID-0007 / SRC-004

This is the level of discipline that turns ordinary searching into useful OSINT.

5.15 Basic Templates

Case Journal Template

Case Journal

Project name:
 Researcher:
 Start date:
 Purpose:
 Scope:
 Exclusions:

Entry
 Date/time:
 Research question:
 Action taken:
 Source or search used:
 Observation:
 Evidence captured:
 Interpretation:
 Confidence:
 Next step:

Evidence Card Template

Evidence Card

Evidence ID:
Short title:
Source ID:
Source type:
URL/reference:
Date/time accessed:
Captured by:
Original file:
Redacted file:
What it shows:
Why it matters:
Reliability:
Limitations:
Related evidence:
Notes:

Source List Template

Source List

Source ID	Source Title	Source Type	Date Accessed	Supports	Reliability	Limitations	Evidence IDs
SRC-001	Official registry profile	Primary	2026-06-07	Corporate status	High	Filing lag	E001, E002

Finding Template

Finding

Finding ID:
Short title:
Question answered:
Summary:
Evidence used:
Confidence:
Limitations:
Alternative explanations:
Recommended action:
Recommended action:

5.16 Mini Exercise - Build a Dummy Evidence Pack

Create a practice folder for a harmless subject, such as your own public website, a public company page, or a made-up training target.

Use this structure:

```
Training_Case_001
├──
├── 00_Admin
├── 02_Notes
├── 03_Sources
├── 04_Screenshots
├── 05_Originals
├── 06_Working_Copies
├── 07_Redacted_For_Report
├── 08_Final_Report
```

Then create:

1. one case journal;
2. one source list;
3. three evidence cards;
4. three screenshots or source references;
5. one short finding;
6. one redacted example copy.

The aim is not to investigate deeply. The aim is to practise evidence discipline before using these habits on real work.

5.17 Common Beginner Mistakes

Avoid these mistakes:

- saving screenshots without URLs or notes;
- mixing personal browsing and project research;
- treating old cached snippets as current evidence;
- copying claims without recording the original source;
- confusing a username match with confirmed identity;
- editing original evidence files;
- collecting unrelated personal data;
- failing to record contradictions;
- using dramatic language in notes;
- reporting a finding without confidence level or limitations.

The safest OSINT work is usually calm, boring, and well documented.

5.18 Chapter Checklist

Before moving on, make sure you can answer yes to these:

Can I separate observation, interpretation, and conclusion?
Can I create a case journal entry?
Can I create a source-list entry?
Can I create an evidence card?
Can I name evidence files clearly?
Can I preserve originals and create redacted copies separately?
Can I record confidence levels and contradictions?
Can I build an audit trail from question to finding?

If yes, you are ready to move into search fundamentals.

5.19 Visual Brief

Visual ID: V12 **Title:** Evidence discipline chain **Concept:** A clean left-to-right workflow showing how an OSINT finding is built from a research question. **Flow:** Research question → source checked → observation → evidence card → confidence rating → finding → report citation. **Style:** Dark technical workbook layout, amber/gold highlights, clean icons, no law-enforcement styling, no hacking imagery. **Purpose:** Show that a conclusion is only as strong as the recorded path behind it.

Chapter Summary

Notes, evidence, and source control are what make OSINT reliable.

The key habits are simple:

- write down what you did;
- separate facts from interpretation;
- capture sources clearly;
- preserve originals;
- redact unnecessary personal information;
- record confidence and limitations;
- keep an audit trail from question to finding.

From this point onward in the OSINT Bible, every technique should be treated through this discipline. Search skills are useful, but evidence discipline is what makes the result worth trusting.

Chapter 6 - Search Fundamentals

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Purpose of This Chapter

Search is the first practical skill most people associate with OSINT, but good OSINT search is not simply typing a name into a search box and hoping for the best.

A professional search is planned, logged, repeated, narrowed, widened, checked, and challenged. The aim is not to collect as many links as possible. The aim is to answer a defined question using public, lawful, and verifiable information.

This chapter introduces the basic search habits that support every later chapter in the OSINT Bible.

By the end of this chapter, the reader should be able to:

- Turn a vague question into searchable components.
- Build simple search strings without overcomplicating the task.
- Use keywords, phrases, exclusions, and variants responsibly.
- Keep a search log that allows the work to be repeated.
- Avoid common search mistakes such as confirmation bias and source drift.
- Decide when to widen, narrow, pause, or stop a search.

1. Search Starts With a Question

Every useful search begins with a question.

Poor starting point:

“Find everything about this subject.”

Better starting point:

“What public information confirms whether this organisation operates at this address?”

Even better:

“Can I find at least two independent public sources showing that Organisation A used Address B during 2024?”

The second and third versions are stronger because they define:

- The subject.
- The claim being tested.
- The type of evidence needed.
- The time period.
- The stopping point.

Without a clear question, OSINT quickly turns into wandering. Wandering creates messy notes, weak findings, and accidental privacy risk.

Working Rule

Before searching, write one sentence that begins with:

“I am trying to establish whether...”

Examples:

- “I am trying to establish whether this company name is connected to this website.”
- “I am trying to establish whether this image appeared online before the date claimed.”
- “I am trying to establish whether this event was reported by a reliable local source.”
- “I am trying to establish whether this username appears on public profiles belonging to the same person.”

The search may evolve, but the starting question keeps the work under control.

2. Break the Question Into Searchable Pieces

A search question usually contains several searchable components.

Example question:

“Is Blue Harbour Repairs Ltd connected to blueharbour-repairs.co.uk?”

Searchable pieces might include:

- Blue Harbour Repairs Ltd
- Blue Harbour Repairs
- blueharbour-repairs.co.uk
- blueharbour repairs uk
- Company number, if known.
- Address, if known.
- Director names, if publicly available and relevant.
- Email domains, if publicly displayed.

Do not search only one version. Real-world data is messy. Names are abbreviated, hyphenated, misspelled, translated, rebranded, and copied between sites.

Component Types

Useful search components include:

Component Type	Examples
Exact names	Person name, organisation name, project name
Identifiers	Company number, charity number, domain, username
Contact details	Public email, public phone number, office address
Dates	Year, month, event date, publication date
Locations	Town, county, country, venue, region
File or page clues	PDF title, page heading, document code
Language variants	Local language spelling, abbreviations, transliterations

The stronger the component, the more useful it is likely to be. A company number is usually stronger than a common trading name. A full domain is usually stronger than a generic brand phrase.

3. Start Broad, Then Narrow

A good search often moves through three stages:

1. **Broad discovery** - find the general landscape.
2. **Targeted search** - focus on specific names, domains, dates, or sources.
3. **Verification search** - test whether the early findings are correct.

Broad Discovery

Broad discovery is useful when you know little about the subject.

Example:

"Blue Harbour Repairs"

This may reveal websites, directory listings, news articles, reviews, archived pages, social profiles, or unrelated results using the same phrase.

Targeted Search

Once you identify stronger clues, target them.

Examples:

"Blue Harbour Repairs" "Kent"
"Blue Harbour Repairs Ltd"
"blueharbour-repairs.co.uk"

Verification Search

Verification search challenges the first story that appears.

Examples:

"Blue Harbour Repairs" "dissolved"
"Blue Harbour Repairs" "complaint"
"Blue Harbour Repairs" "Companies House"
"blueharbour-repairs.co.uk" "contact"

The purpose is not to assume wrongdoing. The purpose is to check whether the early information is complete, current, and reliable.

4. Use Exact Phrases Carefully

Quotation marks ask many search engines to look for an exact phrase.

Example:

"Blue Harbour Repairs Ltd"

This is useful when the words must appear together in that order.

Exact phrase searching is helpful for:

- Full names.
- Company names.
- Document titles.
- Specific claims.
- Unique phrases from a webpage or article.
- Error messages or technical strings.

But exact phrases can also hide useful results. If a page says `Blue Harbour Repair Limited` instead of `Blue Harbour Repairs Ltd`, an exact phrase search may miss it.

Working Rule

Run both exact and loose versions.

Example:

"Blue Harbour Repairs Ltd"

Blue Harbour Repairs Ltd
Blue Harbour Repairs Limited
"Blue Harbour Repairs"

Record which version produced the useful result.

5. Use Variants and Misspellings

People, companies, and platforms do not write names consistently.

A person called Jonathan Smith might appear as:

- Jonathan Smith
- Jon Smith
- J Smith
- J. Smith
- Johnny Smith
- Jonathan A Smith
- A username or nickname.

A company might appear as:

- Full legal name.
- Trading name.
- Abbreviated name.
- Former name.
- Domain name.
- Social handle.
- Misspelled directory listing.

This does not mean all matches are the same entity. Variants are leads, not proof.

Variant Table

When working on a subject, create a small variant table:

Type	Variant	Notes
Legal name	Example Repairs Ltd	From official register
Trading name	Example Repairs	Seen on website
Domain	example-repairs.co.uk	Public website
Social handle	@examplerepairs	Needs verification
Possible abbreviation	ER Ltd	Weak lead only

This prevents confusion later.

6. Search by Source Type

Not all searches should begin in a general search engine. Sometimes it is better to search a specific source type.

Common source categories include:

Source Type	Use Case
Official registers	Companies, charities, licences, public bodies
News archives	Events, controversies, announcements, timelines
Maps and business listings	Addresses, premises, local context

Source Type	Use Case
Academic sources	Research, technical claims, expert publications
Social platforms	Public statements, profiles, community activity
Domain records	Website ownership clues, historical technical clues
Archive services	Earlier versions of public webpages
Court or regulator pages	Formal decisions, sanctions, notices

A search engine may help find these sources, but the source itself often gives better context.

Working Rule

Ask:

“What type of source would know this best?”

If you are checking a company registration, an official company register is better than a random directory.

If you are checking whether an image appeared before a certain date, an archive, reverse image search, or earlier publication may be better than a recent repost.

If you are checking an event, local news, official statements, and dated posts may be more useful than commentary.

7. Search Logs

A search log records what you searched, where you searched, when you searched, and what happened.

This matters because search results change. Ranking changes. Pages disappear. Search engines personalise results. A useful result found today may be harder to find tomorrow.

Basic Search Log Template

Date/Time	Search Tool	Query	Result	Action
2026-06-07 10:20	Search engine	"Example Repairs Ltd"	Official register found	Saved evidence card E001
2026-06-07 10:24	Search engine	"example-repairs.co.uk"	Website and directory listing found	Captured screenshots
2026-06-07 10:31	Official register	Company name	Active company found	Added company number

A search log does not need to be fancy. It needs to be consistent.

What to Record

At minimum, record:

- Date and time.
- Search tool or source.
- Exact query or source path.
- Useful result found.
- Evidence card number or screenshot reference.
- Dead ends if they matter.

Dead ends matter when they prevent repeated wasted work.

Example:

“Searched local news archive for organisation name and town. No result found between 2020 and 2024.”

That note may be useful later.

8. Do Not Trust the Snippet Alone

Search result snippets are previews. They are not evidence by themselves.

A snippet can be:

- Out of date.
- Automatically generated.
- Taken from old page content.
- Missing context.
- Based on text that no longer appears on the page.
- Misleading because of nearby words.

Always open the source, check the page, and capture the relevant evidence properly.

Working Rule

A search result can create a lead. It cannot normally prove a finding on its own.

9. Watch for Personalisation and Location Effects

Search results may vary depending on:

- Country.
- Language.
- Search history.
- Browser profile.
- Device type.
- Logged-in accounts.
- Search settings.
- Date and time.

This does not make search useless, but it means results should be handled with care.

For important work:

- Record the search tool used.
- Record the date and time.
- Use a clean browser profile where appropriate.
- Avoid mixing personal browsing with case work.
- Compare results across more than one source if needed.

Do not pretend search results are fixed and universal.

10. Avoid Confirmation Bias

Confirmation bias happens when you search only for evidence that supports the answer you already expect.

Poor search pattern:

```
"Example Repairs" scam  
"Example Repairs" fraud  
"Example Repairs" fake
```

Those searches may have a place if there is a legitimate reason to check risk indicators, but they should not be the only searches.

Balanced pattern:

"Example Repairs"
"Example Repairs Ltd"
"Example Repairs" "official"
"Example Repairs" "address"
"Example Repairs" "reviews"
"Example Repairs" "complaint"
"Example Repairs" "dissolved"

The aim is to understand the subject, not force a conclusion.

Challenge Search

For any early conclusion, run a challenge search.

If the early conclusion is:

"This organisation appears active."

Challenge it with:

- Dissolution searches.
- Regulator notices.
- Archive checks.
- Recent date checks.
- Address conflict checks.

If the early conclusion is:

"This image appears recent."

Challenge it with:

- Reverse image search.
- Earlier publication search.
- Metadata checks where lawful and available.
- Event timeline checks.

A finding becomes stronger when it survives challenge.

11. Use Time Carefully

Dates are one of the most important parts of OSINT search.

A page found today may describe something from ten years ago. A current-looking profile may be abandoned. A company may have changed name, ownership, address, or status.

When searching, include dates when they matter.

Examples:

"Example Repairs" 2024
"Example Repairs" "2025"
"Example Repairs" "March 2026"

Use date filters where the search tool supports them, but do not rely on date filters alone. Search engines sometimes date pages by crawl date, update date, or visible page date, and these can be misleading.

Working Rule

Separate three dates:

Date Type	Meaning
Event date	When the thing happened
Publication date	When the source published it

Date Type	Meaning
Capture date	When you collected it

Do not mix them up.

12. Language and Local Context

Search often improves when you use the language and terminology of the place, industry, or community being searched.

For example, depending on context:

- **company** may also be **firm**, **business**, **limited**, **ltd**, **inc**, **gmbh**, **sarl**, or **pty**.
- **address** may appear as **registered office**, **head office**, **HQ**, **contact**, or **location**.
- **licence** may be spelled **license** in some countries.
- A town may have local spellings, abbreviations, or nearby administrative regions.

A searcher should not assume their own wording is the only wording.

Working Rule

When results are thin, change the vocabulary before assuming there is nothing to find.

13. Widening and Narrowing

Search is a controlled movement between wide and narrow.

Narrow When

- Too many unrelated results appear.
- The subject name is common.
- You have a strong identifier such as a domain, registration number, or exact title.
- You need a specific date range.
- You need a specific source type.

Narrowing methods:

- Add exact phrase.
- Add location.
- Add date.
- Add source type.
- Add known identifier.
- Exclude unrelated meanings.

Widen When

- No results appear.
- Exact search is too restrictive.
- The subject may use aliases or variants.
- The spelling may differ.
- The source may not be indexed.
- The event may be described in different words.

Widening methods:

- Remove quotation marks.

- Remove dates.
- Use synonyms.
- Use partial names.
- Search related entities.
- Search by location or event instead of name.

Good searchers move deliberately. They do not randomly add words until something appears.

14. Safe and Lawful Search Boundaries

OSINT uses publicly available or properly authorised information. Search must stay inside legal, ethical, and platform boundaries.

Do not:

- Attempt to bypass passwords, paywalls, private groups, or access controls.
- Use stolen, leaked, or unlawfully obtained material as a shortcut.
- Harass, intimidate, or contact private individuals unnecessarily.
- Use deception to gain access to private information.
- Collect sensitive personal information without a lawful, necessary, and proportionate reason.
- Publish personal data simply because it can be found.

Do:

- Use public sources.
- Record where information came from.
- Respect privacy and safety.
- Redact unnecessary personal information.
- Stop and escalate if a matter requires legal, safeguarding, or law-enforcement handling.

Search skill is not a licence to intrude.

15. Practical Search Workflow

Use this simple workflow for most beginner OSINT searches.

Step 1 - Write the Question

I am trying to establish whether:

Step 2 - List Known Facts

Record only what is already known.

Known facts:
 - Name:
 - Location:
 - Date range:
 - Source of initial claim:
 - Identifiers:

Step 3 - Create Search Components

Core terms:
 Variants:
 Identifiers:
 Locations:
 Date terms:
 Source types:

Step 4 - Run Broad Searches

Use simple searches first. Capture promising leads.

Step 5 - Run Targeted Searches

Use stronger identifiers and source-specific searches.

Step 6 - Verify and Challenge

Look for independent support, contradictions, and older or newer versions.

Step 7 - Record Findings

Create evidence cards and source entries. Note confidence level.

Step 8 - Stop or Refocus

If the question is answered, stop. If the question changes, write a new question.

16. Example: Verifying a Public Event Claim

Initial claim:

"A community technology workshop was held in Maidstone in April 2025."

Search question:

"Can I find public sources confirming whether this workshop took place, where it happened, and who organised it?"

Search components:

"community technology workshop" Maidstone April 2025
"technology workshop" Maidstone "April 2025"
Maidstone "community workshop" technology
Maidstone events April 2025 technology

Source types to consider:

- Event listings.
- Local council pages.
- Library or community centre pages.
- Local news.
- Organiser website.
- Public social posts by the organiser.

Evidence needed:

- Event title.
- Date.
- Venue.
- Organiser.
- Public source link.
- Capture date.

Possible finding language:

"I found one public event listing and one organiser page stating that the workshop was scheduled for 12 April 2025 at [venue]. I have not yet found independent reporting confirming attendance, so confidence is moderate rather than high."

This is careful. It separates scheduled from confirmed and avoids overstating the result.

17. Common Beginner Mistakes

Mistake 1 - Searching Before Defining the Question

This creates scattered results and weak evidence.

Mistake 2 - Keeping Only Useful Links

Record dead ends when they matter. They show what was checked.

Mistake 3 - Treating Search Ranking as Truth

The first result is not necessarily the best result.

Mistake 4 - Ignoring Dates

Old information can look current. Current pages can describe old events.

Mistake 5 - Overusing Advanced Operators Too Early

Simple searches often work best at the start. Operators are tools, not magic.

Mistake 6 - Collecting More Than Needed

More data means more risk, more storage, more review, and more chance of error. Collect what answers the question.

Mistake 7 - Failing to Challenge the First Good Result

A good-looking result may still be wrong, outdated, copied, or incomplete.

18. Mini Checklist

Before ending a search session, ask:

- Did I write the search question?
- Did I record the exact searches used?
- Did I capture sources properly?
- Did I separate claims from evidence?
- Did I check dates?
- Did I search for variants?
- Did I challenge my early conclusion?
- Did I avoid collecting unnecessary personal information?
- Did I note confidence level?
- Did I record what still needs checking?

19. Chapter Exercise

Create a practice search plan for a harmless public subject, such as:

- A local public event.
- A charity fundraiser.
- A company press release.
- A public planning application.
- A museum exhibition.
- A product announcement.

Do not choose a private individual for this exercise.

Fill in the following:

Search question:

Known facts:

Search components:

Likely source types:

First five searches to run:

- 1.
- 2.
- 3.
- 4.
- 5.

Evidence needed:

Possible contradictions to check:

Stopping point:

Then run the searches and create at least three evidence cards.

20. Key Takeaways

- Search is a disciplined process, not a random hunt.
- Every search should start with a clear question.
- Search terms should be broken into names, variants, identifiers, places, dates, and source types.
- Exact phrases are useful, but they can also hide results.
- Search results are leads; sources provide evidence.
- Dates, context, and source reliability matter.
- A search log protects the work from confusion and makes the process repeatable.
- Good OSINT search includes challenge searches, not only supporting searches.
- Safe OSINT respects privacy, law, platform boundaries, and proportionality.

Visual Brief - V13 Search Funnel and Search Log

Purpose: Show how a broad question becomes controlled, logged, and verified search activity.

Style: Dark technical workbook style with gold/amber highlights, matching the OSINT Bible visual register.

Layout:

Left side: a funnel diagram labelled:

1. Question
2. Known facts
3. Search components
4. Broad search
5. Targeted search
6. Verification search
7. Evidence card
8. Finding

Right side: a simple search log table with columns:

- Time
- Tool/source

- Query
- Result
- Evidence reference

Footer text:

Search results create leads. Verified sources create findings.

Avoid any imagery suggesting hacking, intrusion, surveillance, or targeting private people.

Suggested File Name

Chapter_06_Search_Fundamentals.md

Chapter 7 - Source Reliability and Bias

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Purpose of This Chapter

OSINT work is only as strong as the sources behind it.

A search result can look convincing. A screenshot can look official. A social post can sound certain. A news article can be widely shared. A directory listing can appear professional. None of that automatically makes the information reliable.

This chapter teaches the reader how to judge sources before relying on them. It does not ask the reader to become cynical about everything. It asks the reader to become disciplined: check who is speaking, how they know, when they said it, what they may be missing, and whether other independent sources support or challenge the claim.

By the end of this chapter, the reader should be able to:

- Separate a source from a claim.
- Identify primary, secondary, and weak sources.
- Assess reliability, bias, intent, and context.
- Recognise copied information and circular reporting.
- Use confidence language carefully.
- Record source assessments in a repeatable way.
- Avoid treating popularity, presentation, or confidence as proof.

1. A Source Is Not the Same as a Claim

A common beginner mistake is to treat the existence of a source as proof that the claim is true.

Example:

“A website says the company moved address in 2025.”

That sentence contains two separate things:

1. The source exists.
2. The source makes a claim about the company address.

The first part may be easy to prove. You can capture the website and record what it says.

The second part still needs assessment. Is the website official? Is it current? Does it show where the information came from? Could it have copied old data? Is there an official record that agrees or disagrees?

Working Rule

Always write findings as:

“Source A states Claim B.”

Do not jump straight to:

“Claim B is true.”

The source may support the claim, but it does not automatically prove it.

2. The Source Ladder

Not all sources carry the same weight. A useful beginner model is the source ladder.

Stronger Sources

These are closer to the original information.

- Official registers.
- Direct statements from the organisation involved.
- Original documents.
- Court, regulator, or government publications.
- First-hand video, images, or audio with verifiable context.
- Dated archive captures of the original page.

Medium Sources

These may be useful but need checking.

- Reputable news reports.
- Specialist publications.
- Trade journals.
- Academic commentary.
- Local reporting.
- Known analysts with a track record.
- Public statements by relevant witnesses.

Weaker Sources

These can generate leads but should not usually support strong findings alone.

- Anonymous posts.
- Unsourced social media claims.
- Aggregator sites.
- Scraped directory listings.
- AI-generated summaries.
- Reposts without original links.
- Forum comments with no supporting material.
- Screenshots with no source path, date, or context.

Weak sources are not always useless. They can point the researcher toward better sources. The mistake is treating them as final evidence.

3. Primary, Secondary, and Tertiary Sources

Primary Source

A primary source is closest to the event, record, person, or organisation being studied.

Examples:

- A company filing on an official register.
- A regulator notice on the regulator's own website.

- An organisation's own press release.
- A public planning document from a council portal.
- A dated original social post from the relevant account.
- A video uploaded by the original source, if authenticity and context can be assessed.

Primary does not mean perfect. An organisation can make mistakes or present itself favourably. But primary sources are usually important because they show what the original party or authority said.

Secondary Source

A secondary source reports, analyses, or comments on primary information.

Examples:

- A news article about a regulator notice.
- A blog explaining a company filing.
- A researcher summarising a public dataset.
- A local report about a public meeting.

Secondary sources can be valuable because they add context, explanation, or independent reporting. They still need checking against primary material where possible.

Tertiary Source

A tertiary source aggregates or summarises information from elsewhere.

Examples:

- Directory listings.
- Knowledge panels.
- Summary databases.
- AI answers.
- "People also ask" snippets.
- Wiki-style summaries.

Tertiary sources are useful for orientation, not final proof.

4. Reliability Is About More Than Truth

A source can be useful even if it is biased. A source can be honest but mistaken. A source can be accurate about one detail and wrong about another.

Reliability is not a simple yes or no label. Assess it by asking:

- Who created the source?
- How would they know the information?
- What evidence do they provide?
- When was it created or updated?
- What is the source's purpose?
- Does it distinguish fact from opinion?
- Does it link to original material?
- Is it consistent with independent sources?
- Are there contradictions?
- Is the source complete or only a fragment?

Working Rule

Assess each claim separately.

A source may be reliable for one claim and weak for another.

Example:

A company website may be reliable for its advertised contact email but less reliable for independent claims about customer satisfaction.

5. Bias Does Not Automatically Make a Source Worthless

Bias means the source has a perspective, interest, preference, incentive, or limitation that may affect what it says or leaves out.

Sources can be biased because of:

- Commercial interest.
- Political position.
- Personal conflict.
- Brand protection.
- Activism.
- Local loyalty.
- Anger or grievance.
- Lack of expertise.
- Limited access to facts.
- Desire for attention.

Bias does not automatically mean the source is lying. It means the researcher must understand the angle.

Example

A company press release may be biased in favour of the company, but it can still be useful for:

- The company's own announcement date.
- Official wording.
- Named executives.
- Product names.
- Stated locations.

It is weaker for:

- Independent performance claims.
- Claims about market leadership.
- Claims about customer satisfaction.
- Claims about competitors.

6. Intent and Incentive

Every source exists for a reason.

Common source intents include:

Intent	What to Watch For
Inform	Does it provide evidence and context?

Intent	What to Watch For
Promote	Does it exaggerate benefits or hide problems?
Persuade	Does it select only supporting facts?
Entertain	Does it trade accuracy for drama?
Sell	Does it push the reader toward a purchase?
Attack	Does it omit context or use loaded language?
Warn	Does it provide verifiable risk indicators?
Summarise	Does it link back to original material?
Automate	Is it scraped, generated, or outdated?

Intent does not automatically invalidate a source, but it changes how the source should be used.

Working Rule

Ask:

“What would this source gain if I believed it?”

That question often reveals useful caution.

7. Date, Time, and Freshness

Source reliability changes over time.

A source may have been accurate when published but wrong now. A company address, phone number, domain owner, job title, product name, or public profile can change.

When assessing a source, record:

- Publication date.
- Last updated date, if visible.
- Event date being discussed.
- Capture date.
- Whether the page appears current or archived.

Example

A 2021 directory listing may be weak evidence for a 2026 address unless supported by current official information.

A 2026 article may still describe a 2018 event, so publication date alone is not enough.

Working Rule

Never write “current” unless you have checked current sources.

Better wording:

“As captured on 7 June 2026, the organisation’s public contact page listed...”

This is safer than:

“The organisation is based at...”

8. Original Reporting vs Copied Information

Many online sources copy from each other.

A claim may appear on ten websites, but all ten may have copied the same original mistake.

This creates a false sense of confirmation.

Signs of Copied Information

- Identical wording across multiple pages.
- Same typo repeated.
- Same old address repeated.
- No links to original sources.
- Similar page templates.
- Directory pages using scraped data.
- Publication dates close together but no independent reporting.
- AI-like summaries with no citations.

Circular Reporting

Circular reporting happens when Source A cites Source B, Source B cites Source C, and Source C is actually based on Source A.

The information appears supported, but it is moving in a circle.

Working Rule

Trace the claim back as close to the original source as possible.

Ask:

“Where did this claim first appear?”

9. Screenshots Need Special Care

Screenshots are useful, but they can be misleading if handled badly.

A screenshot may lack:

- URL.
- Date captured.
- Full page context.
- Source account name.
- Comments or surrounding thread.
- Time zone.
- Whether the image was edited.
- Whether the page still exists.

Screenshots can also be cropped, staged, altered, or separated from context.

Better Screenshot Practice

When capturing a screenshot:

- Include the URL where possible.
- Include the date and time in the evidence card.
- Capture enough surrounding context.
- Record the source path separately.
- Save the original capture unchanged.
- Create redacted copies only when needed for sharing.
- Do not rely on a screenshot alone if the live source or archive can also be recorded.

Working Rule

A screenshot is a record of what you captured. It is not automatically proof of what happened.

10. Social Media Source Assessment

Public social posts can be useful, but they require caution.

Assess:

- Is the account authentic?
- Is the post original or a repost?
- Is the post dated?
- Is the date shown in local time or platform time?
- Does the post include media?
- Can the media be independently checked?
- Is the account known for satire, commentary, or impersonation?
- Has the post been edited, deleted, quoted, or taken out of thread context?
- Are replies adding evidence or just opinion?

Do Not Overstate Social Evidence

Weak wording:

“This proves the event happened.”

Better wording:

“A public post from Account A, captured on [date], states that the event happened. I have not yet found independent confirmation.”

Or:

“The post is useful as a lead, but confidence is low until supported by stronger sources.”

11. Official Sources Can Still Have Limits

Official sources are often strong, but they are not magic.

They may contain:

- Administrative errors.
- Delayed updates.
- Limited fields.
- Legal wording that needs interpretation.
- Historical data that is no longer current.
- Missing context.
- Self-filed information.
- Different naming conventions.

Example:

An official register may confirm that a company exists and show its registered office, but that does not necessarily prove where it physically trades from every day.

Working Rule

Use official sources for the claims they are designed to support.

Do not stretch them beyond their purpose.

12. Reputation, Popularity, and Presentation

A source can look professional and still be wrong.

A source can be ugly and still be useful.

Do not judge reliability only by:

- Web design.
- Logo quality.
- Follower count.
- Search ranking.
- Confident language.
- Number of shares.
- Being repeated by many accounts.
- Appearing in an AI answer.

These may affect how the source spreads, but they do not prove accuracy.

Working Rule

Professional presentation is not evidence. Evidence is evidence.

13. Independent Confirmation

Independent confirmation means another source supports the claim without simply copying the same source.

Two sources are not independent if:

- One copied the other.
- Both copied the same press release.
- Both rely on the same unnamed source.
- Both use identical scraped data.
- One is a summary of the other.

Independent support is stronger when sources differ in type.

Example:

A stronger combination:

- Official register entry.
- Organisation website.
- Local news article.
- Archived copy of an earlier page.

A weaker combination:

- Four directory pages with the same copied address.

Working Rule

Look for different source types, not just more sources.

14. Contradictions Are Valuable

Contradictions are not a failure. They are part of good OSINT.

A contradiction may reveal:

- Old information.
- A name change.
- A rebrand.
- A copied error.
- A fake profile.
- A mistaken assumption.
- Multiple entities with similar names.
- A timeline problem.
- A source that is not reliable for that claim.

Example

Source A lists an organisation at Address 1 in 2022.

Source B lists the same organisation at Address 2 in 2025.

This does not automatically mean one is false. The organisation may have moved. The next step is to build the timeline.

Working Rule

Record contradictions. Do not delete them because they are inconvenient.

15. Confidence Levels

Good OSINT uses careful confidence language.

Use confidence to describe how strongly the available evidence supports the finding.

Simple Confidence Scale

Confidence	Meaning
High	Supported by strong, relevant, independent sources with no serious contradictions.
Moderate	Supported by useful sources, but with some gaps, age issues, or limited independence.
Low	Based on weak, single, unclear, old, or unverified sources.
Unknown	Not enough evidence to assess.

Example Wording

High confidence:

“I assess with high confidence that the company used this registered name during 2025 because it appears in the official register and on the company’s own archived website capture from that period.”

Moderate confidence:

“I assess with moderate confidence that the event was scheduled, because it appears on the organiser page and a local event listing. I have not found independent reporting confirming attendance.”

Low confidence:

“Confidence is low because the claim currently relies on one anonymous social post and no supporting source has been found.”

16. The Source Assessment Card

For important sources, create a source assessment card.

Source ID:
Source title/name:
Source type:
URL/path/reference:
Captured by:
Capture date/time:
Publication date:
Event date discussed:
Creator/publisher:
Claim(s) made:
Evidence shown by source:
Likely intent:
Known bias or limitation:
Independence:
Contradictions:
Reliability for this claim:
Confidence supported:
Notes:

This does not need to be completed for every tiny source, but it should be used when a source supports an important finding.

17. Source Assessment Questions

Use this checklist when reviewing a source:

1. What exact claim am I using this source for?
2. Who created the source?
3. How would they know?
4. Is this primary, secondary, or tertiary?
5. Is it dated?
6. Is the date relevant to the claim?
7. Is the source current, historical, or archived?
8. Does it provide evidence or only assertion?
9. Does it link to original material?
10. Could it be copied from another source?
11. Is there a commercial, political, personal, or reputational incentive?
12. Does the source use loaded or emotional language?
13. Are there independent sources that support it?
14. Are there credible sources that contradict it?
15. What confidence level does it support?
16. What should not be inferred from this source?

The final question is especially important. Many OSINT mistakes happen when the researcher infers more than the source actually shows.

18. What Not to Infer

A source may show one thing but tempt the researcher to claim another.

Source Shows	Do Not Automatically Infer
A person has a public profile	The profile is current or authentic
A company has a registered office	The company trades from that address daily
A social post mentions an event	The event happened as described
A directory lists a phone number	The number is still active or controlled by the subject
A domain exists	The subject owns or controls it
A photo appears online	The caption is accurate
A news article reports an allegation	The allegation has been proven
A page is highly ranked	The information is reliable

Careful OSINT is often about refusing to overclaim.

19. Handling Unreliable Sources

Sometimes a source is weak, biased, or messy but still useful.

Use unreliable sources as:

- Leads.
- Search terms.
- Timeline clues.
- Names to verify.
- Contradictions to investigate.
- Indicators of public narrative.

Do not use them as:

- Final proof.
- Sole support for serious claims.
- Grounds for naming or accusing private individuals.
- Evidence of wrongdoing without stronger support.

Working Rule

A weak source can start a question. It should not end the investigation.

20. Practical Example: Address Claim

Claim:

“Example Training Ltd is based at 25 Market Street.”

Sources found:

1. Directory listing from 2021 showing 25 Market Street.
2. Official company register showing a registered office at 10 Station Road in 2026.
3. Company website contact page showing 10 Station Road, captured today.
4. Old archived company page from 2020 showing 25 Market Street.

Assessment:

- The directory listing is old and likely copied.
- The official register is current for registered office information.
- The company website is current for public contact information.

- The archive suggests the company may previously have used 25 Market Street.

Careful finding:

“I found historical references to 25 Market Street in a 2020 archived company page and a 2021 directory listing. Current sources captured on [date], including the official register and company contact page, list 10 Station Road. I therefore assess with moderate to high confidence that 25 Market Street is historical rather than current, pending any additional trading-location evidence.”

This finding avoids the trap of choosing one source and ignoring the timeline.

21. Practical Example: Social Media Claim

Claim:

“A public post says a local event was cancelled.”

Sources found:

1. Public post by an attendee saying the event was cancelled.
2. Organiser page still showing the event as scheduled.
3. Venue page showing no update.
4. Later organiser post saying the event was moved indoors, not cancelled.

Assessment:

- The attendee post may be honest but incomplete.
- The organiser is closer to the event decision.
- The wording “cancelled” may have been a misunderstanding.
- The later organiser post changes the timeline.

Careful finding:

“A public attendee post described the event as cancelled, but a later organiser post stated that the event was moved indoors. Based on the sources currently found, the stronger interpretation is that the event format changed rather than being fully cancelled.”

22. Red Flags in Source Assessment

Be cautious when a source:

- Makes serious claims without evidence.
- Uses only anonymous screenshots.
- Crops away context.
- Has no date.
- Has no author or publisher information.
- Uses highly emotional or threatening language.
- Claims certainty while showing little evidence.
- Repeats claims from unknown accounts.
- Contains obvious factual errors in areas you can check.
- Encourages harassment or exposure of private individuals.
- Uses “everyone knows” instead of evidence.
- Cannot be traced back to an original source.

A red flag does not always mean the source is false. It means the source needs stronger verification before use.

23. Safe Use of Source Criticism

Source criticism should not become personal attack.

When writing notes or reports, avoid unnecessary insults or loaded labels.

Poor wording:

“This source is rubbish and clearly lying.”

Better wording:

“This source is weak for this claim because it is anonymous, undated, provides no original evidence, and is contradicted by two stronger dated sources.”

Professional language makes the work more credible.

24. Mini Workflow for Source Reliability

Use this simple process:

1. Identify the exact claim.
2. Identify the source type.
3. Check who created it.
4. Check the date.
5. Check how the source could know.
6. Look for original material.
7. Look for independent support.
8. Look for contradictions.
9. Record limitations.
10. Assign a confidence level.

This process should become routine before writing findings.

25. Chapter Exercise

Choose a harmless public claim, such as:

- A local public event date.
- A company’s public office address.
- A museum opening time.
- A product launch announcement.
- A charity fundraiser total.
- A public planning application status.

Do not choose a private individual for this exercise.

Find at least four sources relating to the claim.

For each source, complete this table:

Source	Type	Date	Claim Made	Strength	Limitation	Confidence Supported
Source 1						
Source 2						

Source	Type	Date	Claim Made	Strength	Limitation	Confidence Supported
Source 3						
Source 4						

Then write a careful finding using one of these formats:

The available sources support the claim with [high/moderate/low] confidence because...

or:

The available sources do not currently support the claim because...

or:

The sources are mixed. Source A suggests..., while Source B suggests... The most cautious assessment is...

26. Key Takeaways

- A source and a claim are not the same thing.
- Primary sources are usually stronger, but still have limits.
- Secondary sources can add useful context and independent reporting.
- Tertiary and AI-generated summaries are useful for orientation, not final proof.
- Bias does not automatically make a source worthless, but it must be understood.
- Copied information can create false confirmation.
- Screenshots require URL, date, context, and careful handling.
- Official sources should be used for the claims they are designed to support.
- Independent confirmation means more than finding the same claim repeated.
- Contradictions are valuable and should be recorded.
- Confidence levels protect the reader from overclaiming.
- Strong OSINT findings are based on relevant, dated, traceable, and proportionate evidence.

Visual Brief - V14 Source Reliability and Bias Assessment Card

Purpose: Show how a source moves from raw discovery to assessed evidence.

Style: Dark technical workbook style with gold/amber highlights, matching the OSINT Bible visual register.

Layout:

Left side: a vertical source ladder labelled:

1. Primary / official / original
2. Reputable secondary
3. Specialist or local source
4. Aggregated or copied source
5. Anonymous or unsupported claim

Middle: a source assessment card with fields:

- Source type
- Date
- Claim made
- Evidence shown

- Bias / intent
- Independence
- Contradictions
- Confidence supported

Right side: a small warning panel labelled:

Do not confuse repetition with confirmation.

Footer text:

Reliable findings come from assessed sources, not loud sources.

Avoid imagery suggesting hacking, intrusion, surveillance, or targeting private people.

Suggested File Name

Chapter_07_Source_Reliability_and_Bias.md

Chapter 8 - Identity, Entities, and Attribution Basics

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Purpose of This Chapter

OSINT work often involves trying to understand what a piece of information actually represents.

A username may look like a person. A company name may point to several different businesses. A phone number may belong to an organisation, a temporary service, a former owner, or a forwarded line. A photograph may show a place, but not necessarily the place claimed in the caption. A profile may use a real name but not belong to the person the reader assumes.

This chapter introduces the basics of identity, entities, and attribution. It is designed to slow the reader down before they make one of the most common OSINT mistakes: treating a clue as a confirmed identity.

By the end of this chapter, the reader should be able to:

- Understand the difference between a person, an account, an identifier, and an entity.
- Build an entity list without making unsupported assumptions.
- Recognise when two records may relate to the same subject and when that is not yet proven.
- Use careful attribution language.
- Record identity links with confidence levels.
- Avoid harmful misidentification, doxxing, harassment, or invasive research.
- Create a safe attribution table for a simple investigation.

1. What Is an Entity?

In OSINT, an entity is anything that can be named, described, linked, or studied.

Common entities include:

- A person.
- A company.
- A charity.
- A public body.
- A website.
- A domain name.
- A social media account.
- A username.
- An email address.
- A phone number.
- A location.

- A vehicle.
- A document.
- A photograph.
- An event.
- A product.
- A group or community.

The important point is that an entity is not always a real-world person. Many beginners collapse everything into “who is this?” too quickly. Good OSINT begins by naming the thing correctly.

Example

A researcher finds the username `riverwatch_72` on a public forum.

At this stage, the known entity is:

Public username: riverwatch_72

It is not yet:

A named person.

It is not yet:

The same individual who uses riverwatch72 on another platform.

It is not yet:

The person shown in a profile photo.

The username is a clue. It may become part of an identity picture later, but by itself it is only an entity.

2. Identity Is a Claim, Not a Starting Assumption

Identity attribution is the process of linking one entity to another.

Examples:

- Linking a username to a real name.
- Linking a company to a director.
- Linking a website to an organisation.
- Linking a phone number to a business.
- Linking a photograph to a location.
- Linking multiple profiles to the same operator.

These links may be strong, weak, disputed, outdated, or false.

A safe OSINT workflow treats each identity link as a claim that must be supported by evidence.

Unsafe Wording

“This account is John Smith.”

Safer Wording

“The account uses the display name John Smith and links to a public website that lists the same email address. This supports, but does not alone prove, a connection between the account and that public identity.”

The second version is longer, but it is more accurate. It separates observation from conclusion.

3. The Entity Separation Rule

The entity separation rule is simple:

Keep every entity separate until evidence justifies linking them.

Do not merge entities because they look similar. Do not assume two accounts are operated by the same person just because they share a name, avatar, city, phrase, or interest. Similarity creates a lead, not a finding.

Separate Entities First

If the reader finds these items:

- `j.smith.design` on Instagram.
- `jsmithdesign` on GitHub.
- John Smith Design Ltd on a company register.
- `john@smithdesign.example` in a public contact page.

The safe first step is to list them separately:

Entity ID	Entity Type	Value	Source	Notes
E01	Social account	<code>j.smith.design</code>	Public profile	Uses design branding
E02	Code account	<code>jsmithdesign</code>	Public profile	Similar handle pattern
E03	Company	John Smith Design Ltd	Company register	Registered organisation
E04	Email	<code>john@smithdesign.example</code>	Public contact page	Contact address

Only after the reader records evidence should they create relationship claims.

4. Identifiers Are Not People

An identifier is a label, address, code, handle, number, or reference that may point toward an entity.

Common identifiers include:

- Username.
- Display name.
- Email address.
- Phone number.
- Domain name.
- IP address.
- Company number.
- Charity number.
- Vehicle registration.
- Social media profile URL.
- Marketplace seller name.
- App store developer name.
- Public key or cryptocurrency address.
- Document author field.

Identifiers can be shared, reused, recycled, spoofed, transferred, inherited, or automatically generated.

Examples of Identifier Risk

A phone number may have changed owner.

A username may be copied by a fan, critic, scammer, or parody account.

A company address may be a registered office, accountant, virtual office, or mail handling service.

A domain may be privately registered, owned by a holding company, managed by an agency, or abandoned by a previous owner.

An email address may be a role inbox, not an individual.

A profile photograph may be stock imagery, AI-generated, copied, or old.

Working Rule

Treat every identifier as a pointer, not proof.

5. Attribution Basics

Attribution is the act of assigning responsibility, ownership, operation, or connection.

In OSINT, attribution can be about:

- Who created an account.
- Who controls a website.
- Which organisation published a document.
- Whether two profiles are connected.
- Whether a business is linked to a director.
- Whether a photo shows the claimed place.
- Whether a statement came from the claimed source.

Attribution is rarely all-or-nothing. It is usually built from small pieces of evidence.

Attribution Strength Levels

A simple beginner model uses four levels:

Level	Meaning	Example Wording
Observed	Directly seen in a source	"The profile displays this username."
Linked	Two entities are connected by a source	"The website links to this account."
Supported	Multiple independent clues point the same way	"The connection is supported by matching contact details and official listings."
Confirmed	Strong, direct, reliable evidence supports the link	"The organisation's official page names this account as its public profile."

Avoid using "confirmed" unless the evidence is direct, reliable, and current.

6. The Attribution Ladder

The attribution ladder helps the reader avoid jumping from a small clue to a strong conclusion.

Step 1: Observe

Record what is visible.

Example:

"The public profile uses the display name 'North Coast Repairs'."

Step 2: Describe

Describe the entity without over-identifying it.

Example:

“This appears to be a public business profile.”

Step 3: Compare

Compare with other public sources.

Example:

“A public business directory also lists ‘North Coast Repairs’ with a similar logo.”

Step 4: Link

Record the possible link and evidence.

Example:

“The directory links to the same website shown in the profile bio.”

Step 5: Assess Confidence

Give the link a confidence level and explain why.

Example:

“Moderate confidence: the profile and directory share the same name, logo, and website, but no official company register entry has been checked yet.”

Step 6: Report Carefully

Use language that matches the evidence.

Example:

“The profile is likely associated with the same public business presence, based on matching name, logo, and website.”

7. Strong Links and Weak Links

Some clues are stronger than others. A strong link is more direct, harder to fake, current, and independently supported. A weak link may be useful but should not carry a finding alone.

Stronger Links

- Official website links to the social account.
- Company register lists a company number matching the business name and address.
- A public document names a person in a role.
- A verified organisation page links to a domain.
- A regulator notice names the entity and reference number.
- Multiple independent official sources agree.
- A current public profile links to the same official domain.

Weaker Links

- Similar usernames.
- Similar profile pictures.
- Same first name.
- Same city.

- Same hobby.
- Same writing style.
- A reposted screenshot.
- A search result snippet with no accessible source.
- A directory listing with no update date.
- A forum comment saying “this is them.”

Weak links can guide further research. They should not be treated as final proof.

8. Names Are Especially Dangerous

Names create many false matches.

Common names can belong to thousands of people. Even uncommon names can be shared by unrelated people. People change names, use initials, use nicknames, use stage names, use married names, or shorten names differently across platforms.

Name Variation Examples

- William Smith.
- Bill Smith.
- Billy Smith.
- W. Smith.
- W J Smith.
- Smithy.
- william.smith.
- wsmith.
- wjs_design.

None of these are automatically the same person.

Safe Name Handling

When working with names:

- Record the exact spelling from each source.
- Note whether it is a legal name, display name, username, nickname, or business name.
- Avoid assuming initials.
- Avoid assuming gender, age, nationality, or personal background from a name.
- Look for direct source links before linking profiles.
- Treat name matches as leads until supported by stronger evidence.

9. Accounts Are Not Always Operated by One Person

An account may represent:

- One individual.
- A team.
- A business.
- A volunteer group.
- A bot.

- A scheduler.
- A social media manager.
- A customer support desk.
- A compromised account.
- A fan account.
- A parody account.
- An impersonator.

Do not assume a single human operator without evidence.

Example

A public account posts personal-sounding messages, business promotions, and customer support replies. The reader might assume one person runs it. But the account could be controlled by several staff members, scheduled software, or an outside agency.

A safer conclusion would be:

“The account publicly represents the business. The available evidence does not establish which individual operates it.”

10. Organisations Are Not Simple Either

Organisations can have complex structures.

A company may have:

- Trading names.
- Registered names.
- Previous names.
- Parent companies.
- Subsidiaries.
- Directors.
- Shareholders.
- Brand names.
- Franchise operators.
- Regional offices.
- Contractors.
- Agencies.
- Dormant or dissolved records.

A charity may have trustees, branches, volunteers, trading arms, and partner organisations.

A website may represent a brand rather than the legal entity behind it.

Working Rule

Separate the public brand from the legal entity.

Example:

“Green Harbour” may be a brand name.

“Green Harbour Services Ltd” may be the registered company.

A website using the Green Harbour brand may be managed by a marketing agency.

Each should be treated as a separate entity until links are documented.

11. Entity Tables

An entity table is a simple way to stay disciplined.

Basic Entity Table

Entity ID	Type	Name / Value	Source	Date Captured	Notes
E01	Website	example.org	Public website	2026-06-07	Main site found by search
E02	Organisation	Example Community Group	About page	2026-06-07	Named on website
E03	Email	contact@example.org	Contact page	2026-06-07	Role address
E04	Social account	@examplegroup	Public profile	2026-06-07	Linked from website

The table prevents the reader from mixing evidence together in their head.

Entity Notes

Each entity should have notes that answer:

- What exactly is this?
- Where was it found?
- When was it captured?
- What source supports it?
- Is the entity current, old, or unknown?
- What other entities might it link to?
- What is still uncertain?

12. Relationship Tables

A relationship table records possible links between entities.

Basic Relationship Table

Relationship ID	Entity A	Relationship	Entity B	Evidence	Confidence
R01	E01 Website	links to	E04 Social account	Website footer link	High
R02	E02 Organisation	uses	E03 Email	Contact page	High
R03	E04 Social account	may represent	E02 Organisation	Same name and website link	Moderate

This keeps the entity list and the attribution claims separate.

Why This Matters

The entity table says what exists.

The relationship table says how things may connect.

If a relationship later turns out to be wrong, the researcher can correct the relationship without corrupting the entity list.

13. Confidence Levels for Identity Links

Confidence levels should be explained, not just labelled.

A useful model:

Low Confidence

There is a possible link, but it is based on weak or limited evidence.

Example wording:

“Low confidence: the two accounts use similar names, but no direct link has been found.”

Moderate Confidence

There are several supporting clues, but at least one important uncertainty remains.

Example wording:

“Moderate confidence: the account and website share a name, logo, and location, but the website does not directly link to the account.”

High Confidence

There is strong direct evidence, usually from reliable sources or direct links.

Example wording:

“High confidence: the official website links directly to the public account, and the account links back to the same domain.”

Confirmed

Use this only where the source is strong enough to remove reasonable doubt for the purpose of the report.

Example wording:

“Confirmed for reporting purposes: the regulator listing names the organisation, registration number, and official website, and the website displays the same registration number.”

Even confirmed findings can have limits. Say what is confirmed and what is not.

14. Handling Contradictions

Identity work often produces contradictions.

Examples:

- Two sources list different addresses.
- A company uses a different trading name from its registered name.
- A profile links to an old website.
- A directory lists an outdated phone number.
- A person’s role changed after the source was published.
- A social account appears inactive but is still linked from an official page.

Contradictions should be recorded, not hidden.

Contradiction Note Template

Contradiction ID:
Entities affected:
Source A states:
Source B states:
Dates of sources:
Possible explanations:
Further checks needed:
Current confidence:

Possible Explanations

A contradiction may be caused by:

- Outdated information.
- Multiple branches or locations.
- A rebrand.
- A dissolved or renamed company.
- A copied directory listing.
- Mistaken data entry.
- Different people with the same name.
- Deliberate impersonation.
- A hacked or abandoned account.

Do not choose the most dramatic explanation unless the evidence supports it.

15. Safe Boundaries in Identity Research

Identity research can affect real people. A false attribution can damage reputations, expose private individuals, or encourage harassment.

This book uses a defensive, lawful OSINT standard.

Safe Practices

- Use public, lawful sources.
- Keep research proportionate to a legitimate purpose.
- Avoid unnecessary personal details.
- Do not publish private addresses, personal phone numbers, family details, or sensitive personal information.
- Do not encourage contact, harassment, intimidation, or vigilantism.
- Redact information that is not necessary to the report.
- Use confidence language.
- Include limitations.
- Escalate serious threats, crimes, or safeguarding issues to appropriate authorities rather than trying to handle them personally.

Unsafe Practices

- Doxxing.
- Harassment.
- Stalking.
- Social engineering.
- Pretending to be someone else to obtain information.
- Accessing private systems or restricted accounts.
- Publishing personal information to shame or threaten someone.
- Encouraging others to target a person.
- Treating weak clues as proof.

Working Rule

The goal is to understand and document public evidence responsibly, not to expose private people for entertainment or pressure.

16. Attribute the Public Role, Not the Private Life

In many defensive OSINT tasks, the reader does not need to identify a private individual at all.

For example, if assessing a suspicious marketplace seller, the useful public entities may be:

- Seller account.
- Store name.
- Payment method.
- Listing pattern.
- Review history.
- Public contact email.
- Claimed business name.
- Domain.

The reader may not need the seller's home address, family members, private social media profiles, or unrelated personal history.

Good Question

"Is this seller account connected to a known public business presence, and are there signs of impersonation or fraud?"

Poor Question

"Who is the person behind this and where do they live?"

A professional OSINT mindset keeps the work proportionate.

17. Common Attribution Mistakes

Mistake 1: Same Username Means Same Person

Two accounts using similar usernames may be connected, but they may also be unrelated.

Mistake 2: Same Name Means Same Identity

Common names create many false positives.

Mistake 3: Profile Photo Equals Owner

A profile picture may be copied, generated, old, symbolic, or used without permission.

Mistake 4: Old Data Is Current

Directory listings, cached pages, and old social posts can remain searchable long after they stop being accurate.

Mistake 5: One Source Is Enough

One source may support a claim, but strong attribution usually needs independent confirmation.

Mistake 6: Ignoring Alternative Explanations

A clue may have several explanations. The researcher must consider them before making a finding.

Mistake 7: Over-Reporting Personal Details

A report should include what is necessary, not everything that was found.

Mistake 8: Confusing Suspicion With Evidence

A pattern may be suspicious, but suspicion is not proof.

18. Practical Workflow: Safe Entity and Attribution Mapping

Use this workflow whenever the task involves accounts, names, organisations, or identifiers.

Step 1: Define the Question

Write the question clearly.

Example:

“Is this public account genuinely connected to the organisation it claims to represent?”

Step 2: List Known Entities

Create separate entries for every account, domain, name, email, address, document, and source.

Do not merge anything yet.

Step 3: Capture Sources

Record where each entity was found.

Include:

- Source title.
- URL or reference.
- Date and time captured.
- Screenshot or saved copy where appropriate.
- Notes about source reliability.

Step 4: Identify Possible Relationships

Record possible links separately.

Examples:

- Website links to profile.
- Profile links to website.
- Register lists company address.
- Public document names director.
- Two accounts use the same contact email.

Step 5: Grade Each Relationship

Use low, moderate, high, or confirmed.

Explain the grade.

Step 6: Look for Contradictions

Actively search for evidence that could weaken the link.

Examples:

- Old website uses different contact details.
- Official source does not mention the profile.
- Multiple organisations use the same name.
- Directory listing appears copied.

Step 7: Write Findings Carefully

Use wording that matches the confidence level.

Avoid unsupported phrases such as:

- “definitely.”
- “obviously.”
- “must be.”
- “proved by.”
- “everyone knows.”

Prefer:

- “appears to.”
- “is consistent with.”
- “is linked by.”
- “is supported by.”
- “is not established by the available evidence.”

Step 8: Redact Unnecessary Personal Data

Before sharing the work, remove personal details that are not needed for the purpose.

19. Example: Public Business Profile Check

This fictional example shows the difference between safe attribution and careless attribution.

Scenario

A public social account claims to represent “Harbour Lane Repairs.” The reader wants to know whether it appears connected to the real business.

Entity Table

Entity ID	Type	Name / Value	Source	Notes
E01	Social account	@harbourlanerepairs	Public social profile	Claims to be Harbour Lane Repairs
E02	Website	harbourlanerepairs.example	Profile bio link	Linked from E01
E03	Business name	Harbour Lane Repairs	Website footer	Public trading name
E04	Email	info@harbourlanerepairs.example	Website contact page	Role inbox
E05	Company listing	Harbour Lane Repairs Ltd	Public register	Similar name; check exact details

Relationship Table

Relationship ID	Entity A	Relationship	Entity B	Evidence	Confidence
R01	E01	links to	E02	Bio link	High
R02	E02	uses	E04	Contact page	High
R03	E02	displays	E03	Website footer	High
R04	E03	may relate to	E05	Similar name	Low until register details checked

Safe Finding

“The public social account links to a website using the Harbour Lane Repairs name and a matching domain. This supports a connection between the account and the public website. The available evidence does not yet confirm whether the website is operated by the registered company Harbour Lane Repairs Ltd.”

Careless Finding

“The account belongs to the company director.”

The careless finding is unsupported. Nothing in the example identifies the account operator or director.

20. Example: Username Correlation Caution

Scenario

The reader finds these public usernames:

- coastalrunner88
- coastal_runner88
- coastalrunner_uk

They all mention running and the coast.

Weak Conclusion

“These are all the same person.”

Better Approach

Create separate entities:

Entity ID	Type	Value	Notes
E01	Username	coastalrunner88	Platform A
E02	Username	coastal_runner88	Platform B
E03	Username	coastalrunner_uk	Platform C

Then record possible links:

Relationship ID	Entities	Evidence	Confidence
R01	E01 / E02	Similar username pattern	Low
R02	E01 / E03	Similar theme	Low
R03	E02 / E03	Similar theme and country hint	Low

The researcher would need stronger evidence before linking them, such as direct cross-links, same public website, same contact address, or self-identification.

21. Attribution Language Library

Use careful wording in notes and reports.

Observed

- “The profile displays...”
- “The page states...”
- “The register lists...”
- “The document names...”
- “The account links to...”

Possible

- “This may indicate...”
- “This is a possible link...”
- “This is consistent with...”

- “This creates a lead for further checking...”

Supported

- “This link is supported by...”
- “Multiple public sources indicate...”
- “The same domain is linked from...”
- “The source directly connects...”

Limited or Unclear

- “The available evidence does not establish...”
- “No direct link was found between...”
- “The relationship remains unconfirmed.”
- “Alternative explanations include...”

Avoid

- “Definitely.”
- “Obviously.”
- “This proves everything.”
- “It has to be them.”
- “Same name, same person.”
- “Guilty.”

22. Privacy and Redaction in Identity Work

Identity notes can quickly collect sensitive details. Not all details belong in the final report.

Keep Internally if Relevant

- Source capture references.
- Public business contact details.
- Public organisation identifiers.
- Publicly listed role information.
- Evidence needed to support the finding.

Redact or Exclude if Not Necessary

- Private home addresses.
- Personal phone numbers.
- Family member names.
- Children’s information.
- Health details.
- Unrelated private social content.
- Personal photographs that do not support the task.
- Sensitive characteristics unrelated to the investigation.

Redaction Note

When redacting, do not silently remove context that changes the meaning. Add a note such as:

“Personal contact details have been redacted as they are not required for the purpose of this report.”

23. Mini Exercise: Safe Attribution Table

Use a fictional or harmless public example. Do not use a private individual.

Task

Pick a public organisation, club, charity, or business that has an official website and one public social media account.

Create:

1. An entity table.
2. A relationship table.
3. A confidence note.
4. One careful finding.

Entity Table Template

Entity ID	Type	Name / Value	Source	Date Captured	Notes
E01	Organisation				
E02	Website				
E03	Social account				
E04	Email or contact page				

Relationship Table Template

Relationship ID	Entity A	Relationship	Entity B	Evidence	Confidence
R01					
R02					
R03					

Careful Finding Template

Finding:

The public evidence shows that [Entity A] is linked to [Entity B] by [source/evidence]. This supports [careful conclusion].

24. Chapter Checklist

Before moving on, the reader should be able to:

- ■ Explain what an entity is.
- ■ Separate people, accounts, usernames, domains, organisations, and documents.
- ■ Treat identifiers as clues rather than proof.
- ■ Build an entity table.
- ■ Build a relationship table.
- ■ Assign confidence levels to identity links.
- ■ Write careful attribution findings.
- ■ Record contradictions instead of ignoring them.
- ■ Avoid doxxing, harassment, or invasive personal research.
- ■ Redact unnecessary personal details from reports.

25. Key Takeaways

Identity work is one of the easiest places to make serious mistakes.

A professional OSINT researcher does not rush from a username to a person, from a name to a full identity, or from a suspicion to an accusation.

The safe method is:

1. List entities separately.
2. Record sources carefully.
3. Create relationship claims only when evidence supports them.
4. Grade confidence honestly.
5. Consider alternative explanations.
6. Report only what is necessary.
7. Protect people from avoidable harm.

The reader is now ready to move from individual clues into structured investigation planning.

The next chapter, **Chapter 9 - Building a Safe Investigation Plan**, turns these foundations into a controlled workflow: objective, scope, exclusions, sources, risks, outputs, and stopping points.

Chapter 9 - Building a Safe Investigation Plan

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Purpose of This Chapter

Good OSINT does not begin with tools. It begins with a plan.

A safe investigation plan protects the researcher, the subject, the client, the evidence, and the final report. It stops the work drifting into guesswork, curiosity, harassment, unlawful access, or unsupported claims.

This chapter gives the reader a simple planning method that can be used before any OSINT task, from a small fact-check to a larger defensive investigation.

By the end of this chapter, the reader should be able to create a clear OSINT plan that defines:

- the investigation question;
- the lawful scope;
- what is included and excluded;
- what sources may be used;
- what actions are not allowed;
- how evidence will be captured;
- how risks will be handled;
- what the final output should look like.

1. Why Planning Matters

Unplanned OSINT creates problems.

A researcher may start with one question, follow an interesting lead, open twenty tabs, save screenshots with unclear names, forget where a claim came from, and end up with a pile of information that cannot be trusted.

Planning prevents this.

A good plan creates boundaries. It tells the researcher what they are trying to answer and what they are not trying to answer. It also gives the final report a clear audit trail.

OSINT is not about collecting everything. It is about collecting what is relevant, lawful, proportionate, and useful.

2. The Investigation Question

Every OSINT task needs a central question.

A weak question is vague:

Find everything about this person.

A better question is limited and testable:

Identify whether the public social media profile claiming to represent this business is connected to the business's official website or public contact channels.

A weak question encourages overcollection. A strong question creates a target for the research.

A Good Investigation Question Should Be

- **Specific** - it says what needs to be answered.
- **Lawful** - it can be answered using permitted sources and methods.
- **Relevant** - it connects directly to the reason for the investigation.
- **Limited** - it does not invite unnecessary private information gathering.
- **Testable** - it can be supported or not supported by evidence.

Planning Prompt

Before starting, write one sentence:

The purpose of this investigation is to determine whether...

If that sentence cannot be completed clearly, the investigation is not ready to begin.

3. Scope: What Is Included

Scope defines the permitted area of work.

It answers:

- What entity is being researched?
- What time period is relevant?
- What platforms or source types are allowed?
- What facts are being checked?
- What outcome is needed?

Example Scope

Included:

- Public website pages connected to Example Ltd.
- Public company registry entries.
- Public social media profiles that claim to represent Example Ltd.
- Domain registration clues where lawfully available.
- Archived public web pages.
- Evidence captured between 7 June 2026 and 10 June 2026.

This gives the researcher a clear working lane.

4. Exclusions: What Is Not Included

Exclusions are just as important as scope.

They prevent mission creep and unsafe behaviour.

Example Exclusions

Excluded:

- Attempting to access private accounts.
- Contacting employees or private individuals.
- Bypassing login pages or technical restrictions.
- Collecting unrelated personal information.
- Making allegations without evidence.
- Publishing findings publicly before review.

If something is excluded, it must not be done unless the plan is formally changed and the change is justified.

5. Legal and Ethical Boundary Check

Before collection begins, perform a boundary check.

Ask:

1. Is the information public or lawfully accessible?
2. Is the collection necessary for the investigation question?
3. Is the method proportionate?
4. Could the action cause harm, distress, or unwanted exposure?
5. Is consent required?
6. Are there special rules for the type of subject, location, or data?
7. Would the method still look reasonable if explained in the final report?

If the answer feels uncertain, stop and reassess before collecting.

A safe OSINT plan should never rely on hidden access, deception, coercion, password guessing, private account intrusion, or harassment.

6. Source Plan

A source plan lists where the researcher will look first.

It prevents random searching and makes the investigation easier to review.

Basic Source Categories

Official sources:

- organisation website
- public registry
- official social media channel
- press releases

Independent sources:

- reputable news reports
- archived pages
- public documents
- specialist databases

Community or social sources:

- forum posts
- public comments
- social media discussions
- review platforms

Verification sources:

- archived copies
- independent references
- date/time checks
- cross-source confirmation

Each source type should have a purpose. Do not search a source merely because it exists.

7. Risk Assessment

Even lawful OSINT can create risk.

The plan should identify obvious risks before work begins.

Common OSINT Risks

- Misidentifying a person or organisation.
- Treating a username as proof of identity.
- Capturing outdated information.
- Relying on copied or circular reporting.
- Saving sensitive information unnecessarily.
- Accidentally exposing private data in a report.
- Allowing personal opinions to influence conclusions.

- Engaging with a subject when passive research was required.
- Failing to separate evidence from assumptions.

Risk Control Table

Risk	Control
False identity match	Use confidence levels and independent confirmation.
Outdated information	Record capture date and source publication date.
Overcollection	Follow scope and exclusions.
Sensitive data exposure	Redact unnecessary personal details.
Weak evidence trail	Use evidence cards and source logs.
Bias	Record alternative explanations.

Risk cannot always be removed, but it can be managed.

8. Collection Rules

Before starting, define the collection rules.

These rules should be simple enough to follow during the investigation.

Example Collection Rules

Collection rules:

1. Capture the original source before making notes.
2. Record the URL or source reference.
3. Record the date and time of capture.
4. Save screenshots with clear filenames.
5. Separate observations from conclusions.
6. Do not collect unrelated personal material.
7. Do not contact subjects unless authorised and necessary.
8. Do not use private, leaked, stolen, or restricted material.
9. Redact sensitive material before sharing.
10. Record confidence level for every finding.

Collection rules keep the work disciplined when the investigation becomes busy.

9. The Investigation Plan Template

The following template can be copied into the case folder before starting.

OSINT INVESTIGATION PLAN

Case name:
Date opened:
Researcher:

1. Investigation question
What are we trying to determine?
2. Purpose
Why is this investigation being carried out?
3. Subject / entity
What person, organisation, account, domain, event, or object is in scope?
4. Included scope
What sources, platforms, time periods, and facts are included?
5. Exclusions
What must not be collected or attempted?
6. Legal / ethical boundaries
What rules, permissions, or sensitivities apply?
7. Source plan
Which source categories will be checked first?
8. Evidence capture method
How will screenshots, URLs, notes, and source records be saved?

9. Risk assessment

What could go wrong, and how will it be controlled?

10. Output required

What final product is needed: short note, evidence pack, timeline, report, briefing, or referral?

11. Review point

When should the work stop for review before continuing?

This plan does not need to be complicated. It simply needs to be clear.

10. Stop Points

A stop point is a planned moment where the researcher pauses and reviews the work before continuing.

Stop points are useful when:

- a possible identity match has been found;
- the research is moving into sensitive personal information;
- the sources contradict each other;
- the investigation is drifting outside the original scope;
- a finding could affect someone's reputation;
- the next step might involve contact, escalation, or reporting.

A stop point prevents careless momentum.

Stop Point Prompt

Before continuing, ask:

- Am I still inside the agreed scope?
- Is this lead relevant to the investigation question?
- Have I captured evidence properly?
- Am I about to make an assumption?
- Does this need review before I continue?

11. Handling Scope Creep

Scope creep happens when the investigation expands without a clear reason.

A researcher might begin by checking whether a business profile is genuine, then drift into researching employees, relatives, old addresses, unrelated disputes, or private lives.

That is unsafe and usually unnecessary.

If a new lead appears, do not automatically follow it. Record it as a lead and decide whether it belongs inside the plan.

Lead Handling Table

Lead	Relevant?	In scope?	Evidence needed?	Action
New company domain found	Yes	Yes	Archive page and domain record	Continue
Employee personal account found	Possibly	No	Not required	Do not collect
Old forum allegation found	Unclear	Maybe	Independent confirmation needed	Record with caution

Not every lead deserves action.

12. Output Planning

The plan should define the final output before collection begins.

Different outputs need different evidence depth.

Common OSINT Outputs

- **Short answer** - a brief finding with sources.
- **Evidence pack** - screenshots, source records, and notes.
- **Timeline** - events arranged by date and source.
- **Entity map** - relationships between accounts, domains, companies, or people.
- **Risk summary** - exposure, impersonation, fraud, or safety concerns.
- **Formal report** - method, findings, evidence, limitations, and recommendations.
- **Referral pack** - material prepared for a platform, employer, solicitor, insurer, or law enforcement contact.

The output should match the purpose. Do not create a large invasive report when a short verification note is enough.

13. Safe Investigation Language

The plan should also guide the language used in the final output.

Avoid overclaiming.

Unsafe Language

This proves the account belongs to John Smith.

Safer Language

The account uses the same username as John Smith's public business profile and links to the same website. This supports Safe language protects accuracy and fairness.

14. Mini Example: Planning a Defensive OSINT Check

Scenario

A small business believes a social media account may be impersonating them.

Investigation Question

Determine whether the public social media account @ExampleSupport is genuinely connected to Example Ltd or is likely to

Scope

- Included:
- Example Ltd official website.
 - Public contact pages.
 - Public social media links from the official website.
 - The public @ExampleSupport profile.
 - Archived public pages.
 - Public platform profile details.

Exclusions

- Excluded:
- Contacting the account.
 - Attempting to access private messages.
 - Researching private employees.
 - Collecting unrelated customer data.

Source Plan

1. Official website.
2. Official social links.
3. Public profile page.
4. Archived versions of website and social profile.
5. Independent mentions of the account.

Output Required

- Short evidence-backed assessment:
- likely genuine;
 - likely not genuine;
 - unclear / requires platform or business confirmation.

This is a focused, proportionate plan.

15. Chapter Checklist

Before starting an OSINT task, confirm:

- The investigation question is clear.
- The scope is written down.
- The exclusions are written down.
- The source plan is proportionate.
- The collection rules are clear.
- The evidence capture method is ready.
- The legal and ethical boundaries have been checked.
- Risks and controls have been listed.
- Stop points are defined.
- The final output is known.

If these items are not ready, the investigation should not begin yet.

Practical Exercise

Create a safe investigation plan for the following scenario:

A charity has found a public fundraising page using its name and logo. The charity needs to know whether the page is of

Your plan should include:

1. Investigation question.
2. Included scope.
3. Exclusions.
4. Source plan.
5. Evidence capture method.
6. Risks and controls.
7. Final output.

Do not attempt to identify private donors, contact page visitors, or access private account areas. Keep the plan focused on public verification of the fundraising page and its claimed connection to the charity.

Visual Brief - Safe Investigation Planning Board

Visual ID: V16

Title: Safe Investigation Planning Board

Purpose: Show the reader how a safe OSINT plan is built before collection starts.

Style: Dark technical workbook style with gold/amber accents, matching the OSINT Bible visual register.

Layout:

- Central board titled **Investigation Plan**.
- Six connected panels:
 1. Question
 2. Scope

3. Exclusions

4. Source Plan

5. Evidence Method

6. Output

- A side column titled **Risk Controls** with small warning icons.
- A bottom strip titled **Stop Points** showing pause markers before sensitive steps.
- Include a small note: **Plan first. Collect second. Conclude last.**

Avoid:

- No hacker imagery.
- No police badge graphics.
- No surveillance-style targeting imagery.
- No crosshairs, red-string conspiracy boards, or illegal-access visuals.

Key Takeaway

A safe investigation plan is the difference between disciplined OSINT and uncontrolled searching.

Plan first. Collect second. Verify constantly. Conclude carefully.

Chapter 10 - First Complete Mini-Investigation

***Safety and lawful-use note:** This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.*

Purpose of This Chapter

The first nine chapters built the foundations: lawful boundaries, disciplined note-taking, source reliability, identity caution, search planning, and safe investigation design.

This chapter brings those pieces together in one complete mini-investigation.

The scenario is fictional. The names, organisations, accounts, websites, and evidence examples are invented for training purposes. The aim is not to investigate a real person or organisation, but to practise the workflow in a safe, controlled way.

By the end of this chapter, the reader should be able to complete a small OSINT task from start to finish by:

- defining a clear question;
- setting scope and exclusions;
- collecting only relevant public information;
- recording sources properly;
- checking source reliability;
- separating observation from conclusion;
- handling contradictions;
- writing a short, evidence-backed assessment;
- listing limitations and next steps.

1. The Training Scenario

Scenario

A fictional community organisation called **Northbank Community Workshop** believes that a public social media page may be pretending to represent them.

The suspected page is called:

Northbank Workshop Support

The organisation wants a simple answer:

Is this public page likely to be genuinely connected to Northbank Community Workshop, or is it likely to be unauthorised?

The organisation does not want private individuals investigated. It does not want anyone contacted. It only wants a public-source verification check.

2. Investigation Question

The investigation question must be clear before collection begins.

Investigation Question

Determine whether the public page named Northbank Workshop Support is publicly linked to, endorsed by, or otherwise ver-

This question is narrow and proportionate. It does not ask for private identity research. It does not ask who owns the page. It asks whether there is public evidence connecting the page to the organisation.

3. Scope

Scope defines what is allowed.

Included Scope

Included:

- Northbank Community Workshop's official website.
- Public contact and social links from the official website.
- Public profile details of the suspected page.
- Public posts made by the suspected page.
- Public archive captures of official pages, if available.
- Public references to the suspected page from independent sources.
- Public consistency checks such as names, logos, contact details, and linked domains.

Excluded Scope

Excluded:

- Contacting the suspected page.
- Contacting staff, volunteers, followers, donors, or members of the public.
- Attempting to access private messages, private groups, hidden content, or login-only material.
- Trying to identify the page administrator.
- Collecting personal information about individuals.
- Making public allegations.
- Using leaked, stolen, breached, or restricted data.

These exclusions keep the investigation passive, lawful, and proportionate.

4. Case Folder Setup

Before collecting evidence, create a case folder.

Suggested Folder Structure

```
Case_Northbank_Page_Check
■
■■■ 00_PLAN
■   ■■■ investigation_plan.md
■
■■■ 01_SOURCES
■   ■■■ source_list.md
■
■■■ 02_SCREENSHOTS_ORIGINAL
■
■■■ 03_NOTES
■   ■■■ case_journal.md
■
■■■ 04_EVIDENCE_CARDS
■
■■■ 05_WORKING_ANALYSIS
■
■■■ 06_REDACTED_EXPORTS
■
■■■ 07_FINAL_REPORT
```

This structure separates original evidence from notes, analysis, redacted material, and final output.

5. Evidence Capture Rules

Use simple collection rules.

Evidence capture rules:

1. Capture the original public source before writing conclusions.
2. Record source name, URL/reference, date captured, and time captured.
3. Save screenshots using clear filenames.
4. Do not collect unrelated personal information.
5. Record uncertainty immediately.
6. Treat profile names, logos, and repeated wording as clues, not proof.
7. Confirm important findings with more than one source where possible.
8. Separate observations from findings.
9. Redact unnecessary personal data before sharing.
10. Write limitations in the final report.

These rules make the work repeatable and reviewable.

6. Source Plan

For this mini-investigation, the source plan is deliberately small.

Step	Source Type	Purpose
1	Official website	Establish official name, domain, contact details, and listed social channels.
2	Official website social links	Check whether the suspected page is linked by the organisation.
3	Suspected public page	Record page name, description, links, contact details, branding, and visible claims.
4	Public posts	Check whether the page makes claims of affiliation, fundraising, support, or official status.
5	Archive or cached public pages	Check whether official links changed over time.
6	Independent public references	Look for external mentions connecting or contradicting the page.

The source plan avoids deep personal searching because that is not needed for the question.

7. Case Journal

A case journal records what happened in order.

Example Case Journal Entry

Case: Northbank Page Check

Date: 7 June 2026

Researcher: Training example

09:30 – Opened case folder.

09:35 – Wrote investigation question and exclusions.

09:40 – Began with official website because it is the strongest source for official social links.

09:48 – Recorded official website contact page.

09:55 – Recorded suspected public page profile details.

10:10 – Compared names, links, logos, and contact details.

10:25 – Noted inconsistency between official website email address and suspected page email address.

10:40 – Checked whether official website links to suspected page. No link observed in training example.

10:55 – Drafted evidence cards.

11:15 – Wrote preliminary assessment with limitations.

The journal does not need to be fancy. It needs to show the route taken.

8. Evidence Card 1 - Official Website

Evidence cards turn raw source captures into structured records.

Evidence Card

Evidence ID: E01
Source type: Official organisation website
Source name: Northbank Community Workshop official website
Capture date: 7 June 2026
Capture time: 09:48
Captured by: Training example

The official website identifies the organisation as Northbank Community Workshop. The contact page lists the fictional domain northbank-workshop.example and provides an official contact email pattern.

Relevant details observed:

- Organisation name: Northbank Community Workshop
- Official domain: northbank-workshop.example
- Official email pattern: @northbank-workshop.example
- Listed social link: NorthbankCommunityWorkshopOfficial
- No visible link to a page named Northbank Workshop Support in this training example.

High for official contact details and official social links, because the source is the organisation's own website in the fictional scenario.

Limitations:

The website could be outdated. A missing link does not alone prove the suspected page is unauthorised.

Confidence supported:

Medium to high for identifying the official website's listed public channels.

This card does not overclaim. It records what was observed and what the limitations are.

9. Evidence Card 2 - Suspected Public Page

Evidence Card

Evidence ID: E02
Source type: Public social media profile
Source name: Northbank Workshop Support
Capture date: 7 June 2026
Capture time: 09:55
Captured by: Training example

The public page uses a similar name to Northbank Community Workshop and uses a similar logo style. The page description claims to provide support updates for workshop users but operates completely outside the primary domain.

Relevant details observed:

- Page name: Northbank Workshop Support
- Claimed purpose: support updates
- External link: northbank-help.example
- Contact email: northbankworkshophelp@exampleemail.test
- Visible wording: "support updates for workshop users"
- No visible statement that the page is unofficial in this training example.

Medium for recording what the page publicly claims about itself. Low for proving any real connection to the organisation without independent confirmation.

Limitations:

A public profile can claim affiliation without being authorised. Branding similarity is a clue but not proof.

Medium confidence that the page presents itself as connected or adjacent to the organisation; low confidence that it is genuinely authorised based on this source alone.

This card carefully separates the page's claim from the truth of that claim.

10. Evidence Card 3 - Link and Contact Detail Comparison

Comparison is often more useful than a single screenshot.

Evidence Card

Evidence ID: E03
Source type: Comparison of official website and suspected page
Capture date: 7 June 2026
Capture time: 10:10
Captured by: Training example

Observation:

The official website and suspected page use different domains and different email patterns.

Official website:

- Domain: northbank-workshop.example
- Email pattern: @northbank-workshop.example
- Listed social page: NorthbankCommunityWorkshopOfficial

Suspected page:

- Linked domain: northbank-help.example
- Contact email: northbankworkshophelp@exampleemail.test
- Page name: Northbank Workshop Support

The suspected page's linked domain and contact email do not match the official website's domain or email pattern in this training example.

Medium. The comparison is based on captured public details, but the organisation could use multiple domains or third-party support channels.

Different contact details are suspicious but not conclusive. Authorisation could exist outside the public sources checked.

Confidence supported:

Medium confidence that the suspected page is not publicly linked through the official website sources checked.

The evidence supports concern, not certainty.

11. Evidence Card 4 - Official Link Check

Evidence Card

Evidence ID: E04
Source type: Official website link check
Capture date: 7 June 2026
Capture time: 10:40
Captured by: Training example

The official website's public social links section lists one official social page. The suspected page name does not appear in the official links section in this layout.

Relevant details observed:

- Official social link listed: NorthbankCommunityWorkshopOfficial
- Suspected page listed: Not observed
- Public support page link: Not observed

Reliability assessment:

High for what the official website visibly lists at the time of capture.

Limitations:

The official website may not list every authorised page. The website may be incomplete or outdated.

Confidence supported:

Medium confidence that the suspected page is not publicly endorsed through the official website at the time of capture.

A missing link should always be handled carefully. Absence of evidence is not always evidence of absence.

12. Working Analysis

After evidence cards are prepared, begin working analysis.

Do not jump straight to a final conclusion. Start with observations.

Observations

Observation 1:

The official website identifies one official social page, and that page name differs from the suspected page.

Observation 2:

The suspected page uses similar branding and a similar organisation name.

Observation 3:

The suspected page uses a different domain and email pattern from the official website.

Observation 4:

The suspected page is not visibly linked from the official website in this training example.

Observation 5:

No independent public confirmation connecting the suspected page to the organisation has been recorded in this mini-investigation.

What These Observations Support

The evidence supports concern that the suspected page may not be officially connected to the organisation.

What These Observations Do Not Prove

The evidence does not prove who created the page.

The evidence does not prove fraud.

The evidence does not prove malicious intent.

The evidence does not prove the page is unauthorised beyond all doubt.

This distinction is central to responsible OSINT.

13. Contradictions and Alternative Explanations

A good mini-investigation should list possible alternative explanations.

Issue	Possible Explanation	How It Affects Confidence
Different email address	Unauthorised page, or third-party support provider, or old contact route.	Reduces certainty.
Different linked domain	Impersonation clue, or separate support domain, or outdated website.	Requires confirmation.
Similar branding	Could indicate official connection, or copying.	Not conclusive.
Missing official link	Page may be unauthorised, or website may be incomplete.	Supports concern but not proof.

Alternative explanations prevent tunnel vision.

14. Confidence Rating

Use confidence levels rather than absolute statements.

Suggested Confidence Scale

High confidence:

Multiple reliable, independent sources support the same finding, with little contradiction.

Medium confidence:

Some reliable evidence supports the finding, but limitations or alternative explanations remain.

Low confidence:

Evidence is limited, indirect, conflicting, or based mainly on claims from one source.

Confidence for This Mini-Investigation

Finding:

The suspected page is not publicly linked or endorsed by the official website in this training example.

Confidence:

Medium.

Reason:

The official website lists a different social page and uses different contact details, but it is still possible that other information is available.

This is a balanced finding.

15. Draft Finding

A finding should be evidence-backed, careful, and limited.

Weak Finding

This is definitely a fake page.

This is unsafe because the evidence does not prove that.

Stronger Finding

Based on the public sources checked in this mini-investigation, the suspected page named Northbank Workshop Support is not visibly linked from the official Northbank Community Workshop domain or its public social register.

This wording is careful, useful, and defensible.

16. Mini Report

A short OSINT report should be easy to read.

Example Mini Report

Title:
Public Source Verification Check - Northbank Workshop Support Page.

Date:
7 June 2026.

Investigation Question:
Determine whether the public page named Northbank Workshop Support is publicly linked to, endorsed by, or otherwise verifiably connected to Northbank Community Workshop.

Scope:
This review used public sources only. It checked the fictional organisation's official website, visible social links, the suspected public page profile, visible page claims, and public domain/contact consistency.

Exclusions:
No private accounts were accessed. No individuals were contacted. No attempt was made to identify the page administrator. No personal information was collected beyond the public page details required for this verification check.

Summary Finding:
The suspected page was not visibly linked from the official website in this training example. The suspected page used a different domain and email pattern from the organisation's official public contact details.

Evidence Summary:
E01 - Official website listed the organisation's official domain and contact email pattern.
E02 - Suspected page used a similar name and branding but different contact details.
E03 - Comparison showed mismatch between official and suspected page domain/email details.
E04 - Official link check did not show the suspected page in the listed official social links.

Confidence:
Medium confidence that the suspected page is not publicly endorsed through the official sources checked.

Limitations:
The public sources reviewed represent a temporal snapshot only.

Recommended Next Steps:
The organisation should verify internally whether the page is authorised. If unauthorised, the organisation may consider platform reporting and a public clarification from official channels.

This mini report is short, proportionate, and evidence-led.

17. Redaction Check Before Sharing

Before sharing a report or evidence pack, check whether any unnecessary personal information appears in screenshots or notes.

Redaction Questions

Before sharing, ask:

- Are private individuals visible in screenshots?
- Are comments, names, profile pictures, or unrelated contact details unnecessary?
- Is any sensitive information included that does not support the finding?
- Can the evidence be cropped or redacted without damaging the meaning?
- Is the final report written in careful, non-accusatory language?

Even public information may not need to be repeated in a report.

18. What This Mini-Investigation Did Well

This investigation stayed safe because it:

- started with a clear question;
- defined scope before collection;
- excluded private identity research;
- used public sources only;
- captured evidence before analysis;
- separated observations from conclusions;
- considered alternative explanations;
- used confidence levels;
- avoided accusations;
- recommended proportionate next steps.

This is the habit the reader should carry into later chapters.

19. Common Mistakes in Mini-Investigations

Mistake 1 - Starting With the Suspected Page Only

If the researcher starts with the suspected page and believes its claims, they may accidentally accept the page's self-description as fact.

Start with official sources first.

Mistake 2 - Treating Similar Branding as Proof

Similar branding can be a clue, but it can also be copied. It is not proof of authorisation.

Mistake 3 - Overclaiming Fraud

A page can look suspicious without the evidence proving fraud. Use careful wording.

Mistake 4 - Collecting Too Much

Do not collect followers, comments, donors, private people, or unrelated personal material unless it is lawful, necessary, and inside scope.

Mistake 5 - Forgetting Limitations

Every report should explain what was not checked and what remains uncertain.

20. Chapter Checklist

A complete mini-investigation should include:

- A written investigation question.
- Scope and exclusions.
- A source plan.
- A case folder.
- A case journal.
- Evidence cards.
- Source reliability notes.
- Observation list.

- Alternative explanations.
- Confidence rating.
- Short evidence-backed finding.
- Limitations.
- Recommended next steps.
- Redaction check.

If these are present, the reader has completed a disciplined first OSINT workflow.

Practical Exercise

Use the same fictional scenario and prepare your own mini-investigation pack.

Scenario

A fictional charity called Rivergate Animal Rescue finds a public fundraising page named Rivergate Rescue Emergency Fund.

Your Task

Create:

1. An investigation question.
2. Scope and exclusions.
3. A source plan.
4. Three evidence card templates.
5. A short observation list.
6. A confidence rating.
7. A mini report of no more than 300 words.
8. A list of limitations.

Safety Rules

Do not investigate real people. Do not contact anyone. Do not collect donor information. Do not access private pages. Keep the exercise fictional and focused on public verification.

End of Volume 1 Note

This chapter completes **Volume 1 - Foundations**.

The reader now has the core discipline needed before moving into more advanced discovery work:

- ethics and boundaries;
- workspace setup;
- evidence control;
- search basics;
- source reliability;
- attribution caution;
- safe planning;
- a complete mini-investigation workflow.

Volume 2 moves into deeper search techniques, query building, archives, public sources, registries, specialist sources, and structured discovery workflows.

VOLUME TWO

Search and Sources

Search operators, archives, public records, specialist sources, monitoring, and source lists.

CHAPTERS 11-20



Chapter 11 - Search Operators and Query Building

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Purpose of This Chapter

Volume 1 built the discipline: define the question, set scope, capture sources, assess reliability, and avoid jumping from clue to conclusion.

This chapter starts Volume 2 by turning ordinary web search into a repeatable OSINT skill. Search operators and query building are not magic tricks. They are a way to ask cleaner questions, reduce noise, find better sources, and document how information was discovered.

By the end of this chapter, the reader should be able to:

- break a research question into searchable parts;
- use basic search operators responsibly;
- build broad, narrow, and verification queries;
- search within specific domains and document types;
- use exclusion terms to remove noise;
- test name, spelling, date, and location variants;
- record searches in a search log;
- avoid unsafe or intrusive searching;
- convert search results into evidence cards rather than unsupported claims.

This chapter is for lawful, defensive, journalistic, academic, business, and personal-safety OSINT. It must not be used to locate private data, credentials, restricted files, personal contact details, or anything obtained through unauthorised access.

1. What Search Operators Are

Search operators are special words, symbols, or patterns added to a search query to guide the search engine.

A normal query might be:

Northbank Community Workshop annual report

An operator-led query might be:

site:northbank-workshop.example "annual report" filetype:pdf

The second query tells the search engine to:

- look within a specific domain;
- look for an exact phrase;
- prefer a particular document type.

Search operators do not guarantee complete results. Search engines differ. Some operators work differently across Google, Bing, DuckDuckGo, and specialist databases. Operators should therefore be treated as tools for discovery, not

proof.

The rule is simple:

A search result is a lead. A captured source is evidence. A verified pattern is a finding.

2. Operator Caution

Search syntax changes over time. Some operators are officially documented. Others are commonly used but inconsistent. Some may stop working, behave differently by region, or be affected by personalisation, browser settings, account status, or search engine updates.

For professional OSINT work, do not rely on memory alone. Test the query, log the search engine used, record the date, and capture the source that supports the finding.

Search Engine Record

Every important query should record:

Search engine:
Browser/profile:
Date:
Time:
Region/language setting:
Exact query:
Top useful result:
Result captured? Yes/No
Notes:

This matters because a query repeated later may not return the same result.

3. The Core Query-Building Method

A strong search starts before the search box.

Use this structure:

1. Define the question.
2. Extract searchable components.
3. List variants.
4. Start broad.
5. Narrow with operators.
6. Verify with independent sources.
7. Log the query.
8. Capture useful sources.
9. Convert observations into evidence cards.

Example Question

Is the fictional organisation Northbank Community Workshop publicly linked to a page named Northbank Workshop Support?

Searchable Components

Organisation name:
Northbank Community Workshop

Suspected page name:
Northbank Workshop Support

Possible domain:
northbank-workshop.example

Possible source types:
official website, contact page, social profile, newsletter, PDF, announcement, archive

Possible relationship words:
partner, support, official, fundraising, volunteer, donation, community, page, campaign

First Broad Query

"Northbank Community Workshop" "Northbank Workshop Support"

Narrower Query

site:northbank-workshop.example "Northbank Workshop Support"

Verification Query

"Northbank Workshop Support" "northbank-workshop.example"

The broad query asks whether both names appear together anywhere. The narrow query asks whether the official domain mentions the suspected page. The verification query asks whether the suspected page and official domain are publicly linked elsewhere.

4. Exact Phrase Searching

Quotation marks are used by many search engines to search for an exact phrase or a close exact match.

Example

"Northbank Community Workshop"

Use exact phrases when:

- the wording is distinctive;
- the name contains common words;
- you want to reduce unrelated results;
- you are searching for a slogan, title, policy name, event name, or quoted statement.

Common Mistake

Do not start too narrow. If an exact phrase returns little or nothing, try variants:

"Northbank Community Workshop"
"Northbank Workshop"
"Northbank Community Centre"
"North Bank Community Workshop"

Exact phrase searching is useful, but it can miss spelling differences, abbreviations, punctuation changes, OCR errors, and translated wording.

5. OR Searches

The OR operator is used to search for one term or another. In many search engines, OR must be written in capital letters.

Example

"Northbank Community Workshop" OR "Northbank Workshop"

This is useful where names vary.

Identity Variant Example

"A. J. Carter" OR "Alex Carter" OR "Alexander Carter"

Organisation Variant Example

"Northbank Community Workshop" OR "Northbank Community Project" OR "Northbank Community Centre"

Use OR carefully. Too many variants can make results noisy. If the query becomes too broad, split it into smaller searches and log each one separately.

6. Excluding Noise with the Minus Sign or NOT

Exclusion terms remove results containing unwanted words. Google-style searches often use the minus sign. Bing also documents NOT as an advanced option when capitalised.

Example

"Northbank Workshop" -furniture -woodwork

This removes results that are probably about a physical workshop rather than a community organisation.

When to Use Exclusions

Use exclusions when:

- a name is shared by unrelated people or organisations;
- a word has multiple meanings;
- a location produces irrelevant tourism or retail results;
- a topic is drowned by current news unrelated to your case.

Caution

Exclusion can hide useful evidence. Always run at least one broad search before excluding terms.

Bad approach:

Start with heavy exclusions immediately.

Better approach:

1. Broad search.
2. Identify recurring noise.
3. Add one or two exclusions.
4. Compare results.
5. Log what changed.

7. Searching Within a Site or Domain

The `site:` operator is one of the most useful operators for OSINT because it limits results to a domain or part of a domain.

Official Domain Search

`site:northbank-workshop.example "volunteer"`

Specific Section Search

`site:northbank-workshop.example/events "fundraising"`

Wider Domain Search

`site:example.org "Northbank Community Workshop"`

Use site searching to answer questions like:

- Does the official website mention this account?
- Does a company domain mention a product, director, policy, or partner?
- Has an organisation published a PDF, newsletter, or archive page?
- Are there public pages not easily visible through site navigation?

Boundary Rule

Searching public pages is different from attempting access. Do not try to bypass logins, permissions, paywalls, robots exclusions, hidden systems, or restricted areas. If a result appears to expose private or sensitive information, stop, record minimal details safely, and escalate appropriately rather than collecting or sharing it.

8. Searching for File Types

The `filetype:` operator can help locate public documents such as PDFs, spreadsheets, presentations, policy documents, manuals, newsletters, agendas, minutes, forms, and reports.

Safe Public-Document Examples

`site:northbank-workshop.example filetype:pdf "annual report"`

`site:northbank-workshop.example filetype:pdf "safeguarding policy"`

`site:northbank-workshop.example filetype:pdf "trustees"`

Use filetype searches for public-interest, public-record, organisational, research, and defensive work.

Unsafe Use

Do not use filetype searches to hunt for:

- passwords;
- private keys;
- access tokens;
- confidential documents;
- personal data dumps;
- exposed backups;
- login portals;
- restricted internal files.

If such material appears unexpectedly, do not download or redistribute it. Record that a potential exposure was observed, preserve only what is necessary, and report it through a lawful route.

9. Title and URL Clues

Some search engines support operators such as `intitle:` or `inurl:`. These can be useful because page titles and URLs often reveal document type, page purpose, or naming conventions.

Title Example

```
intitle:"annual report" "Northbank Community Workshop"
```

URL Example

```
inurl:news "Northbank Community Workshop"
```

Safer Uses

Use title and URL clues to find:

- public reports;
- public policy pages;
- event pages;
- press releases;
- official notices;
- public directories;
- public help pages.

Caution

Do not use title and URL operators to search for exposed administrative systems, login pages, misconfigured panels, or sensitive infrastructure. This guide is not a hacking manual.

10. Date and Time Queries

Dates are critical in OSINT. A true statement from five years ago may be misleading today. A page may have changed. A claim may have been copied from an old source.

Search engines and advanced search pages often allow date filtering. Some support query operators or filters for date ranges. Because support varies, record exactly how the date range was applied.

Date Variant Queries

```
"Northbank Community Workshop" "2024"
```

```
"Northbank Community Workshop" "2025" "annual report"
```

"Northbank Workshop Support" "March 2026"

Date Discipline

For every useful result, capture:

Published date:
Updated date:
Capture date:
Date mentioned in the content:
Date range searched:

These are not the same thing.

Example

A web page captured on 7 June 2026 may contain a press release from 2022 that was updated in 2024. The correct evidence card should preserve all three dates.

11. Location Queries

Locations help disambiguate names and events.

Example

"Northbank Community Workshop" "Kent"
"Northbank Community Workshop" "High Street"
"Northbank Workshop Support" "Tunbridge Wells"

Location searches should be proportionate. For organisations and public events, location can be legitimate and necessary. For private individuals, avoid unnecessary address-level collection unless there is a lawful, consent-based, or safeguarding reason and a clear escalation route.

12. Name Variant Queries

Names vary. People abbreviate. Organisations rebrand. Social pages shorten titles. Documents contain typos.

Variant Types

Full name:
Northbank Community Workshop

Short name:
Northbank Workshop

Acronym:
NCW

Spacing variant:
North Bank Community Workshop

Hyphen variant:
North-Bank Community Workshop

Old name:
Northbank Community Project

Trading or campaign name:
Northbank Workshop Support

Variant Query Set

"Northbank Community Workshop"
"Northbank Workshop"
"North Bank Community Workshop"
"Northbank Community Project"
"NCW" "Northbank"

Do not assume that a variant proves identity. A variant is only a clue.

13. Building Query Families

A query family is a set of related searches designed to answer one part of the investigation question.

Example Query Family: Official Link Check

```
site:northbank-workshop.example "Northbank Workshop Support"
site:northbank-workshop.example "support page"
site:northbank-workshop.example "Facebook"
site:northbank-workshop.example "social media"
site:northbank-workshop.example "donate"
site:northbank-workshop.example "fundraising"
```

Example Query Family: External Mention Check

```
"Northbank Workshop Support" "Northbank Community Workshop"
"Northbank Workshop Support" "official"
"Northbank Workshop Support" "donation"
"Northbank Workshop Support" "community"
"Northbank Workshop Support" "northbank-workshop.example"
```

Example Query Family: Document Check

```
site:northbank-workshop.example filetype:pdf "Northbank Workshop Support"
site:northbank-workshop.example filetype:pdf "social media"
site:northbank-workshop.example filetype:pdf "fundraising"
site:northbank-workshop.example filetype:pdf "annual report"
```

Query families prevent random searching. They also make the work easier to explain later.

14. Search Logs

A search log is the bridge between discovery and evidence.

Simple Search Log Template

Search ID	Date/Time	Engine	Exact Query	Purpose	Useful Result?	Captured?	Notes
S01	2026-06-07 10:00	Google	"Northbank Community Workshop" "Northbank Workshop Support"	Check direct link between names	No clear result	No	Broad search; no immediate link observed.
S02	2026-06-07 10:05	Bing	site:northbank-workshop.example "Northbank Workshop Support"	Check official site	No clear result	No	No official-domain mention observed in this training case.
S03	2026-06-07 10:15	DuckDuckGo	"Northbank Workshop Support" "donation"	Check fundraising context	One public post result	Yes	Create evidence card E03.

Why Logs Matter

Search logs show:

- what was searched;
- where it was searched;
- when it was searched;
- what the search was meant to prove or disprove;
- whether evidence was captured;
- what limitations remain.

Without a search log, later readers cannot easily tell whether the investigation was thorough or lucky.

15. From Result to Evidence

A search result is not enough.

Search snippets can be outdated, personalised, truncated, or misleading. The page may no longer match the snippet. The same snippet may appear across copied pages.

Correct Workflow

1. Run search.
2. Identify potentially useful result.
3. Open public source.
4. Check page context.
5. Capture source details.
6. Save screenshot or export where appropriate.
7. Record observation.
8. Assess reliability.
9. Decide whether it supports, contradicts, or does not affect the finding.

Evidence Card Conversion

Evidence ID: E11-03
Search ID: S03
Source type: Public page
Capture date: 7 June 2026
Capture time: 10:18

Observation:

The public page named Northbank Workshop Support contains wording that asks for donations for community equipment. It d

Assessment:

The source is useful for recording the page's public claim, but it is not enough to prove official affiliation.

Confidence impact:

Supports the need for further verification. Does not prove authenticity.

16. Combining Operators Safely

Operators are most useful when combined carefully.

Good Combination

`site:northbank-workshop.example "annual report" filetype:pdf`

This is clear, lawful, and proportionate. It looks for public annual reports on a known public domain.

Another Good Combination

`"Northbank Community Workshop" "trustees" filetype:pdf`

This may locate public governance documents.

Overloaded Query

`site:northbank-workshop.example "Northbank" OR "NCW" filetype:pdf -events -news -donate intitle:report`

This is too crowded. It may behave unpredictably. Split it into smaller queries.

Better Split

`site:northbank-workshop.example "Northbank" filetype:pdf`
`site:northbank-workshop.example "NCW" filetype:pdf`
`site:northbank-workshop.example intitle:"report"`
`site:northbank-workshop.example "annual report"`

Good OSINT is usually methodical, not flashy.

17. Search Engine Differences

Different search engines may produce different results.

Reasons include:

- different indexes;
- different ranking systems;

- regional settings;
- freshness differences;
- privacy settings;
- safe-search settings;
- operator support differences;
- personalisation or account state;
- AI summaries or answer boxes changing what is displayed.

Use more than one search engine when the result matters.

Comparison Log

Query	Google	Bing	DuckDuckGo	Notes
"Northbank Workshop Support"	Few results	One useful public page	No useful result	Capture useful page from Bing and verify directly.
site:northbank-workshop.example "social media"	Official contact page	Official contact page	Official contact page	Stronger confidence because multiple engines point to same source.

The engine is not the source. The source is the page, document, record, image, archive, or dataset found through the engine.

18. Query Building for Organisations

Organisation searches usually focus on official presence, documents, people in public roles, domains, public filings, press, policies, and public statements.

Organisation Query Components

Name:

"Northbank Community Workshop"

Domain:

site:northbank-workshop.example

Documents:

filetype:pdf "annual report"

filetype:pdf "policy"

filetype:pdf "minutes"

Role words:

trustee, director, founder, chair, volunteer coordinator, contact

Relationship words:

partner, sponsor, funder, official, affiliated, supported by

Date words:

2024, 2025, 2026, latest, annual, updated

Safe Organisation Query Examples

"Northbank Community Workshop" "annual report"

site:northbank-workshop.example "trustees"

"Northbank Community Workshop" "partner"

"Northbank Community Workshop" "press release"

These searches focus on public organisational information, not private lives.

19. Query Building for Public Claims

Public claims should be tested directly.

Claim Example

The page claims to be the official fundraising page for Northbank Community Workshop.

Search Questions

Does the official organisation mention this page?
Does the page link to the official domain?
Do independent sources describe it as official?
Do official documents list the same donation method?
Are there contradictions in contact details, names, dates, or wording?

Query Examples

site:northbank-workshop.example "Northbank Workshop Support"
"Northbank Workshop Support" "official fundraising"
"Northbank Workshop Support" "Northbank Community Workshop"
"Northbank Community Workshop" "donate" "Northbank Workshop Support"

Avoid making the query prove what you already believe. Build queries that could support or contradict the claim.

20. Query Building for Images and Documents

Search operators can help find pages that contain images or documents, but image verification itself belongs to later chapters.

Safe Image-Context Query

"Northbank Community Workshop" "open day" "photo"

Safe Document-Context Query

"Northbank Community Workshop" "open day" filetype:pdf

What to Record

For any useful image or document result, record:

Where was it found?
Who published it?
When was it published?
What does the page claim it shows?
Is the image/document original or copied?
Is there a higher-quality original source?
Does the content match the surrounding context?

Do not treat image search results as proof without source context.

21. Query Building for Archives

Archived material can show how a public page looked at an earlier time. However, archive coverage is incomplete and may not capture every page, every image, or every update.

Archive Search Approach

1. Identify the official domain or page URL.
2. Search for public mentions of historical versions.
3. Check reputable archive services manually where appropriate.
4. Record archive date separately from original publication date.
5. Compare archived pages with current pages.

Search Examples

"northbank-workshop.example" "archive"
"Northbank Community Workshop" "old website"
"Northbank Community Workshop" "formerly"

Archives are covered in more depth in Chapter 12.

22. Avoiding Search Bias

Search bias happens when the researcher writes queries designed only to confirm a belief.

Biased Query

"Northbank Workshop Support" scam fake fraud

This query assumes the conclusion before the evidence.

Better Balanced Query Set

"Northbank Workshop Support" "official"
"Northbank Workshop Support" "Northbank Community Workshop"
site:northbank-workshop.example "Northbank Workshop Support"
"Northbank Workshop Support" "donation"
"Northbank Workshop Support" "not affiliated"

This query set allows several possibilities:

- official page;
- unofficial supporter page;
- unrelated page;
- misleading page;
- false positive caused by name similarity;
- no meaningful evidence either way.

Good OSINT tests alternatives.

23. Handling No Results

No results does not prove something does not exist.

It may mean:

- the query was too narrow;
- the wording was different;
- the page is not indexed;
- the content is new;
- the content was removed;
- the search engine missed it;
- the relevant source is in another language;
- the relevant source is in a PDF, image, archive, or database;
- the material is not public.

No-Result Log Example

Search ID: S11-09
Query: site:northbank-workshop.example "Northbank Workshop Support"
Engine: Google
Date: 7 June 2026
Result: No relevant result observed.
Interpretation: No indexed official-site mention found using this exact query at this time. This does not prove the page
Next step: Check official website manually and test name variants.

Careful wording protects the investigation from overclaiming.

24. Handling Too Many Results

Too many results usually means the query is too broad.

Narrowing Tools

Use:

Exact phrase: "Northbank Community Workshop"
Site limit: site:northbank-workshop.example

File type: filetype:pdf
Location: "Kent"
Date term: "2026"
Relationship word: "official" or "partner"
Exclusion: -furniture

Example

Broad:

Northbank Workshop

Improved:

"Northbank Community Workshop" "Kent"

More targeted:

site:northbank-workshop.example "Northbank Community Workshop" "trustees"

25. Working With AI Search Summaries

Modern search engines may display AI summaries, answer boxes, or generated overviews. These can be useful pointers, but they should not be treated as evidence.

Rules for AI Search Summaries

1. Treat AI summaries as leads only.
2. Open the cited source.
3. Confirm the source actually says what the summary claims.
4. Capture the original source, not just the AI summary.
5. Record if an AI summary influenced your search path.
6. Do not quote AI output as factual evidence unless the task is specifically to analyse the AI output itself.

AI can help find routes. It does not replace source handling.

26. Unsafe Query Patterns to Avoid

A responsible OSINT practitioner avoids queries designed to locate private, restricted, or exploitable material.

Avoid searches aimed at finding:

- passwords;
- private keys;
- tokens;
- exposed databases;
- backup files;
- private documents;
- medical records;
- personal addresses unrelated to the task;
- doxxing material;
- login portals or admin panels;
- vulnerabilities or exploit paths;
- leaked or stolen datasets.

If the research question genuinely involves a security exposure, treat it as an incident-handling matter. Minimise collection, avoid downloading sensitive material, preserve only necessary context, and escalate through lawful disclosure or internal security channels.

27. Practical Query Builder Template

Use this worksheet before searching.

Investigation question:

Main entity:

Entity type:

Person / organisation / domain / event / document / location / claim / other

Known facts:

Unknowns:

Searchable names:

Spelling variants:

Acronyms:

Associated domains:

Associated locations:

Date range:

Likely source types:

Official site / public register / news / PDF / archive / social page / forum / academic / other

Words that may prove relationship:

official / partner / sponsor / director / trustee / affiliated / endorsed / published / registered

Words that may disprove or qualify relationship:

unofficial / not affiliated / impersonation / warning / correction / fake / parody / fan page

Noise terms to exclude:

First broad query:

Second targeted query:

Verification query:

Alternative explanation query:

Search log started? Yes/No

28. Practical Exercise

Scenario

A fictional local event called **Rivergate Makers Fair** appears on a public page claiming that it is sponsored by **Northbank Community Workshop**.

Your task is not to identify private individuals. Your task is to check whether there is public evidence that the sponsorship claim is genuine.

Investigation Question

Is there public evidence that Northbank Community Workshop sponsors or endorses the fictional Rivergate Makers Fair?

Scope

Included:

- Public official pages for Northbank Community Workshop.
- Public pages for Rivergate Makers Fair.
- Public press releases, event pages, PDFs, and newsletters.
- Public archive captures if needed.

Excluded:

- Contacting organisers or private individuals.
- Searching private social media content.
- Collecting personal addresses or unrelated contact details.
- Accessing restricted systems or hidden material.

Build a Query Family

Start with broad association:

"Rivergate Makers Fair" "Northbank Community Workshop"

Check official domain:

site:northbank-workshop.example "Rivergate Makers Fair"

Check sponsorship wording:

"Rivergate Makers Fair" "sponsored by" "Northbank"

Check public documents:

"Rivergate Makers Fair" filetype:pdf

Check event pages:

"Rivergate Makers Fair" "sponsor"

Check alternative wording:

"Rivergate Makers Fair" "partner" "Northbank"

Check contradiction or correction:

"Rivergate Makers Fair" "not affiliated" "Northbank"

Create a Search Log

Search ID	Query	Purpose	Result	Captured?
S01	"Rivergate Makers Fair" "Northbank Community Workshop"	Test direct association		
S02	site:northbank-workshop.example "Rivergate Makers Fair"	Check official source		
S03	"Rivergate Makers Fair" "sponsored by" "Northbank"	Check sponsorship wording		
S04	"Rivergate Makers Fair" filetype:pdf	Locate public documents		
S05	"Rivergate Makers Fair" "not affiliated" "Northbank"	Check contradiction		

Write a Mini Assessment

Use cautious language:

Based on the public searches completed, I found [no / limited / moderate / strong] evidence that Northbank Community Workshop is affiliated with Rivergate Makers Fair.

The strongest supporting source was:

The strongest contradicting or limiting source was:

Limitations:

Confidence level:

Low / Medium / High

Recommended next step:

29. Visual Brief - Search Operator Cheat Sheet and Query Builder

Visual ID

V18. Search operator and query-building board

Purpose

Create a clean workbook-style visual showing how a vague OSINT question becomes a structured set of safe searches.

Layout

Dark technical background with gold/amber accents.

Left panel:

Research Question

↓

Searchable Components

↓
Variants
↓
Query Family

Middle panel:

Core Operators
"exact phrase"
OR
-minus / NOT
site:
filetype:
intitle:
inurl:
date filters

Right panel:

Search Log
Search ID
Engine
Exact query
Purpose
Useful result
Captured?
Notes

Bottom caution strip:

Search result = lead
Captured source = evidence
Verified pattern = finding

Style requirements:

- no hacker imagery;
- no padlocks, skulls, masks, or exploit styling;
- use clean cards, arrows, and checklist elements;
- should look like a professional investigation workbook page.

30. Chapter Checklist

Before moving on, the reader should be able to answer yes to the following:

Can I turn an investigation question into searchable components?
Can I create name, spelling, date, location, and source-type variants?
Can I use exact phrase searching responsibly?
Can I use OR without making the query too broad?
Can I use exclusions without hiding useful evidence?
Can I search within a public domain using site:?
Can I search for public document types safely?
Can I split a complex search into a query family?
Can I record searches in a search log?
Can I explain why a search result is only a lead?
Can I convert useful sources into evidence cards?
Can I avoid unsafe query patterns?
Can I write careful no-result wording?

31. Key Takeaways

Search operators are not shortcuts around evidence discipline. They are a way to ask better questions.

The strongest search workflow is:

Question → Components → Variants → Query Family → Search Log → Source Capture → Evidence Card → Verified Finding

A good OSINT searcher is not the person who runs the most impressive query. It is the person who can explain exactly what was searched, why it was searched, what was found, what was not found, and how much confidence the evidence deserves.

Chapter 12 builds on this by looking at news, archives, cached material, and historical source handling.

Chapter 12 - News, Archives, and Cached Material

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Purpose of This Chapter

News pages, archive captures, cached snippets, press releases, public notices, and deleted or edited pages can all help an OSINT researcher understand what was publicly available at a particular point in time.

This chapter teaches the reader how to use news and archive material safely and carefully. The goal is not to dig for private information. The goal is to preserve public sources, compare versions, establish timelines, and avoid relying on rumours or disappearing web pages without evidence.

By the end of this chapter, the reader should be able to:

- distinguish current news, historical news, archived pages, cached snippets, and preserved documents;
- record publication dates, access dates, update dates, and archive capture dates;
- compare live pages against archived versions;
- avoid treating an archive capture as automatically true;
- preserve public pages responsibly;
- build a simple timeline from news and archive sources;
- recognise limitations in archived material;
- cite archived and live material clearly in a report.

This chapter is for lawful research, brand monitoring, public-interest verification, historical research, scam checking, incident support, and defensive OSINT.

It must not be used to recover private data, bypass access controls, harass people, expose vulnerable individuals, or republish sensitive personal information.

1. Why News and Archive Sources Matter

The live web changes constantly. A page may be edited, removed, moved, hidden behind a login, blocked by robots rules, or replaced with a short statement.

That means a researcher must ask four separate questions:

What does the page say now?
What did it say before?
When was each version available?
Who else independently reported the same fact?

News and archive sources help answer those questions.

Examples of useful public material include:

news articles
press releases
public statements
company announcements
court notices
public meeting minutes

- planning notices
- public procurement notices
- charity reports
- regulator announcements
- archive captures
- cached search snippets
- PDF copies
- newsletter posts
- blog updates
- social media announcements

None of these sources should be treated as perfect. A news article can be wrong. A press release can be self-serving. An archive capture may be incomplete. A search snippet may show text that no longer appears on the page. The OSINT discipline is to preserve, compare, and verify.

2. Live Page, Archive Page, Cache, and Snippet

A common mistake is mixing up different kinds of source.

Live Page

A live page is the current page visible on the web at the time of access.

Record:

- URL:
- Title:
- Publisher/owner:
- Date accessed:
- Time accessed:
- Visible publication/update date:
- Screenshot filename:
- Saved copy filename:

Archived Page

An archived page is a preserved capture of a page at a particular time. It may come from a public web archive, an organisational archive, or an internally preserved evidence copy.

Record:

- Original URL:
- Archive URL/reference:
- Archive service/source:
- Capture date:
- Capture time if available:
- Date accessed:
- What loaded correctly:
- What failed to load:

Cache

A cache is a temporary stored copy or preview held by a service. Cached pages can disappear quickly and may not preserve all content.

Record:

- Cache provider:
- Original URL:
- Cache access date:
- Visible cached date if shown:
- Screenshot filename:
- Limitations:

Snippet

A snippet is a short extract shown in search results. It can be useful as a lead, but it is weak evidence unless supported by a captured page or independent source.

Record snippets carefully:

- Search engine:
- Exact query:
- Date/time:
- Snippet text:
- Result title:

Result URL:
Follow-up capture completed? Yes/No

A snippet alone should normally be written as:

Search results suggested that...

not:

The page proved that...

3. Dates Matter More Than They Look

News and archive work depends on date discipline.

At minimum, separate these dates:

Event date: when the thing reportedly happened.
Publication date: when the source was first published.
Update date: when the source says it was changed.
Capture date: when the page was archived.
Access date: when you viewed it.
Report date: when you wrote the finding.

Example:

Event date: 3 March 2026
Publication date: 5 March 2026
Update date: 7 March 2026
Archive capture date: 8 March 2026
Access date: 10 March 2026
Report date: 11 March 2026

Those dates do different jobs. If a report says a page was published before an event, that may change the meaning. If a page was updated after an allegation appeared, the earlier archive capture may be important.

Date Log Template

Source ID:
Source title:
URL/reference:
Event date:
Publication date:
Update date:
Archive capture date:
Access date:
Researcher note:

4. Searching News Sources

News search should begin broad and then narrow.

Broad Search

"Northbank Community Workshop" news
"Northbank Community Workshop" announcement
"Northbank Community Workshop" statement

Date-Limited Search

Use search engine tools or query wording:

"Northbank Community Workshop" "March 2026"
"Northbank Community Workshop" after:2026-03-01 before:2026-04-01

Not all search engines support the same date syntax. When date precision matters, use the search engine's visible date filter and record that filter in the search log.

Source-Specific News Search

site:localnews.example "Northbank Community Workshop"
site:council.example "Northbank Community Workshop" "meeting"
site:gov.example "Northbank Community Workshop" "grant"

Phrase Variants

News sources often shorten names.

"Northbank Workshop"
"Northbank Community"
"Northbank CW"
"NCW"

Do not assume a short form is the same entity. Treat it as a lead until confirmed.

5. Archive Searching

Archive searching usually works best when the researcher already has a URL or domain.

Useful archive questions:

Did this page exist before the current version?
When did this wording first appear?
Was a claim removed or added?
Did contact details change?
Did a product, service, address, team member, or policy appear earlier?
Was a public statement edited?

Archive work is comparison work. Never rely on one capture without checking what loaded.

Archive Capture Checklist

Did the main text load?
Did images load?
Did PDFs load?
Did navigation links work?
Were scripts required?
Was the page blocked, incomplete, or redirected?
Was the timestamp visible?
Was the timezone clear?

Live-vs-Archive Comparison Table

Item checked	Live page	Archived page	Meaning	Confidence
Page title				
Main claim				
Date shown				
Contact details				
Named people				
Documents linked				

6. Preserving a Public Page

When a public page is important, preserve it early.

A safe preservation method should include:

screenshot of the visible page
saved HTML/PDF where lawful and technically possible
source URL copied exactly
date and time recorded
browser and profile recorded
notes about login/paywall/cookies
archive submission if appropriate
hash of downloaded file if used as evidence

Do not attempt to bypass paywalls, authentication, technical restrictions, or private areas. If the source requires access you do not have, record that limitation and seek lawful routes.

Page Preservation Record

Evidence ID:
Page title:
Original URL:
Preservation method:
Screenshot filename:
Saved file filename:
Archive URL/reference:
Date/time captured:
Researcher:
Limitations:

7. Comparing Edited Statements

When a statement changes, the wording matters.

Use a three-column method:

Earlier version | Later version | Analytical note

Example:

Earlier version:

"The event will take place at Northbank Hall."

Later version:

"The venue will be confirmed soon."

Analytical note:

The public venue reference appears to have been removed between the two captures. This does not prove why it was removed.

Avoid dramatic wording unless supported.

Safer language:

The wording changed between captures.

The earlier version included X.

The later version omitted X.

The available sources do not establish the reason for the change.

Unsafe language:

They covered it up.

They deleted the evidence.

They lied.

8. News Source Reliability

News sources vary. Assess them the same way as any other source.

Ask:

Who published it?

Is the author named?

Is the outlet reputable for this topic?

Does the article cite documents or named sources?

Is it original reporting or copied from another outlet?

Is it opinion, analysis, sponsored content, or straight reporting?

Has it been corrected?

Is the headline stronger than the body text?

Do independent sources support the same fact?

News Evidence Card

Evidence ID:

Headline:

Outlet:

Author:

Publication date:

Update date:

URL:

Archive URL:

Claim being used:

Source type:

Reliability assessment:

Independence check:

Limitations:

Confidence:

9. Building a Timeline From News and Archive Material

Timeline building is one of the strongest uses of news/archive work.

Use this format:

Date | Event/source | Evidence ID | Confidence | Notes

Example:

1 March 2026 | Organisation publishes event page | E001 | Medium | Live page no longer shows venue.

3 March 2026 | Archive capture shows venue listed | E002 | Medium | Capture loaded main text but not images.

5 March 2026 | Local article reports venue change | E003 | Medium | Secondary source; needs confirmation.
7 March 2026 | Official update says venue pending | E004 | High | Current official page captured.

A good timeline separates what happened from what was reported.

10. Common Mistakes

Mistake: Treating an Archive as Proof of Truth

An archive proves that a page appeared a certain way when captured. It does not prove the content itself was accurate.

Mistake: Ignoring Timezones

Archive times may be UTC or local. Record exactly what is shown.

Mistake: Forgetting Dynamic Content

Some pages rely on scripts, embedded feeds, or external images. An archive may preserve text but not the complete visual layout.

Mistake: Relying on One News Outlet

One article may repeat another. Look for independent reporting or primary documents.

Mistake: Failing to Preserve Immediately

Important public pages can change quickly. Preserve lawful sources before analysis, not after.

11. Practical Exercise

Use a fictional organisation:

Northbank Community Workshop
northbank-workshop.example

Create a mini archive/news case file:

1. Write the research question.
2. List three possible news queries.
3. List three possible archive questions.
4. Create a source log.
5. Create one evidence card for a fictional news item.
6. Create one evidence card for a fictional archived page.
7. Build a four-entry timeline.
8. Write a cautious three-sentence finding.

Example cautious finding:

The available public material suggests that the Northbank Community Workshop event page changed between 3 March and 7 March 2026.

12. Chapter Checklist

Before closing a news/archive task, confirm:

Research question written
Live page captured
Archive source checked
Dates separated
Search queries logged
News sources assessed
Independent confirmation attempted
Timeline built
Limitations recorded
Cautious wording used

Visual Brief - V19 News and Archive Timeline Board

Create a dark technical workbook graphic showing:

- a live web page panel;
- an archived capture panel;

- a news article panel;
- a timeline strip with event date, publication date, archive date, and access date;
- a caution banner: "Archive capture proves page state, not truth of the claim";
- gold/amber highlights for dates and evidence IDs.

Chapter 13 - Government, Public Records, and Registries

***Safety and lawful-use note:** This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.*

Purpose of This Chapter

Public records and official registries can be among the most useful OSINT sources, but they must be handled carefully. A public record is not always complete, current, easy to interpret, or free from error. It may also contain personal information that should not be repeated unnecessarily.

This chapter teaches the reader how to use official and registry sources responsibly. The aim is to confirm facts, identify public documents, understand official context, and avoid unsupported claims.

By the end of this chapter, the reader should be able to:

- recognise common categories of public records;
- distinguish official sources from unofficial copies;
- search registries using clear names, numbers, and dates;
- record public-record evidence correctly;
- understand limitations and jurisdiction differences;
- avoid overexposing personal information;
- combine public records with other open sources safely;
- write cautious findings from official data.

This chapter does not teach evasion, unauthorised access, impersonation, private database use, or exploitation of leaked data.

1. What Counts as a Public Record?

A public record is information made publicly accessible by an official body, court, regulator, public authority, register, or other lawful source.

Common categories include:

company registers
charity registers
planning applications
property notices
public procurement notices
court listings where public
regulator decisions
licensing registers
professional registers
public meeting minutes
parliamentary or council records
sanctions lists
public safety notices
business filings
trademark and patent databases

Not every country publishes the same material. Not every registry uses the same search rules. Not every result is current.

The first rule is:

Know the jurisdiction before interpreting the record.

2. Official Source vs Unofficial Copy

An official source is hosted by the responsible authority. An unofficial copy may be useful for discovery, but it should not be treated as the final evidence if an official version can be obtained.

Official Source Examples

government register
regulator website
official gazette
court service website
local authority portal
company registry
charity commission/register
public procurement portal
professional licensing body

Unofficial Copy Examples

commercial data broker page
third-party company profile
scraped directory
old PDF reposted by another site
news article describing a filing
search result snippet

Use unofficial copies as leads. Use official records as evidence where possible.

Source Status Field

Add this to public-record evidence cards:

Source status: Official / Unofficial copy / Secondary report / Unknown

3. Search Inputs for Registries

Many registry searches fail because the researcher starts with a vague name only.

Build a search set:

exact organisation name
previous names
trading names
registration number
charity number
company number
licence number
address fragment
postcode/ZIP code
named officer or director where lawful and relevant
date range
jurisdiction

Example Fictional Search Set

Entity: Northbank Community Workshop Ltd
Possible trading name: Northbank Workshop
Possible company number: 00000000
Town: Northbank
Country/Jurisdiction: Exampleland
Date range: 2022-2026

This structure prevents scattergun searching and reduces false matches.

4. Public-Record Evidence Card

Use a consistent template.

Evidence ID:
Registry/source name:
Official body:
Jurisdiction:
Search input used:
Result title/name:

Registration/reference number:
Document/date:
URL/reference:
Date accessed:
Screenshot/file saved:
Claim supported:
Limitations:
Personal data minimised? Yes/No
Confidence:

The most important field is **claim supported**. A registry page does not support every conclusion a researcher might want to make. It supports only the facts it actually states.

Example:

Supported: The registry lists Northbank Community Workshop Ltd as incorporated on 2 May 2024.

Not supported: The organisation is trustworthy.

5. Company and Organisation Records

Company registers can show useful public information, depending on jurisdiction.

Possible fields include:

legal name
registration number
incorporation date
registered office
company status
filing history
officers/directors
accounts or returns
charges/security interests
previous names
dissolution or insolvency notices

Interpretation caution:

A registered address may be an accountant, formation agent, serviced office, or virtual office.
A director name may match many people.
A company status may lag behind real-world events.
A filing being late may have multiple explanations.
A company being new is not proof of risk.

Use company records to establish legal facts, not character judgments.

6. Charity, Non-Profit, and Community Records

Charity and non-profit registries can show public purpose, trustees, filings, accounts, regulator notes, and status.

Useful questions:

Is the organisation registered?
What official name does it use?
What public purpose does it state?
Who are the listed responsible persons?
Are accounts or annual returns available?
Are there regulator notes or warnings?
Is the status active, removed, dissolved, or suspended?

Careful wording:

The public register lists...
The latest available filing states...
The register does not show...
No current public filing was found in the sources checked.

Avoid:

They are hiding something.
They are fake.
They are guilty.

Unless a competent official source states it, do not write it as fact.

7. Planning, Property, and Local Records

Local authority records may include planning applications, meeting minutes, public notices, environmental records, licensing applications, and enforcement notices.

Useful search inputs:

- address
- postcode/ZIP
- application number
- applicant name
- business name
- street name
- ward/district
- proposal keywords
- date range

Important caution:

Planning records often include neighbours, personal objections, addresses, signatures, and contact details. Minimise and

A defensive OSINT report usually does not need to reproduce private addresses of uninvolved individuals.

8. Court, Legal, and Regulator Sources

Court and regulator material can be high-impact and high-risk.

Rules:

- Use official sources where possible.
- Check the jurisdiction.
- Check whether the result is final, pending, appealed, stayed, withdrawn, or corrected.
- Do not treat allegations as findings.
- Do not publish personal information unnecessarily.
- Do not give legal conclusions unless qualified to do so.

Safer wording:

- The regulator published a decision dated...
- The court listing records a hearing scheduled for...
- The document states an allegation, not a finding.
- The available material does not show the outcome.

Unsafe wording:

- They broke the law.
- They are criminals.
- The case proves everything.

9. Public Record Limitations

Public records can be wrong, delayed, duplicated, incomplete, or misunderstood.

Record limitations such as:

- search only covered one jurisdiction
- name may have variants
- registry search does not support exact matching
- records may have been updated after access
- historical filings may not be digitised
- some documents require payment or formal request
- public data may be redacted
- same name may refer to different people/entities

A limitation does not make the work weak. It makes it honest.

10. Minimising Personal Data

Public does not mean harmless.

Before including personal data, ask:

- Is it relevant to the question?
- Is it necessary to prove the finding?
- Can it be summarised instead of repeated?
- Can it be redacted?

Could it expose an uninvolved person?
Could it create harassment or safety risk?

Example redaction:

Registered office: shown in evidence copy; redacted from public report.
Officer name: included only where directly relevant to official role.
Residential address: not reproduced.
Date of birth: month/year only if the official source already limits it; otherwise avoid.

11. Public Records Workflow

Use this repeatable process:

1. Define the entity and jurisdiction.
2. List official registries likely to apply.
3. Search exact names and variants.
4. Record search inputs.
5. Capture official result pages and documents.
6. Create evidence cards.
7. Compare with secondary sources.
8. Note limitations.
9. Minimise personal information.
10. Write cautious findings.

12. Practical Exercise

Fictional case:

Question: Is Northbank Community Workshop a registered organisation in Exampleland?

Create:

1. A search set.
2. A list of likely official registries.
3. A public-record evidence card.
4. A limitation note.
5. A careful finding.

Example careful finding:

The fictional Exampleland company register lists Northbank Community Workshop Ltd as an active private company under re

Visual Brief - V20 Public Registry Evidence Card

Create a dark workbook-style visual showing:

- official registry search box;
- result record with registration number;
- evidence card beside it;
- redaction strip covering unnecessary personal information;
- caution footer: "Official record supports stated facts only";
- amber highlights for jurisdiction, reference number, and access date.

Chapter 14 - Academic, Technical, and Specialist Sources

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Purpose of This Chapter

Not every useful OSINT source is a normal web page. Some of the strongest sources are found in academic databases, standards documents, patents, technical manuals, specialist directories, professional publications, public datasets, and industry reports.

This chapter teaches the reader how to locate and evaluate specialist sources without becoming overwhelmed by technical detail.

By the end of this chapter, the reader should be able to:

- identify when a specialist source is needed;
- search academic, technical, patent, standards, and sector-specific sources;
- separate expert evidence from marketing material;
- read abstracts, metadata, methods, and limitations;
- capture specialist sources in evidence cards;
- avoid misquoting or overclaiming from technical material;
- convert specialist information into plain-language findings.

This chapter is not about bypassing paywalls, obtaining restricted documents, scraping private databases, or misusing technical material for harm.

1. When Specialist Sources Are Useful

Specialist sources are useful when ordinary search results are too shallow.

Use them when the question involves:

science or medicine
engineering or technology
cybersecurity concepts
law or regulation
finance or markets
aviation, shipping, or transport
radio, telecommunications, or spectrum
company technology claims
product safety
technical standards
patents and inventions
public datasets
academic claims
specialist terminology

Example ordinary question:

Does this company really use AI to detect defects?

Specialist-source version:

What public technical, patent, academic, standards, or procurement sources support or contradict the company's claim that

2. Source Types

Academic Papers

Useful for:

- research claims
- methods
- performance comparisons
- historical development
- technical concepts
- limitations and uncertainty

Record:

- title
- authors
- journal/conference/preprint server
- publication date
- DOI or stable identifier
- abstract
- method summary
- limitations
- claim supported

Technical Standards

Useful for:

- definitions
- compliance language
- protocols
- industry practice
- safety requirements
- interoperability

Record:

- standard number
- issuing body
- version/date
- scope
- relevant clause/section
- whether access is public or restricted

Patents

Useful for:

- claimed inventions
- inventor names
- assignees
- filing dates
- priority dates
- technical descriptions
- company research direction

Caution:

- A patent does not prove a product exists.
- A patent application does not prove the invention works.
- A patent owner may not be the current commercial operator.

Public Datasets

Useful for:

- statistics
- geography
- business counts
- government performance
- public safety indicators
- research replication
- trend analysis

Record:

- dataset title
- publisher
- release date
- last updated date
- licence

geography/time range
field definitions
download filename
limitations

Specialist Directories

Useful for:

professional registrations
industry bodies
certifications
trade associations
supplier lists
conference speakers
technical committees

Caution:

Directory inclusion may be self-submitted.
Membership may have expired.
Names may be duplicated.
Some directories are marketing products, not official sources.

3. Searching Academic Sources

Academic search should start with concepts, not just names.

Example:

"AI defect detection" manufacturing inspection
"computer vision" "defect detection" "quality control"
"surface defect detection" "deep learning" review

Use variants:

artificial intelligence
machine learning
computer vision
deep learning
automated inspection
visual inspection
quality assurance
anomaly detection

Useful metadata fields:

author
institution
year
paper title
abstract
keywords
citations
funding statement
conflicts of interest

Reading an Abstract Safely

An abstract is a summary, not the full evidence.

Ask:

What exactly did the study test?
What data did it use?
Was it laboratory, simulated, or real-world?
What limitations did the authors state?
Does the paper support the claim being assessed?

4. Searching Technical Sources

Technical searches work best with exact terms.

Example:

"LoRaWAN" "regional parameters" PDF
"ADS-B" "1090 MHz" standard
"RDAP" "registration data" protocol
"ISO 27001" "statement of applicability"

Use document-type searches where appropriate:

```
filetype:pdf "technical specification" "Northbank"  
filetype:pdf "user manual" "Model ABC"  
filetype:pdf "safety data sheet" "Product Name"
```

Be careful: finding a PDF does not mean it is current or authoritative.

Record:

```
publisher  
version  
revision date  
document status  
whether superseded
```

5. Specialist Source Evidence Card

```
Evidence ID:  
Source type:  
Title:  
Author/publisher:  
Date:  
Identifier:  
URL/reference:  
Access date:  
Relevant section/page:  
Claim supported:  
Plain-language summary:  
Limitations:  
Reliability assessment:  
Confidence:
```

Plain-language summary is important. Reports should not force the reader to interpret specialist jargon unaided.

Example:

```
The paper describes a machine-learning method for detecting defects in sample images. It supports the general feasibility
```

6. Avoiding Overclaiming

Specialist sources are often misused because they look authoritative.

Overclaim

```
This academic paper proves the company product works.
```

Better

```
The paper supports the general technical plausibility of image-based defect detection. It does not independently verify
```

Overclaim

```
The patent proves they invented it.
```

Better

```
The patent application lists the claimed invention and filing history. It does not prove commercial deployment.
```

Overclaim

```
The dataset proves crime is rising in this exact street.
```

Better

```
The dataset shows reported incidents in the wider area for the recorded period. The data has reporting and categorisation
```

7. Specialist Source Reliability Questions

Ask:

```
Who produced the source?  
What expertise do they have?  
Is it peer-reviewed, official, commercial, or self-published?  
Is the source current?  
Is there a newer version?  
Does the source cite methods or data?  
Are conflicts of interest disclosed?
```


Is the source describing facts, claims, guidance, or opinion?
Can another independent source confirm the key point?

8. Handling Paywalled or Restricted Sources

Do not bypass access controls.

Safe options:

- use the abstract
- look for an open-access version
- use a library or institutional access you are entitled to use
- request the document through lawful channels
- find official summaries
- use alternative public sources
- record that full text was unavailable

Evidence wording:

Only the abstract was reviewed.
The full text was not publicly accessible during this research.
The finding is limited accordingly.

9. Specialist Sources in a Report

Use specialist material to support specific points.

Report structure:

Claim assessed:
Specialist source used:
What it supports:
What it does not support:
Limitations:
Confidence:

Example:

Claim assessed: The product uses image recognition to identify manufacturing defects.

Specialist source used: Public technical literature on computer-vision defect detection.

What it supports: The general technique is technically plausible and documented.

What it does not support: It does not verify this company's implementation, performance, customers, or deployment.

10. Practical Exercise

Fictional question:

Northbank Systems claims its handheld device detects counterfeit documents using AI. What public specialist sources could you use to verify this claim?

Build:

1. Five concept keywords.
2. Five technical phrase searches.
3. Three possible source types.
4. One specialist evidence card.
5. One cautious analytical paragraph.

Example paragraph:

Public specialist literature supports the general feasibility of automated document-image analysis. However, the sources

Visual Brief - V21 Specialist Source Evaluation Board

Create a dark technical workbook graphic showing:

- academic paper card;
- technical standard card;
- patent card;
- public dataset card;

- evidence card translating specialist detail into plain English;
- caution banner: "Plausible technique ≠ verified product";
- amber highlights for date, version, identifier, and limitation fields.

Chapter 15 - Company and Domain Research

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Purpose of This Chapter

Companies and domains leave public traces: websites, registrations, filings, press releases, public directories, certificate records, nameserver history, official pages, archived versions, job adverts, product documents, and support material.

This chapter teaches a safe, passive approach to researching companies and domains. The goal is to understand public identity and public infrastructure clues without scanning, probing, logging in, bypassing controls, or touching systems without permission.

By the end of this chapter, the reader should be able to:

- separate a legal company from a brand, website, trading name, and domain;
- collect public company and domain clues;
- understand basic domain registration concepts;
- use passive public sources such as registry data, archive captures, certificate transparency, and official website pages;
- avoid overclaiming from shared hosting, privacy services, and name matches;
- create a company/domain evidence table;
- write cautious findings.

This chapter is passive OSINT only. Do not scan, exploit, test logins, enumerate private systems, or interact with services beyond ordinary public viewing unless you have clear authorisation.

1. Company, Brand, Website, and Domain Are Different Things

A common mistake is treating a domain as the company.

Separate these entities:

Legal entity: the registered company or organisation.
Brand: the public-facing name used for marketing.
Website: the pages and content shown online.
Domain: the registered internet name.
Subdomain: a named section under a domain.
Hosting/infrastructure: systems serving the site.
People: officers, employees, authors, contacts, or named representatives.
Documents: PDFs, manuals, policies, filings, brochures.

Example:

Legal entity: Northbank Community Workshop Ltd
Brand: Northbank Workshop
Domain: northbank-workshop.example
Website title: Northbank Workshop Support
Registered office: official record
Public email: contact page

Do not merge these without evidence.

2. Company Research Questions

Start with clear questions:

What is the official legal name?
What public registration number is listed?
What brand names are used?
What official websites are linked?
What documents does the organisation publish?
What public addresses, contacts, or officers are relevant?
What historical names or domains appear?
What sources independently connect the company and the domain?

Avoid vague questions like:

Find everything about this company.

Better:

Identify public sources linking the legal entity Northbank Community Workshop Ltd to the domain northbank-workshop.example

3. Domain Basics

A domain record may include or link to:

domain name
registrar
registration date
updated date
expiry date
nameservers
registrant organisation where public
privacy/proxy service where used
RDAP/WHOIS record
DNS records
certificate transparency records
historical archive captures

Caution:

Many registrants use privacy protection.
A registrar is not the owner.
Nameservers may belong to a hosting provider.
Shared hosting can put unrelated domains on similar infrastructure.
Old records may be stale.
DNS changes do not prove ownership changes by themselves.

4. Passive Domain Research Sources

Passive means observing public information without probing or testing the target systems.

Useful passive sources include:

official website
site search results
public domain registration/RDAP pages
certificate transparency search pages
web archives
search engine cached snippets where available
public DNS lookup services
public company records
public social profiles linked from official pages
published PDFs and documents
press releases
app store listings
public support pages

Do not perform unauthorised scans, vulnerability checks, login tests, password reset checks, directory brute forcing, or exploit attempts.

5. Company-Domain Link Table

Use a structured table to avoid loose assumptions.

Claim	Source	Evidence ID	Strength	Notes
Legal entity exists	Company register	E001	High	Official registry.
Domain exists	RDAP/domain lookup	E002	Medium	Privacy service used.
Website uses brand	Live website	E003	High	Page title and footer captured.
Company links domain	Company filing/contact page	E004	High/Medium	Depends on source.
Domain links company	Website footer/legal page	E005	High/Medium	Depends on wording.
Historical link existed	Archive capture	E006	Medium	Check capture completeness.

Use strength ratings carefully:

High: official source directly states link.

Medium: public source indicates link but not official or not current.

Low: name similarity, search snippet, or indirect clue only.

6. Website Content Review

Website review should be methodical.

Capture:

- homepage
- about page
- contact page
- privacy policy
- terms page
- legal/imprint page
- press/news page
- product/service pages
- support pages
- download pages
- PDFs linked from official pages
- footer information
- metadata visible in documents

Record:

- URL
- page title
- date accessed
- visible date/version
- claim supported
- screenshot filename
- saved file filename
- archive reference if used

Do not rely only on the homepage. Important legal and identity clues often sit in footer pages, privacy policies, terms pages, PDFs, and old news posts.

7. Public Document Clues

Company websites often publish PDFs and documents.

Potential clues:

- author organisation
- publication date
- revision date
- product version
- contact email
- legal entity name
- registered number
- address
- copyright notice
- file name pattern
- metadata where visible through normal tools

Caution:

Document metadata can be wrong, inherited from templates, or created by a contractor. Treat it as a clue, not proof.

Evidence wording:

The PDF metadata/displayed footer lists...

This supports a possible connection, but requires confirmation from an official source.

8. Archive and Domain History

Archive captures can show:

- old branding
- previous contact details
- old product pages
- prior legal names
- policy changes
- historical announcements

retired documents
previous website structure

But archives may miss:

images
scripts
forms
downloads
pages blocked from crawling
private or login-only content

Write carefully:

An archived capture from [date] shows the homepage displaying...
The capture does not prove the content was accurate.
The capture appears incomplete because...

9. Certificate Transparency as a Public Clue

Certificate transparency records can show that certificates were issued for a domain or subdomain.

Use them as clues for:

historical hostnames
brand-related subdomains
service naming patterns
approximate time windows

Caution:

A certificate record does not prove a service was publicly accessible.
A subdomain name does not prove sensitive content exists.
Do not use certificate clues to target or test systems without permission.

Safe use:

The certificate log shows a certificate for support.northbank-workshop.example issued in May 2025. This supports that the

10. Company and Domain Evidence Card

Evidence ID:
Entity/domain:
Source type:
Source title:
URL/reference:
Date accessed:
Relevant field/page:
Claim supported:
Relationship type:
Strength:
Limitations:
Personal data minimised:

Relationship types:

company owns domain
company uses domain
brand uses domain
domain mentions company
third-party links company and domain
historical link only
unconfirmed similarity

11. Practical Exercise

Fictional task:

Assess whether Northbank Community Workshop Ltd is publicly linked to northbank-workshop.example.

Create:

1. An entity list.
2. A company-domain link table.
3. Three passive source types.
4. Two evidence cards.
5. One cautious finding.

Example finding:

The available public sources support a likely link between the fictional legal entity Northbank Community Workshop Ltd a

Visual Brief - V22 Company and Domain Relationship Map

Create a dark technical workbook visual showing:

- legal entity card;
- brand card;
- domain card;
- website page card;
- public record card;
- archive card;
- certificate transparency clue card;
- relationship arrows with confidence labels;
- caution banner: "Shared clue ≠ ownership proof".

Technical Note on Modern Infrastructure

1. WHOIS vs. RDAP: When conducting domain research, rely primarily on the Registration Data Access Protocol (RDAP) via secure endpoints rather than legacy Port 43 WHOIS queries. RDAP handles modern data privacy boundaries natively under current global frameworks and prevents empty data or silent timeout errors.

2. Identifiers and Shared Proxies: When tracking IP addresses, always verify the host infrastructure first. An enormous percentage of modern web presence sits behind reverse proxies and Content Delivery Networks (such as Cloudflare or AWS). Never infer an organizational link between two entities based solely on a matching infrastructure IP address, as a single proxy address can map to thousands of completely unrelated third-party web assets.

Chapter 16 - Social Platform Search Basics

***Safety and lawful-use note:** This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.*

Purpose of This Chapter

Social platforms are rich sources of public information, but they are also high-risk sources for error, privacy harm, impersonation, harassment, and false attribution.

This chapter teaches basic, safe social-platform search. The focus is public information, careful evidence handling, and avoiding overreach.

By the end of this chapter, the reader should be able to:

- search public social content responsibly;
- separate account, handle, display name, page, group, and person;
- capture public posts accurately;
- assess social-source reliability;
- recognise impersonation and parody risk;
- avoid doxxing and harassment;
- build a public social-source table;
- write cautious findings from social-platform material.

This chapter does not teach stalking, harassment, private-account access, bypassing privacy controls, fake engagement, phishing, scraping personal data, or mass account enumeration.

1. The Social Platform Problem

Social media feels immediate, but it is messy.

Problems include:

display names are not unique
handles can change
accounts can be parody, fan, abandoned, hacked, or impersonated
posts can be edited or deleted
screenshots can be fabricated
context can be missing
platform search can be incomplete
recommendation algorithms distort visibility
timezones can mislead
private individuals can be harmed by unnecessary exposure

The rule:

A social post is a source, not a conclusion.

2. Account, Person, Page, and Handle

Separate the objects:

Person: a real individual.
Account: a platform identity.
Handle: the username or URL slug.
Display name: visible name chosen by account user.
Page: brand/organisation/community presence.

Group: community space.
Post: individual item of content.
Comment/reply: attached discussion.
Profile image: visual claim or decoration.
Bio: self-description, not independent proof.

Example:

@northbankhelp is an account handle.
"Northbank Support Team" is a display name.
It is not automatically the official support team unless verified.

3. Starting With Public Platform Search

Safe social search begins with public, non-invasive methods.

Possible searches:

"Northbank Community Workshop" site:social.example
"Northbank Workshop" "official"
"northbank-workshop.example" "profile"
"Northbank" "community workshop" "support"

Search within the platform where available, but remember that platform search may omit posts, personalise results, or rank popular content over relevant content.

Use external search engines as a second route:

site:platform.example/NorthbankWorkshop
site:platform.example "Northbank Community Workshop"
site:platform.example "northbank-workshop.example"

4. Verifying Official Accounts

Official account indicators may include:

linked from the official website
listed in official documents
verified badge where meaningful
consistent branding
consistent contact links
long posting history
cross-links between official channels
matching legal or brand details
announcements mirrored on official site

Caution:

A verified badge may confirm identity type, not truthfulness.
A logo can be copied.
A link in a bio can be fake.
An account can be compromised.
An old official account can be abandoned.

Best evidence:

The official website links to the social account, and the social account links back to the official website.

Even then, record dates and capture both sides.

5. Capturing Social Evidence

Social evidence should include context.

Capture:

post URL
account URL
handle
visible display name
post text
image/video presence
timestamp as shown
platform timezone if available
date accessed
reply/quote context if relevant
engagement counts only if relevant

screenshot of full post area
screenshot of profile context if needed
archive/save method if lawful and available

Do not crop so tightly that context disappears.

Social Evidence Card

Evidence ID:
Platform:
Account handle:
Display name:
Account URL:
Post URL:
Visible timestamp:
Access date/time:
Content summary:
Claim supported:
Official status:
Reliability notes:
Privacy/redaction needed:
Confidence:

6. Handling Images and Videos on Social Platforms

Images and videos need extra caution.

Ask:

Is the media original or reposted?
Does the caption match the image?
Is there an earlier version elsewhere?
Are there visible location, language, weather, or time clues?
Could the image be old, staged, AI-generated, edited, or unrelated?

Do not identify private individuals unless necessary and lawful.

Safer wording:

The post contains an image described by the account as...
The image itself has not been independently verified.

7. Social Source Reliability

Assess the account and the content separately.

Account Assessment

creation age if visible
posting history
profile completeness
external links
cross-platform consistency
name/handle changes where visible
behaviour pattern
impersonation indicators

Content Assessment

first-hand or reposted?
linked evidence?
date and location clear?
consistent with independent sources?
emotionally manipulative language?
missing context?

A reliable account can still post wrong information. An unreliable account can still post something true. Verify the claim, not just the account.

8. Privacy and Harm Reduction

Social OSINT can easily become invasive.

Avoid:

collecting irrelevant family details

tracking private individuals across platforms without strong lawful reason
publishing home addresses or private contact details
encouraging others to contact or confront people
using personal tragedy or health information unnecessarily
misgendering, outing, or exposing sensitive attributes

Minimise:

faces of uninvolved people
children's information
private addresses
phone numbers
personal emails
medical details
relationship details

Public availability does not remove ethical responsibility.

9. Social Platform Search Table

Platform | Search query | Account/post found | Evidence ID | Link strength | Notes

Link strength examples:

High: linked from official website.
Medium: account links to official domain, but official site does not link back.
Low: similar name only.
None: no supporting link.

10. Practical Exercise

Fictional question:

Is @NorthbankWorkshopHelp an official account for Northbank Community Workshop?

Create:

1. Account/person/entity separation.
2. Three public search queries.
3. Official-account verification checklist.
4. Social evidence card.
5. Cautious finding.

Example finding:

The account @NorthbankWorkshopHelp uses the Northbank Workshop name and links to northbank-workshop.example. However, th

Visual Brief - V23 Social Account Verification Board

Create a dark workbook visual showing:

- account card;
- handle/display name/person separation;
- website cross-link check;
- post evidence card;
- privacy redaction strip;
- confidence badge;
- caution banner: "Account similarity is not identity proof".

Chapter 17 - Forums, Marketplaces, and Community Sources

***Safety and lawful-use note:** This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.*

Purpose of This Chapter

Forums, marketplaces, review sites, community boards, Q&A sites, local groups, hobby communities, and specialist message boards can reveal public context that ordinary search results miss.

They can also be noisy, biased, anonymous, commercial, outdated, or hostile.

This chapter teaches safe handling of community sources. The goal is to understand public claims, patterns, reputation signals, and context without harassment, private contact, or unauthorised access.

By the end of this chapter, the reader should be able to:

- identify relevant community-source types;
- search public forums and marketplaces responsibly;
- separate claims, reviews, adverts, and evidence;
- assess account and post reliability;
- preserve public posts with context;
- avoid interacting where observation is enough;
- reduce privacy harm;
- use community sources as leads rather than final proof.

This chapter must not be used for stalking, doxxing, scam enablement, prohibited goods sourcing, fake reviews, social engineering, or bypassing private community access controls.

1. Community Sources Defined

Community sources include:

- public forums
- Q&A sites
- local community boards
- review sites
- marketplace listings
- classified adverts
- hobby groups
- professional discussion boards
- public issue trackers
- public mailing-list archives
- comments sections
- specialist directories
- support communities

Community material is often useful because people discuss practical details not found in official sources.

But it is rarely final evidence by itself.

2. What Community Sources Can Help With

They can help identify:

- common complaints
- repeated scam patterns
- product issues
- historical usernames
- public reputation signals
- local event context
- seller behaviour
- technical support history
- known aliases or brand variants
- publicly reported timelines
- community warnings

They cannot automatically prove:

- identity
- criminality
- intent
- ownership
- truth of accusations
- safety of a seller
- accuracy of a product claim

A forum post is usually a lead requiring corroboration.

3. Search Methods

Use ordinary public search first.

Examples:

- "Northbank Workshop" forum
- "Northbank Workshop" review
- "Northbank Workshop" complaint
- "northbank-workshop.example" "forum"
- "Northbank" "marketplace" "support"

Site-specific examples:

- site:forum.example "Northbank Workshop"
- site:reviews.example "Northbank Workshop"
- site:marketplace.example "northbank-workshop.example"

Variant searches:

- "Northbank Community Workshop"
- "Northbank Workshop"
- "Northbank CW"
- "NCW support"

Avoid searches designed to uncover private contact details of individuals unless directly relevant, lawful, and necessary.

4. Reading Community Threads Properly

Never quote a single reply without thread context.

Record:

- thread title
- forum/community name
- original post date
- relevant reply dates
- usernames involved
- whether poster claims first-hand experience
- links or documents provided
- moderator notes
- edits or deleted-content markers
- thread status locked/open
- access date

Thread context matters because later replies may correct the original claim.

5. Community Evidence Card

Evidence ID:
Community/source:
Thread/listing title:
URL/reference:
Username/display name:
Post date:
Access date:
Claim made:
First-hand or second-hand:
Supporting material linked:
Contradictions in thread:
Privacy concerns:
Reliability assessment:
Confidence:

Confidence should usually be low or medium unless independently supported.

6. Marketplace Listings

Marketplace listings can show public seller claims, product descriptions, dates, images, prices, and contact channels.

Capture:

listing title
seller display name
listing URL
item description
posted/updated date
visible location area
price
images
shipping/collection terms
seller profile link if relevant
platform warning indicators

Caution:

Listings can be copied.
Images can be stolen.
Seller names can be disposable.
Locations can be approximate.
Prices can be bait.
Deleted listings may not prove wrongdoing.

Do not attempt to buy, message, provoke, test, or entrap unless you have lawful authority and a clear safety plan. For normal OSINT work, observation and preservation are enough.

7. Reviews and Reputation Signals

Reviews can be useful but unreliable.

Assess:

review date distribution
specificity of details
repeated phrases
verified-purchase indicators where meaningful
response from business
reviewer history
sudden bursts of positive or negative reviews
same complaint repeated across independent platforms

Do not treat review averages as truth. Treat them as reputation signals.

Safer wording:

Multiple public reviews allege delayed delivery between March and May 2026. The reviews are not independently verified,

8. Public Issue Trackers and Support Communities

Technical projects often leave public traces in support forums, GitHub-style issue trackers, changelogs, and discussion boards.

Useful details:

bug reports
feature requests
release dates
maintainer comments
linked documentation
known limitations
security advisories where official

Caution:

Do not turn bug details into exploitation instructions.
Do not test vulnerable systems without authorisation.
Do not publish actionable attack steps.

Use for defensive awareness, product assessment, and historical context.

9. Interaction Policy

Most OSINT should be passive.

Before interacting with a community, ask:

Is interaction necessary?
Could it alert, influence, or harm subjects?
Could it be seen as deception?
Could it break platform rules?
Could it expose the researcher or client?
Could observation alone answer the question?

Default:

Do not engage. Capture public material. Verify elsewhere.

10. Practical Exercise

Fictional task:

Assess whether public community sources mention delivery problems for Northbank Workshop products.

Create:

1. Four community search queries.
2. A forum/thread evidence card.
3. A review-pattern table.
4. A limitation note.
5. A cautious finding.

Example finding:

Public community sources reviewed contain several claims of delayed delivery for Northbank Workshop products during Apr.

Visual Brief - V24 Community Source Reliability Board

Create a dark workbook visual showing:

- forum thread panel;
- marketplace listing card;
- review pattern chart;
- evidence card;
- passive observation shield icon;
- caution banner: "Community claim = lead until verified";
- amber confidence labels.

Chapter 18 - Alerts, Monitoring, and Change Detection

Safety and lawful-use note: This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.

Purpose of This Chapter

OSINT is not always a one-time search. Sometimes the task is to monitor public sources for new information: a company filing, a domain change, a news article, a new public statement, or a page update.

This chapter teaches safe, proportionate monitoring and change detection. The goal is to track public changes without stalking, scraping aggressively, bypassing controls, or collecting unnecessary personal data.

By the end of this chapter, the reader should be able to:

- identify when monitoring is appropriate;
- build safe alert queries;
- decide what to monitor and what not to monitor;
- record alert results;
- compare page changes responsibly;
- avoid alert fatigue;
- create a monitoring register;
- write change-detection findings carefully.

This chapter is for defensive, compliance, brand, research, public-interest, and incident-support monitoring. It is not for harassment, stalking, surveillance of private individuals, platform abuse, or unauthorised automation.

1. Monitoring vs Investigation

Investigation asks:

What can we establish from available sources now?

Monitoring asks:

What changes in public sources over time?

Monitoring is useful when:

an organisation may publish updates
a regulator may release a decision
a domain or website may change
a news story is developing
a public record may receive a new filing
a scam brand may reappear under variants
a safety notice may be updated

Monitoring should have a written scope and stop date.

2. Monitoring Scope

Write a monitoring plan before setting alerts.

Monitoring objective:

Entities included:
Entities excluded:
Sources included:
Sources excluded:
Keywords:
Frequency:
Review owner:
Start date:
Stop/review date:
Escalation trigger:
Privacy controls:

Example:

Objective: Monitor public sources for official updates about Northbank Workshop product recall.
Included: official site, regulator page, major news, company register.
Excluded: personal accounts of staff, family members, private groups.
Frequency: daily review for 30 days.

3. Alert Query Building

Good alerts are specific enough to reduce noise but broad enough to catch variants.

Exact Phrase Alerts

"Northbank Community Workshop"
"Northbank Workshop"
"northbank-workshop.example"

Event-Specific Alerts

"Northbank Workshop" "recall"
"Northbank Workshop" "statement"
"Northbank Workshop" "regulator"

Exclusion Alerts

"Northbank Workshop" -fictional -unrelated

Source-Specific Alerts

site:regulator.example "Northbank Workshop"
site:northbank-workshop.example "recall"

Not every alert service supports every operator. Test queries manually first and record the alert system used.

4. Monitoring Register

Monitor ID:
Objective:
Query/source:
Tool/service:
Frequency:
Start date:
Review/stop date:
Owner:
Last checked:
Result count:
Useful results:
False positives:
Action taken:
Privacy notes:

This prevents uncontrolled alert sprawl.

5. Page Change Detection

Change detection compares a page now against an earlier copy.

Track:

page title
URL
text added
text removed
documents added/removed
contact details changed

- policy version changed
- visible publication/update date
- layout or navigation changes
- redirects
- errors or downtime

Change does not automatically imply wrongdoing.

Safe wording:

The page changed between the capture on 4 May and the capture on 9 May. The later version removes the phrase "independence".

6. Alert Result Triage

Every alert result should be triaged.

- Relevant: directly supports monitoring objective.
- Related: possibly useful context.
- Duplicate: already captured.
- False positive: same words, different entity.
- Sensitive: contains personal data; minimise or redact.
- Escalate: meets defined trigger.

Alert Triage Table

Date	Alert/query	Result	Category	Evidence ID	Action
------	-------------	--------	----------	-------------	--------

7. Avoiding Alert Fatigue

Too many alerts make monitoring useless.

Reduce noise by:

- using exact phrases
- excluding common false positives
- separating high-priority official sources from broad web alerts
- reviewing queries weekly
- turning off alerts when the task ends
- recording false-positive patterns
- creating digest reviews instead of constant interruptions

An alert system should support the researcher, not become the investigation.

8. Privacy and Monitoring

Monitoring can easily become surveillance.

Avoid monitoring:

- private individuals without strong lawful reason
- family members of a subject
- children or vulnerable people
- personal accounts irrelevant to the question
- private groups or restricted spaces
- sensitive attributes or health information

Prefer monitoring:

- official websites
- public registries
- regulators
- news sources
- brand/domain mentions
- public safety notices
- public company filings

Use minimisation by default.

9. Change Evidence Card

Evidence ID:
Page/source monitored:
Original URL:
Earlier capture/reference:
Later capture/reference:
Change observed:
Date range:
Claim supported:
Possible explanations:
Limitations:
Privacy notes:
Confidence:

Always include possible explanations. Changes happen for many normal reasons.

10. Practical Exercise

Fictional task:

Monitor public sources for updates about a Northbank Workshop safety notice for 30 days.

Create:

1. Monitoring scope.
2. Five alert queries.
3. Monitoring register.
4. Alert triage table.
5. Change evidence card.
6. Cautious update paragraph.

Example paragraph:

Monitoring of public official sources identified one update to the fictional Northbank Workshop safety notice between 1

Visual Brief - V25 Monitoring and Change Detection Dashboard

Create a dark workbook-style dashboard showing:

- monitoring scope panel;
- alert query list;
- source watchlist;
- change comparison panel;
- triage table;
- stop/review date marker;
- caution banner: "Monitor public sources, not private lives".

Chapter 19 - Building Source Lists

***Safety and lawful-use note:** This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.*

Purpose of This Chapter

A good OSINT researcher does not simply search the web at random. They build source lists: structured collections of trusted, relevant, repeatable sources for particular tasks.

This chapter teaches the reader how to build, maintain, and use source lists without becoming dependent on tools or outdated bookmarks.

By the end of this chapter, the reader should be able to:

- build a source list for a research question;
- categorise sources by type, jurisdiction, reliability, and use case;
- record limitations and access notes;
- maintain source lists over time;
- avoid tool worship;
- separate discovery sources from evidence sources;
- create a source-list card for future work.

This chapter is about lawful, open sources. Do not add leaked databases, credential dumps, private data brokers, restricted systems, or unauthorised sources to a normal OSINT source list.

1. What a Source List Is

A source list is a controlled list of places to look.

It may include:

search engines
official registries
government portals
regulators
archive services
news sources
specialist databases
company records
mapping sources
social platforms
community sources
technical references
public datasets

A source list is not just bookmarks. It includes the reason each source is useful and its limitations.

2. Discovery Source vs Evidence Source

Separate sources into two roles.

Discovery Source

A discovery source helps find leads.

Examples:

- search engine
- community thread
- third-party directory
- social search
- news aggregator
- old bookmark list

Evidence Source

An evidence source supports a finding.

Examples:

- official registry
- captured webpage
- primary document
- official announcement
- regulator decision
- public filing
- archived page with clear timestamp

A discovery source can become evidence only if it is reliable enough and properly captured.

3. Source List Fields

Use a table like this:

- Source name:
- URL/reference:
- Source type:
- Jurisdiction/coverage:
- Best used for:
- Reliability level:
- Access requirements:
- Cost/free:
- Update frequency:
- Search tips:
- Limitations:
- Privacy concerns:
- Last checked:
- Owner/notes:

Example:

- Source name: Exampleland Company Register
- Source type: Official registry
- Jurisdiction: Exampleland
- Best used for: legal entity names, status, filings
- Reliability: high for registry facts
- Limitations: may not show trading activity or beneficial ownership
- Last checked: 7 June 2026

4. Source Categories

Common categories:

- General search
- News and archives
- Official records
- Company and charity registers
- Domain and website sources
- Academic/technical sources
- Social platforms
- Community and marketplace sources
- Maps and imagery
- Media verification
- Public datasets
- Monitoring and alerts
- Reporting and preservation tools

Each category should include no more than the useful sources needed for the work. A list of 500 unused tools is less valuable than 30 tested sources with notes.

5. Reliability Ratings

Use simple ratings:

High: official/primary source for the specific fact.
Medium: reputable secondary source or reliable specialist source.
Low: user-generated, unofficial, incomplete, or unverified.
Lead-only: useful for discovery but not evidence without confirmation.
Unknown: not yet assessed.

Reliability is tied to the claim.

Example:

A company register is high reliability for incorporation date.
It is not high reliability for whether the company provides good customer service.

6. Access, Cost, and Terms

Record whether the source is:

free
paid
account required
API-based
rate-limited
geographically restricted
requires permission
licensed for reuse
contains personal data
restricted by terms of service

Do not assume that technically accessible means permitted for your use.

7. Maintaining Source Lists

Sources change.

Review source lists periodically:

Does the URL still work?
Has the search interface changed?
Have terms or access requirements changed?
Is the source still authoritative?
Is there a new official source?
Are old notes misleading?
Are privacy risks higher than before?
Should the source be retired?

Add review dates:

Last checked:
Next review:
Change notes:

8. Avoiding Tool Worship

A tool is not a method.

Bad workflow:

Open favourite tool.
Paste name.
Believe output.

Good workflow:

Define question.
Choose source types.
Use tools only where appropriate.
Capture sources.
Verify independently.
Record limitations.

Tools can disappear, change pricing, produce false matches, or hide methodology. The researcher remains responsible.

9. Building a Source List for a Case

For each case, create a focused list.

Example case:

Question: Is Northbank Community Workshop publicly linked to a product recall?

Source list:

official website
web archive
regulator safety notice page
company register
news search
review/community sources
alert query

Each source has a purpose. If a source has no purpose, remove it.

10. Source List Quality Checklist

Question linked to source list
Official sources identified
Discovery sources separated from evidence sources
Jurisdiction recorded
Limitations recorded
Access rules recorded
Privacy risk noted
Last checked date included
Redundant sources removed
Review date set

11. Practical Exercise

Fictional task:

Build a source list for researching public claims about Northbank Workshop's safety notice.

Create:

1. Ten sources maximum.
2. Source category for each.
3. Best-used-for field.
4. Reliability rating.
5. Limitation note.
6. Review date.

Example finding about the source list:

The source list prioritises official and primary sources first, then uses news, archive, and community material for discovery.

Visual Brief - V26 Source List Matrix

Create a dark workbook visual showing:

- rows of source categories;
- columns for purpose, reliability, jurisdiction, limitations, and review date;
- separate colour labels for discovery source and evidence source;
- caution banner: "Tools do not replace method".

Chapter 20 - Search Workflow Case Study

***Safety and lawful-use note:** This chapter is for lawful, defensive, educational, journalistic, verification, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose. This guide is not legal advice; when a matter is sensitive, regulated, or potentially criminal, seek proper legal or professional guidance.*

Purpose of This Chapter

This chapter closes Volume 2 by combining search operators, news and archives, public records, specialist sources, company/domain research, social-platform checks, community sources, alerts, and source lists into one complete workflow.

The case study is fictional and safe. It is designed to teach method, not target real people or organisations.

By the end of this chapter, the reader should be able to:

- turn a broad concern into a defined research question;
- build a source list;
- run staged searches;
- capture sources into evidence cards;
- compare official, news, archive, social, and community sources;
- handle contradictions;
- create a timeline;
- write a careful search workflow report;
- identify what remains unknown.

1. Fictional Case Scenario

A fictional local organisation called **Northbank Community Workshop** has published a notice about a product named **SafeLamp Mini**. Several public comments claim that the notice is linked to a safety recall, but the official website uses cautious wording.

The task is not to prove wrongdoing. The task is to establish what public sources show.

Initial Question

What do public sources show about Northbank Community Workshop, the SafeLamp Mini notice, and any official safety-related information?

Scope

Included:

official website
archived versions of official pages
public company/organisation records
public regulator pages
news sources
public social accounts only where official status can be assessed
public community/review sources as leads
alerts for future public updates

Excluded:

private individuals
staff family members
private groups
login-only content
password reset testing

contacting subjects
technical probing of websites
unverified personal details

2. Source List

Source	Type	Purpose	Reliability	Notes
Official website	Primary/official	Current notice and statements	High for its own statements	Capture current page
Web archive	Archive	Compare earlier versions	Medium	Check capture completeness.
Company register	Official registry	Legal identity	High for registry facts	Does not prove product facts.
Regulator page	Official	Safety notices	High if direct match	Search exact product name and company variants.
News search	Secondary	Public reporting	Medium	Verify with primary sources.
Social platform search	Public social	Official account/public statements	Variable	Confirm official status.
Community/review sources	User-generated	Complaints/patterns/leads	Low/lead-only	Require corroboration.
Alert service	Monitoring	Future updates	N/A	Log queries and review date.

3. Search Plan

Stage 1 - Identity and Official Source

"Northbank Community Workshop"
"Northbank Community Workshop" "SafeLamp Mini"
site:northbank-workshop.example "SafeLamp Mini"
site:northbank-workshop.example "safety"
site:northbank-workshop.example "recall"

Goal:

Find the current official wording and capture it.

Stage 2 - Archive Comparison

Original URL of notice in public web archive
Domain captures around date notice appeared
Archived homepage around announcement date

Goal:

Identify whether wording changed and when.

Stage 3 - Official Records and Regulators

"SafeLamp Mini" site:regulator.example
"Northbank Workshop" site:regulator.example
"Northbank Community Workshop" "safety notice"

Goal:

Find official safety or regulatory sources, if any.

Stage 4 - News and Public Commentary

"SafeLamp Mini" "Northbank"
"Northbank Workshop" "SafeLamp Mini" "recall"
"Northbank Workshop" "SafeLamp" "warning"

Goal:

Find public reporting and compare it with official sources.

Stage 5 - Social and Community Leads

"SafeLamp Mini" "review"
"SafeLamp Mini" "problem"
"Northbank Workshop" "SafeLamp" forum
"northbank-workshop.example" "SafeLamp"

Goal:

Identify public lead patterns without treating them as proof.

4. Evidence Cards

Evidence Card E001 - Current Official Notice

Evidence ID: E001
Source type: Official website
Title: SafeLamp Mini customer notice
URL/reference: northbank-workshop.example/safelamp-notice
Access date: 7 June 2026
Claim supported: The official site published a customer notice about SafeLamp Mini.
Reliability: High for the organisation's current public wording.
Limitations: Does not independently verify product safety status.
Confidence: High for page existence and wording.

Evidence Card E002 - Archived Earlier Notice

Evidence ID: E002
Source type: Web archive
Original URL: northbank-workshop.example/safelamp-notice
Archive capture date: 4 June 2026
Access date: 7 June 2026
Claim supported: Earlier captured wording included "pause use until further update".
Reliability: Medium; capture appears to load main text.
Limitations: Archive capture does not prove accuracy of the claim.
Confidence: Medium.

Evidence Card E003 - Regulator Search

Evidence ID: E003
Source type: Official regulator search
Search inputs: "SafeLamp Mini", "Northbank Workshop", "Northbank Community Workshop"
Access date: 7 June 2026
Claim supported: No matching regulator notice was found in the fictional regulator source checked.
Reliability: Medium to high for that source checked.
Limitations: Search may miss variants; other jurisdictions not checked.
Confidence: Medium.

Evidence Card E004 - Community Review Pattern

Evidence ID: E004
Source type: Community/review sources
Claim observed: Several users report overheating concerns.
Access date: 7 June 2026
Claim supported: Public user-generated claims exist.
Reliability: Low/lead-only.
Limitations: Claims are unverified and may not refer to the same product batch.
Confidence: Low for factual safety claim; medium for existence of public complaints.

5. Timeline

Date	Source/Event	Evidence ID	Confidence	Notes
1 June 2026	Official product page live with normal sales wording	E000	Medium	Historical capture assumed for existence
4 June 2026	Archive capture includes "pause use until further update"	E002	Medium	Archive loaded main text.
6 June 2026	Current official page uses "customer notice" wording	E001	High	Captured live page.
7 June 2026	Regulator search finds no direct match in checked source	E003	Medium	Variants and other jurisdictions not checked.
7 June 2026	Community sources contain overheating claims	E004	Low/lead-only	User-generated claims.

6. Contradictions and Alternatives

Observed issue:

Community posts call it a recall, but the official page says customer notice.

Possible explanations:

- The organisation may be using cautious wording before a formal recall.
- Users may be exaggerating or misunderstanding the notice.
- A regulator notice may exist under a different product or company name.
- The issue may affect only some batches.
- The community posts may be unrelated or inaccurate.
- The official page may have changed wording.

A good report lists alternatives rather than forcing one story.

7. Draft Finding

Public sources reviewed show that the fictional Northbank Community Workshop published a SafeLamp Mini customer notice

8. Limitations

Only public sources were reviewed.
No private, login-only, or restricted systems were accessed.
Only the listed fictional regulator source was searched.
Community claims were not independently verified.
Archive captures may be incomplete.
The official page may change after the report date.
The product name may have variants not searched.

Limitations keep the report honest and defensible.

9. Monitoring Plan

Objective: Monitor public sources for updates about SafeLamp Mini.
Duration: 30 days.
Sources: official website, regulator page, news search, archive capture, public alert queries.
Frequency: daily official-source check, weekly community-source review.
Stop date: 7 July 2026.
Escalation trigger: official regulator notice, formal recall wording, new official safety instruction.
Privacy rule: do not collect personal details from reviewers unless directly necessary, and redact by default.

Alert queries:

"SafeLamp Mini"
"SafeLamp Mini" "recall"
"SafeLamp Mini" "Northbank"
"Northbank Workshop" "customer notice"
site:northbank-workshop.example "SafeLamp Mini"

10. Final Report Skeleton

Title: Public-source review of Northbank Workshop SafeLamp Mini notice
Date:
Researcher:
Question:
Scope:
Sources checked:
Method:
Findings:
Evidence table:
Timeline:
Contradictions and alternatives:
Limitations:
Monitoring recommendation:
Appendix:

11. End-of-Volume Checklist

A Volume 2 reader should now be able to:

build search queries
use operators safely
search news and archives
separate public records from unofficial copies
use specialist sources carefully
research companies and domains passively
check public social sources without overclaiming
handle forums and marketplaces as lead sources
set proportionate alerts
build source lists
complete a structured search workflow case study

Visual Brief - V27 Complete Search Workflow Case Board

Create a dark technical case-board graphic showing:

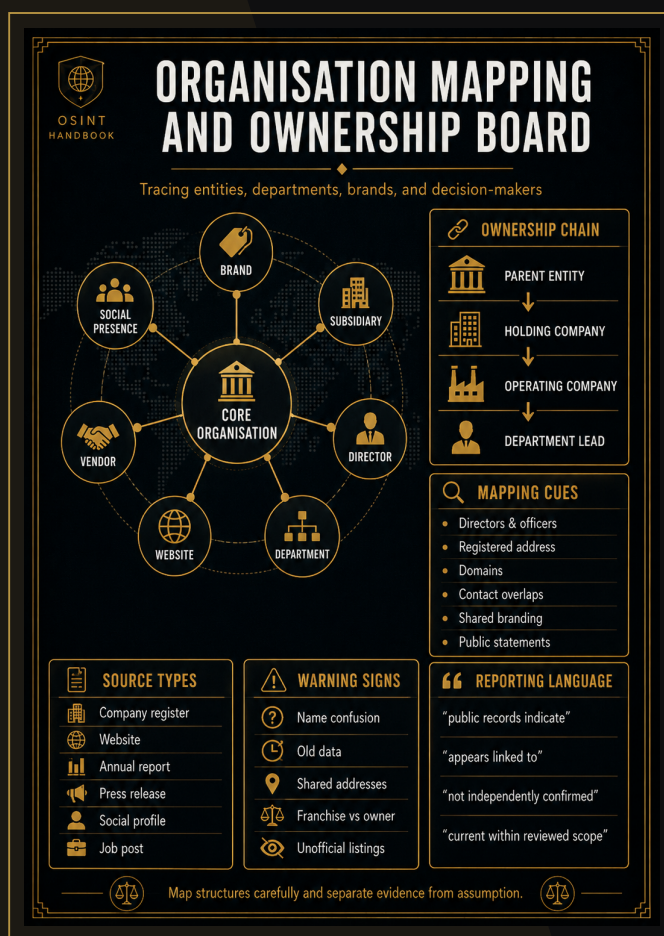
- research question at the top;
- source list column;
- query plan column;

VOLUME THREE

People, Companies, and Communities

Careful entity research, organisation mapping, reputation checks, and identity ambiguity.

CHAPTERS 21-30



Chapter 21 - Person-of-Interest Research, Safely and Lawfully

***Safety and lawful-use note:** This chapter is written for defensive, educational, journalistic, compliance, anti-fraud, and public-interest research. It does not authorise harassment, stalking, doxxing, impersonation, credential attacks, private-account access, bypassing restrictions, or collecting more personal data than is necessary for a legitimate purpose.*

Purpose of This Chapter

Person-of-interest research is one of the most sensitive areas of OSINT because it often involves living people, their names, their public posts, their employers, their family links, their locations, and their routines. The goal of this chapter is to teach a safe framework that protects the investigator, the subject, and anyone else named in the material.

This chapter does **not** teach stalking, intimidation, doxxing, social engineering, credential testing, or private-account access. It teaches how to decide whether research should be done at all, how to define a narrow purpose, how to collect only what is necessary, and how to write findings without turning leads into accusations.

By the end of this chapter, the reader should be able to:

- define a legitimate research purpose;
- decide whether a person should be researched or excluded;
- separate public-interest research from curiosity;
- apply consent, necessity, proportionality, and minimisation;
- avoid harmful collection of sensitive personal data;
- build a person-of-interest research plan;
- create cautious findings with confidence levels;
- stop when the work becomes unnecessary, unsafe, or intrusive.

1. What “Person of Interest” Means Here

In this guide, a person of interest is not a criminal label. It simply means a person whose public footprint may be relevant to a defined research question.

Examples of legitimate contexts may include:

verifying whether a public spokesperson is connected to a company;
checking whether a public scam warning names a real public-facing operator;
confirming whether a named officer appears on an official business register;
reviewing public professional claims made by a service provider;
assisting a person to understand and reduce their own public digital footprint;
researching a public figure within a clear public-interest boundary.

Examples that should be excluded:

researching someone out of curiosity;
collecting home addresses or family details without a necessary reason;
tracking a private person's movements;
trying to identify anonymous users for retaliation;
building a dossier for harassment or embarrassment;
attempting to access private messages, restricted groups, accounts, or passwords.

The central test is simple:

Can I clearly explain why this research is necessary, lawful, proportionate, and safe?

If the answer is no, stop.

2. Start With a Written Purpose

Never begin person research by searching a name. Begin by writing the research purpose.

Poor purpose:

Find out everything about Alex.

Safe purpose:

Establish whether the public-facing LinkedIn profile using the name Alex Morgan is connected to the registered company I

A safe purpose includes:

subject or entity;
public relevance;
specific question;
sources allowed;
sources excluded;
output needed;
stop condition.

Purpose Card

Case ID:
Research question:
Legitimate reason:
Subject type: private person / professional role / public figure / company officer / unknown
Allowed sources:
Excluded sources:
Sensitive data risk:
Expected output:
Stop condition:
Reviewer:

3. The Necessity and Proportionality Test

Person research should pass four checks.

1. Lawful and legitimate

There must be a legitimate reason for collecting or recording personal information. In UK contexts, the ICO explains that organisations handling personal data need a lawful basis and must process personal data lawfully, fairly, and transparently. For independent learners, the same concept is a useful safety discipline: do not collect personal information merely because it is accessible.

2. Necessary

Only collect information that answers the research question.

Question: Is this person a director of a company?
Relevant: official company register entry.
Irrelevant: family photos, school history, personal relationship status.

3. Proportionate

The more private or sensitive the information is, the stronger the justification must be. A public professional profile is different from a private family post. A company director listing is different from a home address found in an old document.

4. Minimised

Keep the smallest useful amount of information. A report rarely needs every source. It needs enough high-quality evidence to support the finding.

4. Subject Categories

Different subject types require different caution.

Subject Type | Examples | Research Caution
Private individual | neighbour, customer, local resident | Highest caution; avoid unless consent or strong lawful basis
Professional role | company officer, spokesperson, service provider | Limit to role-relevant public material
Public figure | elected official, senior executive, media figure | Public-interest scope only; avoid family/private life

Unknown account | username, avatar, forum identity | Do not claim real identity without strong corroboration
Organisation-linked person | director, trustee, employee in public role | Use official and professional sources first
Victim/witness/minor | vulnerable person, child, abuse victim | Avoid collection unless legally authorised and safety-co

The rule is: **the more vulnerable or private the person, the narrower the research must be.**

5. Build a Person Research Plan

A safe plan prevents wandering.

1. Define the question.
2. Identify the subject category.
3. List allowed source types.
4. List excluded source types.
5. Decide what counts as sufficient evidence.
6. Decide what must be redacted.
7. Decide when to stop.

Example Safe Plan

Question:

Does the public profile “Jordan Vale – Operations Director” correspond to the director named Jordan Vale on the official

Allowed:

- official company register;
- company website staff page;
- public professional profile;
- archived official company pages;
- public press releases.

Excluded:

- family profiles;
- private social accounts;
- home address research;
- password reset checks;
- contacting the subject;
- speculative identity claims.

Sufficient evidence:

Two independent public sources, one of which must be official or directly controlled by the company.

6. Sensitive Data Warning

Avoid collecting or repeating sensitive personal data unless the research is legally authorised and strictly necessary.

Sensitive categories may include:

health information;
children and family details;
precise home location;
religion or belief;
political views;
trade union involvement;
sexual orientation;
race or ethnicity;
criminal allegations;
financial hardship;
biometric or identity documents.

Even if a person has posted something publicly, that does not automatically make it fair, necessary, or safe to reproduce in your own report.

7. Evidence Collection Rules

When person research is justified, use the same evidence discipline as earlier chapters, but with stronger redaction.

For each item, capture:

source title;
source type;
URL or reference;
date and time captured;
what the source directly shows;
what it does not show;
relevance to the research question;
confidence level;

redaction needed;
retention decision.

Direct Observation vs Interpretation

Direct observation:

The public company register lists Jordan Vale as an active director of Vale Workshop Ltd.

Interpretation:

This supports, but does not by itself prove, that the professional profile using the same name belongs to the same person.

Unsafe leap:

Jordan Vale is definitely the same person and is hiding something.

8. Stop Points

Stop the research immediately when:

the question has been answered;
the remaining sources are intrusive rather than useful;
the work drifts into private life;
you find vulnerability or safeguarding concerns;
you are tempted to contact friends, family, employers, or associates;
you would be embarrassed to explain the research purpose to a reviewer;
you cannot clearly justify retention of the material.

A disciplined investigator does not collect more because it is available. They collect what is needed and stop.

9. Safe Reporting Language

Avoid labels and accusations.

Use:

Public sources reviewed indicate...
The sources support a possible link between...
The available evidence does not establish...
This finding is assessed as low / medium / high confidence because...
No conclusion should be drawn about private conduct.

Avoid:

This proves they are guilty.
They are definitely behind it.
They are hiding something.
Everyone connected to them is suspicious.

10. Exercise - Safe Person Research Plan

Create a plan for a fictional case.

Scenario:

A community group received a public email from someone claiming to represent Northbank Events Ltd. The group wants to verify the claim.

Complete:

Research question:
Legitimate purpose:
Subject category:
Allowed sources:
Excluded sources:
Sensitive data risks:
Evidence threshold:
Stop condition:
Report wording:

Key Takeaways

- Person research starts with a lawful, necessary, proportionate purpose.
- Public availability does not remove privacy, fairness, or harm considerations.

- Always separate observation from interpretation.
- Avoid sensitive data unless strictly authorised and necessary.
- Stop when the question is answered.
- Write findings cautiously and redact unnecessary personal information.

Visual Brief

V28. Person research safety gate

A dark technical flowchart showing: purpose → lawful/legitimate check → necessity → proportionality → minimisation → allowed sources → evidence threshold → redaction → stop/report. Add warning side-panel: “Do not collect private-life detail just because it is visible.”

Official Reference Points

Use these as boundary markers when designing or reviewing real work:

- ICO - lawful basis for processing personal data:
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>
- ICO - data protection principles: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>
- NCSC - social media safety and digital footprint guidance:
<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- GOV.UK / Companies House - company information service: <https://www.gov.uk/get-information-about-a-company>
- ICANN - RDAP information for registration data: <https://www.icann.org/rdap>
- GOV.UK - reporting suspicious emails, websites, phishing and fraud:
<https://www.gov.uk/report-suspicious-emails-websites-phishing>

Chapter 22 - Username and Profile Correlation

Safety and lawful-use note: This chapter is written for defensive, educational, journalistic, compliance, anti-fraud, and public-interest research. It does not authorise harassment, stalking, doxxing, impersonation, credential attacks, private-account access, bypassing restrictions, or collecting more personal data than is necessary for a legitimate purpose.

Purpose of This Chapter

Username and public profiles can be useful clues, but they are also one of the easiest ways to make false matches. Many people share the same handle. One person may use different handles. A username may be copied, spoofed, abandoned, parody-based, or randomly generated. This chapter teaches a careful correlation method that treats usernames as clues, not proof.

By the end of this chapter, the reader should be able to:

- record usernames and profile clues cleanly;
- compare public profiles without overclaiming;
- distinguish weak, medium, and strong correlation indicators;
- handle reused handles safely;
- avoid identity accusations;
- produce an attribution matrix.

1. Username Correlation Is Not Identification

A username can suggest a link, but it rarely proves identity by itself.

Weak claim:

The same username appears on two sites.

Unsafe claim:

Therefore the accounts are definitely the same person.

Better analytical wording:

The same distinctive username appears on two public profiles. This is a weak-to-medium correlation indicator and requires further investigation.

Correlation means “these items may be connected.” Identification means “this account belongs to this person.” They are not the same thing.

2. Profile Clue Categories

When reviewing public profiles, collect only role-relevant, non-intrusive clues.

Clue Type | Examples | Risk Level | Notes

Handle | aldermere_ops, jvale_radio | Low to medium | Common handles are weak; distinctive handles are stronger

Display name | Jordan V, J. Vale | Medium | Names alone are weak

Avatar | logo, face, cartoon | Medium to high | Do not use face matches casually

Bio text | “Director at...” | Medium | Capture exact wording and date

Links | website, portfolio, official company page | Medium | Stronger when controlled by same entity

Dates | joined, post dates | Low | Useful for timeline only

Location text | city/region | Medium | Avoid precise private locations

Cross-posted content | same announcement on multiple profiles | Medium to high | Strong if timestamped and official

Contacts | public business email | Medium | Avoid private phone/home details

Do not collect friends, family, followers, children, private interests, or political/health data unless there is a strict and lawful need.

3. The Correlation Matrix

Use a matrix to keep the analysis disciplined.

Profile A:
Platform:
URL/reference:
Capture date:
Visible handle:
Visible display name:
Visible links:
Visible organisation claims:
Relevant public posts:
Private/sensitive data excluded:

Profile B:
Platform:
URL/reference:
Capture date:
Visible handle:
Visible display name:
Visible links:
Visible organisation claims:
Relevant public posts:
Private/sensitive data excluded:

Correlation indicators:
- same handle:
- same display name:
- same avatar/logo:
- same external link:
- same public email/domain:
- same posting pattern:
- same organisation reference:
- same writing style:
- contradictory details:

Assessment:
Weak / Medium / Strong / Not enough evidence
Reason:

4. Weak, Medium, and Strong Indicators

Weak Indicators

same first name;
same common username;
similar avatar style;
same general location;
similar interests;
similar posting times;
matching but common phrases.

Weak indicators are leads only.

Medium Indicators

distinctive username reused across platforms;
same public portfolio link;
same organisation named in bios;
same public profile photo used for a professional purpose;
similar public project descriptions;
matching role and location at the same time.

Medium indicators support further checking.

Strong Indicators

one profile links directly to the other;
a verified/company-controlled page links to the profile;
the same controlled domain email appears publicly;
public press release names the profile holder and links the account;
official organisation page confirms the person/account relationship;
archived official page supports the same connection.

Even strong indicators should be described carefully and sourced.

5. Distinctiveness Matters

A handle like johnsmith1984 is not strong. A handle like northbank_safelamp_dev may be stronger if it appears with the same project, links, and dates.

Ask:

- Is the handle common?
- Could another person plausibly use it?
- Does it appear on unrelated accounts?
- Is it connected to a controlled website or organisation?
- Are there contradictions?

6. Contradictions Are Evidence Too

Do not ignore mismatches.

- Profile A claims London.
- Profile B claims Glasgow.
- Profile A links to northbank.example.
- Profile B links to a different unrelated business.
- Profile A was active in 2021.
- Profile B only appeared in 2026.
- Profile A uses a professional tone.
- Profile B is a parody account.

A contradiction may mean:

- same person with changed details;
- different people;
- impersonation;
- fan/parody/repost account;
- old abandoned account;
- mistaken source;
- platform metadata error.

Record contradictions rather than forcing a match.

7. Handling Profile Images

Profile images are sensitive. Do not use them to identify private people without a strong lawful basis.

Safer uses:

- noting that a public company logo appears on two company-controlled pages;
- noting that a product image is reused in public listings;
- noting that an official speaker headshot appears on an official event page.

Risky uses:

- trying to identify a private person from a face;
- matching family photos;
- collecting images of children;
- using appearance as proof of identity;
- publishing unredacted face images unnecessarily.

When in doubt, describe the image generally and redact it from the working report.

8. Safe Workflow

1. Start from the research question.
2. Record the known public handle/profile.
3. Capture the source as evidence.
4. Search only within allowed public sources.
5. Add possible matches to the matrix.
6. Score indicators as weak, medium, or strong.
7. Record contradictions.
8. Seek independent confirmation from official or controlled sources.
9. Write a cautious assessment.
10. Redact personal details not needed for the report.

9. Example Assessment

Finding:

The public profile @northbank_workshop and the website northbank-workshop.example appear linked.

Evidence:

- The website footer links to @northbank_workshop.
- The profile bio links back to the same website.
- Both sources use the same organisation name and project description.

Confidence:

High that the profile is connected to the organisation.

Limitations:

This does not identify the individual operating the account. No private account or personal identity conclusion is made.

10. Exercise - Username Correlation Matrix

Use a fictional handle:

@ValeSafetyNotes

Create a matrix comparing three public profiles:

Profile 1: company blog author page
Profile 2: public professional profile
Profile 3: public forum account

Decide:

Which indicators are weak?
Which are medium?
Which are strong?
What contradictions exist?
What should not be collected?
What wording belongs in the final report?

Key Takeaways

- A username is a clue, not proof.
- Correlation and identification are different findings.
- Strongest indicators come from controlled links, official pages, and direct cross-references.
- Contradictions must be recorded.
- Avoid collecting private-life and sensitive data.
- Reports should state what the sources support, not what the investigator suspects.

Visual Brief

V29. Username correlation matrix

A dark workbook-style matrix with columns for profile A, profile B, shared indicators, contradictions, confidence, and redaction needed. Include a warning banner: “Same handle ≠ same person.”

Official Reference Points

Use these as boundary markers when designing or reviewing real work:

- ICO - lawful basis for processing personal data:
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>
- ICO - data protection principles: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>
- NCSC - social media safety and digital footprint guidance:
<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- GOV.UK / Companies House - company information service: <https://www.gov.uk/get-information-about-a-company>

- ICANN - RDAP information for registration data: <https://www.icann.org/rdap>
- GOV.UK - reporting suspicious emails, websites, phishing and fraud:
<https://www.gov.uk/report-suspicious-emails-websites-phishing>

Chapter 23 - Email and Contact Clue Analysis

Safety and lawful-use note: This chapter is written for defensive, educational, journalistic, compliance, anti-fraud, and public-interest research. It does not authorise harassment, stalking, doxxing, impersonation, credential attacks, private-account access, bypassing restrictions, or collecting more personal data than is necessary for a legitimate purpose.

Purpose of This Chapter

Email addresses, contact forms, phone numbers, and public business contact details can help connect organisations, domains, projects, and public claims. They can also expose private people to harm if handled carelessly. This chapter teaches contact-clue analysis for defensive verification, anti-fraud review, and public-source research without intrusive testing or account enumeration.

This chapter does not teach password reset probing, account existence testing, spam, phishing, social engineering, SIM-swap research, harassment, or scraping personal contact lists.

By the end of this chapter, the reader should be able to:

- distinguish public business contacts from private personal contacts;
- record contact clues safely;
- connect contact details to domains, companies, and official pages;
- avoid dangerous account-enumeration behaviour;
- assess contact clues as evidence;
- redact contact data in reports.

1. What Counts as a Contact Clue?

A contact clue is any public item that may connect a person, organisation, profile, or domain.

business email address;
public role email;
website contact form;
public phone number;
registered office contact channel;
support inbox;
sales inbox;
press contact;
public profile contact link;
newsletter sender address;
public document footer;
WHOIS/RDAP registration contact where visible;
company filing contact details where legally published.

Not all contact clues should be collected. A public business email may be relevant. A private phone number on an old cached page may not be fair or necessary.

2. Public, Semi-Public, and Private Contacts

Category	Examples	Handling
Public business	support@example.com, press@example.com	Usually safe if relevant
Public role	named director email on official page	Use only if role-relevant
Semi-public	event attendee list, old PDF contact sheet	Assess necessity and harm
Private	home phone, personal email, family contact	Exclude unless legally authorised and essential
Sensitive	child, victim, medical, safeguarding contact	Avoid and escalate to appropriate safeguarding route if needed

A contact appearing online does not automatically make it appropriate to reproduce.

3. Safe Contact Analysis Questions

Before recording a contact clue, ask:

Is this contact detail public and intentionally published?
Is it connected to the research question?
Is it a business/role contact rather than private personal data?
Can the report answer the question without storing the full contact?
Could publication cause harassment, fraud, or unwanted attention?
Should it be redacted?

4. Email Structure Clues

Email addresses can provide organisational clues.

Pattern	Possible Meaning	Caution
first.last@company	organisation naming convention	Does not prove current employment
role@company	business function	Usually not person-specific
support@domain	support channel	Can support domain/company link
press@domain	media contact	Usually public role contact
personalname@gmail	personal account	Higher privacy risk
old-domain email	historical link	May be outdated

Do not test whether an email has accounts on platforms. Do not use password reset forms. Do not attempt to verify inbox ownership by sending unwanted messages.

5. Domain and Contact Consistency

A legitimate organisation often has coherent contact patterns:

- website domain matches email domain;
- company filings match public trading name;
- social profiles link back to the same website;
- press releases use same domain;
- archived pages show continuity;
- contact page and privacy page use consistent organisation identity.

Potential concerns:

- free email used for a company claiming large-scale operations;
- contact email domain does not match the official website;
- recently changed contact details without explanation;
- multiple unrelated companies sharing one contact channel;
- public warnings or regulator notices about impersonation;
- copy-pasted contact pages across unrelated sites.

These are leads, not proof of fraud.

6. Phone Number Clues

Phone numbers are sensitive. Use extreme caution.

Safe role-based uses:

- checking whether the phone number on a company website matches the number on an official public listing;
- recording that two public business pages use the same switchboard number;
- noting a support number that appears on official fraud-warning pages.

Unsafe uses:

- searching private numbers out of curiosity;
- calling or texting the subject;
- trying to identify a private person from a number;
- checking messaging app profiles;
- using reverse lookup services that expose personal details without a legitimate basis.

If the number is not required for the finding, redact it.

7. Contact Evidence Card

Evidence ID:
Contact clue type:
Exact source:
URL/reference:
Capture date/time:
Public/role/private category:
What the source directly shows:
Why it is relevant:
Linked domain/company/profile:
Risks:
Redaction required:
Confidence level:
Notes:

Example

Evidence ID: C23-04
Type: public business email
Source: official Northbank Workshop contact page
Observation: The page lists support@northbank-workshop.example as the support contact.
Relevance: The same email appears in the official product notice, supporting that the notice is organisation-controlled.
Risk: Low; role inbox, not private person.
Report treatment: Show domain only or partially redact local part if not necessary.

8. Contact Clue Confidence

Low:
Contact appears on one unverified page.

Medium:
Contact appears on two public sources with matching organisation context.

High:
Contact appears on an official/controlled website and an official register, filing, press release, or verified organisation.

Even a high-confidence contact link does not prove intent, wrongdoing, or current control.

9. Reporting Contact Details Safely

Use minimal disclosure.

Full detail may be unnecessary:

Unsafe:
The report lists the subject's full private email address and mobile number.

Safer:
The public business contact page and product notice use the same organisation email domain.

Safer when needed:
The public role inbox appears as support@[domain redacted in public copy]. The unredacted value is retained only in the

10. Exercise - Contact Clue Review

Fictional scenario:

A website selling safety equipment lists a company name, a free email address, a mobile number, and a registered-office

Complete:

Which contact clues are public business clues?
Which are private or risky?
Which clues should be redacted?
Which sources would confirm or contradict the company link?
What wording avoids accusing anyone of fraud?

Key Takeaways

- Contact details are evidence only when they are relevant and properly sourced.
- Avoid account enumeration, password reset checks, unwanted contact, and private-number research.
- Public business contacts are usually safer than personal contacts, but still need minimisation.

- Domain consistency can support organisation-link analysis.
- Reports should redact contact details unless disclosure is essential.

Visual Brief

V30. Contact clue safety ladder

A ladder from low-risk role inbox to high-risk private personal contact. Include decision points: public? role-based? relevant? necessary? redact? exclude?

Official Reference Points

Use these as boundary markers when designing or reviewing real work:

- ICO - lawful basis for processing personal data:
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>
- ICO - data protection principles: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>
- NCSC - social media safety and digital footprint guidance:
<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- GOV.UK / Companies House - company information service: <https://www.gov.uk/get-information-about-a-company>
- ICANN - RDAP information for registration data: <https://www.icann.org/rdap>
- GOV.UK - reporting suspicious emails, websites, phishing and fraud:
<https://www.gov.uk/report-suspicious-emails-websites-phishing>

Chapter 24 - Organisation Mapping

Safety and lawful-use note: This chapter is written for defensive, educational, journalistic, compliance, anti-fraud, and public-interest research. It does not authorise harassment, stalking, doxxing, impersonation, credential attacks, private-account access, bypassing restrictions, or collecting more personal data than is necessary for a legitimate purpose.

Purpose of This Chapter

Organisation mapping connects public entities: companies, charities, clubs, websites, brands, officers, trading names, addresses, projects, public profiles, and official documents. The aim is not to create a sensational spiderweb. The aim is to understand what public sources show, what they do not show, and where uncertainty remains.

By the end of this chapter, the reader should be able to:

- define an organisation entity;
- distinguish legal names from trading names and brands;
- map official records, websites, public profiles, and documents;
- separate current facts from historical facts;
- avoid guilt-by-association;
- produce an organisation map with confidence levels.

1. Organisation Entities

An organisation can appear under several labels:

registered company name;
trading name;
brand name;
product name;
charity name;
community group name;
club name;
campaign name;
website/domain name;
social account handle;
project name;
parent or subsidiary name.

Do not assume these are identical. A brand may be owned by a company. A domain may be controlled by an agency. A social page may be unofficial. A project may outlive a company.

2. Legal Name vs Trading Name

A legal name is the name on an official register. A trading name is the name the organisation uses publicly.

Example:

Legal name: Northbank Workshop Ltd
Trading name: SafeLamp Studio
Product: SafeLamp Mini
Domain: safelamp.example
Social handle: @safelampstudio

A safe finding might say:

Public sources indicate that SafeLamp Studio is presented as a trading style of Northbank Workshop Ltd, based on the of

Unsafe wording:

They are all the same thing and everyone involved is responsible for everything.

3. Organisation Source Types

Source Type | Use | Caution
Official register | legal existence, officers, filings | May lag behind real-world changes
Organisation website | current public claims | Controlled source, may be promotional
Archived website | historical claims | Capture date and archive date
Press releases | announcements | Confirm issuer and date
Regulator pages | warnings, sanctions, guidance | Read exact wording
Professional profiles | role claims | May be outdated or self-authored
Social profiles | public messaging | Confirm official status
News articles | context and reporting | Check source reliability
Community reports | leads and complaints | Verify independently

4. The Organisation Map

Create a map as a table before drawing any visual.

Entity	Type	Source	Current/Historical	Confidence	Notes
Northbank Workshop Ltd	registered company	official register	current	high	company number recorded
Safelamp Studio	trading name	website footer	current	medium	needs official confirmation
safelamp.example	domain	website/RDAP	current	medium	no private contact details reproduced
@SafeLampStudio	social profile	website link	current	high for organisation link	not person identity
Jordan Vale	officer	official register	current	high for directorship	no private life research
Safelamp Mini	product	website notice	current	high	product page captured

5. Current vs Historical

Organisation footprints change. A person may leave. A company may dissolve. A domain may be sold. An archived page may be true for its time but not true now.

Always label:

- current at capture date;
- historical as of archive date;
- unconfirmed current status;
- contradicted by newer source;
- source unavailable at time of review.

Example:

An archived 2021 page listed Northbank Labs as a partner. The current 2026 website does not list that partner. No conclusion.

6. Avoid Guilt by Association

Organisation maps can easily imply wrongdoing where none exists.

Weak association:

Two companies share an address at a serviced office.

This may mean:

- registered office provider;
- accountant's address;
- co-working space;
- old filing;
- common agent;
- actual operational link.

Do not write:

They are clearly part of the same operation.

Write:

The two companies share the same registered-office address. This is a weak association and requires further evidence before concluding.

7. Organisation Relationship Types

Use specific relationship labels.

- owns;
- operates;
- trades as;
- formerly known as;

director of;
listed partner;
registered at;
links to;
same phone number as;
same domain as;
same public contact as;
mentions;
reported by;
alleged by;
contradicted by.

Avoid vague labels like “connected to” unless you define the connection.

8. Evidence Thresholds

Organisation findings should be supported by reliable sources.

High confidence:
official register + organisation-controlled website;
regulator page + official company identifier;
archived official page + current official confirmation.

Medium confidence:
organisation website + social profile cross-link;
press release + news article;
public document + matching domain.

Low confidence:
community post only;
uncited forum claim;
similar name only;
shared address only;
old cached page only.

9. Exercise - Organisation Map

Fictional task:

Map the public relationship between Northbank Workshop Ltd, SafeLamp Studio, SafeLamp Mini, safelamp.example, and @SafeLamp.

Complete:

Entity table;
relationship table;
current vs historical labels;
confidence level for each relationship;
contradictions;
redactions;
summary finding.

Key Takeaways

- Organisations appear as legal names, brands, domains, products, profiles, and projects.
- Shared addresses or names are not proof of control.
- Current and historical sources must be separated.
- Relationship labels should be precise.
- Organisation maps should show confidence and limitations.

Visual Brief

V31. Organisation relationship map

A clean entity map with company, trading name, product, domain, public social profile, officer, document, and regulator nodes. Use line labels such as “registered as,” “trades as,” “links to,” and “historical mention.” Include confidence tags.

Official Reference Points

Use these as boundary markers when designing or reviewing real work:

- ICO - lawful basis for processing personal data:
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>
- ICO - data protection principles: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>
- NCSC - social media safety and digital footprint guidance:
<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- GOV.UK / Companies House - company information service: <https://www.gov.uk/get-information-about-a-company>
- ICANN - RDAP information for registration data: <https://www.icann.org/rdap>
- GOV.UK - reporting suspicious emails, websites, phishing and fraud:
<https://www.gov.uk/report-suspicious-emails-websites-phishing>

Chapter 25 - Company Ownership and Directorships

***Safety and lawful-use note:** This chapter is written for defensive, educational, journalistic, compliance, anti-fraud, and public-interest research. It does not authorise harassment, stalking, doxxing, impersonation, credential attacks, private-account access, bypassing restrictions, or collecting more personal data than is necessary for a legitimate purpose.*

Purpose of This Chapter

Company records can reveal official facts: company numbers, incorporation dates, status, registered addresses, officers, filings, charges, and sometimes persons with significant control. These records are powerful but easy to misread. A registered office is not necessarily a trading address. A director may have resigned. A shared address may be a service provider. A filing may be late, amended, or historical.

By the end of this chapter, the reader should be able to:

- read company records cautiously;
- separate legal facts from operational assumptions;
- understand directorship and control indicators;
- avoid overclaiming ownership or responsibility;
- build a company officer timeline;
- report company findings with evidence and limitations.

1. What Company Registers Can Show

Official company information services can show details such as:

```
company name;  
company number;  
status;  
incorporation date;  
registered office;  
filing history;  
accounts;  
confirmation statements;  
current and resigned officers;  
persons with significant control where applicable;  
charges and insolvency information where applicable;  
previous company names.
```

For UK companies, GOV.UK explains that Companies House information can include registered address, previous company names, current and resigned officers, document images, mortgage charge data, previous company names, and insolvency information.

2. Registered Office Is Not Always Operational Address

A common mistake is treating the registered office as the place where the business actually operates.

A registered office may be:

```
accountant's office;  
formation agent;  
serviced office;  
virtual office;  
solicitor's office;  
home address;  
historical address;  
actual trading address.
```

Safe wording:

The company is registered at [address redacted in public copy]. This does not by itself establish that the company opera

3. Officer Records

Officer records can show a public legal role, but not necessarily day-to-day control.

Officer Type | Meaning | Caution

Director | legally appointed director | May be nominal, resigned, or one of several

Secretary | administrative/legal role | Not necessarily operational control

PSC | person with significant control | Legal control indicator, read exact category

Resigned officer | historical role | Not current unless confirmed elsewhere

Do not infer motive, wrongdoing, or personal responsibility from a role alone.

4. Company Timeline

Create a timeline before drawing conclusions.

Date | Event | Source | Confidence | Notes

2021-03-12 | Company incorporated | official register | high | company number captured

2022-06-01 | Name changed | filing history | high | previous name recorded

2023-09-15 | Director appointed | officer page | high | current as of capture date

2025-01-10 | Product launched | company website | medium | controlled source

2026-05-04 | Safety notice published | company website/archive | high | captured

Timelines prevent mixing old and current facts.

5. Ownership vs Association

Do not say “owns” unless the source supports ownership.

Evidence | Safe Interpretation

PSC record | may support legal control as defined by register

Director record | supports directorship, not ownership by itself

Website footer | supports presented operator, not legal ownership alone

Shared phone | supports contact overlap, not ownership

Shared address | weak association only

Press quote | supports public claim, needs verification

6. Red Flags and Caution Flags

Company records may contain indicators worth further review, but they are not proof of fraud.

rapid name changes;

recent incorporation with grand claims;

overdue filings;

multiple dissolved companies with similar names;

frequent officer changes;

unclear trading name;

domain recently created compared with long trading claim;

public warnings or regulator notices;

copy-pasted documents;

misuse of another company's name or number.

Report as caution indicators:

The records show several caution indicators requiring verification. These indicators do not establish wrongdoing.

7. Officer Network Mapping

Officer network maps can be useful but must be restrained.

Person | Company | Role | Start | End | Source | Confidence

Jordan Vale | Northbank Workshop Ltd | Director | 2023-09-15 | current | official register | high

Jordan Vale | Vale Safety Ltd | Former Director | 2019-04-01 | 2021-02-20 | official register | high

Avoid:

family members;

home addresses;

private social profiles;

children;

unrelated personal material;

old addresses unless necessary and redacted.

8. Filing Documents

Filing documents can contain useful evidence and sensitive details.

Record:

```
document title;
filing date;
event date if different;
company number;
what the document states;
redactions needed;
current or historical relevance.
```

Be careful: the filing date is not always the event date.

9. Company Finding Template

Finding:

Official records show that Northbank Workshop Ltd, company number [redacted in public copy if needed], was incorporated

Evidence:

- Official company register page captured on [date].
- Filing history reviewed for current and previous names.

Limitations:

The registered office does not establish the operational premises. Officer roles do not by themselves prove day-to-day

Confidence:

High for official registration facts; medium/low for operational interpretation unless supported by additional sources.

10. Exercise - Company Record Review

Fictional case:

SafeLamp Studio claims to be “a 20-year British safety company.” The official register shows Northbank Workshop Ltd was

Complete:

```
What official facts can be stated?
What claims need additional evidence?
What should not be inferred?
What sources could support the 20-year claim?
What cautious wording belongs in the report?
```

Key Takeaways

- Company registers show legal facts, not every operational fact.
- Registered office does not equal trading address.
- Directorship does not automatically equal ownership or wrongdoing.
- Timelines prevent outdated conclusions.
- Shared addresses and officer overlaps require careful wording.
- Redact personal details where not necessary.

Visual Brief

V32. Company officer and filing timeline

A horizontal timeline with incorporation, name change, officer appointment, filing, product launch, and public notice. Add side cards for “legal fact,” “operational claim,” and “requires verification.”

Official Reference Points

Use these as boundary markers when designing or reviewing real work:

- ICO - lawful basis for processing personal data:
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>
- ICO - data protection principles: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>
- NCSC - social media safety and digital footprint guidance:
<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- GOV.UK / Companies House - company information service: <https://www.gov.uk/get-information-about-a-company>
- ICANN - RDAP information for registration data: <https://www.icann.org/rdap>
- GOV.UK - reporting suspicious emails, websites, phishing and fraud:
<https://www.gov.uk/report-suspicious-emails-websites-phishing>

Chapter 26 - Job Posts, Leaks of Process, and Public Footprints

***Safety and lawful-use note:** This chapter is written for defensive, educational, journalistic, compliance, anti-fraud, and public-interest research. It does not authorise harassment, stalking, doxxing, impersonation, credential attacks, private-account access, bypassing restrictions, or collecting more personal data than is necessary for a legitimate purpose.*

Purpose of This Chapter

Organisations reveal a surprising amount through public job adverts, supplier pages, staff pages, conference talks, documentation, procurement notices, GitHub-style public project pages, help-centre articles, and marketing material. These sources can help understand what an organisation publicly says about itself, how mature its processes may be, and whether public claims are consistent. They must not be used for targeting staff, phishing, social engineering, or intrusion.

By the end of this chapter, the reader should be able to:

- review job adverts and public process clues safely;
- distinguish capability claims from evidence;
- avoid turning staff details into targets;
- map public organisational footprint without exploitation;
- assess claims about scale, technology, geography, and maturity.

1. Public Footprint Sources

job adverts;
careers pages;
public staff biographies;
speaker biographies;
conference schedules;
press releases;
procurement portals;
policy documents;
public documentation;
help-centre pages;
status pages;
public repository descriptions;
product manuals;
supplier case studies;
customer testimonials;
terms, privacy, and cookie pages.

These sources are useful because they are normally published intentionally by the organisation or a partner. They still need careful interpretation.

2. What Job Posts Can Reveal

Job posts may reveal:

locations;
team structure;
technology stack;
seniority gaps;
growth stage;
outsourcing;
regulatory environment;
security maturity;
customer segment;
product direction;
operational pressure;
contract type;
working patterns.

A job advert asking for “first compliance hire” may indicate a different maturity level from a company claiming a large compliance department. But it does not prove misconduct.

3. Safe Use of Staff-Related Material

Staff information is personal data. Keep it role-relevant and minimal.

Use:

- public role title;
- public professional biography;
- organisation-controlled staff page;
- conference speaker page;
- public authored article relevant to role.

Avoid:

- private family content;
- personal addresses;
- personal phone numbers;
- non-work social accounts;
- medical or political details;
- collecting employee lists for targeting;
- contacting staff for verification without authority.

4. Process Leakage Without Exploitation

Sometimes an organisation publicly discloses process details. OSINT analysis can record what is public without using it to attack.

Examples:

- manual explains support escalation route;
- job post names a ticketing platform;
- status page shows incident history;
- privacy policy names processors;
- case study names cloud provider;
- procurement notice reveals planned system change;
- manual names product version.

Safe analysis:

The public materials suggest the organisation uses a named support platform and maintains a public status page. This may

Unsafe analysis:

Use these details to craft staff phishing messages or probe the platform.

5. Capability Claims vs Evidence

Organisations may claim:

- world-leading;
- fully certified;
- military grade;
- AI-powered;
- trusted by thousands;
- UK-based;
- 24/7 support;
- regulated;
- award winning.

Convert claims into evidence questions:

- What specific certification is named?
- Who issued it?
- Is it current?
- Is there a public certificate number?
- Which entity holds it?
- Does the company name match?
- What source confirms the customer or award claim?

6. Public Footprint Table

Source | Public Claim | What It Supports | What It Does Not Prove | Confidence | Notes
Careers page | hiring first security manager | possible growth in security function | does not prove previous insecurity
Privacy policy | names analytics processor | processor relationship | full data architecture | high for statement only
Press release | “trusted by 10,000 users” | marketing claim | verified user count | low without independent source | need
Status page | 3 incidents in May | public incident history | full outage impact | high for published data | record time

7. Change Over Time

A public footprint is time-sensitive. Use archive checks where appropriate and label dates.

2024 careers page: hiring “first operations lead.”
2025 team page: operations team of six.
2026 press release: claims expanded operations division.

This sequence may support growth. It does not prove service quality.

8. Risk Language

Use cautious language.

The job advert may indicate...
The public documentation suggests...
The claim is not independently confirmed by the sources reviewed...
The evidence supports a public-claim consistency issue, not a finding of fraud.

Avoid:

They are lying.
Their security is weak.
Their staff are targets.
This proves they are fake.

9. Exercise - Public Footprint Review

Fictional case:

A product website claims “24/7 UK-based expert support.” Current job posts advertise for the company's first support manager.

Complete:

What can be stated?
What remains unknown?
What source is most reliable?
What wording is fair?
What staff data should be excluded?

Key Takeaways

- Job posts and public documents can reveal organisational maturity and claimed capabilities.
- Do not use staff details for targeting or contact.
- Process details are for defensive understanding, not exploitation.
- Marketing claims must be converted into evidence questions.
- Time labels are essential.

Visual Brief

V33. Public organisational footprint board

A board with cards for job adverts, privacy policy, help docs, status page, press release, procurement notice, and conference talk. Lines connect each card to claims: capability, technology, geography, staffing, maturity. Add warning: “Analyse public claims - do not target staff.”

Official Reference Points

Use these as boundary markers when designing or reviewing real work:

- ICO - lawful basis for processing personal data:
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>
- ICO - data protection principles: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>
- NCSC - social media safety and digital footprint guidance:
<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- GOV.UK / Companies House - company information service: <https://www.gov.uk/get-information-about-a-company>
- ICANN - RDAP information for registration data: <https://www.icann.org/rdap>
- GOV.UK - reporting suspicious emails, websites, phishing and fraud:
<https://www.gov.uk/report-suspicious-emails-websites-phishing>

Chapter 27 - Community and Network Mapping

***Safety and lawful-use note:** This chapter is written for defensive, educational, journalistic, compliance, anti-fraud, and public-interest research. It does not authorise harassment, stalking, doxxing, impersonation, credential attacks, private-account access, bypassing restrictions, or collecting more personal data than is necessary for a legitimate purpose.*

Purpose of This Chapter

Many investigations involve communities rather than isolated individuals: clubs, forums, local groups, professional circles, scam-report communities, open-source projects, marketplace sellers, review ecosystems, and campaign networks. Community mapping helps understand public relationships and information flow without invading private spaces or encouraging harassment.

By the end of this chapter, the reader should be able to:

- identify public community structures;
- map roles and relationships without exposing private people;
- distinguish community claims from evidence;
- avoid brigading, dogpiling, and harassment;
- produce a network map with anonymisation and confidence levels.

1. Community Sources

public forums;
public social groups;
project issue boards;
marketplace reviews;
public comment sections;
local club websites;
charity/community pages;
newsletter archives;
public Discord/Slack invite pages where content is accessible without joining private spaces;
conference/event attendee pages;
public scam-report boards;
open-source contribution pages.

Excluded:

private groups;
closed messaging rooms;
leaked chat logs;
invitation-only spaces;
accounts obtained through deception;
screenshots provided without consent or provenance;
anything requiring bypassing access controls.

2. Community Roles

A community map should focus on roles, not private lives.

administrator;
moderator;
official representative;
seller;
buyer/reviewer;
project maintainer;
frequent contributor;
event organiser;
complainant;
witness;
amplifier;
external source;
unknown account.

Role labels are safer than identity labels.

3. Claims vs Evidence in Communities

Community posts are often leads. They may be honest, mistaken, exaggerated, malicious, sarcastic, or copied from elsewhere.

Treat community claims as:

- lead;
- public allegation;
- reported experience;
- opinion;
- rumour;
- copy of another source;
- first-hand evidence only if the post includes verifiable material and context.

Do not treat a pile of repeated claims as independent evidence unless they come from independent sources.

4. Network Map Table

Node	Role	Source	Relationship	Confidence	Redaction
@NorthbankHelp	official support profile	website link	official channel	high	none
ForumUser42	complainant	public forum	reports delayed refund	low	anonymise
SafeLamp Studio	brand	company website	product operator	medium	none
LocalMakersClub	community group	public website	hosted event	medium	none
ReviewSite A	review source	public review page	customer reviews	medium	anonymise reviewers

5. Avoiding Harm

Community research can create harm even when sources are public.

Do not:

- publish private individuals' usernames unnecessarily;
- encourage others to contact or confront people;
- collect follower/friend lists without a defined need;
- turn complaints into accusations;
- name vulnerable complainants;
- expose minors;
- join private communities under false pretences;
- archive personal disputes that are irrelevant.

Use anonymised labels where possible:

- Reviewer A;
- Forum complainant 1;
- Moderator account;
- Public support account;
- Local club website.

6. Information Flow

Mapping information flow helps explain how a claim spreads.

Original source → repost → forum discussion → news mention → official response → correction

Capture:

- first observed source;
- earliest archived source;
- who links to whom;
- whether sources quote each other;
- whether independent sources exist;
- whether official response exists.

This prevents circular reporting.

7. Community Reputation Signals

Reputation signals can be useful but must be treated carefully.

- number of complaints;
- age of complaints;
- source independence;

review verification status;
response from organisation;
pattern consistency;
resolved vs unresolved reports;
moderator warnings;
platform enforcement notices;
official regulator notice.

Avoid simplistic conclusions:

Bad reviews = fraud.
Few reviews = fake.
Many positive reviews = legitimate.

All reputation data requires context.

8. Reporting Community Findings

Safe wording:

Public community sources contain multiple complaints about delayed delivery. The complaints are leads and should be considered.

Unsafe wording:

The community says they are scammers, so they are scammers.

9. Exercise - Community Claim Mapping

Fictional scenario:

A public forum has eight complaints about SafeLamp Mini delivery delays. Three posts quote the same original review. One

Complete:

Which sources are independent?
Which are circular?
Which usernames should be anonymised?
What role labels should be used?
What finding can be stated safely?

Key Takeaways

- Communities produce leads, not automatic proof.
- Map roles and information flow rather than private identities.
- Avoid private groups, deception, and harassment.
- Repeated claims are not independent if they copy the same source.
- Anonymise private community members unless naming is necessary and justified.

Visual Brief

V34. Community information-flow map

A node map showing original source, reposts, forum claims, news mention, official response, and correction. Use dotted lines for circular reporting and solid lines for independent sources. Include anonymised user labels.

Official Reference Points

Use these as boundary markers when designing or reviewing real work:

- ICO - lawful basis for processing personal data:
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>
- ICO - data protection principles: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>
- NCSC - social media safety and digital footprint guidance:
<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>

- GOV.UK / Companies House - company information service: <https://www.gov.uk/get-information-about-a-company>
- ICANN - RDAP information for registration data: <https://www.icann.org/rdap>
- GOV.UK - reporting suspicious emails, websites, phishing and fraud:
<https://www.gov.uk/report-suspicious-emails-websites-phishing>

Chapter 28 - Reputation, Scams, and Fraud Indicators

***Safety and lawful-use note:** This chapter is written for defensive, educational, journalistic, compliance, anti-fraud, and public-interest research. It does not authorise harassment, stalking, doxxing, impersonation, credential attacks, private-account access, bypassing restrictions, or collecting more personal data than is necessary for a legitimate purpose.*

Purpose of This Chapter

OSINT is often used to assess whether a public offer, seller, website, company, contact, or message has warning signs. This chapter teaches how to collect and report fraud indicators responsibly. It does not teach how to scam, impersonate, evade detection, or exploit victims.

By the end of this chapter, the reader should be able to:

- distinguish indicators from proof;
- identify common public warning signs;
- use official reporting and advice sources;
- compare reputation data with company and domain evidence;
- protect victims and complainants;
- write a cautious risk assessment.

1. Indicator Is Not Proof

A fraud indicator is a reason to check further. It is not a verdict.

Examples of indicators:

pressure to pay quickly;
requests for unusual payment methods;
generic or copied website content;
recent domain with long-history claims;
company name mismatch;
contact email mismatch;
fake-looking reviews;
unverifiable certifications;
public complaints with consistent pattern;
impersonation of known organisations;
links that do not match the claimed organisation;
unexplained urgency or secrecy.

Safe finding:

The reviewed public sources show several caution indicators consistent with known scam-warning patterns. This does not

2. Common Scam Patterns

Official consumer-protection guidance often highlights patterns such as impersonation, urgency, claimed problems or prizes, and pressure to pay or act quickly. In UK contexts, suspicious emails, websites, phishing, and fraud can be reported through GOV.UK routes; in the US, the FTC publishes consumer scam guidance.

For analysis, group indicators by type:

identity mismatch;
contact mismatch;
payment risk;
urgency/pressure;
technical/domain mismatch;
public complaint pattern;
official warning;
regulatory concern;

image/content reuse;
review manipulation concern.

3. Reputation Source Types

Source Type | Value | Caution
Official warning | high-value indicator | read exact wording
Regulator page | strong source | may be jurisdiction-specific
Consumer advice page | pattern guidance | general, not case-specific
Review platform | public experience reports | may include fake or biased reviews
Forum complaints | leads | verify independently
News report | context | check source reliability
Company response | official position | controlled source
Archived page | historical claims | may be outdated
Marketplace profile | transaction/reputation clues | platform-specific limits

4. Fraud Indicator Matrix

Indicator | Source | Direct Observation | Alternative Explanation | Confidence | Next Check
Recent domain | RDAP/website | domain appears recent | rebrand/new site | medium | archive/company records
Company mismatch | website/register | name differs | trading name | medium | website footer/filings
Urgent payment | public advert | "pay today only" | limited offer | low/medium | compare official pricing
Complaints | forum/reviews | multiple delivery complaints | backlog | medium | independent reviews/company response
Official warning | regulator | named warning | may relate to impersonator | high | check exact entity identifiers

Alternative explanations keep the work fair.

5. Victim and Complainant Protection

Do not expose people who report scams.

Avoid publishing:

victim names;
private contact details;
transaction IDs;
addresses;
photos of documents;
bank details;
screenshots with personal data;
medical, family, or vulnerability details.

Use anonymised summaries:

Three public complainants describe a similar delivery-delay pattern between March and May 2026. Their usernames are redacted.

6. Safe Reporting Routes

If the work suggests someone may have been defrauded or phished, direct them to official reporting routes rather than attempting private confrontation.

Examples:

UK suspicious emails/websites/phishing and fraud guidance via GOV.UK;
NCSC suspicious website reporting routes;
Report Fraud / police routes for England, Wales and Northern Ireland;
Police Scotland routes for Scotland;
FTC consumer guidance and reporting routes for US contexts;
platform-specific report buttons for marketplace abuse.

Do not contact suspected scammers, their families, or staff. Do not attempt retaliation.

7. Scam-Risk Finding Template

Finding:

Public sources reviewed show [number] caution indicators relating to [identity/contact/payment/reputation].

Evidence:

- [source 1] shows [direct observation].
- [source 2] shows [direct observation].
- [source 3] contradicts or limits the finding by showing [direct observation].

Assessment:

The indicators warrant caution and further verification before payment or engagement. The available evidence does not es

Recommended action:

Use official reporting routes if money has been lost or phishing is suspected. Avoid contacting or confronting the suspo

Confidence:

Low / medium / high for the presence of indicators; separate confidence for any entity link.

8. Exercise - Scam Indicator Review

Fictional scenario:

A website claims to sell discounted radio equipment. The domain is new, the contact email is a free webmail account, the

Complete:

- List the indicators.
- List possible innocent explanations.
- Identify official sources to check.
- Decide what should be redacted.
- Write a cautious risk assessment.
- List safe next steps for a potential victim.

Key Takeaways

- Scam indicators are warning signs, not proof.
- Compare identity, contact, payment, domain, reputation, and official-warning evidence.
- Protect victims and complainants.
- Use official reporting routes.
- Avoid confrontation, retaliation, or private investigations outside the safe scope.

Visual Brief

V35. Scam-risk indicator matrix

A matrix with rows for identity mismatch, contact mismatch, payment pressure, domain age, reviews, public complaints, official warnings, and alternative explanations. Use amber risk tags, not red “guilty” labels.

Official Reference Points

Use these as boundary markers when designing or reviewing real work:

- ICO - lawful basis for processing personal data:
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>
- ICO - data protection principles: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>
- NCSC - social media safety and digital footprint guidance:
<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- GOV.UK / Companies House - company information service: <https://www.gov.uk/get-information-about-a-company>
- ICANN - RDAP information for registration data: <https://www.icann.org/rdap>
- GOV.UK - reporting suspicious emails, websites, phishing and fraud:
<https://www.gov.uk/report-suspicious-emails-websites-phishing>

Chapter 29 - Handling Ambiguous Identity Matches

***Safety and lawful-use note:** This chapter is written for defensive, educational, journalistic, compliance, anti-fraud, and public-interest research. It does not authorise harassment, stalking, doxxing, impersonation, credential attacks, private-account access, bypassing restrictions, or collecting more personal data than is necessary for a legitimate purpose.*

Purpose of This Chapter

Ambiguous identity matches are common in OSINT. Names repeat. People move jobs. Companies rebrand. Usernames are copied. Old pages remain online. Automated tools may produce false positives. This chapter teaches how to handle uncertainty without making harmful claims.

By the end of this chapter, the reader should be able to:

- recognise ambiguous matches;
- list alternative explanations;
- score confidence honestly;
- separate entity match from person identity;
- avoid confirmation bias;
- write “unknown” when the evidence is not enough.

1. Why Ambiguity Happens

common names;
shared initials;
old usernames;
recycled phone numbers;
changed domains;
company rebrands;
serviced-office addresses;
family members with similar names;
multiple people in same profession;
copied profile photos;
spoofed accounts;
fan/parody accounts;
archived content;
search-engine snippet errors;
AI-generated summaries that mix sources.

Ambiguity is not a problem to hide. It is a finding to report.

2. Match Types

Match Type	Meaning	Example
Exact entity match	same official identifier	company number matches
Likely organisation match	official site links profile	company website links social account
Possible profile match	shared distinctive handle	same unusual username
Weak name match	same common name	John Smith in same town
Contradicted match	clear conflict	different company numbers
Unknown	not enough evidence	no reliable source connects them

3. The Alternative Explanations Rule

For every identity match, list at least three alternatives.

Example:

Observation:

A public profile named “J Vale” says “operations director” and a company register lists Jordan Vale as a director.

Alternative explanations:

1. The profile belongs to the registered director.
2. The profile belongs to a different person with a similar name.
3. The profile is outdated or self-authored inaccurately.
4. The company role changed after the profile was written.
5. The profile is parody, impersonation, or unauthorised.

This prevents the investigation from becoming a hunt for confirmation.

4. Confidence Levels

High confidence:

Multiple independent reliable sources connect the same entity using strong identifiers.

Medium confidence:

Several indicators align, but at least one key identifier is missing.

Low confidence:

Only weak clues align, such as name similarity or shared interest.

No finding:

The evidence does not support a responsible conclusion.

Confidence should be attached to each specific finding, not the whole case.

5. Identity Match Checklist

What exact item is being matched?

Name? username? email? company number? domain? photo? role?

Is there an official identifier?

Is the source current?

Is the source controlled by the entity?

Are there contradictions?

Could this be a common-name collision?

Could this be a reused or spoofed handle?

Could this be historical rather than current?

What personal data can be redacted?

What is the lowest-risk wording?

6. Evidence Thresholds by Claim

Claim | Minimum Evidence Needed

Company exists | official register or equivalent

Person is a director | official register current/resigned status

Profile belongs to organisation | official website cross-link or verified source

Private person controls account | avoid unless legally authorised and strongly evidenced

Organisation operates domain | website content + registration/official links

Scam indicator exists | direct observation + source capture

Fraud occurred | do not claim without appropriate legal authority/outcome

7. Writing Ambiguity

Good report wording:

The sources support a possible link between the public profile and the company officer record, but the evidence is insufficient to confirm.

The shared registered-office address is a weak association because it may represent a service provider rather than operational premises.

No responsible conclusion can be drawn from the available sources.

Bad wording:

It must be the same person.

They are obviously connected.

This proves the hidden network.

8. When to Stop

Stop when:

only intrusive sources remain;

the finding would require private-life research;

the evidence stays weak after reasonable public checks;

the risk of false accusation outweighs the value;

the research question can be answered as "not established."

An honest “not established” is better than a confident false match.

9. Exercise - Ambiguous Match Review

Fictional case:

A public forum user “JValeSafety” complains about a product. A company register lists Jordan Vale as director of a relat

Complete:

List matching indicators.
List contradictions or missing evidence.
List alternative explanations.
Assign confidence to each possible link.
Write a safe finding.
Decide what not to collect.

Key Takeaways

- Ambiguity is normal and must be documented.
- Same name or handle is not enough.
- List alternative explanations before writing a finding.
- Confidence levels belong to specific claims.
- “Unknown” and “not established” are valid conclusions.

Visual Brief

V36. Ambiguous match decision tree

A decision tree from “possible match” through exact identifier, controlled link, independent confirmation, contradiction, private-data risk, confidence, and final wording. Include “No finding” as a valid endpoint.

Official Reference Points

Use these as boundary markers when designing or reviewing real work:

- ICO - lawful basis for processing personal data:
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>
- ICO - data protection principles: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>
- NCSC - social media safety and digital footprint guidance:
<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- GOV.UK / Companies House - company information service: <https://www.gov.uk/get-information-about-a-company>
- ICANN - RDAP information for registration data: <https://www.icann.org/rdap>
- GOV.UK - reporting suspicious emails, websites, phishing and fraud:
<https://www.gov.uk/report-suspicious-emails-websites-phishing>

Chapter 30 - Entity Investigation Case Study

***Safety and lawful-use note:** This chapter is written for defensive, educational, journalistic, compliance, anti-fraud, and public-interest research. It does not authorise harassment, stalking, doxxing, impersonation, credential attacks, private-account access, bypassing restrictions, or collecting more personal data than is necessary for a legitimate purpose.*

Purpose of This Chapter

This chapter closes Volume 3 by combining person research, username correlation, contact clues, organisation mapping, company records, public footprint review, community mapping, scam indicators, and ambiguous identity handling into one safe fictional workflow.

The case study is fictional. It is designed to teach method, caution, and reporting discipline, not to target real people or organisations.

By the end of this chapter, the reader should be able to:

- scope an entity investigation;
- map people, companies, domains, profiles, and communities;
- identify safe and unsafe source types;
- protect private individuals;
- handle scam indicators without accusations;
- produce a clear report with confidence and limitations.

1. Fictional Scenario

A local amateur radio club receives a promotional email about discounted portable radio batteries from **FieldVolt Direct**. The email links to a website claiming:

"20 years supplying UK field operators."
"Official partner of Northbank Workshop Ltd."
"Trusted by emergency volunteers."
"Bank transfer discount today only."

Several public forum users say orders have not arrived. One user claims the site is connected to a person named **Jordan Vale**. The club wants a safe OSINT review before members place orders.

The task is not to identify or expose a private person. The task is to assess what public sources show about the organisation, website, claims, contact details, company links, and public reputation indicators.

2. Research Question

What do public sources show about FieldVolt Direct, its claimed company/partner links, its public contact details, and a

3. Scope

Included:

FieldVolt Direct website;
archived versions of the website;
public company register searches;
public partner claim checks;
public domain/RDAP registration data where visible;
public official social profiles linked from the site;
public forum/review complaints as leads;
official scam/fraud advice sources;
public payment and contact claims shown on the website.

Excluded:

private individuals;
home addresses;
family or associates;
private social accounts;
closed groups;
password reset checks;
email account existence testing;
contacting the suspected operator;
technical probing of the website;
collecting complainant identities beyond anonymised evidence.

4. Evidence Log

Evidence ID	Source	Observation	Confidence	Notes
E30-01	FieldVolt website	claims 20 years supplying UK field operators	high for claim only	unsupported by source
E30-02	Website contact page	lists fieldvoltdirect.example email and mobile number	high for displayed contact	mobile number redacted
E30-03	Company register	no exact FieldVolt Direct company found	high for search result as of date	search terms may be incorrect
E30-04	Company register	Northbank Workshop Ltd exists	high	does not prove partnership
E30-05	Northbank official website	no FieldVolt partner mention found	medium	absence not proof
E30-06	Public forum	7 complaints about delayed delivery	low/medium	usernames anonymised
E30-07	RDAP/domain page	domain appears recently registered	medium	depends on visible data
E30-08	Payment page	offers bank transfer discount today only	high for claim	caution indicator, not proof

5. Organisation Map

Entity	Type	Evidence	Relationship	Confidence
FieldVolt Direct	trading/site name	website	presents seller identity	high for presentation
fieldvoltdirect.example	domain	website/RDAP	hosts seller website	high
Northbank Workshop Ltd	registered company	official register	claimed partner, not confirmed	low for partnership
@FieldVoltDirect	social profile	linked from website	likely public seller profile	medium/high if cross-linked
Jordan Vale	named by forum user	forum claim only	not established	no finding
Forum complainants	private users	public forum	report delivery issues	anonymised

6. Contact Clue Review

Clue	Risk	Assessment
Website domain email	lower risk role/business contact	relevant to site control
Mobile number	higher privacy risk	record in restricted evidence only if necessary; redact report
Free webmail fallback	caution indicator	not proof; compare with company claims
Bank details	sensitive/payment risk	do not reproduce publicly
Contact form	business channel	do not use without authority

Safe wording:

The site uses contact details presented as business contacts. A mobile number and payment details are redacted from this report.

7. Partner Claim Check

Claim:

"Official partner of Northbank Workshop Ltd."

Checks:

FieldVolt website: claim present.
Northbank official website: no partner page mention found during review.
Northbank press releases: no matching announcement found.
Archived Northbank pages: no matching reference found.
Company records: no direct ownership/control link found from reviewed sources.

Safe finding:

The reviewed public sources confirm that FieldVolt Direct makes a partnership claim. The reviewed sources do not independently confirm the claim.

8. Scam Indicator Matrix

Indicator	Present?	Evidence	Alternative Explanation	Assessment
Urgency/payment pressure	yes	bank transfer discount today only	promotion	caution indicator
Recent domain vs long-history claim	possible	RDAP/domain evidence	rebrand/new site	needs archive/company support
Company mismatch	possible	no exact company found	trading name	needs more evidence
Public complaints	yes	forum posts	delivery backlog	lead only
Unconfirmed partner claim	yes	no independent confirmation found	private partnership	caution indicator
Free email fallback	yes	contact page	small business	caution indicator

Assessment:

Multiple caution indicators are present. They warrant further verification before payment. The available sources do not

9. Ambiguous Identity Claim

Forum claim:

"This is Jordan Vale again."

Evidence reviewed:

forum claim only;
no official source linking Jordan Vale to FieldVolt Direct;
no controlled profile link found;
company records do not establish the claimed connection;
no direct evidence reviewed that identifies the website operator as Jordan Vale.

Finding:

The identity claim is not established by the reviewed public sources. It should not be repeated as fact.

10. Community Mapping

Source | Role | Treatment
Public radio forum | complaint lead source | anonymise users
Marketplace reviews | reputation source | assess verification status
Official website | controlled source | capture claims
Northbank official site | partner-claim check | capture absence/contradiction carefully
Official advice pages | safety guidance | cite for reporting routes

Avoid:

asking forum users for private order details;
publishing screenshots with names/order IDs;
encouraging members to confront seller;
searching private accounts of named individuals;
posting accusations in club groups.

11. Mini Report

Executive Summary

Public sources reviewed show that FieldVolt Direct presents itself as a seller of portable radio batteries and makes cl

Findings

Finding 1 – Seller identity presentation
The website presents FieldVolt Direct as the seller. Confidence is high for the existence of the public claim, but this

Finding 2 – Company/partner claim
The site claims partnership with Northbank Workshop Ltd. The reviewed official/controlled sources did not independently

Finding 3 – Public reputation leads
Public community sources contain several delivery-delay complaints. These are leads and are anonymised. Confidence is m

Finding 4 – Payment caution
The site promotes a time-limited bank-transfer discount. This is a caution indicator because payment pressure and unusu

Finding 5 – Identity allegation
A public forum allegation naming Jordan Vale is not supported by reviewed official or controlled sources. No identity f

Recommended Safe Actions

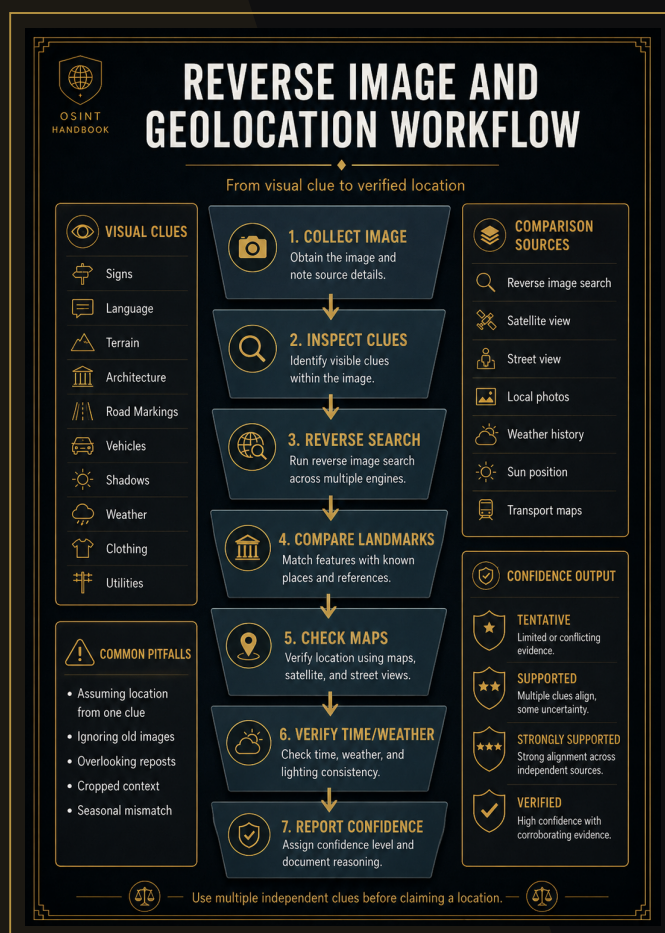
Members should verify seller identity and payment protections before ordering.
Avoid bank transfer where buyer protection is unclear.
Use official reporting routes if money has been lost or phishing/fraud is suspected.
Do not contact, confront, or publish allegations about named individuals.
Retain evidence privately with redaction.

VOLUME FOUR

Images, Maps, and Geolocation

Visual verification, metadata, maps, weather clues, video, events, and reporting.

CHAPTERS 31-40



Chapter 31 - Image Search and Reverse Image Search

***Safety and lawful-use note:** This chapter is for defensive, educational, journalistic, verification, safety, and public-interest OSINT. Do not use these methods to stalk, harass, expose a private home, identify vulnerable people, bypass access controls, trespass, or publish precise location details where disclosure could cause harm. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, and stop when the task no longer has a legitimate purpose.*

Purpose of This Chapter

Images are often the fastest way to break open an OSINT question, but they are also easy to misread. A picture can be old, cropped, mirrored, staged, reposted, AI-generated, captioned falsely, or used in the wrong context. This chapter teaches a safe workflow for using image search and reverse image search as a lead-generation and verification method, not as a shortcut to certainty.

By the end of this chapter, the reader should be able to:

- use image search to find earlier appearances, copies, crops, and related context;
- separate what the image shows from what the caption claims;
- record search results in a way that can be audited later;
- compare multiple reverse-image tools without over-trusting any one result;
- avoid privacy harm when images include private people, homes, vehicles, children, or vulnerable groups.

1. What Image Search Can and Cannot Prove

Reverse image search can help answer questions such as:

Where else has this image appeared?
Is there an older version?
Has the image been cropped, mirrored, captioned differently, or reused?
Is there a higher-resolution copy?
Is the image connected to an article, product listing, location, or event page?

It cannot, by itself, prove:

who took the image;
why the image was posted;
whether the caption is true;
whether the visible person is who someone says they are;
whether the location should be publicly disclosed;
whether the image is fully authentic.

Treat image search as a way to create leads. A lead becomes evidence only when it is captured, cited, compared, and verified.

2. Start With the Claim, Not the Tool

Before searching, write the claim as a simple sentence.

Claim: This image shows the protest outside Northgate Station on 6 June 2026.

Then split it:

Image claim: The picture shows a protest.
Location claim: It is outside Northgate Station.
Time claim: It was taken on 6 June 2026.
Context claim: It relates to the named event.

Each part needs different evidence. Image search may find an older copy. Maps may confirm location. Weather or shadows may support time. News and social posts may support event context.

3. Preserve the Starting Image

Before uploading or searching the image, save the starting item exactly as received.

Recommended evidence note:

Evidence ID: IMG31-01
Received from: public post URL / supplied case file / archived page
Date captured: YYYY-MM-DD HH:MM timezone
Original filename: if available
Visible caption: exact wording
Visible account/page: public name only
Action taken: saved original copy; no edits
Hash: optional, if using a hash workflow

If the image contains private people, faces, children, number plates, medical details, or a private residence, create a working redacted copy for reporting. Keep the original only where lawful and necessary.

4. Run a Search Family

Do not rely on one upload to one tool. Use a search family:

1. Full image reverse search.
2. Cropped subject search.
3. Cropped background sign/logo/searchable object search.
4. Text visible in image searched as plain text.
5. Object or landmark description searched as text.
6. Date/event keywords searched separately.

This avoids the common mistake of assuming “no result” means “new image”. A tool may miss a result because the image is too new, too cropped, too compressed, or visually common.

5. Useful Image Search Routes

Examples of routes to record in a source list:

Google Lens / Google image search – broad visual and object matching.
TinEye – reverse-image matches, modified copies, and older appearances when indexed.
Bing Visual Search – alternative visual-index results.
Yandex image search – sometimes useful for visual similarity, but treat carefully and verify independently.
Pinterest / marketplace image search – useful for product, fashion, design, and reposted item clues.
Search engine text queries – sometimes better than visual search when signs, logos, or captions are visible.

Use tool names in your notes, but do not present the tool output as truth. The finding comes from the verified source you open and capture, not from the search-result thumbnail alone.

6. Compare Earlier Uses

When you find earlier appearances, capture:

URL or archive reference;
page title;
publisher/account;
date visible on page;
date captured by you;
caption/context;
whether the image is identical, cropped, mirrored, filtered, or edited;
whether the page itself is reliable.

A strong finding might say:

The image appeared on a public local-news page dated 14 March 2024, where it was captioned as flooding in Westport. This

A weaker finding might say:

No earlier indexed copy was found during this review. This does not prove the image is original or recent.

7. Cropping Without Misleading Yourself

Crops are useful, but they can create false matches. Crop only to test specific clues:

shop sign;
road sign;
building facade;
uniform badge;
vehicle marking;
unique landscape feature;

poster or event banner;
product packaging;
watermark or logo.

Do not crop faces from private individuals for identification unless there is a strong lawful basis and a clear public-interest need. In most defensive training scenarios, faces should be irrelevant and redacted.

8. AI-Generated or Manipulated Image Caution

Image search may not catch AI-generated or heavily manipulated images. Look for:

inconsistent shadows;
warped text;
incorrect reflections;
repeated textures;
strange hands or edges;
unrealistic road markings;
object scale problems;
missing context;
source account with repeated synthetic-looking media.

Do not claim an image is AI-generated based on vibes. Use cautious wording:

The image contains visual inconsistencies that require further verification. No conclusion is made on manipulation from

9. Evidence Table Template

Image ID	Search route	Result found	Date/context	Relevance	Confidence	Notes
IMG31-01	Full reverse search	older news article	2024 flooding article	high	high	same image, earlier use
IMG31-02	Crop of shop sign	map listing found	same visible sign	medium	medium	may support location
IMG31-03	Text search caption	no reliable source	none	low	low	no finding

A good table prevents the report from becoming a pile of screenshots.

10. Safe Report Language

Use:

The image appears to have been used earlier in...
The reviewed source predates the current post.
The caption is not supported by the image evidence reviewed.
The image search produced no verified earlier copy.
The visual match is similar but not sufficient for attribution.

Avoid:

This is definitely fake.
This proves who posted it.
This person lives here.
No search result means the image is original.

Practical Exercise

Use a fictional public image claim: A viral post says this photo shows a power cut in Northbank today. Create a search plan without using a real person. Write the claim, list five image-search routes, design an evidence table, and draft three possible findings: supported, contradicted, and inconclusive.

Visual Brief

V38. Reverse image search workflow board

A dark technical workflow panel showing: starting image → claim split → preserve original → full reverse search → crop searches → text/object searches → earlier-use comparison → evidence table → cautious finding. Include a warning strip: image result = lead, verified source = evidence.

Chapter Checklist

Before moving on, confirm that you can:

- explain the difference between a clue, a source, an observation, and a finding;

- record where an image, map, video, or geolocation clue came from;
- avoid publishing precise personal-location information unnecessarily;
- state confidence levels and limitations clearly;
- preserve enough evidence for another person to follow your reasoning;
- stop the investigation when the legitimate question has been answered.

Chapter 32 - Metadata and File Clues

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, and public-interest OSINT. Do not use these methods to stalk, harass, expose a private home, identify vulnerable people, bypass access controls, trespass, or publish precise location details where disclosure could cause harm. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

Files often carry clues beyond the visible content: filenames, timestamps, dimensions, camera information, editing software, GPS tags, document properties, thumbnails, and compression artefacts. This chapter explains how to handle metadata carefully, what it can tell you, and why it is never enough on its own.

By the end of this chapter, the reader should be able to:

- identify common metadata fields in images, video, PDFs, and documents;
- preserve original files before inspection;
- understand EXIF, XMP, IPTC, file-system timestamps, and embedded thumbnails at a beginner-friendly level;
- avoid overclaiming from metadata that may be missing, stripped, edited, or misleading;
- redact sensitive metadata before sharing reports or training material.

1. Metadata Is Context, Not Truth

Metadata can answer questions such as:

What device or software may have created this file?
Are there GPS coordinates embedded?
When does the file claim it was created or modified?
Is there an embedded thumbnail?
What are the image dimensions and compression details?
Does the filename contain useful context?

Metadata cannot prove:

who took the photo;
whether the device clock was correct;
whether the file has been edited;
whether the GPS tag points to the true scene;
whether a timestamp is genuine;
whether the filename was original.

Treat metadata as one evidence stream to compare against visual, source, timeline, and archive evidence.

2. Preserve Before Inspecting

Create at least three states:

01_ORIGINAL – exact file as received.
02_WORKING_COPY – inspected copy.
03_REDACTED_EXPORT – safe version for report or sharing.

Do not open the only original in editing software that might rewrite metadata. If you need to run tools, run them on the working copy unless your evidence procedure requires read-only inspection of the original.

3. Common Metadata Types

EXIF – camera/device, lens, exposure, timestamp, sometimes GPS.
XMP – editing and descriptive metadata, often from Adobe or content workflows.
IPTC – caption, credit, rights, keywords, newsroom-style fields.
File-system metadata – created/modified/accessed dates on your device; often changes during download or copying.
Document properties – author, title, software, revision details, embedded objects.
Video metadata – codec, frame rate, duration, dimensions, creation time, sometimes device/software tags.
Embedded thumbnails – small preview images that may differ from the main image after editing.

Different platforms strip or rewrite metadata. A social-media download may contain little useful original metadata.

4. Tooling Without Tool Worship

Typical metadata routes:

- ExifTool – command-line inspection and reporting for many file types.
- Operating-system file properties – quick first look, but not complete.
- Image/document viewer properties – useful but limited.
- Forensic or specialist viewers – stronger preservation and reporting if needed.

Record the tool and version if the case is serious:

```
Tool: ExifTool
Version: recorded version
Command/output saved: yes/no
File inspected: working copy path
Date/time: YYYY-MM-DD HH:MM timezone
```

A tool output is not a conclusion. It is a source to interpret.

5. GPS Metadata Handling

GPS fields are sensitive. They can expose homes, workplaces, schools, clinics, and places of worship. Only record precise coordinates when necessary and lawful.

Safer reporting levels:

- Exact coordinate – restricted evidence only; rarely needed in public report.
- Street/block level – only when necessary and safe.
- Town/city level – often enough for verification.
- General region – suitable when precise disclosure creates risk.
- Redacted – use when location is irrelevant.

Safe wording:

The file contains GPS metadata consistent with the Northbank town area. The precise coordinate is omitted because it is

6. Timestamp Caution

Timestamps can be wrong because:

- device clock was wrong;
- time zone was not recorded;
- file was copied or exported;
- editing software rewrote fields;
- platform stripped or changed metadata;
- creator intentionally altered metadata;
- archive/download changed file-system times.

Always record what kind of timestamp you are using:

- EXIF DateTimeOriginal;
- XMP CreateDate;
- file-system modified time;
- webpage visible publication date;
- archive capture date;
- platform post date.

These are not interchangeable.

7. Filename and Folder Clues

Filenames can be useful:

- IMG_20260605_183300.jpg – possible device timestamp pattern.
- Northbank_open_day_final_v3.png – possible project/event clue.
- Screenshot_2026-06-05-19-22-01.png – possible screenshot timestamp.
- DCIM/Camera path – possible mobile-origin clue.

But filenames are easy to rename. Use them as clues only.

8. Embedded Thumbnail Checks

Some edited images keep an old embedded thumbnail. This can reveal:

- cropping;
- redaction failure;

previous version of a document;
rotation/preview mismatch;
editing history clue.

Handle this carefully. If a thumbnail reveals personal information that was meant to be redacted, do not republish it. Record the issue privately and create a safer report version.

9. Metadata Evidence Card

Evidence ID: META32-01
File: working_copy_image_01.jpg
Source: public post download URL
Tool: ExifTool / file properties / viewer
Observation: GPS fields present / no GPS fields found / camera model visible
Timestamp fields: list exact field names
Privacy risk: low / medium / high
Interpretation: clue only; compare with visual map evidence
Confidence: low / medium / high
Redaction decision: exact coordinates omitted from report

This keeps the metadata separate from the interpretation.

10. Redacting Metadata Before Sharing

Before sharing a report, training file, screenshot, or image pack, check for:

GPS coordinates;
device serial numbers;
creator names;
document author fields;
hidden comments;
tracked changes;
embedded thumbnails;
original filenames;
private folder paths;
client names;
internal IDs.

Use a clean exported copy. Never assume a screenshot or PDF automatically removes sensitive metadata.

Practical Exercise

Create a fictional evidence card for a photo named IMG_20260606_142000 . jpg. Assume it contains a visible town sign but no GPS metadata after being uploaded to a social platform. Write what the metadata supports, what it does not support, and what visual/map checks would be needed next.

Visual Brief

V39. Metadata handling and redaction board

A three-column board: Original file, Working copy, Redacted export. Include metadata cards for EXIF, GPS, timestamp, filename, embedded thumbnail, and document properties, with red warning badges for privacy-sensitive fields.

Chapter Checklist

Before moving on, confirm that you can:

- explain the difference between a clue, a source, an observation, and a finding;
- record where an image, map, video, or geolocation clue came from;
- avoid publishing precise personal-location information unnecessarily;
- state confidence levels and limitations clearly;
- preserve enough evidence for another person to follow your reasoning;
- stop the investigation when the legitimate question has been answered.

Chapter 33 - Visual Geolocation Basics

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, and public-interest OSINT. Do not use these methods to stalk, harass, expose a private home, identify vulnerable people, bypass access controls, trespass, or publish precise location details where disclosure could cause harm. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

Visual geolocation is the process of using visible clues in an image or video to narrow down or verify where it was taken. This chapter teaches a careful, non-invasive method based on public scenes, landmarks, environmental clues, and evidence discipline.

By the end of this chapter, the reader should be able to:

- extract visible location clues without jumping to conclusions;
- separate unique clues from generic clues;
- build a geolocation hypothesis table;
- use maps and imagery safely and proportionately;
- avoid exposing private addresses or sensitive sites.

1. The Geolocation Rule

A location finding is not made from one clue. It is made from a pattern of independent clues that fit better than reasonable alternatives.

Weak clue:

The road has yellow lines.

Stronger clue:

The image shows a distinctive church tower, a named shop sign, a one-way road layout, a bus stop code, and a hill profile.

Even then, report confidence and limitations.

2. Start With a Clue Inventory

Do not open maps first. Look carefully at the image first and list what is visible.

Signs: road names, shop signs, adverts, warning boards.
Transport: bus stops, taxi colours, road markings, rails, cycle lanes.
Architecture: brick style, rooflines, balconies, shopfronts, church towers.
Landscape: hills, coast, rivers, fields, mountains, tree species.
Utilities: power poles, streetlights, bins, post boxes, road signs.
Language: alphabet, spelling, accents, local terms.
Weather/season: snow, leaves, wet road, clothing.
People/vehicles: avoid identifying private people unless necessary; focus on environmental clues.

Mark each clue as unique, common, or uncertain.

3. Unique vs Generic Clues

Unique clue: named business, landmark, road junction layout, public sculpture, station sign.
Semi-unique clue: chain shop beside a distinctive building, bus route number, regional road sign style.
Generic clue: brick wall, white van, traffic light, cloudy sky.

Generic clues are not useless. They help eliminate impossible locations, but they rarely prove a location.

4. Build Hypotheses

Use a table before deciding.

Hypothesis | Supporting clues | Contradicting clues | Missing checks | Confidence
H1: Northbank High Street | shop sign, road layout, clock tower | bus stop colour uncertain | street view match | medium
H2: Westport Market Road | similar clock tower | shop sign does not match | check archives | low
H3: Generic UK town | road signs only | too broad | find named clue | low

This prevents tunnel vision.

5. The Match Standard

A good geolocation match should include several of these:

- same landmark shape;
- same building alignment;
- same road geometry;
- same sign position;
- same window/door pattern;
- same skyline/horizon;
- same street furniture;
- same relative object positions;
- same direction of view;
- same public-source date range.

One matching sign is useful. A full spatial match is stronger.

6. Do Not Over-Disclose

Geolocation can create real harm. Avoid publishing exact locations for:

- private homes;
- schools and children;
- domestic abuse shelters;
- medical or mental-health settings;
- religious minority sites under threat;
- refugee or protester locations;
- current live positions;
- private vehicles tied to individuals;
- vulnerable people.

You can often report the conclusion at a safer level:

The image is consistent with a public high-street location in Northbank town centre. The precise viewpoint is withheld.

7. Direction of View

Once you have a likely spot, estimate where the camera stood and which direction it faced.

Ask:

- What is in foreground, middle ground, background?
- Which objects appear left/right of each other?
- Are signs facing the camera or facing away?
- Which side of the road is visible?
- Can the horizon or shadows indicate direction?

Draw a simple arrow on a map screenshot for your private notes. Redact or generalise it in public reporting if necessary.

8. Avoid the Single-Tool Trap

Map databases, street-level imagery, satellite images, and user-contributed photos differ in age and coverage. If a shop sign is missing from street view, it may mean:

- the imagery is old;
- the shop changed names;
- the sign is hidden by angle;
- the database has incomplete coverage;
- you are in the wrong place.

Check more than one source where possible.

9. Geolocation Evidence Log

Clue ID	Visible clue	Possible meaning	Source checked	Supports	Contradicts	Confidence
G33-01	station sign partially visible	rail station nearby	map/street view	H1	none yet	medium
G33-02	red brick clock tower	landmark	image search/map photos	H1/H2	no exact match yet	low
G33-03	bus stop code NBK012	local transport stop	public transport map	H1	H2	high

Good notes make the reasoning reviewable.

10. Safe Finding Language

Use:

The visible clues are consistent with...
The strongest match found is...
The match is based on the following visible public features...
The precise point is withheld/redacted.
No confident location finding is made.

Avoid:

This is definitely where they live.
Go there and check.
The person must be from this town.
The location is proven because one sign matched.

Practical Exercise

Use a fictional photo of a public town square. List ten possible visible clues, classify each as unique/semi-unique/generic, and create three location hypotheses with supporting and contradicting evidence columns.

Visual Brief

V40. Visual geolocation clue board

A board showing an image divided into clue zones: signs, architecture, transport, landscape, language, weather, and direction of view. Include a hypothesis table and a privacy/redaction shield.

Chapter Checklist

Before moving on, confirm that you can:

- explain the difference between a clue, a source, an observation, and a finding;
- record where an image, map, video, or geolocation clue came from;
- avoid publishing precise personal-location information unnecessarily;
- state confidence levels and limitations clearly;
- preserve enough evidence for another person to follow your reasoning;
- stop the investigation when the legitimate question has been answered.

Chapter 34 - Maps, Satellite View, and Street-Level Clues

***Safety and lawful-use note:** This chapter is for defensive, educational, journalistic, verification, safety, and public-interest OSINT. Do not use these methods to stalk, harass, expose a private home, identify vulnerable people, bypass access controls, trespass, or publish precise location details where disclosure could cause harm. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, and stop when the task no longer has a legitimate purpose.*

Purpose of This Chapter

Maps and imagery help test geolocation hypotheses, but each source has gaps, dates, permissions, and distortions. This chapter teaches how to compare map, satellite, and street-level sources without pretending they are live truth.

By the end of this chapter, the reader should be able to:

- use maps and imagery to test a location hypothesis;
- compare road layout, building footprint, street furniture, and skyline clues;
- check imagery dates and source limitations;
- capture map evidence safely;
- avoid relying on a single map layer or outdated street view.

1. Maps Are Evidence Sources, Not Reality Itself

A map is a representation. It may be old, incomplete, simplified, or wrong. Satellite imagery may be months or years old. Street-level imagery may show an earlier tenant, road layout, building facade, or season.

Record:

```
map source;  
layer used;  
imagery date if visible;  
URL or coordinates if safe;  
date you captured it;  
what exactly it supports;  
what it does not support.
```

2. Map Layers to Compare

```
Standard map: road names, businesses, transit stops, public buildings.  
Satellite imagery: roof shape, fields, coastline, large buildings, road geometry.  
Street-level imagery: facades, signs, street furniture, lane markings.  
Terrain/topographic layer: hills, slopes, ridgelines, valleys.  
Transport layer: rail, bus, metro, stations, stops.  
Historic imagery/archives: changed buildings, older signs, previous events.  
User photos: landmarks and angles not covered by street-level imagery.
```

No layer is enough alone. Use them together.

3. Road Layout Matching

Road geometry is often more reliable than shop names because shops change.

Compare:

```
junction shape;  
one-way direction;  
traffic islands;  
pedestrian crossings;  
cycle lanes;  
roundabouts;  
kerb shape;  
parking bays;  
rail crossings;
```


bridge/underpass layout.

A matching road layout plus matching building position is stronger than a matching shop sign alone.

4. Building Footprints and Facades

Look for:

- window counts;
- door positions;
- roofline;
- chimneys;
- balconies;
- shopfront widths;
- brick/stone style;
- building height;
- corner shape;
- setback from street;
- adjacent alleyways.

Do not use private-home details unless necessary. When verifying a public image, you often only need public frontage and street layout.

5. Street Furniture

Street furniture can be highly local:

- lamp posts;
- traffic-light style;
- bollards;
- bus shelters;
- post boxes;
- benches;
- waste bins;
- public notice boards;
- cycle racks;
- parking meters;
- road signs.

These can change, so check imagery dates. A missing bin or changed sign may not disprove a location.

6. Imagery Date Problems

Before treating a mismatch as meaningful, ask:

- Is the street-level image older than the claimed event?
- Is the satellite image from a different season?
- Has the building been renovated?
- Did roadworks change the view?
- Did a temporary sign/event structure appear only briefly?
- Could the image be from another angle not covered by street view?

Record date uncertainty in the report.

7. Coordinate Handling

Coordinates are powerful and sensitive. In private notes, exact coordinates may help reproduce analysis. In public reports, generalise when exact disclosure is unnecessary.

- Private evidence note: exact coordinate or map pin, restricted.
- Working report: town centre / public station entrance / approximate area.
- Public release: avoid precise private locations and sensitive live positions.

If the purpose is to debunk a false public claim, you often need only prove “not here” or “older image from elsewhere”, not publish a precise point.

8. Map Evidence Capture

A clean map evidence capture should include:

- source/layer;
- visible scale;
- north arrow or orientation where available;
- imagery date if available;
- annotation showing matched features;
- redactions for private homes/vehicles/people if needed;
- brief text explaining why the map matters.

Do not overload screenshots with messy arrows. Use numbered callouts and a separate legend.

9. Map Comparison Table

Feature	Image observation	Map/street-level observation	Match?	Notes
Clock tower	behind shop, left of road	visible left of road from candidate viewpoint	yes	strong
Crossing	zebra crossing before junction	present in current map	yes	medium
Bus shelter	glass shelter right side	older street view shows no shelter	partial	imagery may predate shelter
Hillline	rising ground behind town	terrain layer supports	yes	medium

This table makes the comparison transparent.

10. When to Say “No Finding”

Say no finding when:

- clues are too generic;
- map coverage is weak;
- several places fit equally well;
- private-location risk outweighs benefit;
- the evidence only supports a broad region;
- the relevant imagery is too old or unavailable.

A responsible no-finding is better than an exciting false match.

Practical Exercise

Create a fictional map-comparison table for a public station photo. Include at least six features: road layout, building facade, station sign, bus stop, crossing, and skyline. Mark which are strong, medium, or weak matches.

Visual Brief

V41. Map and street-level comparison panel

A split-screen visual: left side public photo clue callouts, right side map/satellite/street-view panels. Include an imagery-date label, scale/orientation tag, and a match table underneath.

Chapter Checklist

Before moving on, confirm that you can:

- explain the difference between a clue, a source, an observation, and a finding;
- record where an image, map, video, or geolocation clue came from;
- avoid publishing precise personal-location information unnecessarily;
- state confidence levels and limitations clearly;
- preserve enough evidence for another person to follow your reasoning;
- stop the investigation when the legitimate question has been answered.

Chapter 35 - Weather, Sun, Shadow, and Time Clues

***Safety and lawful-use note:** This chapter is for defensive, educational, journalistic, verification, safety, and public-interest OSINT. Do not use these methods to stalk, harass, expose a private home, identify vulnerable people, bypass access controls, trespass, or publish precise location details where disclosure could cause harm. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, and stop when the task no longer has a legitimate purpose.*

Purpose of This Chapter

Time is often the hardest part of image and video verification. Weather, sunlight, shadows, clothing, vegetation, and environmental conditions can support or contradict a claimed date or time, but they must be handled carefully. This chapter introduces safe, beginner-friendly temporal clues.

By the end of this chapter, the reader should be able to:

- use weather and daylight as supporting evidence, not standalone proof;
- understand basic shadow direction and sun-angle reasoning;
- compare visible weather with public weather records;
- identify seasonal clues and limitations;
- write cautious time-related findings.

1. Time Clues Are Usually Supportive, Not Decisive

A wet road does not prove it rained at the claimed time. A long shadow does not prove a precise hour without location, date, and camera geometry. A winter coat does not prove winter.

Time clues become useful when they align with other evidence:

visible event banner;
archive/post date;
weather records;
sun direction;
seasonal vegetation;
news reporting;
transport timetable;
public event schedule.

2. Weather Clues

Visible clues:

rain, puddles, wet roads;
snow or ice;
fog or haze;
cloud type;
wind direction from flags, smoke, waves, trees;
shadows or lack of shadows;
clothing and umbrellas;
seasonal leaves/blossom;
floodwater or drought conditions.

Weather records can support or contradict a claim, but local conditions vary. A weather station may be miles away.

3. Weather Evidence Table

Claimed place/time: Northbank Square, 6 June 2026, 14:00
Visible clue: strong sunlight, dry road, short shadows
Weather source: nearest public station / official weather archive / local forecast archive
Record: rain reported 13:00–15:00 at station 18km away
Assessment: possible contradiction, but station distance and local variation limit confidence

Never say “impossible” unless the evidence truly excludes it.

4. Basic Shadow Reasoning

Shadows can help estimate direction and broad time window.

Ask:

- Where is the shadow falling?
- Which way is north in the candidate location?
- Is the sun likely east, south, or west at that time and latitude?
- Are shadows long or short?
- Is the ground level or sloped?
- Are there reflections or artificial lights confusing the scene?

Use this to test a location/time hypothesis, not to over-precision a conclusion.

5. Sun and Shadow Tools

Sun-position tools can estimate sun azimuth and elevation for a date, time, and location. Use them responsibly:

- Input candidate location and date.
- Compare predicted sun direction with visible shadows.
- Record the tool/source and settings.
- Treat results as support, not proof.
- Check whether the image may be mirrored, rotated, or cropped.

A rough match can strengthen a hypothesis. A strong mismatch can challenge it.

6. Seasonal Clues

Seasonal clues include:

- leaf cover;
- flowering trees;
- snow;
- holiday decorations;
- school uniforms or event clothing;
- market stalls;
- advertising posters;
- sports season banners;
- roadworks schedules;
- festival signage.

Seasonal clues can narrow a window but may also mislead. Decorations remain after events; old posters stay up; weather can be unusual.

7. Reflections and Light Sources

Check for:

- reflections in windows;
- vehicle glass;
- wet pavement;
- artificial lighting;
- multiple light sources;
- indoor/outdoor mixed scenes;
- shadows cast by signs or overhead structures.

False shadow interpretation is common. If the scene is complex, say the shadow evidence is inconclusive.

8. Time Zones and Publication Times

Post times are not always local scene times. Record:

- platform timestamp;
- time zone shown by platform;
- your local capture time;
- claimed local event time;
- source publication time;
- archive capture time;
- metadata timestamp if any.

Convert carefully. For cross-border events, errors of one or more hours are common.

9. Temporal Finding Wording

Use:

The weather evidence is consistent with the claimed date but does not independently prove it.
The visible shadows appear broadly consistent with a morning/evening scene at the candidate location.
The weather record creates a possible contradiction that requires further checking.
The reviewed evidence does not allow a precise time finding.

Avoid:

The shadow proves it was exactly 3:12pm.
The photo cannot be real because it rained nearby.
The metadata timestamp is the event time.

10. Time-Clue Checklist

Location hypothesis established? yes/no
Claimed date/time recorded? yes/no
Weather clues listed? yes/no
Nearest reliable weather source recorded? yes/no
Shadow direction compared? yes/no
Seasonal clues checked? yes/no
Timezone noted? yes/no
Alternative explanations listed? yes/no
Confidence assigned? yes/no

Practical Exercise

Take a fictional claim: This image shows Northbank Pier during the storm at 08:00 yesterday. Build a time-verification table using weather, shadows, clothing, sea state, post time, and archive/event sources. Write one cautious finding and one limitation.

Visual Brief

V42. Weather and shadow time-check board

A board with weather clues, sun/shadow direction, seasonal indicators, timezone conversion, and a time-confidence meter. Include a caution: time clues support or challenge, they rarely prove alone.

Chapter Checklist

Before moving on, confirm that you can:

- explain the difference between a clue, a source, an observation, and a finding;
- record where an image, map, video, or geolocation clue came from;
- avoid publishing precise personal-location information unnecessarily;
- state confidence levels and limitations clearly;
- preserve enough evidence for another person to follow your reasoning;
- stop the investigation when the legitimate question has been answered.

Chapter 36 - Transport, Buildings, Signs, and Language Clues

***Safety and lawful-use note:** This chapter is for defensive, educational, journalistic, verification, safety, and public-interest OSINT. Do not use these methods to stalk, harass, expose a private home, identify vulnerable people, bypass access controls, trespass, or publish precise location details where disclosure could cause harm. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, and stop when the task no longer has a legitimate purpose.*

Purpose of This Chapter

Some of the strongest geolocation clues are ordinary things people overlook: bus stops, road signs, building styles, public notices, bins, shopfronts, number formats, alphabets, and local language. This chapter teaches how to catalogue these clues safely and test them without over-identifying people.

By the end of this chapter, the reader should be able to:

- recognise transport, signage, architecture, and language clues;
- use clue categories to narrow location hypotheses;
- avoid false confidence from generic regional features;
- treat vehicle and personal identifiers with care;
- turn environmental details into evidence cards.

1. Everyday Details Matter

A dramatic landmark is useful, but many images do not include one. Instead, look for mundane details:

road signs;
bus stop codes;
train station furniture;
lane markings;
parking meters;
shopfront rules;
recycling bins;
public health posters;
language and spelling;
phone-number formats;
license-plate style without recording private plates;
architecture and rooflines.

The goal is not to identify private individuals. The goal is to test the public scene.

2. Transport Clues

Transport clues can include:

bus route number;
stop name/code;
rail station signs;
taxi colours/licensing marks;
road side driven on;
lane markings;
cycle-lane design;
tram/metro signage;
airport or port signs;
traffic-light style;
parking restrictions.

When vehicles are visible, avoid publishing full number plates unless there is a lawful reason. In most OSINT workbook examples, plates should be redacted.

3. Building and Architecture Clues

Architecture can narrow a region:

- brick colour and bond;
- stone type;
- roof pitch;
- balconies;
- shutters;
- shopfront proportions;
- building height;
- fire escapes;
- window style;
- public housing design;
- religious/civic architecture;
- coastal or mountain construction styles.

Be careful. Similar styles appear in many places, and old buildings can be moved, copied, or renovated.

4. Signs and Public Notices

Look for:

- road names;
- parking conditions;
- public safety notices;
- planning notices;
- health warnings;
- littering fines;
- election posters;
- event banners;
- shop opening hours;
- QR codes;
- regulatory logos;
- local council names.

Even partial text can be searched carefully. Record exactly what is visible and what is inferred.

5. Language and Writing Systems

Language clues include:

- alphabet/script;
- spelling conventions;
- road-sign terminology;
- currency symbols;
- phone prefixes;
- domain endings on posters;
- local place-name suffixes;
- bilingual signs;
- accents/diacritics;
- units of measurement.

A language does not always equal a country. Tourist areas, embassies, border regions, and minority-language areas can mislead.

6. Numbers and Codes

Codes can be powerful:

- bus stop ID;
- postal code format;
- phone number format;
- road route number;
- rail platform sign;
- business registration number;
- planning notice reference;
- parking zone code;
- public asset number on street furniture.

Do not publish codes that tie directly to private individuals or sensitive assets unless necessary.

7. The Clue Stack

A reliable environmental match uses a stack:

- Country/region indicators: road side, signs, language.
- Town/city indicators: transit routes, local authority, road names.

Street/area indicators: shop signs, building alignment, bus stop IDs.
Viewpoint indicators: facade angles, road geometry, foreground/background order.
Time indicators: weather, shadows, event posters, construction state.

Each layer narrows the search. Each layer should have evidence.

8. Avoiding Cultural Stereotyping

Do not make claims like:

This looks Eastern European.
This person looks local.
That architecture means X country.
The language proves nationality.

Use observable details instead:

The sign uses the Cyrillic alphabet.
The road sign design resembles the public road-sign standard used in...
The phone number format begins with...
The bus stop code appears in the public transport database for...

9. Environmental Clue Evidence Card

Clue ID: ENV36-01
Category: transport/sign/building/language
Visible observation: exact visible clue
Search/source used: map, official transit page, image search, public register
What it supports: location hypothesis / time hypothesis / source context
Alternative explanations: tourist sign, reused image, old imagery, generic design
Confidence: low/medium/high
Privacy action: plate/faces/redacted/not applicable

10. Reporting Environmental Clues

Good wording:

The visible bus stop code matches a public stop in Northbank town centre.
The shopfront and adjacent building pattern are consistent with the candidate street-level imagery.
The language clue narrows the likely region but does not identify a specific country by itself.

Poor wording:

The people must be from there.
The vehicle plate proves the owner was there.
This architecture is obviously from one country.

Practical Exercise

Create a clue stack for a fictional street image: transport, buildings, signs, language, numbers/codes, and privacy risks.
For each clue, write what it might support and one alternative explanation.

Visual Brief

V43. Environmental clue stack

Layered visual stack showing region, town, street, viewpoint, and time clues. Add icons for transport, buildings, signs, language, and numbers, plus redaction masks over faces and number plates.

Chapter Checklist

Before moving on, confirm that you can:

- explain the difference between a clue, a source, an observation, and a finding;
- record where an image, map, video, or geolocation clue came from;
- avoid publishing precise personal-location information unnecessarily;
- state confidence levels and limitations clearly;
- preserve enough evidence for another person to follow your reasoning;

- stop the investigation when the legitimate question has been answered.

Chapter 37 - Video Verification

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, and public-interest OSINT. Do not use these methods to stalk, harass, expose a private home, identify vulnerable people, bypass access controls, trespass, or publish precise location details where disclosure could cause harm. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

Video feels persuasive because it moves and sounds real, but it can be old, clipped, mirrored, edited, AI-generated, miscaptioned, or presented without context. This chapter teaches a safe workflow for verifying videos using frames, audio clues, metadata clues, source history, and timeline checks.

By the end of this chapter, the reader should be able to:

- turn a video into verifiable frames and observations;
- separate upload context from scene context;
- check for earlier uploads, cuts, edits, and mirrored footage;
- use audio and sequence clues carefully;
- report video findings with confidence and limitations.

1. Video Is Multiple Evidence Streams

A video contains:

visual frames;
audio;
captions/subtitles;
platform metadata;
filename/container metadata;
upload account history;
comments/reposts;
scene sequence;
compression and edit artefacts.

Each stream can support or contradict the claim. Do not rely on one frame or the uploader's caption alone.

2. Preserve the Starting Video

Record:

Video ID: VID37-01
Source URL/account/page: public link
Visible caption: exact wording
Upload date/time/timezone if visible
Duration and resolution
Filename if downloaded lawfully
Hash if using evidence hashing
Date captured by you
Redaction needs: faces, number plates, private interiors, children

If you are not authorised to download, capture permitted screenshots/notes and use platform-visible information only.

3. Extract Key Frames

Do not analyse every frame manually. Extract key moments:

opening frame;
clearest sign/landmark frame;
clearest transport/building frame;
frame with shadows/weather;
frame with event banner or clock;
frame before/after a cut;
frame with audio-relevant event;
ending frame.

Name them clearly:

VID37-01_frame_0005_sign.jpg
VID37-01_frame_0018_station.jpg
VID37-01_frame_0042_shadow.jpg

Redact as needed for reports.

4. Reverse Search Frames, Not Just Thumbnails

A thumbnail may be custom or misleading. Search several frames:

full frame reverse search;
cropped landmark frame;
cropped sign/text frame;
cropped unique object frame;
caption text search;
quoted phrases from subtitles/comments.

If an older upload is found, compare duration, sequence, cropping, audio, and caption.

5. Audio Clues

Audio can reveal or mislead:

language;
public announcements;
sirens;
train/bus announcements;
church bells/call to prayer;
stadium chants;
weather/wind;
music overlay;
edits/cuts;
sync mismatch.

Do not identify private people by voice unless there is a lawful, strong reason. For training, focus on environmental and public context.

6. Edit and Sequence Checks

Look for:

abrupt cuts;
missing context before/after event;
inconsistent lighting;
changed audio ambience;
jump in camera position;
mirrored signs/text;
overlaid captions;
watermarks from earlier platforms;
compression mismatch;
reused news footage.

A cut does not mean deception. It means the video is edited and context needs checking.

7. Platform Context

Record public uploader context cautiously:

Is the uploader original source or repost account?
Does the account frequently repost viral clips?
Are there watermarks from another platform?
Do comments point to an earlier source?
Is there an official event/source account?
Does the upload time match the claimed event timeline?

Do not brigade, contact, harass, or expose uploaders.

8. Timeline the Video

Create a mini timeline:

00:00 – camera facing station entrance; sign visible.
00:07 – crowd moves toward road; siren heard.
00:14 – cut; camera angle changes.
00:21 – banner visible: Northbank Fair.
00:36 – clip ends before claimed incident.

Then compare to public event schedules, news reports, weather, and other videos.

9. Video Evidence Table

Frame/time	Observation	Source/check	Supports	Limits	Confidence
00:05	station sign visible	map/street view	location H1	old imagery	high
00:14	abrupt cut	visual review	context gap	not proof of manipulation	medium
00:21	event banner	public event page	date range	banner could remain	medium

This is more useful than a vague statement that the video “looks real”.

10. Safe Video Findings

Use:

The reviewed frames are consistent with...
The video appears to be a repost because...
An earlier upload predates the current claim.
The clip is edited; the missing context limits what can be concluded.
The video supports location but not the claimed cause of the event.

Avoid:

This video proves everything.
The uploader is lying.
The people shown are guilty.
The voice identifies the person.

Practical Exercise

Use a fictional 45-second public event video. Build a key-frame list, a timeline, a frame-search plan, and a cautious finding that distinguishes location, date, and event context.

Visual Brief

V44. Video verification timeline

A horizontal video timeline with key frames, cut markers, audio clues, reverse-frame-search icons, and evidence table rows. Add warning labels: clip context may be incomplete; uploader context is not scene truth.

Chapter Checklist

Before moving on, confirm that you can:

- explain the difference between a clue, a source, an observation, and a finding;
- record where an image, map, video, or geolocation clue came from;
- avoid publishing precise personal-location information unnecessarily;
- state confidence levels and limitations clearly;
- preserve enough evidence for another person to follow your reasoning;
- stop the investigation when the legitimate question has been answered.

Technical Note on Video Metadata Stripping

Researchers must account for the platform transmission variable when evaluating video or image assets. Major public social platforms aggressively strip all embedded EXIF, XMP, and device metadata upon video upload. A defensive researcher should not expect to extract device serial numbers or capture coordinates from an uploaded file stream unless the asset is acquired as a raw binary download directly from a primary self-hosted portal or independent local system.

Chapter 38 - Event Verification

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, and public-interest OSINT. Do not use these methods to stalk, harass, expose a private home, identify vulnerable people, bypass access controls, trespass, or publish precise location details where disclosure could cause harm. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

Event verification asks whether a claimed thing happened, where it happened, when it happened, and what public evidence supports or contradicts it. This chapter combines image, video, maps, weather, social posts, official statements, and news sources into one disciplined workflow.

By the end of this chapter, the reader should be able to:

- separate event, location, time, actor, and cause claims;
- build a timeline from independent public sources;
- compare official, media, eyewitness, and platform sources;
- avoid amplifying rumours or exposing private people;
- write event findings that are useful without being reckless.

1. Split the Event Claim

A typical viral claim contains several claims:

“A fire broke out at Northbank Market today after an electric scooter exploded.”

Split it:

Event claim: there was a fire.
Location claim: Northbank Market.
Time claim: today.
Cause claim: electric scooter explosion.
Impact claim: damage/injuries/evacuation.
Actor claim: who was involved.
Source claim: who first reported it.

You may verify some parts and leave others unresolved.

2. Source Families for Event Verification

Official sources: fire service, police, council, transport operator, emergency alerts.
News sources: local reputable media, wire services, specialist outlets.
Platform sources: public eyewitness posts, videos, photos, reposts.
Open data: traffic, transit disruptions, weather, aviation/marine if relevant.
Archives: archived pages, cached public statements, deleted post captures if lawful.
Maps/geolocation: public scene verification.
Time evidence: metadata, post times, weather, shadows, schedules.

Treat official sources as strong for official statements, not as automatically complete truth about every detail.

3. Build a Timeline

Time	Source	Observation	Claim supported	Confidence	Notes
13:04	public video	smoke visible near market	event/location	medium	geolocation pending
13:11	fire service post	crews attending Market Road	event/location	high	official source
13:18	transport alert	buses diverted near market	impact/location	high	independent support
13:45	local news	reports fire under control	event/time	medium/high	cites fire service
14:20	viral post	claims scooter caused fire	cause	low	no source provided

The timeline should show what is known, not just the most dramatic claim.

4. Eyewitness Posts as Leads

Public eyewitness posts can be valuable, but they are not automatically reliable. Record:

- was the post original or a repost?
- does it contain original media?
- does the media geolocate to the event area?
- does the timestamp fit?
- does the poster claim to be present?
- are there edits, deletions, or changed captions?
- can the key claim be confirmed independently?

Do not contact eyewitnesses unless authorised and necessary.

5. Cause Claims Need Extra Caution

Cause is usually harder than event/location/time.

You may confirm:

- there was a fire;
- crews attended;
- road was closed;
- video is from that street;
- post predates later reposts.

But not confirm:

- who caused it;
- what object started it;
- whether someone acted intentionally;
- whether injuries occurred;
- whether a rumour is true.

Use “cause not established by reviewed sources” when appropriate.

6. Contradictions Are Useful

Contradictions can reveal false claims or simply uncertainty.

- One video says 11:00; official post says crews called at 13:10.
- A photo appears older than the claimed event.
- A map match shows a different town.
- Weather does not match the claimed day.
- Two posts use the same video for different events.

Record contradictions instead of hiding them.

7. Do Not Amplify Harm

Avoid publishing:

- unverified names of injured/deceased people;
- faces of victims or minors;
- private addresses;
- vehicle plates tied to private individuals;
- rumoured suspect names;
- precise live emergency locations if response is ongoing;
- unverified cause claims framed as fact.

If the event is active, safety comes before completeness.

8. Event Verification Matrix

Claim part	Evidence found	Independent support	Contradiction	Finding	Confidence
Event happened	official fire post + video	transport diversion	none	supported	high
Location	geolocated video + official road	map match	none	supported	high
Time	official timestamp + video post	local news	timezone unclear	broadly supported	medium/high
Cause	viral caption only	none	official source silent	not established	low
Impact	bus diversion	no injury source	rumours online	limited finding	medium

This keeps the report balanced.

9. Event Report Language

Use:

The reviewed evidence supports that an incident occurred at...

The location is supported by official reporting and visual geolocation.
The cause claimed in viral posts is not established by reviewed sources.
The available evidence supports a broad time window of...
No finding is made on individual responsibility.

Avoid:

The internet says...
Everyone knows...
The video proves the cause.
The person in the clip did it.

10. Active Event Stop Points

Stop or escalate when:

there is an immediate safety risk;
private/vulnerable people are being identified;
a law-enforcement/emergency response is ongoing;
you are tempted to publish precise live coordinates;
your evidence is too weak but rumours are spreading;
the matter requires professional/legal escalation.

Defensive OSINT should reduce harm, not create it.

Practical Exercise

Use a fictional public claim about a market fire. Split the claim into event, location, time, cause, and impact. Build a five-row event verification matrix and write a finding that confirms only what the evidence supports.

Visual Brief

V45. Event verification matrix

A central event claim split into event/location/time/cause/impact, connected to official sources, public media, maps, weather, and timeline. Include a red caution strip: cause and actor claims require extra evidence.

Chapter Checklist

Before moving on, confirm that you can:

- explain the difference between a clue, a source, an observation, and a finding;
- record where an image, map, video, or geolocation clue came from;
- avoid publishing precise personal-location information unnecessarily;
- state confidence levels and limitations clearly;
- preserve enough evidence for another person to follow your reasoning;
- stop the investigation when the legitimate question has been answered.

Chapter 39 - Geolocation Reporting

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, and public-interest OSINT. Do not use these methods to stalk, harass, expose a private home, identify vulnerable people, bypass access controls, trespass, or publish precise location details where disclosure could cause harm. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

A geolocation report must explain how the location finding was reached without exposing unnecessary sensitive details. This chapter gives a safe structure for reporting image, video, map, weather, and event findings with confidence levels, limitations, redactions, and privacy controls.

By the end of this chapter, the reader should be able to:

- structure a geolocation report clearly;
- present visual evidence with callouts and source references;
- write confidence and limitation statements;
- redact private and sensitive details;
- distinguish internal evidence packs from public summaries.

1. Reporting Is Part of the Investigation

A location finding that cannot be explained is not useful. A report should allow another responsible person to understand:

what was asked;
what was reviewed;
what was found;
what was not found;
how the conclusion was reached;
what level of confidence is justified;
what privacy protections were applied.

Do not include every screenshot just because you collected it. Include what supports the finding.

2. Report Structure

Recommended structure:

1. Executive summary.
2. Research question.
3. Scope and exclusions.
4. Source list and method.
5. Key visual observations.
6. Map/street-level comparison.
7. Time/weather checks if relevant.
8. Findings and confidence.
9. Limitations and alternatives.
10. Redaction/privacy note.
11. Evidence appendix.

For public-facing work, use a shorter version with sensitive details removed.

3. Executive Summary

Example:

The reviewed public image is consistent with a public street scene in Northbank town centre, not the claimed location of

The summary should state what matters, not show off the investigation.

4. Visual Callouts

When showing an image, use numbered callouts:

1. Civic clock tower profile.
2. Bus stop code visible on sign.
3. Distinctive corner building facade.
4. Zebra crossing position.
5. Road bends left behind foreground shop.

Then provide a table matching those callouts to map/street-level evidence. Redact faces, plates, private interiors, and unrelated personal details.

5. Confidence Levels

Use simple levels:

- High – multiple independent clues match; reasonable alternatives checked.
- Medium – several clues match but some uncertainty remains.
- Low – clue pattern is weak, generic, or not independently confirmed.
- No finding – evidence is insufficient or privacy risk outweighs benefit.

Confidence is not a mood. It should be justified by evidence.

6. Limitations Section

Always include limitations:

- Street-level imagery date predates the claimed event by two years.
- Weather source is from a station 18km away.
- The image is cropped and lacks a visible full skyline.
- No original file metadata was available.
- Only public sources were reviewed.
- No private or restricted data was accessed.

Limitations protect the reader from over-interpreting the report.

7. Redaction and Sensitive Detail

Redact or generalise:

- faces of private people;
- children;
- vehicle plates;
- house numbers;
- private doorways/interiors;
- GPS coordinates;
- live locations;
- medical/school/shelter details;
- unrelated social handles;
- phone numbers or emails in posters if not needed.

Use the least precise location that answers the question.

8. Internal vs Public Reports

Internal evidence pack may contain:

- full-resolution originals;
- exact coordinates;
- private notes;
- unredacted captures;
- tool outputs;
- hash logs;
- working hypotheses.

Public report should contain:

- necessary evidence only;
- redacted images;
- generalised coordinates where appropriate;
- clear findings;
- limitations;
- no unnecessary personal data.

9. Geolocation Finding Template

Finding: The image is most consistent with [general location].
Confidence: High / Medium / Low / No finding.
Basis: [list 3-6 strongest matched public features].
Contradictions checked: [list].
Limitations: [list].
Privacy handling: [what was redacted or withheld].

Example:

Finding: The image is most consistent with Northbank Market Street. Confidence is medium/high. This is based on the vis:

10. Quality-Control Questions

Before finalising, ask:

Can another person follow the reasoning?
Are the strongest clues shown clearly?
Have alternatives been considered?
Are any sensitive details unnecessary?
Have exact coordinates been justified or removed?
Are confidence and limitations plain?
Is the report useful without being harmful?

If any answer is weak, revise before sharing.

Practical Exercise

Draft a one-page fictional geolocation report summary for a public image that is miscaptioned as Westport but actually matches Northbank. Include scope, finding, basis, confidence, limitations, and redaction note.

Visual Brief

V46. Geolocation report anatomy

A clean report layout showing executive summary, callout image, comparison table, confidence meter, limitation box, and redaction/privacy footer.

Chapter Checklist

Before moving on, confirm that you can:

- explain the difference between a clue, a source, an observation, and a finding;
- record where an image, map, video, or geolocation clue came from;
- avoid publishing precise personal-location information unnecessarily;
- state confidence levels and limitations clearly;
- preserve enough evidence for another person to follow your reasoning;
- stop the investigation when the legitimate question has been answered.

Chapter 40 - Geolocation Case Study

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, and public-interest OSINT. Do not use these methods to stalk, harass, expose a private home, identify vulnerable people, bypass access controls, trespass, or publish precise location details where disclosure could cause harm. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter closes Volume 4 with a full fictional case study. It combines reverse image search, metadata caution, visual geolocation, maps, weather, video verification, event verification, and reporting into one safe workflow. The scenario is designed to verify a public claim without targeting private people or exposing sensitive locations.

By the end of this chapter, the reader should be able to:

- run a complete image/video geolocation workflow;
- build a clue inventory and hypothesis table;
- compare maps, imagery, weather, and event evidence;
- write a balanced finding with limitations;
- prepare a redacted report suitable for safe sharing.

1. Fictional Scenario

A public post claims:

“Breaking: crowd panic at Westport Pier today after a drone crash. This photo and video prove it.”

The post includes:

one still image of a crowd near a waterfront;
one 28-second video clip with sirens in the background;
a caption claiming Westport Pier;
a claim that the footage is from today;
a claim that a drone crash caused the panic.

The task is to verify the public claim safely. The task is not to identify private people in the crowd or publish exact live coordinates.

2. Research Question

Do the public image and video support the claim that a drone-related crowd panic occurred at Westport Pier today?

Sub-questions:

Where does the image/video appear to have been taken?
When might it have been taken?
Is there evidence of a drone crash?
Is the footage original or reused?
What can be reported without exposing private people?

3. Scope and Exclusions

Included:

public post and visible caption;
public reverse image searches;
key frames from the public video;
public map/street-level/satellite comparison;
public weather records;
public local event/news/official sources;
public transport or emergency notices if available;
redacted screenshots for reporting.

Excluded:

identifying private crowd members;
collecting faces or vehicle plates;
contacting uploaders or witnesses;
using private groups or restricted data;
publishing exact live coordinates;
claiming cause without independent evidence;
tracking drones/operators/individuals.

4. Starting Evidence Log

Evidence ID	Source	Observation	Privacy risk	Action
CASE40-01	public post	caption claims Westport Pier today	medium	capture URL/date; redact handles in public report
CASE40-02	attached image	crowd/waterfront/buildings visible	high for faces	preserve; create redacted working copy
CASE40-03	video clip	28 seconds, sirens, crowd movement	high for faces/audio	extract redacted key frames
CASE40-04	visible watermark	repost-platform watermark	low	search for earlier uploads

The starting evidence proves only what the post claimed and what was visible, not whether the claim is true.

5. Image Search Results

Search family:

full still image reverse search;
crop of waterfront building;
crop of pier sign/banner;
crop of distinctive blue railings;
text search for visible sign fragments;
key video frame reverse search;
caption phrase search.

Fictional result:

An earlier public tourism article from 2024 uses a very similar still image of Northbank Harbour Festival.
A later repost uses the same image with a different caption.
No reliable source is found linking the still image to Westport Pier.

Finding so far:

The image appears likely reused or at least not newly evidenced by the current post. Further checks are needed before conclusion.

6. Metadata Review

The public-platform image download contains no useful original EXIF GPS data.

Evidence note:

File metadata inspected: platform download copy.
GPS metadata: not present.
Camera/device metadata: not present.
Timestamp fields: platform/file-system only, not original capture time.
Interpretation: metadata does not support date or location.

Safe finding:

No original metadata was available from the public platform copy. Metadata does not establish the image's location or capture time.

7. Visual Clue Inventory

Clue	Category	Observation	Initial value
Blue railings	public infrastructure	distinctive waterfront railings	semi-unique
Clock tower	skyline/landmark	tower visible behind crowd	strong if matched
Ferry sign fragment	transport/sign	partial "NBK Ferry" visible	strong if confirmed
Pier layout	map/structure	pier runs east-west with kiosk near entrance	strong
Weather	time	dry ground, broken cloud	supportive only
Crowd clothing	season/event	summer clothing	weak
Siren audio	video/audio	siren heard, not visible source	weak for cause
No visible drone	video/content	no drone seen in key frames	limits cause claim

Faces and clothing are not used to identify individuals.

8. Hypothesis Table

Hypothesis	Supporting clues	Contradictions	Missing checks	Confidence
H1: Westport Pier today	caption only	ferry sign appears NBK; tower not known at Westport	map/street view/weather/night	low
H2: Northbank Harbour Festival, older image	blue railings, NBK sign, clock tower, earlier tourism article	video still not found	search for earlier uploads	medium
H3: Similar waterfront elsewhere	water/railings/crowd generic	distinctive tower/sign point to Northbank	search other locations	low

The caption is not enough to carry H1.

9. Map and Street-Level Comparison

Fictional comparison:

Feature	Image/video	Northbank map/street-level	Westport map/street-level	Assessment
Blue railings	visible along waterfront	match	no match found	supports Northbank
Clock tower	behind crowd left	match from candidate viewpoint	absent	supports Northbank
Ferry sign	partial NBK Ferry	Northbank ferry terminal uses NBK	Westport signs differ	supports Northbank
Pier kiosk	near entrance	match	different layout	supports Northbank
Road bend	visible behind crowd	match	no matching bend	supports Northbank

The strongest location finding is Northbank Harbour area, not Westport Pier.

10. Weather and Time Checks

Claimed time: “today” in the post.

Fictional checks:

Public weather record for Westport today: heavy rain during afternoon.
Image/video: dry ground and strong broken sunlight.
Northbank festival archive from 2024: same blue railings and summer event setup.
Earlier tourism image: predates current claim.
Video upload: current post appears to be a repost; no original timestamp available.

Assessment:

The time claim is not supported. Weather creates a possible contradiction for Westport today, while the earlier image ev

11. Video Verification

Key-frame review:

00:03 – blue railings and crowd visible.
00:08 – clock tower visible.
00:13 – abrupt cut to crowd moving.
00:18 – siren audible, no emergency vehicle visible.
00:23 – no visible drone or crash site.
00:28 – clip ends before cause is shown.

Video finding:

The video supports a waterfront crowd scene consistent with Northbank Harbour. It does not establish a drone crash or p

12. Event Verification Matrix

Claim part	Evidence found	Independent support	Contradiction	Finding	Confidence	
Crowd at waterfront	image/video	visual evidence	none	supported as scene only	medium/high	
Westport Pier	caption only	none	map clues point to Northbank	not supported	high against claim	
Today	caption only	no original metadata	earlier image and weather mismatch	not supported	medium/high	
Drone crash	caption only	no visible drone/crash	no official source	no support	not established	low
Panic	crowd movement	no context before/after	clip short/cut	not established	low	

This separates what is visible from what is claimed.

13. Redaction Decisions

For the public report:

blur faces;
blur vehicle plates;
remove exact map pin;
refer to “Northbank Harbour public waterfront area” rather than exact camera point;
do not include uploader handle unless necessary;
do not reproduce private comments;
do not speculate on people’s actions or identities.

The public purpose is misinformation correction, not exposure.

14. Final Finding

The reviewed public image and video do not support the claim that the scene shows Westport Pier today. Visual comparison

Limitations:

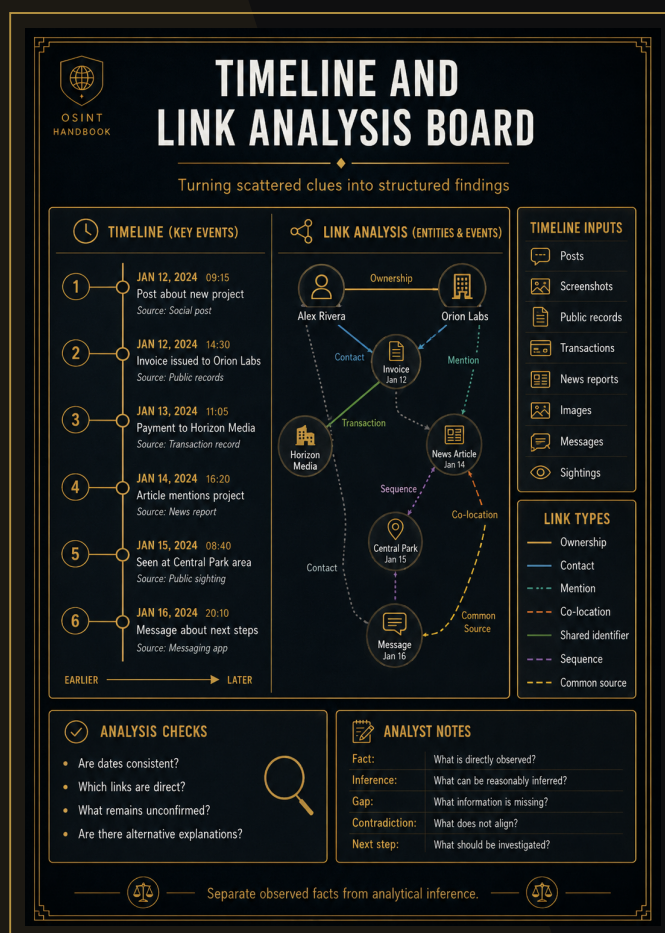
The original file metadata was not available.
The video is short and edited.
Weather comparison is supportive, not decisive.
Only public sources were reviewed.

VOLUME FIVE

Analysis, Workflows, and Reporting

Turning clues into findings, timelines, confidence language, evidence packs, redaction, and quality control.

CHAPTERS 41-50



Chapter 41 - Turning Clues into Findings

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter teaches the most important shift in OSINT analysis: a clue is not a finding. A clue is something noticed. A finding is something supported, checked, bounded, and written in a way that a reader can understand and challenge.

By the end of this chapter, the reader should be able to:

- separate raw clues from observations, inferences, and findings;
- avoid over-claiming when evidence is incomplete;
- convert evidence cards into cautious findings;
- write findings that include method, confidence, and limitations;
- spot when a clue should remain only a lead;

1. The Four-Level Evidence Ladder

Use a simple ladder for every piece of information.

Clue	Something noticed: a username, date, image detail, quote, document, post, or link.
Observation	What the source visibly shows or says, without interpretation.
Inference	A reasoned explanation that connects observations.
Finding	A checked analytical statement supported by cited evidence and limitations.

Most OSINT mistakes happen when an investigator jumps from clue directly to conclusion. The safest habit is to write the observation first: “The page displayed the phone number X on the capture date,” not “this person owns the number.”

2. The Clue Handling Table

Every clue should be placed into a small handling table before it is used.

Clue ID	Source	What was observed	Possible meaning	Other explanations	Next check	Status
C41-01	archived page	brand used same logo in 2024	possible continuity	copied logo/template	check legal entity.	
C41-02	company register	director name matches	possible same person	common name	compare address/role/date	un
C41-03	official notice	domain listed by regulator	direct link to organisation	none obvious	preserve notice	e

This forces the reader to see how each clue was treated. It also prevents a later report from quietly relying on weak material.

3. Finding Formula

A safe finding uses four parts.

Finding = claim + supporting evidence + confidence + limitation

Example:

The domain example-training.test appears linked to the fictional organisation Northbank Training Ltd with moderate conf.

The limitation is not weakness. It is honesty. Good OSINT shows exactly where the evidence stops.

4. Lead, Finding, or No Finding

Not everything belongs in the final report. Use this decision test.

Lead: interesting but unchecked or weak.
Finding: checked, relevant, proportionate, and supported.
No finding: too speculative, irrelevant, private, harmful, or contradicted.

A responsible report may say: “No reliable public source was found to support the claim.” That is often more valuable than forcing a dramatic answer.

5. Worked Example

Fictional question: “Is the public fundraising page connected to the real local charity?”

Clues:

- Similar charity name.
- Same town mentioned.
- Different donation processor.
- No charity number visible.
- Local Facebook posts sharing it.

Possible finding after checking:

The fundraising page cannot be confirmed as an official page of the charity from public sources reviewed. The page uses

6. Chapter Exercise

Take five clues from a fictional case and classify each as lead, observation, inference, finding, or no finding. Then rewrite any overconfident sentence into cautious analytical language.

Bad: “This proves the account is fake.”

Better: “The account shows indicators commonly associated with imitation, but public evidence is insufficient to identify

Additional Practice - Practical Analyst Habit

Before accepting a finding, write the strongest sentence against it. If the finding still stands after that challenge, it is stronger. If it becomes weaker, lower the confidence or keep the point as a lead.

Finding: the page appears unofficial.

Challenge: the official charity may have a separate campaign page not linked from the main site.

Response: check official social links, campaign pages, and contact route before final wording.

This habit prevents the report from becoming a one-sided argument.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - The Analyst's Finding Sheet

For a professional workbook, every finding should be traceable to a repeatable sheet. The sheet does not need to be complicated; it needs to force the analyst to slow down before writing a conclusion.

Finding ID:

Question being answered:

Short finding sentence:

Evidence items used:

Evidence items rejected:

Alternative explanations considered:

Privacy / harm check:

Confidence level:

Limitation sentence:

Recommended next action:

Reviewer notes:

The important line is “evidence items rejected.” Weak material often influences thinking even when it is not cited in the final report. By recording why a clue was rejected, the analyst prevents it from quietly shaping the final wording.

8. Example - From Mixed Clues to a Bounded Finding

Fictional case: a small business wants to know whether a new website using a similar name is connected to a former supplier. The analyst finds a matching town, a similar design, one shared phrase in the privacy notice, and a domain registered through a privacy-protected registrar.

A poor finding would say:

The former supplier has created a copycat website.

A careful finding would say:

The new website shows branding and wording similarities to the former supplier's previous public material, but the publ.

This wording gives the client something useful without accusing a person or organisation beyond the evidence.

9. Clue Retirement

A mature investigation does not keep every clue alive forever. Some clues should be retired when they become irrelevant, contradicted, duplicated, disproportionate, or too private for the task.

Retire the clue when:

- it does not answer the investigation question;
- it concerns a private person and is not necessary;
- it cannot be verified from a reliable source;
- it depends on speculation about motive or intent;
- a better official or primary source replaces it;
- continuing to pursue it would expand the scope unfairly.

Retired clues can stay in the case journal with a clear reason, but they should not appear in the final report unless the reason for exclusion is itself important.

10. Workbook Drill - Three Versions of One Finding

Take one fictional finding and write it three ways:

Version A: Too strong.

Version B: Too weak or vague.

Version C: Balanced, evidence-led, and bounded.

Example:

A: The account is definitely pretending to be the company.

B: Something may or may not be wrong with the account.

C: The account displays several public indicators of impersonation, including copied branding, no link from the company

The third version is the one that belongs in a professional OSINT report.

Visual Brief

V48. Clue-to-finding analysis pipeline: raw clue, source, observation, verification, alternative explanation, confidence, finding, report citation.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 42 - Link Analysis and Entity Graphs

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter explains how to map relationships without pretending that every line on a diagram is proof. Link analysis is useful because it shows structure, gaps, repeated connections, and contradictions. It becomes dangerous when lines are drawn without labels or confidence.

By the end of this chapter, the reader should be able to:

- create clean entity graphs;
- label relationship types and confidence;
- separate confirmed links from possible links;
- avoid visual exaggeration;
- turn a graph into report-ready findings;

1. What an Entity Graph Is

An entity graph is a structured map of things and their relationships. In OSINT, entities can include people, accounts, organisations, domains, email addresses, documents, phone numbers, locations, events, products, and public records.

The graph should not be a conspiracy board. It is a working analysis tool. Every node should have a source. Every edge should explain what kind of connection is being claimed.

2. Node and Edge Rules

Use a consistent rule set.

Node = identifiable item.
Edge = observed relationship between two items.
Edge label = nature of the relationship.
Confidence = how strongly the public evidence supports the edge.
Citation = evidence card or source reference.

Example edge labels:

registered_to
links_to
mentions
uses_same_address_as
shares_contact_detail_with
appears_in_same_event_as
claimed_by_source

Avoid vague labels such as “connected to” unless the report explains exactly what that means.

3. Confidence on a Graph

Use visual confidence markers in the working file and plain wording in the report.

Solid line independently supported by reliable source(s).
Dashed line plausible but needs confirmation.
Dotted line weak clue only.
Red X marker contradiction or rejected link.

A graph without confidence markers makes weak clues look as strong as official records.

4. Graph Hygiene

A useful graph is usually smaller than the investigator wants it to be. Remove noise. Merge duplicates carefully. Do not combine two entities only because they have the same name. Keep personal data minimised.

Good graph notes include:

- Entity naming convention.
- Date range of sources.
- Which nodes are public organisations and which are private individuals.
- Which links are directly sourced.
- Which links are inferred.
- Which links were rejected.

5. Mini Case

Fictional case: a suspicious investment website claims to be operated by “Harbour North Capital.” Public records show a similarly named dormant company, the website uses a privacy-hidden domain registration, and a social profile links to a Telegram channel.

The graph should show:

- Website -> claims brand name -> Harbour North Capital
- Website -> links to -> social profile
- Social profile -> links to -> Telegram channel
- Dormant company -> shares similar name -> brand claim

The graph should not say the dormant company operates the website unless a reliable source supports that exact relationship.

6. Reporting the Graph

In a final report, include the graph as a summary, not as the evidence itself. Under the graph, add a relationship table.

Relationship	Evidence	Confidence	Limitation
Website links to social profile	homepage footer captured 7 Jun 2026	high	page may change
Brand resembles dormant company	company register/name comparison	low	no direct official link

This lets the reader audit the diagram.

Additional Practice - Graph Review Checklist

Before using a graph in a report, check:

- Are all nodes defined?
- Are private people minimised or masked?
- Does every edge have a label?
- Does every strong edge have a citation?
- Are weak links visually different from confirmed links?
- Have rejected links been recorded somewhere?
- Could the graph be misunderstood as stronger than the evidence?

The final graph should help the reader understand the evidence, not dazzle them into accepting it.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Graph Rules Before Graph Tools

Entity graphs are useful, but they can also make weak relationships look stronger than they are. Before using graph software, define the rules for nodes and edges.

- Node rule: what counts as an entity?
- Edge rule: what counts as a relationship?

Evidence rule: what source supports the edge?
Date rule: when was the relationship observed?
Confidence rule: how strong is the link?
Privacy rule: should this entity be shown, redacted, or omitted?

A graph without rules is just a drawing. A graph with rules becomes an analytical instrument.

8. Edge Strength Table

Use an edge table alongside every graph.

Edge ID	Entity A	Entity B	Relationship	Source	Date observed	Strength	Notes
E42-01	Domain	Company	Website footer lists company number	archived page	2026-04-10	strong	direct public st
E42-02	Username	Person name	same display name	platform profile	2026-04-12	weak	common name, no corroborat
E42-03	Brand page	Payment account	linked checkout page	current website	2026-04-13	moderate	public link, op

This prevents the final diagram from becoming misleading. A weak shared username should not be visually equal to an official registration record.

9. Redaction in Graphs

Graphs are often copied into presentations, reports, and screenshots. That makes redaction essential. Before sharing a graph, remove or mask unnecessary private details.

Show: organisation names, public domains, official accounts, generic role labels.
Mask: private phone numbers, home addresses, non-relevant family names, private emails.
Omit: unrelated individuals, minors, private social connections outside scope.

If a private person is essential to the case, use a role label such as **Complainant**, **Reporter**, **Customer A**, or **Director 1** unless the audience has a lawful need for the real name.

10. Worked Mini-Graph

Fictional entities:

Northbank Training Ltd
northbank-training.example
@northbanktraining
Payment page A
Archived website page
Director 1

Safe graph interpretation:

The domain, archived site, and official social account can be grouped with moderate-to-high confidence because they cross

The graph shows relationships between public entities. It does not prove personal intent.

11. Graph Review Questions

Before a graph goes into a report, ask:

Does every edge have a source?
Are weak edges visually different from strong edges?
Are dates visible or recorded nearby?
Could a reader mistake a lead for a finding?
Have private people been redacted where possible?
Does the graph answer the investigation question?

If the answer to any of these is no, the graph needs revision before publication.

Visual Brief

V49. Entity graph workspace: nodes for people/accounts/domains/organisations/events, edge labels, confidence badges, source citations, and privacy redaction layer.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 43 - Timeline Building

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter teaches timeline discipline. OSINT is often about sequence: what happened first, what was claimed later, and what can be proven at a particular date. A timeline prevents reused media, old claims, reposts, and late edits from being mistaken for live truth.

By the end of this chapter, the reader should be able to:

- separate event date, publication date, and capture date;
- create reliable timeline entries;
- handle uncertainty in dates and time zones;
- show contradictions over time;
- use timelines in reports;

1. Three Dates That Must Not Be Confused

For every source, record three different date concepts.

Event date: when the thing allegedly happened.
Publication date: when the source was published or posted.
Capture date: when you saved or viewed it.

A post published today may contain a photo from years ago. A screenshot captured today may show a page that was edited yesterday. A record filed last month may describe a change that happened earlier.

2. Timeline Entry Template

Use a consistent entry format.

Timeline ID: T43-004
Date/time: 2026-05-28 14:20 BST
Date type: publication date
Event described: public statement posted by organisation
Source: official website news page
Evidence ID: E43-009
Confidence in date: high
Notes: page displays date and archive capture supports page state

Do not hide uncertainty. If the date is approximate, say so.

3. Time Zones and Local Context

When working across countries, convert times carefully and preserve the original.

Original: 2026-06-07 09:10 PDT
Converted: 2026-06-07 17:10 BST
Reason: comparison with UK press release

Avoid creating false precision. If a platform only shows “2 days ago,” capture that wording and calculate cautiously.

4. Contradiction Markers

Timelines are excellent for spotting contradictions.

Claim: company launched product in March.
Timeline: domain first observed in May; press release in June; archived page in April describes a pre-launch page.

Possible interpretation: claim may refer to private beta, not public launch.
Next check: look for official announcement or app-store listing.

The contradiction may not prove deception. It may show wording ambiguity.

5. Timeline Types

Choose the timeline type that matches the case.

Event timeline: what happened and when.
Source timeline: when evidence appeared or changed.
Account timeline: profile creation, name changes, posts, deletions.
Company timeline: incorporation, filings, officer changes, product claims.
Incident timeline: detection, preservation, reporting, response.

6. Exercise

Build a fictional timeline for a reused image claim. Include original upload, repost, news mention, archive capture, platform deletion, and final report date. Mark which dates are proven and which are inferred.

Additional Practice - Timeline Quality Questions

Ask these questions before relying on a timeline:

Which entries are directly dated by reliable sources?
Which entries are inferred from surrounding evidence?
Are platform-relative dates converted cautiously?
Are time zones recorded?
Could a page edit or repost explain the sequence?
Do any entries depend on deleted or unpreserved sources?

A timeline is only as good as its weakest date labels.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Timeline Types

There are three useful timeline types in OSINT work.

Event timeline: what happened and when.
Collection timeline: when the analyst found and preserved each item.
Publication timeline: when a source appeared, changed, disappeared, or was archived.

Do not mix these without labels. A post written in January, found in March, and archived in April has three dates. Confusing those dates can distort the entire analysis.

8. Timeline Entry Template

Every timeline entry should be written in a structured way.

Timeline ID:
Date/time shown by source:
Timezone:
Date/time collected:
Source:
Event described:
Evidence file:
Reliability:
Uncertainty:
Notes:

Timezone deserves its own field. Many online platforms display local time, browser time, or platform time differently. When in doubt, write exactly what the source displayed and avoid converting it unless necessary.

9. Handling Unknown or Approximate Dates

Approximate dates should be visible, not hidden.

Exact: 2026-06-07 14:32 BST
Date only: 2026-06-07, time not shown
Month only: June 2026, exact date not shown
Relative: "posted 3 days ago" captured on 2026-06-07
Inferred: likely before 2026-05-20 because it appears in an archive snapshot from that date

Do not turn an inferred date into an exact date. The wording should preserve the uncertainty.

10. Worked Example - Conflicting Dates

Fictional case: a public event page claims a charity collection was launched on 1 May. A social post promoting it is dated 28 April. An archive snapshot shows the donation page existed on 27 April.

A careful timeline would say:

The campaign was publicly promoted before the stated launch date. The earliest preserved indication found in this review

This is more accurate than saying: "The charity lied about the launch date."

11. Timeline Quality Checklist

- Are all entries sourced?
- Are collection dates separate from event dates?
- Are archive dates clearly labelled?
- Are timezones recorded or uncertainty stated?
- Are inferred dates marked as inferred?
- Are gaps in the timeline described?
- Are irrelevant private events excluded?
- Does the timeline answer the investigation question?

A good timeline is not just a list of events. It is an argument about sequence, supported by evidence and bounded by uncertainty.

12. Workbook Drill - Build a Three-Layer Timeline

Create a fictional case with five public sources. Build three rows for each source: the event date, the collection date, and the publication/archive date. Then write a short paragraph explaining what can and cannot be concluded from the sequence.

Visual Brief

V50. Timeline strip: event date, publication date, capture date, source reliability, contradiction marker, and confidence bands.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 44 - Confidence Levels and Analytical Language

***Safety and lawful-use note:** This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.*

Purpose of This Chapter

This chapter provides a practical confidence language system. OSINT reporting should be clear without being reckless. Confidence wording protects the reader, the subject, and the investigator.

By the end of this chapter, the reader should be able to:

- use standard confidence levels;
- avoid words that overstate proof;
- write balanced findings;
- communicate uncertainty clearly;
- separate absence of evidence from evidence of absence;

1. Why Confidence Matters

Readers often remember the headline and forget the caveat. If a report says “X is linked to Y,” a weak inference can become a damaging accusation. Confidence wording keeps the claim proportional to the evidence.

2. Confidence Ladder

Use a simple ladder.

Confirmed: directly supported by authoritative or multiple independent reliable sources.
High confidence: strongly supported, minor limitations remain.
Moderate confidence: supported by several indicators, but key gap or alternative remains.
Low confidence: plausible lead only; not enough for a firm finding.
Unsupported: searched but not supported by reliable public evidence.
Contradicted: reliable evidence conflicts with the claim.

Never use “confirmed” just because several social posts repeat the same claim.

3. Words to Use and Avoid

Prefer careful verbs.

Use: indicates, suggests, is consistent with, appears to, public sources show, no reliable source was found.
Avoid: proves, definitely, exposed, caught, guilty, fake, scammer, owner, operator, unless evidence truly supports it.

Even when a case looks obvious, let the evidence do the work.

4. Absence of Evidence

A common mistake is writing: “There is no record, therefore it did not happen.” A safer version is:

No reliable public record was identified in the sources reviewed. This does not prove the event did not occur; it means

State the sources reviewed and the search limits.

5. Confidence Notes in Evidence Cards

Each evidence card should include a confidence note.

Evidence: archived homepage with company number

Confidence: high for page content at capture date; moderate for current ownership; limitation: website may not be controlled

6. Exercise

Rewrite the following sentence safely:

"The director is behind the fake investment site."

Safer version:

Public sources reviewed show a name match between the dormant company director and the name used in the investment site

Additional Practice - Reader Impact Test

Imagine the subject, client, journalist, court, employer, or a member of the public reading your sentence without the surrounding notes. Would they understand the uncertainty? If not, rewrite it.

Too strong: "The account is operated by the company."

Better: "The account presents itself as associated with the company, but no official cross-link was found in the public

Good wording reduces the risk of unfair harm.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Confidence Is Not Certainty

Confidence language should describe the strength of the evidence, not the analyst's personal feeling. A confident-sounding sentence without evidence is still weak. A cautious sentence supported by strong sources is often more useful.

Use a simple scale:

High confidence: multiple reliable sources, direct evidence, low ambiguity.

Moderate confidence: some corroboration, plausible link, remaining gaps.

Low confidence: limited evidence, indirect indicators, significant alternative explanations.

Insufficient evidence: not enough public information to assess responsibly.

Avoid pretending to be more precise than the evidence allows.

8. Words to Avoid or Control

Some words create legal, ethical, or analytical risk.

Avoid unless directly supported:

- proves
- definitely
- fake
- scammer
- criminal
- owner
- operator
- linked beyond doubt
- deliberately
- secretly

Safer alternatives:

- indicates
- appears
- is consistent with
- is publicly associated with
- could not be confirmed
- public evidence reviewed supports
- public evidence reviewed does not support
- remains unresolved

The aim is not to make the report timid. The aim is to make it defensible.

9. Confidence Sentence Patterns

High confidence:

Public evidence strongly supports [finding] because [evidence]. The main limitation is [limitation].

Moderate confidence:

Public evidence supports [finding] with moderate confidence. The strongest indicators are [evidence], but [gap] remains.

Low confidence:

The available public evidence is consistent with [possibility], but it is not enough to treat this as a finding. Further

Insufficient evidence:

No reliable public source reviewed confirms [claim]. This review cannot determine [unknown] from lawful public sources.

These patterns help keep the tone consistent across the whole book.

10. Worked Example - Changing the Legal Risk

Risky wording:

The account is a fraud account run by the company director.

Safer wording:

The account displays public indicators commonly associated with impersonation, including copied branding and an external

The second version still communicates the risk. It avoids unsupported personal accusation.

11. Reviewer Exercise

Give a reviewer five findings and ask them to mark each one:

Supported / overclaimed / unclear / missing limitation / missing source / privacy risk

Then revise the findings until every claim has evidence, confidence, and limitation language.

Visual Brief

V51. Confidence language ladder: confirmed, high, moderate, low, unsupported, contradicted, with evidence and limitation fields.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 45 - Contradictions and Alternative Explanations

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter teaches analysts to actively look for reasons they might be wrong. Contradictions are not an annoyance. They are one of the best protections against false findings.

By the end of this chapter, the reader should be able to:

- identify contradictions;
- build alternative explanation tables;
- avoid confirmation bias;
- decide when evidence is unresolved;
- report conflicting evidence fairly;

1. The Duty to Try to Disprove Yourself

A strong OSINT workflow does not simply gather evidence for a favourite answer. It tests the answer against alternatives. If the finding survives that test, confidence increases. If it does not, the report should say the matter remains unresolved.

2. Contradiction Types

Common contradiction types include:

Date contradiction: source dates do not line up.
Identity contradiction: identifiers point to different entities.
Location contradiction: visual clues conflict with claimed place.
Source contradiction: official source conflicts with social claim.
Context contradiction: wording is technically true but misleading.
Data contradiction: one database is stale or incomplete.

3. Alternative Explanation Table

Use a table before writing findings.

Claim: account belongs to person A.
Supporting evidence: same handle, same city, shared hobby.
Contradicting evidence: account uses different workplace and age range.
Benign alternatives: fan account, reused handle, coincidence, parody.
Higher-risk alternatives: impersonation, scam account.
Next checks: controlled cross-link, official profile, archive history.
Current position: unresolved; do not attribute.

4. Benign First

Do not assume malice when a simpler explanation fits. Old websites, copied templates, shared addresses, agencies, stock photos, and recycled usernames create many false connections.

5. Reporting Contradictions

A professional report can include a contradiction section.

Contradiction noted: the caption states the photograph was taken in June 2026, but reverse image search located a visual

Do not bury contradictions in an appendix. Important limitations belong near the finding.

6. Exercise

Take a fictional claim and list at least three alternative explanations before deciding confidence. The exercise is complete only when the final wording mentions the strongest alternative.

Additional Practice - Contradiction Handling Decision

When a contradiction appears, choose one of four outcomes.

Resolve: further evidence explains it.
Downgrade: finding remains, but confidence falls.
Split: two separate findings are needed.
Stop: evidence is too conflicted for a finding.

The most professional answer is sometimes “unresolved.”

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Contradiction Log

Contradictions are not failures. They are signals that the case needs sharper thinking. Keep a contradiction log instead of hiding awkward evidence.

Contradiction ID:
Finding affected:
Source A says:
Source B says:
Possible reasons:
Current status:
Impact on confidence:
Next check:

This protects the analyst from cherry-picking and protects the reader from being misled.

8. Common Causes of Contradiction

- old page versus current page;
- copied text or templates;
- platform display errors;
- different timezones;
- shared names or reused usernames;
- rebranded organisations;
- inactive or abandoned accounts;
- unofficial fan/support pages;
- archive snapshots taken at different times;
- deliberate misinformation;
- simple human error.

Do not assume deception when ordinary explanations remain plausible.

9. Alternative Explanation Method

For every important finding, write at least two alternative explanations.

Finding draft: the website appears connected to the organisation.
Alternative 1: the site copied the organisation's text without authorisation.
Alternative 2: the site is an old campaign page no longer linked from the main website.
Alternative 3: the shared address is a registered office used by many companies.

Then ask: what evidence would separate these explanations? That question creates the next research step.

10. Worked Example - Shared Address

A company address appears on several unrelated websites. A weak analysis might treat that as a network. A stronger analysis checks whether the address is a virtual office, accountant, registered agent, shared workspace, or old template text.

Careful wording:

The same address appears across multiple public records, but this does not by itself establish operational connection b

11. Decision Matrix

Contradiction minor + finding strong = mention limitation.

Contradiction major + finding strong = lower confidence and explain.

Contradiction major + finding weak = keep as lead only.

Contradiction unresolved + high harm risk = do not publish as a finding.

The higher the potential harm, the stronger the evidence must be.

12. Workbook Drill - Build the Counter-Case

Take one fictional report finding and deliberately build the strongest counter-case against it. Add three sources that might weaken it, then rewrite the finding to include the uncertainty fairly.

Visual Brief

V52. Alternative explanation matrix: claim, supporting evidence, contradicting evidence, benign explanations, harmful explanations, next checks, conclusion.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 46 - Report Structure and Evidence Packs

***Safety and lawful-use note:** This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.*

Purpose of This Chapter

This chapter shows how to turn OSINT work into a report that is useful, readable, and auditable. A good report does not dump every note. It answers the question with enough evidence for the reader to verify the reasoning.

By the end of this chapter, the reader should be able to:

- structure OSINT reports;
- build evidence packs;
- write executive summaries;
- separate method from findings;
- prepare appendices without exposing unnecessary personal data;

1. Report Structure

A standard OSINT report can use this structure.

1. Title and case reference
2. Executive summary
3. Scope and limitations
4. Method
5. Key findings
6. Evidence table
7. Analysis and alternatives
8. Recommendations or next steps
9. Redaction note
10. Appendix / evidence pack index

The order helps a busy reader understand the answer first and audit the evidence second.

2. Executive Summary

The executive summary should be short, plain, and careful.

This review found moderate-confidence indicators that the public website is not currently linked from the official char

Avoid drama. Avoid speculation. Avoid unnecessary names.

3. Evidence Pack

An evidence pack contains preserved material supporting the report. It should be structured.

```
/Evidence
/Original
/Working
/Redacted
evidence_log.csv
source_list.md
timeline.md
hash_manifest.txt
```

If sensitive personal data appears in the original evidence, the public report should use redacted copies and explain that originals are retained only where lawful and necessary.

4. Evidence Table

The report should have an evidence table.

ID	Source	Date captured	Relevance	Reliability	Privacy handling
E46-01	official charity site	2026-06-07	no link to fundraising page found	high for site content	no personal data
E46-02	fundraising page	2026-06-07	displays similar charity name	medium	donor names redacted

5. Recommendations

Recommendations must match confidence.

Good: "Verify through official contact route before donating."

Risky: "Report this as fraud immediately," unless the evidence genuinely supports that step.

If escalation is needed, tell the reader which authority or internal owner should review it rather than encouraging public accusation.

6. Exercise

Draft a one-page report from a fictional evidence log of six items. Include one finding, one limitation, one contradiction, and one safe recommendation.

Additional Practice - Report Length Control

A report should be as long as needed and no longer. Use the main report for findings and the appendix for supporting detail.

Executive reader: summary, findings, recommendations.
Technical reviewer: method, source list, evidence table.
Legal/privacy reviewer: scope, limitations, redactions, retention.
Future investigator: evidence pack index and change log.

Design for all four readers without overwhelming any one of them.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Report Tiers

Not every OSINT output should be a long report. Choose the right report type for the job.

One-page brief: urgent summary, low detail, clear next action.
Standard report: findings, evidence, confidence, limitations, recommendations.
Evidence pack: preserved source files, screenshots, hashes if used, source index.
Executive summary: plain-language overview for non-technical readers.
Technical appendix: detailed methods, source list, tables, and timeline.

Separating these tiers helps different readers get the right level of detail without exposing unnecessary personal data.

8. Evidence Pack Index Template

Evidence ID	File name	Source URL or description	Capture date	Related finding	Redaction status	Notes
E46-001	screenshot_homepage.png	public website homepage	2026-06-07	F1	redacted copy available	original stored
E46-002	archive_snapshot.pdf	archive capture	2026-06-07	F1/F2	no personal data	date visible
E46-003	company_record.pdf	official register	2026-06-07	F3	director details masked in client copy	public of

A report without an evidence index becomes difficult to audit later.

9. Report Writing Order

Write the report in this order, even if the final document appears differently:

1. Scope and question.

2. Evidence inventory.
3. Findings.
4. Confidence and limitations.
5. Recommendations.
6. Executive summary.
7. Redaction pass.
8. Quality-control pass.

Writing the executive summary last prevents it from becoming a sales pitch or a guess.

10. Recommendation Discipline

Recommendations should match the finding and avoid overreach.

Finding: public impersonation indicators exist.

Good recommendation: preserve evidence, report through platform channels, notify users via official channels if appropriate.

Poor recommendation: accuse a named person online.

Finding: domain registration is privacy protected.

Good recommendation: check official links and DNS/website evidence.

Poor recommendation: attempt to bypass privacy controls.

A safe report gives practical next steps without encouraging harassment, unauthorised access, or public shaming.

11. Final Report Checklist

- Scope is clear.
- Methods are lawful and public-source based.
- Findings are numbered.
- Each finding has evidence and confidence.
- Limitations are visible.
- Personal data is minimised.
- Screenshots are labelled.
- Redacted and original evidence are separated.
- Recommendations are proportionate.
- A reviewer can reproduce the reasoning.

12. Workbook Drill - Build a Mini Evidence Pack

Use a fictional case and create five evidence items, a two-finding report, and a redaction note. The goal is not volume; it is traceability.

Visual Brief

V53. Final report anatomy board: cover, executive summary, scope, method, findings, evidence table, limitations, redactions, appendix.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 47 - Redaction and Privacy Protection

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter explains how to protect people, clients, witnesses, bystanders, minors, employees, and investigators when preparing OSINT outputs. Redaction is not cosmetic. It is a safety control.

By the end of this chapter, the reader should be able to:

- identify data that should be redacted;
- create original, working, and public copies;
- avoid leaking metadata;
- balance transparency and privacy;
- document redaction decisions;

1. What to Redact

Consider redacting:

private addresses; private phone numbers; personal email addresses; faces of bystanders; children; vehicle plates; signs

The rule is simple: if the reader does not need it to understand the finding, remove or mask it.

2. Three-Copy Model

Keep three copies where lawful and necessary.

Original: preserved, unchanged, access restricted.

Working: annotated for analysis.

Public/report: redacted and checked.

Never overwrite the original. Never rely on a black box drawn over text unless you are sure the underlying text cannot be recovered.

3. Metadata Checks

Files can leak more than their visible content. Before sharing, check for document properties, EXIF data, revision history, hidden layers, comments, tracked changes, and embedded thumbnails.

Safe habit:

Export to a clean copy.

Open the exported copy separately.

Inspect metadata/properties.

Test copy-paste from redacted areas.

Confirm no hidden text remains.

4. Privacy Impact Note

For significant reports, write a short privacy impact note.

What personal data is included?

Why is it necessary?

Who will receive it?

What has been redacted?

How long will it be retained?

What harm could disclosure cause?

5. Redaction Log

Record what you changed.

Item	Redaction	Reason	Version
Screenshot 03	faces blurred	bystanders not relevant	public v1
PDF 02	home address masked	not needed for finding	client v2
Timeline	private username removed	irrelevant personal data	public v1

6. Exercise

Take a fictional screenshot containing a username, photo, phone number, location, and public company name. Decide what remains visible in: internal working copy, client copy, and public copy.

Additional Practice - Redaction Failure Modes

Common redaction failures include:

black boxes placed over selectable PDF text; blurred faces that remain recognisable; filenames containing private names.

Always inspect the final shared file, not only the editor view.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Redaction Is an Analytical Step

Redaction is not only a final cosmetic task. It should influence collection, analysis, and reporting. If a piece of personal data is not necessary, the safest version is not to collect it in the first place.

Use three levels:

Do not collect: irrelevant private material.
Collect but restrict: necessary sensitive evidence.
Collect and share redacted: necessary evidence where details can be masked.

This protects the subject, the client, and the analyst.

8. Redaction Decision Table

Data type	Needed for finding?	Harm if exposed?	Report version	Evidence version
Home address	usually no	high	omit or generalise	restrict if legally necessary
Business address	sometimes	medium	show if public and relevant	preserve source
Personal phone	rarely	high	mask	restrict
Company number	often	low	show	preserve
Minor's name	almost never	very high	omit	avoid collection
Username	sometimes	variable	mask if private person	preserve if necessary

9. Common Redaction Mistakes

- black boxes that can be removed from a PDF layer;
- filenames that reveal the redacted name;
- metadata left inside images or documents;
- screenshots with browser bookmarks or account names visible;
- sharing originals when a redacted copy was intended;
- leaving private data in alt text, captions, comments, or change history.

The redaction check should include the document, filename, metadata, folder path, and export settings.

10. Redacted Copy Workflow

1. Preserve original evidence in a restricted folder.
2. Create a working copy.
3. Redact the working copy.
4. Export to a flattened format where possible.
5. Review the exported file on a separate viewer.
6. Store original and redacted versions separately.
7. Record the redaction decision in the evidence index.

Never rely on visual masking alone if the file format preserves hidden text underneath.

11. Worked Example - Small Business Report

A report about fake social pages does not need to expose the home address of a sole trader. It may need to show the official business website, official social links, and the public impersonation page. The personal address can be removed unless it is directly relevant to the defensive purpose and the audience has a clear lawful need.

Safer wording:

The official business contact route was verified through the public website. Personal address details shown in public r

12. Workbook Drill - Redaction Review

Take a fictional evidence pack and create two versions: analyst-only and client-safe. Write a short note explaining every redaction.

Visual Brief

V54. Redaction workflow: original evidence, working copy, public copy, hidden metadata check, privacy risk flags, and disclosure decision gate.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 48 - Automation Without Losing Control

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter covers safe automation for OSINT workflows. Automation can save time, but it can also multiply errors, privacy problems, and legal risks. The core rule is human control: automate collection and organisation only where lawful, transparent, logged, and reviewable.

By the end of this chapter, the reader should be able to:

- choose low-risk automation tasks;
- avoid uncontrolled scraping or harassment;
- build review queues;
- log automated actions;
- use AI assistance without delegating judgement;

1. Good Uses of Automation

Low-risk automation includes:

renaming evidence files; generating evidence-card templates; checking whether a saved source URL still resolves; compar

Automation should support evidence discipline, not replace judgement.

2. Automation Boundaries

Avoid automation that creates harm or violates terms, law, or privacy. Do not use automation to mass-profile private people, bypass access controls, overload services, evade blocks, scrape restricted communities, harvest contact details for targeting, or generate accusations without human review.

3. Human Review Queue

Every automated output should land in a review queue.

Item ID	Automation result	Source	Risk	Human action
A48-01	page title changed	saved watchlist URL	low	review manually
A48-02	possible name match	public register	high	do not use until checked
A48-03	AI summary of article	captured source	medium	compare with source text

Automation result is never automatically a finding.

4. Logging Automated Work

Record:

what ran; when it ran; what sources it touched; what parameters were used; what files it created; errors; rate limits; h

Logs protect against silent contamination of the evidence base.

5. AI Assistance

AI can help summarise, cluster notes, suggest search variants, draft report structure, and identify possible contradictions. It should not be treated as a source unless the task is specifically to analyse AI output.

Safe AI rule:

AI may suggest. Human verifies. Sources decide. Report cites sources, not AI confidence.

6. Exercise

Design an automation plan for a defensive brand-monitoring project. Include allowed sources, frequency, stop conditions, review queue, and a rule that no public accusation is generated automatically.

Additional Practice - Automation Stop Conditions

Every automation should have stop conditions.

Unexpected personal data appears.
A source blocks or rate-limits requests.
A tool begins returning inconsistent results.
A case becomes safety-sensitive.
A result could trigger public accusation or enforcement action.
A human reviewer cannot explain how the output was produced.

Automation without a stop switch is not a professional OSINT workflow.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Automation Boundaries

Automation is useful for organising, monitoring, summarising, and de-duplicating. It should not be allowed to make unreviewed claims about people, intent, guilt, identity, or risk.

Safe automation tasks:

- collect public URLs already in scope;
- check whether a known public page changed;
- extract dates and titles;
- de-duplicate source lists;
- summarise already-preserved documents for review;
- flag items for human checking.

Tasks requiring human review:

- identity attribution;
- scam/fraud labelling;
- legal or disciplinary conclusions;
- decisions to contact, report, publish, or escalate;
- interpretation of sensitive personal data.

8. Human-in-the-Loop Log

Automation task:
Tool used:
Input data:
Output produced:
Human reviewer:
Accepted / rejected / modified:
Reason:
Privacy check:
Date:

If a tool output influences a finding, the report should say how it was checked. “The AI said so” is not an evidence standard.

9. Prompt Hygiene for OSINT Work

When using an AI assistant for drafting or summarising, avoid pasting unnecessary personal data. Use placeholders where possible.

Instead of: John Smith at 14 Example Road...
Use: [Person A] at [private address redacted]...

Ask for structure, wording, checklists, and alternative explanations rather than asking the tool to declare someone guilty or identify a private person.

10. Automation Failure Modes

- hallucinated sources;
- outdated summaries;
- duplicated leads treated as corroboration;
- scraped snippets without context;
- false confidence from polished language;
- accidental collection outside scope;
- private data copied into logs or cloud tools.

Every automated output should be treated as a lead until a human verifies it against the original source.

11. Worked Example - Monitoring a Brand

A small business monitors public pages for brand impersonation. Automation can check known platforms for new public mentions and collect URLs. A human still reviews whether the pages are official, parody, criticism, impersonation, or unrelated.

Safe finding:

Automated monitoring flagged three public pages using similar wording. Human review confirmed one page copied the official

12. Workbook Drill - Automation Control Plan

Write a control plan for one automated workflow. Include allowed sources, excluded data, review gates, stop conditions, and where logs will be stored.

Visual Brief

V55. Human-in-the-loop automation board: task, allowed sources, rate limits, logging, review queue, confidence gate, stop switch.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 49 - Quality Control Checklist

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter provides a final gate before any OSINT output is sent, published, or acted upon. Quality control catches mistakes while they are still fixable.

By the end of this chapter, the reader should be able to:

- run a structured QC process;
- catch unsupported claims;
- check redactions and evidence links;
- identify legal/privacy concerns;
- produce a report-ready sign-off;

1. The Eight QC Gates

Use eight gates.

1. Scope: did the work answer the agreed question?
2. Source: are sources lawful, public, and recorded?
3. Evidence: can each finding be traced to evidence?
4. Analysis: are alternatives and contradictions addressed?
5. Language: is confidence clear and proportionate?
6. Privacy: has unnecessary personal data been removed?
7. Legal/escalation: does anything need specialist review?
8. Handover: can the reader understand the limits and next steps?

2. Finding Audit

For every finding, ask:

What evidence supports it?
Is the source independent?
Is there contrary evidence?
What confidence level is justified?
Is any wording stronger than the evidence?
Would the subject be unfairly harmed if this is wrong?

3. Citation Check

A report should not have orphan claims. If a sentence could damage someone or cause action, it needs source support or softer wording. Check every citation opens the correct source, matches the claim, and was captured on the date stated.

4. Redaction Check

Open the final shared files on a clean viewer, not just the editing program. Try selecting masked text. Check document properties. Inspect image exports. Confirm that filenames do not leak private information.

5. Peer Review

Where possible, ask a second reviewer to challenge the main finding. Their job is not to be polite. Their job is to find overclaims, missing alternatives, privacy risks, and confusing wording.

6. QC Sign-Off Template

Report title:
Reviewer:
Date:
Scope checked: yes/no
Evidence trace checked: yes/no
Contradictions addressed: yes/no
Redactions checked: yes/no
Confidence language checked: yes/no
Escalation required: yes/no
Notes:

Additional Practice - Final Send Checklist

Before sending a report, check:

Correct recipient.
Correct version.
No draft notes left in the file.
No hidden metadata.
Evidence links work.
Findings match confidence levels.
Redactions are irreversible in the shared copy.
Escalation language is proportionate.
Retention instructions are included.

Many serious mistakes happen after the analysis is finished, during rushed handover.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Two-Pass Quality Control

Use two different QC passes.

Analytical QC: Are the findings supported, bounded, and logical?
Production QC: Are files, links, captions, redactions, and formatting correct?

Do not combine them. When you try to check everything at once, you miss both reasoning errors and packaging errors.

8. Analytical QC Checklist

- Does each finding answer the scope question?
- Is every finding supported by cited evidence?
- Are confidence levels justified?
- Are alternative explanations considered?
- Are contradictions logged?
- Are private details minimised?
- Are recommendations proportionate?
- Is there any unsupported personal accusation?
- Has the report avoided motive claims unless directly evidenced?

9. Production QC Checklist

- File names are consistent.
- Evidence IDs match the report.
- Local links work.
- Screenshots show capture dates where possible.
- Redacted copies are actually redacted.
- Original evidence is stored separately.
- Tables are readable.
- Dates and timezones are labelled.
- Version number and date are visible.
- Final export opens correctly on another device.

10. Reviewer Sign-Off Template

Reviewer:
Date:
Scope reviewed:
Evidence pack checked:
Findings checked:
Redaction checked:
Outstanding issues:
Approved for release: yes / no
Conditions:

A sign-off template is useful even for solo work because it creates a pause before sharing.

11. Common Final Errors

- a finding number changed but the evidence index did not;
- a screenshot was renamed after being cited;
- a redacted PDF still contains selectable text;
- a limitation was removed to make the summary sound stronger;
- a private address appears in an appendix;
- a recommendation sounds like legal advice;
- a lead is described as a confirmed finding.

12. Workbook Drill - QC a Bad Report

Create a deliberately flawed one-page fictional report. Include one unsupported claim, one broken evidence ID, one missing limitation, one privacy problem, and one unclear recommendation. Then mark it up as a reviewer.

Visual Brief

V56. OSINT quality-control gate: scope, source, evidence, analysis, privacy, legal, report, and handover checks.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 50 - Full Investigation Report Case Study

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter closes Volume 5 with a full fictional report workflow. It combines clue handling, link analysis, timelines, confidence language, contradiction handling, reporting, redaction, automation control, and QC.

By the end of this chapter, the reader should be able to:

- complete a report from evidence log to final summary;
- use a timeline and entity graph together;
- include limitations and alternative explanations;
- prepare a safe evidence pack;
- perform QC before handover;

1. Fictional Scenario

A local community group asks for a defensive public-source review of a website claiming to collect donations for “Northbank Winter Shelter.” The concern is whether the donation page is officially connected to the real registered charity.

The task is not to identify private donors, confront the page operator, or make a public fraud accusation. The task is to assess public-source indicators and recommend safe next steps.

2. Scope

Included:

official charity website; public charity/company records; donation page; domain and archive clues; public social posts;

Excluded:

private donor identification; hacking or account access; contacting suspected operators; payment testing; private groups

3. Evidence Summary

E50-01 Official charity website captured; no donation-page link found.

E50-02 Donation page uses similar name and logo.

E50-03 Donation page has no charity registration number visible.

E50-04 Archive shows donation page first appeared two weeks before campaign.

E50-05 Social post from local volunteer shares official charity website, not donation page.

E50-06 Domain privacy limits ownership inference.

4. Timeline

2026-05-10: donation domain first appears in public archive.

2026-05-18: public social post promotes official charity campaign.

2026-05-21: donation page begins circulating in local group.

2026-06-07: OSINT review captures sources.

The timeline does not prove fraud. It shows the donation page appeared separately from the official campaign channels reviewed.

5. Findings

Finding 1 – Official public confirmation not found.

No reliable public source reviewed confirmed that the donation page is operated by, or officially linked from, the registered charity.

Finding 2 – The donation page uses similarity indicators.

The page uses a similar name and visual branding to the charity, but lacks visible charity registration details and does not link to the charity's official website.

Finding 3 – Safe next step is direct verification.

Potential donors should verify through the charity's official website or published contact route before using the donation page.

6. Redaction and QC

Public report redactions:

donor names removed; private comments excluded; social handles masked where irrelevant; screenshots cropped to show page content only.

QC result:

Scope matched. Findings traced to evidence. No direct fraud accusation. Confidence levels included. Redactions checked.

Additional Practice - Volume 5 Review Questions

After completing the case study, the reader should be able to answer:

What is the difference between a clue and a finding?

Which evidence supports each finding?

Which contradiction most affected confidence?

What was redacted and why?

What recommendation was safe, proportionate, and useful?

What would require escalation rather than more OSINT?

If those questions cannot be answered, the report is not ready.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Full Case Study Structure

A premium final case study should show the whole chain from question to report. Use this structure for the fictional case.

1. Request received.
2. Authority and scope confirmed.
3. Sources selected.
4. Evidence collected.
5. Clues sorted.
6. Findings drafted.
7. Alternatives considered.
8. Confidence assigned.
9. Report written.
10. Redaction and QC completed.
11. Recommendations issued.
12. Closeout recorded.

8. Fictional Scenario - Community Charity Impersonation

A community charity reports that supporters have seen a public page using its name and asking for donations. The charity wants to know whether the page is official, unofficial, or unsafe to share.

Scope:

Allowed: public website, official social links, public platform pages, archive checks, public donation-page information.

Not allowed: contacting private individuals, attempting account access, scraping private groups, publishing accusations.

VOLUME SIX

Defensive OSINT and Professional Practice

Exposure review, fraud checks, monitoring, incident support, escalation, maintenance, and playbooks.

CHAPTERS 51-60



Chapter 51 - Personal Digital Footprint Audit

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter opens Volume 6 with defensive OSINT applied to yourself. A personal footprint audit helps reduce avoidable exposure and understand what others can learn from lawful public sources.

By the end of this chapter, the reader should be able to:

- map personal public exposure;
- separate harmless visibility from risky exposure;
- create an action plan;
- avoid panic deletion that destroys useful records;
- set review intervals;

1. Audit Scope

Start with a clear scope.

Name variants; usernames; public social profiles; old websites; public images; public documents; professional listings;

Do not audit other private people without a legitimate reason and appropriate consent.

2. Footprint Inventory

Create an inventory.

Item	Source	Exposure type	Risk	Action
Old forum profile	public search	username + town	medium	update/delete if possible
Company filing	public register	official director address	lawful public record	consider service address options
Photo album	social profile	family faces/location	high	restrict audience/redact

3. Risk Rating

Use practical risk levels.

Low: already intended public information.
Medium: contextual clues that could aid impersonation or unwanted contact.
High: private address, family details, exact routines, children, financial or security details.
Critical: credentials, tokens, identity documents, active location, or material enabling immediate harm.

4. Action Types

Possible actions:

remove; edit; restrict audience; replace with business contact; request correction; use service address; update privacy

Avoid deleting evidence of harassment or fraud before preserving it safely.

5. Review Cycle

A personal audit is not one-off. Review after major life changes, new business registrations, new domains, media appearances, house moves, or security incidents.

6. Exercise

Build a fictional personal footprint table for “Alex North.” Include one public professional listing, one risky old forum post, one family-image exposure, one company-record issue, and one action for each.

Additional Practice - Personal Audit Safety

A personal footprint audit can feel uncomfortable. Do not panic-delete everything. Prioritise immediate risks first: credentials, active location, home address exposure, family details, identity documents, and public security information. Keep a simple action log so you know what changed and why.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Defensive Audit Boundaries

A personal footprint audit is about reducing exposure, not investigating someone's private life. The subject should be the person requesting the audit or someone they are clearly responsible for protecting, such as their own business identity or a dependent with proper consent.

Allowed: your own public profiles, your own domains, public search results about you, exposed contact routes, old forgotten

Not allowed: invading another person's accounts, bypassing privacy settings, collecting intimate details, exposing relationships

8. Personal Exposure Inventory

Category	Example	Risk	Action
Name variants	old usernames	medium	record and review
Email addresses	public contact email	low/medium	separate personal and public use
Phone numbers	personal mobile in public post	high	remove or replace where possible
Addresses	home address in old document	high	request removal if appropriate
Photos	identifiable home/work clues	medium/high	review and reduce
Old accounts	unused profiles	medium	close or secure
Data-broker entries	people-search pages	variable	opt-out where available

9. Prioritising Fixes

Handle high-harm and easy-fix items first.

Priority 1: home address, personal phone, exposed family details, account recovery clues.

Priority 2: reused usernames, old emails, outdated profiles, public documents.

Priority 3: image clutter, duplicated biographies, low-risk old mentions.

Do not try to erase the internet in one sitting. A defensive audit is a maintenance routine.

10. Safe Search Set

Use a controlled set of searches for yourself:

```
"Full Name"
"Full Name" "Town"
"Full Name" "Email"
"Known username"
"Known email address"
"Business name" "Full Name"
```

Record only what is necessary to remove, secure, or monitor. Do not build dossiers on unrelated people who appear in the results.

11. Action Log Template

Item found:
Source:
Risk level:
Action taken:
Removal/contact URL:
Date requested:
Follow-up date:
Result:
Notes:

12. Workbook Drill - Your Public Profile Snapshot

Create a fictional personal profile and identify ten exposure points. Group them into remove, secure, monitor, and ignore. Write a short action plan that avoids panic and focuses on practical risk reduction.

Visual Brief

V58. Personal footprint dashboard: accounts, emails, usernames, images, addresses, documents, breaches, privacy settings, and action tracker.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 52 - Family and Small-Business Exposure Review

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter applies defensive OSINT to households, clubs, sole traders, and small businesses. The goal is not secrecy. The goal is controlled visibility: the right information public, unnecessary risk reduced.

By the end of this chapter, the reader should be able to:

- review exposure for families and small organisations;
- protect vulnerable people;
- separate personal and business contact routes;
- reduce routine/location leakage;
- document consent and boundaries;

1. Consent and Sensitivity

Family and small-business reviews can involve sensitive personal details. Get consent where appropriate, especially for adults. Treat children, vulnerable people, home addresses, medical details, school locations, and routines as high-risk by default.

2. Exposure Categories

Review:

websites; social pages; club pages; event listings; business directories; company records; domain records; public photos

3. Home and Business Separation

Small businesses often leak personal life because the home is also the office. Defensive options include:

service address or registered office provider where lawful; business phone number; generic role inbox; separate social p

4. Photo and Event Risks

Event photos can reveal children, badges, whiteboards, vehicle plates, addresses, expensive equipment, alarm panels, and travel routines. Build a simple photo check before posting.

5. Small-Business Review Table

Asset	Public exposure	Risk	Mitigation	Owner
Website contact page	personal mobile visible	medium	replace with business number	owner
Google listing	home address public	high	assess service-area setup	owner
Team photo	ID badges readable	medium	replace image/redact	admin

6. Exercise

Design a defensive review for a fictional family-run radio shop. Include website, social page, domain, public photos, reviews, and staff contact routes.

Additional Practice - Small Organisation Pitfalls

Small organisations often create risk accidentally:

using personal mobiles as official numbers; publishing volunteer home addresses; reusing personal emails for business; p

Most fixes are simple once someone looks carefully.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Consent and Proportionality

Family and small-business reviews require extra care. A person may want help protecting relatives or staff, but that does not give unlimited permission to collect information about them. Use consent wherever possible and keep the review focused on exposure reduction.

Good scope: public business contact details, official pages, exposed documents, impersonation risks.

Poor scope: private relationships, personal arguments, hidden account discovery, unnecessary location tracking.

8. Small-Business Exposure Areas

- official website contact details;
- domain registration and renewal reminders;
- public director or officer information;
- old PDFs with private metadata;
- staff names and roles;
- exposed email patterns;
- duplicate or fake social pages;
- outdated phone numbers;
- public reviews containing sensitive incident details;
- supplier/customer references that reveal more than intended.

9. Family Safety Review Areas

- children's school or activity clues;
- home-location clues in photos;
- public birthday or routine information;
- shared family surnames and addresses;
- old marketplace listings;
- pet names used as password clues;
- public holiday posts that reveal absence from home.

The goal is not fear. The goal is reducing avoidable exposure.

10. Review Meeting Template

Who requested the review?
Who is included?
What consent exists?
What sources are allowed?
What will not be checked?
What risks matter most?
How will findings be shared?
What will be deleted after the review?

11. Recommended Output

For a family or small business, use a simple action report.

Issue | Why it matters | Evidence | Recommended action | Owner | Priority | Follow-up date

Avoid long dramatic reports. People need clear actions they can actually complete.

12. Workbook Drill - Exposure Reduction Plan

Create a fictional small-business footprint with a website, Facebook page, old PDF menu, Companies House record, and staff page. Identify what should stay public, what should be redacted, and what should be monitored.

Visual Brief

V59. Household and small-business exposure map: people, roles, public contact points, assets, routines, web presence, and mitigation actions.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 53 - Scam, Fraud, and Impersonation Checks

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter gives a safe public-source workflow for checking suspicious messages, donation pages, shops, recruiters, investment claims, and impersonation attempts without engaging the suspect or putting the investigator at risk.

By the end of this chapter, the reader should be able to:

- triage suspicious claims;
- check official confirmation routes;
- identify common public indicators;
- avoid direct engagement;
- escalate safely when needed;

1. Triage First

Ask:

What is being requested? Money, credentials, remote access, personal data, urgency, secrecy?
Who is allegedly asking?
What official channel can confirm it?
What evidence exists without clicking risky links?
What harm could occur if the claim is wrong?

2. Indicator Matrix

Indicator	Examples	Meaning	Caution
Identity	similar name/logo	possible impersonation	brands can have subsidiaries
Domain	new or lookalike domain	risk signal	new domains can be legitimate
Payment	unusual route/crypto/gift cards	high concern	verify official policy
Contact	pressure/urgency/secrecy	scam pattern	not proof alone
Social proof	reposts/testimonials	weak support	can be copied or faked
Official confirmation	link from official site	strong support	page may be compromised; preserve carefully

3. Do Not Engage Recklessly

Do not bait, threaten, harass, click unknown downloads, enter fake credentials, test stolen cards, or try to “hack back.”
Preserve evidence and use official reporting routes or internal security processes.

4. Impersonation Review

For a suspected impersonation:

compare official website links; check verified social links; inspect wording and contact route; search exact phrases; cl

5. Reporting and Escalation

Depending on context, escalation might go to a bank, platform abuse route, Action Fraud or local equivalent, internal security, domain registrar abuse contact, hosting provider abuse contact, or the impersonated organisation. The report should state evidence and avoid public naming unless legally safe and necessary.

6. Exercise

Review a fictional invoice email claiming bank details changed. Build a safe verification plan using only known contact routes and public evidence.

Additional Practice - Verification Without Engagement

The safest verification route is usually sideways, not forwards. Do not interact with the suspicious link if you can verify through an official site, known phone number, bank, platform report route, or independent public notice. Sideways verification reduces risk and preserves evidence.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Indicators Are Not Proof

Scam and impersonation checks must be written carefully. Indicators can justify caution, preservation, and reporting, but they do not automatically prove who is behind the activity.

Indicator: copied logo.

Possible meaning: impersonation or unauthorised reuse.

Alternative: old partner, fan page, template, or careless user.

Required next step: compare with official links and preserve evidence.

8. Public Scam Indicator Checklist

- payment route differs from official source;
- urgent pressure language;
- copied branding with no official link;
- newly created page claiming established authority;
- mismatched contact email domain;
- poor or inconsistent legal/company details;
- requests for unusual payment methods;
- comments from users reporting confusion;
- no privacy/contact information where expected;
- claims that cannot be verified from official channels.

Use this checklist to decide whether caution is warranted, not to name a culprit.

9. Verification Route

1. Preserve the suspicious public page.
2. Identify the official source separately.
3. Compare contact routes and payment routes.
4. Check whether official pages link to the questioned page.
5. Record uncertainty.
6. Recommend safe contact through official channels.
7. Report through platform/provider routes where appropriate.

10. Reporting Language

Unsafe:

This person is running a scam.

Safer:

The page displays public indicators consistent with impersonation and should not be treated as official unless confirmed

11. Evidence Preservation for Scam Checks

- screenshot the full page;
- capture the URL;
- record date and time;
- preserve payment/contact details if visible;
- avoid entering personal data;
- do not test payments;
- do not engage with suspected operators;
- keep originals restricted and share redacted copies.

12. Workbook Drill - Impersonation Triage

Create three fictional pages: one official, one fan page, and one suspicious donation page. Write the indicators, alternative explanations, confidence level, and recommended action for each.

Visual Brief

V60. Defensive scam-check matrix: identity, domain, payment, contact method, social proof, complaints, official confirmation, and escalation route.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 54 - Brand and Domain Monitoring

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter shows how organisations can monitor public sources for brand misuse, lookalike domains, fake profiles, unauthorised marketplaces, and misleading claims while staying proportionate and lawful.

By the end of this chapter, the reader should be able to:

- define brand-monitoring scope;
- build keyword and asset lists;
- triage alerts;
- document lookalike indicators;
- escalate safely;

1. Asset Register

Start with your own official assets.

Brand names; trading names; product names; domains; social handles; logos; slogans; support email patterns; phone numbers

Monitoring without an asset register creates noise.

2. Monitoring Sources

Use lawful public sources such as search alerts, platform search, domain/RDAP lookups, certificate transparency search interfaces, marketplace searches, app stores, review sites, and news/community sources. Respect terms, rate limits, robots instructions, and privacy boundaries.

3. Lookalike Domain Checks

Look for safe public indicators:

extra hyphens; swapped letters; different TLD; added words like support/login/payments; copied logos; unusual payment methods

Do not attempt to access admin areas or test login forms.

4. Triage Queue

Alert	Type	Risk	Evidence	Action
brand-support.example	lookalike domain	high	screenshot + RDAP data	legal/security review
marketplace listing	unauthorised product	medium	listing capture	platform report
social profile	parody/criticism	low/rights-sensitive	public profile	no action unless impersonation

5. Escalation Pack

For takedown or abuse reports, prepare:

proof of official brand ownership; captured offending page; why it is misleading; dates; URLs; screenshots; redacted personal data

6. Exercise

Build a brand-monitoring plan for fictional “Aldermere Field Tools.” Include official assets, five alert queries, triage levels, and an escalation pack checklist.

Additional Practice - Monitoring Noise Control

Brand monitoring can drown a small team in false positives. Reduce noise by using tiers.

Tier 1: exact brand + payment/login/support words.
Tier 2: lookalike domains and copied logos.
Tier 3: general mentions, reviews, complaints, forum posts.

Review high-risk tiers first and record why low-risk mentions were ignored.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Monitoring Without Over-Collecting

Brand and domain monitoring should focus on assets, names, and public references relevant to the organisation. It should not become mass surveillance of customers, critics, or private individuals.

Monitor: brand name, domain variants, official social handles, public impersonation pages, public phishing indicators.
Do not monitor: private users, closed groups, unrelated critics, staff personal lives, or personal accounts outside scope.

8. Monitoring Register

Asset	Official value	Variants to monitor	Source type	Frequency	Owner	Notes
Domain	example.org	example-support.org, example.org	domain/RDAP/search	weekly	admin	watch for impersonation
Brand	Example Charity	Example Donations	search/social	weekly	comms	donation scam risk
Email	info@example.org	support@example-donations.org	public reports only	monthly	admin	do not solicit emails

9. Domain Variant Thinking

Domain variants can include typos, added words, different top-level domains, hyphenated versions, and lookalike characters. Treat these as leads only. A similar domain may be benign, parked, unrelated, or malicious.

Safer wording:

The domain resembles the organisation's brand and should be reviewed before any public warning is issued. Public evidence

10. Alert Review Workflow

1. Alert received.
2. Check whether it matches scope.
3. Preserve public evidence if relevant.
4. Compare against official assets.
5. Classify: benign / monitor / suspicious / escalate.
6. Record action and reviewer.
7. Avoid contacting suspected operators directly.

11. Monthly Brand Safety Report

New public mentions:
New suspicious domains:
Impersonation indicators:
False positives closed:
Actions taken:
Items needing escalation:
Recommended communication:

A monthly summary is often more useful than a pile of raw alerts.

12. Workbook Drill - Build a Monitoring Plan

Create a fictional organisation with one domain, two official social accounts, and three likely brand variants. Build a monitoring register and define what would trigger escalation.

Visual Brief

V61. Brand monitoring board: official assets, keywords, lookalike domains, social profiles, marketplaces, alerts, triage, and escalation.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 55 - Incident Support and Evidence Preservation

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter explains how OSINT skills can support incidents such as impersonation, phishing, harassment, misinformation, scam pages, or public data exposure. The focus is preservation and structured support, not investigation theatrics.

By the end of this chapter, the reader should be able to:

- preserve public evidence safely;
- avoid contaminating an incident;
- build an incident timeline;
- support internal or official reporting;
- know when to escalate;

1. First Rule: Preserve Before Acting

If a harmful page or message is live, preserve evidence before reporting or confronting. Reporting may remove the content, which is good, but it can also remove material needed for investigation. Preserve only what is lawful and necessary.

2. Incident Evidence Log

ID	Time noticed	Source	What happened	Preservation	Risk	Escalation
I55-01	2026-06-07 09:30	email	invoice bank change request	header/body PDF, screenshot	high	finance/security
I55-02	2026-06-07 10:05	website	lookalike payment page	screenshot, URL, archive if safe	high	hosting/platform

3. Do Not Contaminate

Avoid replying, clicking risky links, downloading unknown attachments, submitting forms, logging into suspicious pages, or changing evidence files. Use screenshots, headers, safe text copies, and controlled capture methods according to your organisation's policy.

4. Timeline and Chain of Custody

Record who collected what and when. Use clear filenames. Keep originals separate. If legal, employment, or law-enforcement action may follow, follow organisational procedure and avoid amateur "enhancement" of evidence.

5. Escalation Triggers

Escalate when there is:

credential theft; financial loss; threats to safety; child or vulnerable-person risk; extortion; malware; active impersonation

6. Exercise

Create a preservation plan for a fictional phishing campaign targeting a small business. Include email headers, screenshots, timeline, internal owner, bank notification, and platform report package.

Additional Practice - Incident Handover Note

An incident handover should be short and factual.

What happened?
When was it noticed?
What has been preserved?
What has not been touched?
Who has been informed?
What risk exists now?
What decision is needed?

This helps technical, legal, financial, or safeguarding responders act quickly.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Incident Support Is Not Incident Command

OSINT can support an incident, but it should not overtake the incident response process. The OSINT role is to preserve relevant public evidence, clarify public exposure, and provide careful context.

OSINT can help with:

- public impersonation evidence;
- visible phishing pages;
- public claims or rumours;
- exposed documents;
- timeline of public posts;
- screenshots and source lists.

OSINT should not:

- access systems without permission;
- engage suspected attackers;
- publish accusations;
- interfere with legal, HR, or technical response;
- collect unrelated private information.

8. Incident Evidence Log

Evidence ID:
Incident reference:
Source:
URL:
Capture date/time:
Captured by:
Method:
What it shows:
Related risk:
Redaction status:
Escalation owner:

9. Preservation Priorities

During an incident, collect volatile public evidence first.

Priority 1: pages likely to disappear, public threats, impersonation pages, active payment/contact routes.
Priority 2: background context, archive checks, historical mentions.
Priority 3: general commentary and low-relevance discussion.

Do not panic-collect everything. Focus on the incident question.

10. Communication During an Incident

Use calm labels:

Observed public claim.
Unverified public report.

Preserved screenshot.
Potential impersonation indicator.
Confirmed official statement.
No reliable public confirmation found.

Avoid inflammatory labels until the organisation has verified the facts and chosen the correct response path.

11. Handover Package

Incident summary;
scope of OSINT support;
evidence index;
key screenshots;
timeline;
known limitations;
recommended next actions;
retention/deletion note.

The handover should be clear enough for a manager, legal adviser, platform support team, or law-enforcement contact to understand without reading every working note.

12. Workbook Drill - Preserve an Impersonation Incident

Create a fictional public impersonation page. Build an evidence log, a three-entry timeline, and a short handover note. Include what you deliberately did not collect.

Visual Brief

V62. Incident evidence preservation flow: detect, preserve, isolate, log, escalate, report, retain, review.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 56 - Working With Clients or Teams

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter covers professional handling when OSINT is done for a client, employer, club, charity, journalist, or team. Most problems in OSINT work come from vague scope, poor expectations, and unclear data handling.

By the end of this chapter, the reader should be able to:

- set engagement scope;
- define authority and exclusions;
- manage sensitive data;
- communicate interim findings safely;
- close out with clear deliverables;

1. Start With Authority

Before work starts, record who requested it, why, and what authority they have. Defensive OSINT for a business website is different from researching a private person. If authority is unclear, narrow the work to public organisational assets or stop.

2. Statement of Work

A lightweight statement of work should include:

objective; scope; exclusions; sources allowed; methods not allowed; data handling; deadline; deliverables; escalation

3. Communication Discipline

Interim notes can cause harm if shared casually. Label them clearly.

Draft lead – not verified.
Preliminary finding – subject to review.
Final finding – QC complete.

Do not send dramatic screenshots without context.

4. Team Roles

Define roles:

collector; analyst; reviewer; client contact; legal/privacy contact; incident owner.

One person may hold several roles on a small project, but the responsibilities should still be named.

5. Closeout

At closeout, provide:

final report; evidence pack index; redaction note; limitations; recommendations; open questions; retention/deletion status

Do not leave sensitive evidence scattered in chat, email, downloads, or personal cloud folders.

6. Exercise

Write a one-page engagement brief for a charity asking you to check impersonation pages. Include what you will not do.

Additional Practice - Expectation Management

Tell clients or team members what OSINT can and cannot do. It can identify public indicators, preserve evidence, map relationships, and assess confidence. It cannot lawfully guarantee hidden identity, replace police powers, bypass privacy controls, or prove intent without adequate evidence.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Intake Form

A professional engagement starts with intake. The intake form prevents vague requests such as “find everything about them” from turning into unsafe work.

Client/team name:
Requester:
Objective:
Legitimate purpose:
Authority:
People or organisations in scope:
Sources allowed:
Sources excluded:
Data sensitivity:
Deadline:
Deliverables:
Escalation contact:
Retention/deletion plan:

If the legitimate purpose cannot be written clearly, the work should not start.

8. Scope Control Phrases

Use plain phrases to hold the boundary.

That is outside the agreed scope.
That would require separate authority.
That involves private personal data and is not necessary for this task.
We can record the lead but not pursue it without a lawful reason.
This finding should be treated as preliminary until reviewed.

These phrases are useful because pressure often appears mid-investigation, especially when early findings are interesting.

9. Team Review Rhythm

Kickoff: confirm scope and exclusions.
Collection review: check evidence quality and privacy boundaries.
Analysis review: test findings and alternatives.
Redaction review: prepare safe deliverable.
Closeout: agree retention, deletion, and next steps.

Even a solo analyst can run these as checkpoints.

10. Client-Safe Interim Updates

Interim updates should be brief and bounded.

We have preserved three public pages relevant to the agreed scope. One page displays indicators of impersonation, but the client has not yet seen it. This avoids drama and prevents the client from acting on unfinished leads.

11. Closeout Checklist

- final report delivered;
- evidence pack index delivered or retained as agreed;
- redaction note completed;
- sensitive working copies cleaned up;
- unresolved leads marked clearly;
- retention/deletion date recorded;
- lessons learned captured for future playbook.

12. Workbook Drill - Refuse Unsafe Scope Politely

Write a response to a fictional client who asks you to identify the private person behind a critical social-media account. Keep it professional, offer safe alternatives, and redirect to public brand-safety monitoring.

Visual Brief

V63. OSINT engagement board: request, scope, authority, data handling, communication rhythm, review gates, deliverables, closeout.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 57 - Legal Boundaries and Escalation

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter gives a practical boundary framework. It is not legal advice. It helps investigators recognise when to stop, seek specialist advice, or escalate to the right authority.

By the end of this chapter, the reader should be able to:

- spot legal and ethical boundary issues;
- understand personal-data caution;
- recognise regulated or safety-sensitive cases;
- prepare escalation packets;
- avoid public accusations;

1. Boundary Questions

Ask before and during the work:

Is the source public and lawfully accessible?
Is the subject a private person, public role, company, or organisation?
What is the legitimate purpose?
Is the collection necessary and proportionate?
Could the output cause unfair harm?
Is specialist advice needed?

2. Hard Stops

Stop and escalate when the work involves:

threats to life or safety; child protection; extortion; active fraud loss; malware; stolen credentials; private intimate

Do not try to handle high-risk matters alone.

3. Personal Data and Minimisation

When personal data appears, keep only what is needed for the purpose, protect it, redact it in outputs, and document why it was used. Public availability does not automatically make use fair, safe, or lawful.

4. Escalation Pack

An escalation pack should be factual.

summary of concern; URLs/sources; screenshots; dates/times; evidence IDs; actions already taken; risk assessment; contact

Avoid speculation, insults, or accusations beyond the evidence.

5. Public Communication Risk

Publishing an allegation can create legal and safety risk. A safer public communication often says:

We are aware of a page/message using our name. Please use only the official contact details listed here while we review

6. Exercise

For five fictional cases, decide whether to continue, narrow scope, seek legal/privacy review, escalate to police/platform/bank, or stop entirely.

Additional Practice - Escalation Wording

Use calm escalation wording.

We identified public indicators that may require review.
The attached evidence pack records what was visible at the time of capture.
We have not attributed the activity to a private person.
We recommend review by the appropriate legal/security/platform channel.

This keeps the work useful without turning it into an accusation.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Boundary Questions

Before collecting or reporting, ask four questions:

Purpose: why is this work being done?
Authority: who has the right to request it?
Necessity: what information is actually needed?
Proportionality: could this cause unnecessary harm?

If any answer is weak, narrow the work or stop.

8. Escalation Triggers

Some situations should move beyond ordinary OSINT handling.

- threats of violence or self-harm;
- suspected child exploitation or safeguarding issues;
- active fraud involving payment loss;
- extortion or blackmail;
- unauthorised access or malware indicators;
- private intimate material;
- doxxing or harassment campaigns;
- legal demands or regulatory matters.

The OSINT role is evidence preservation and referral through appropriate channels, not vigilante action.

9. What Not to Do

Do not contact suspected offenders to confront them.
Do not publish personal details.
Do not attempt account access.
Do not bypass privacy controls.
Do not buy stolen data.
Do not pretend to be someone else.
Do not give legal advice if you are not qualified.
Do not continue collecting once the legitimate purpose is gone.

10. Escalation Note Template

Issue:
Why it may require escalation:
Evidence preserved:
Immediate risk:
People affected:
Recommended recipient:
What has not been done:
Analyst name/date:

The “what has not been done” line is important. It shows restraint and protects the integrity of the work.

11. Legal Language in Reports

Avoid legal labels unless they come from an authority or qualified adviser.

Risky: This is fraud.

Safer: The public page displays indicators commonly associated with donation fraud and should be escalated to the platform.

12. Workbook Drill - Escalation Decision

Given five fictional situations, decide whether to continue, narrow scope, escalate, or stop. For each, write one sentence explaining the boundary.

Visual Brief

V64. Legal and escalation decision tree: public source, personal data, safety risk, regulated issue, evidence preservation, specialist review, official report.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 58 - Tooling, Maintenance, and Updates

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter explains how to keep an OSINT toolkit reliable without chasing every shiny tool. Tools change, break, get acquired, lose access, or become unsafe. A professional workflow survives because it is method-led, not tool-led.

By the end of this chapter, the reader should be able to:

- build a tool register;
- review tools for safety and privacy;
- track versions and source changes;
- avoid dependency on one platform;
- retire risky tools;

1. Method Before Tool

A tool is only useful if you know the question, source, evidence standard, and limitation. Do not write “Tool X found...” as if the tool is the source. Write what source was checked and what was observed.

2. Tool Register

Tool	Purpose	Data entered	Source checked	Version/date	Risk	Notes
Reverse image service	find earlier use	image/crop	public web index	reviewed monthly	medium	avoid sensitive
Timeline spreadsheet	organise dates	evidence log	internal notes	local	low	backup weekly
AI summariser	draft summaries	redacted notes	internal	reviewed quarterly	medium	human verifies

3. Update Routine

Review tools periodically.

Does it still work?
Has pricing or access changed?
Does it collect uploaded data?
Are results reproducible?
Is there an export option?
Are there safer alternatives?
Does it encourage overcollection?

4. Tool Safety

Avoid uploading sensitive evidence to services unless authorised and necessary. Check privacy terms. Prefer redacted samples for testing. Keep API keys out of reports and screenshots. Use separate browser profiles for research and personal life.

5. Retirement

Retire a tool when it becomes unreliable, legally questionable, privacy-hostile, unsupported, or unnecessary. Keep a note of why it was retired so future users do not reintroduce it casually.

6. Exercise

Create a five-tool register for a defensive OSINT workstation: search, archive, image, timeline, and reporting. Add one risk and one mitigation for each.

Additional Practice - Tool Change Log

Keep a tool change log.

Date	Tool	Change	Impact	Action
2026-06-07	reverse image service	upload terms reviewed	sensitive images not uploaded	use crops/redactions only
2026-06-07	report template	redaction note added	safer handover	update playbook

When tools change, the playbook should change too.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Tool Register

A professional OSINT workspace needs a tool register. Tools change, websites change, APIs change, and browser extensions can introduce risk.

Tool name:
Purpose:
Official website:
Installed version:
Last checked:
Data handled:
Account/API required:
Privacy considerations:
Replacement option:
Keep / update / remove:

8. Update Routine

Weekly: check bookmarks and critical source links.
Monthly: review browser extensions, saved logins, and tool versions.
Quarterly: test templates, export formats, and backup restoration.
Annually: review legal/safety wording, tool list, and training examples.

Maintenance is part of professional practice, not admin fluff.

9. Tool Risk Categories

Low risk: official public registers, archive services, manual search.
Medium risk: browser extensions, AI summarisation tools, alert services.
High risk: bulk scrapers, unofficial APIs, tools requiring sensitive uploads, tools of unclear origin.

High-risk tools are not automatically forbidden, but they require stronger justification and controls. For this book's defensive workflow, prefer official sources and transparent methods.

10. Broken Tool Contingency

Every important workflow should have a manual fallback.

If reverse image search changes: use multiple services and manual visual checks.
If alert service fails: run scheduled manual searches.
If archive service is unavailable: preserve screenshots and source notes.
If AI summary is unreliable: return to original documents and analyst notes.

11. Workspace Hygiene

- separate OSINT browser profile;
- remove unused extensions;
- clear downloads after evidence is filed;
- keep case folders separate;
- back up templates;
- record tool changes in the changelog;
- avoid installing random scripts into the main work machine.

12. Workbook Drill - Tool Audit

List ten tools or websites used in the course. Mark each as keep, replace, test, or remove. Add a reason and a last-checked date.

Visual Brief

V65. OSINT toolkit maintenance board: tool register, purpose, version, data handled, update date, risk, replacement, and retirement status.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 59 - Building Your OSINT Playbook

Safety and lawful-use note: This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.

Purpose of This Chapter

This chapter helps the reader turn the book into repeatable playbooks. A playbook is not a script to follow blindly. It is a controlled starting point that reduces mistakes and makes good practice easier under pressure.

By the end of this chapter, the reader should be able to:

- write reusable OSINT playbooks;
- include safety gates and stop points;
- create templates for common tasks;
- maintain playbooks over time;
- train others consistently;

1. What a Playbook Contains

A practical playbook includes:

purpose; when to use; when not to use; required authority; allowed sources; prohibited methods; steps; evidence template

2. Playbook Types

Useful defensive playbooks:

personal footprint audit; brand impersonation check; donation-page verification; phishing evidence preservation; domain

3. Decision Gates

Every playbook should have gates.

Gate 1: legitimate purpose confirmed.
Gate 2: scope and exclusions recorded.
Gate 3: high-risk personal data encountered?
Gate 4: finding confidence sufficient?
Gate 5: legal/privacy escalation needed?
Gate 6: redaction complete before sharing?

4. Template Library

Keep templates in one folder.

case_folder_template; evidence_card; source_list; timeline; entity_table; graph_relationship_table; redaction_log; report

5. Review and Training

Schedule playbook reviews. Update when platforms change, laws or policies change, tools fail, a mistake is found, or a new case reveals a better workflow. Training should include examples of what not to do.

6. Exercise

Write a short brand-impersonation playbook for a small business. Include one hard stop, one escalation route, and one public-message template.

Additional Practice - Playbook Ownership

Every playbook needs an owner. The owner does not have to do all the work, but they must review the playbook, approve changes, retire unsafe steps, and make sure users know the boundaries. An ownerless playbook slowly becomes stale advice.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - What a Playbook Contains

A playbook is a reusable method. It should be specific enough to guide action but flexible enough to adapt.

Playbook name:
Use case:
Scope:
Allowed sources:
Excluded actions:
Step-by-step workflow:
Evidence required:
Decision points:
Escalation triggers:
Report output:
Redaction rules:
QC checklist:

8. Starter Playbooks

Personal footprint audit.
Small-business exposure review.
Brand impersonation check.
Domain monitoring review.
Public event verification.
Image/geolocation verification.
Incident evidence preservation.
Final report QC.

Each playbook should link to the relevant chapter and template.

9. Playbook Decision Points

A useful playbook includes stop/go decisions.

Continue when: evidence is public, relevant, proportionate, and in scope.
Narrow when: private data appears or scope becomes too broad.
Escalate when: immediate harm, fraud, safeguarding, legal, or technical incident triggers appear.
Stop when: purpose is unclear, authority is missing, or continued collection would be harmful.

10. Example - Brand Impersonation Playbook

1. Confirm official brand assets.
2. Preserve questioned public page.
3. Compare links, payment routes, logos, and wording.
4. Check whether official channels link to the page.
5. Record indicators and alternatives.
6. Assign confidence.
7. Recommend platform reporting and official public clarification if needed.
8. Avoid naming private operators without verified evidence.

11. Playbook Maintenance

Review playbooks after every case.

What worked?
What caused delay?
What created privacy risk?

What wording was unclear?
What template needs improvement?
What tool changed?

A playbook should become cleaner over time.

12. Workbook Drill - Build One Playbook

Choose one use case from this volume and write a complete one-page playbook. Include scope, stop conditions, evidence list, and final output.

Visual Brief

V66. OSINT playbook binder: triggers, scope templates, workflows, checklists, report templates, escalation contacts, and review cycle.

Design direction: dark technical workbook style, amber/gold accents, clean labels, no police branding, no hacking imagery, and clear privacy/safety markers.

End-of-Chapter Reminder

Good OSINT is not measured by how much information is collected. It is measured by whether the work is lawful, necessary, proportionate, verifiable, and reported with honest limits.

Chapter 60 - Capstone: Defensive OSINT Operation

***Safety and lawful-use note:** This chapter is for defensive, educational, journalistic, verification, safety, compliance, and public-interest OSINT. Do not use these methods to stalk, harass, intimidate, dox, expose private people, bypass access controls, obtain restricted data, impersonate anyone, or assist fraud. Work only with lawful public sources, keep collection proportionate, redact unnecessary personal data, record uncertainty clearly, and stop when the task no longer has a legitimate purpose.*

Purpose of This Chapter

This final chapter brings the entire OSINT Bible together in one fictional defensive operation. It uses foundations, search, entity work, geolocation caution, analysis, reporting, redaction, and professional practice.

By the end of this chapter, the reader should be able to:

- run a complete defensive OSINT operation;
- combine multiple volumes safely;
- produce a final report and evidence pack;
- escalate proportionately;
- capture lessons learned for a playbook;

1. Fictional Operation

A small public-facing organisation, “Aldermere Community Tools,” is concerned about fake support pages, a suspicious donation request, and reposted images claiming to show one of its events. The goal is to review public evidence, reduce harm, and recommend safe action.

2. Operation Scope

Included:

official asset register; search and archive checks; lookalike domain review; social profile verification; image reuse checks

Excluded:

private-person attribution; account access; baiting suspects; mass scraping; public accusations; payment testing; contact tracing

3. Workflow

1. Confirm legitimate purpose and authority.
2. Create case folder and evidence log.
3. Build official asset register.
4. Run search/source workflow.
5. Check domains and brand lookalikes.
6. Review public social profiles and community posts.
7. Verify reused images and event claims.
8. Build entity graph and timeline.
9. Write findings with confidence and limitations.
10. Redact, QC, and prepare escalation pack.

4. Findings Example

Finding 1: One lookalike support page uses Aldermere branding and a non-official payment link. No official public source found.

Finding 2: A photo used to criticise the organisation’s latest event appears in an earlier public post from a different source.

Finding 3: Public asset hygiene can be improved by publishing a single official support/contact page, standardising social media links.

5. Escalation and Communication

Recommended safe actions:

platform impersonation report; registrar/hosting abuse report if policy criteria are met; bank/payment provider warning

Neutral public notice example:

We are aware of pages using similar branding. Please use only the official contact and donation links listed on our web

6. Final Lessons

The capstone lesson is that OSINT is not about dramatic discovery. It is disciplined public-source work: ask the right question, collect proportionately, verify carefully, analyse honestly, report safely, and review your own limits. The best OSINT practitioner is not the one who finds the most material. It is the one who can show what the material means, what it does not mean, and what should happen next.

Additional Practice - Final Capstone Deliverables

The capstone operation should produce:

case folder; source list; evidence log; timeline; entity graph; image-verification notes; findings table; redaction log

These deliverables prove that the operation was controlled from start to finish.

Chapter Output

At the end of this chapter, the reader should add the following to their OSINT workbook:

- one completed worksheet or table from the chapter exercise;
- one short example of cautious analytical wording;
- one evidence or decision record that can be audited later;
- one note describing limitations, privacy considerations, or stop conditions;

7. Practical Expansion - Capstone Scenario

The final capstone combines the whole book into one safe defensive operation.

Fictional brief: Rivergate Community Workshop, a small non-profit, has seen a public page using its name and collecting bookings for paid training. The organisation wants a lawful public-source review to understand whether supporters may be confused and what action is safe.

Scope:

Allowed: official website, official social accounts, public search results, public platform page, archive snapshots, don
Excluded: private messages, closed groups, account access, contacting suspected operators, collecting staff/family priv

8. Operation Plan

1. Confirm authority from Rivergate contact.
2. Set up case folder and evidence log.
3. Preserve official sources.
4. Preserve questioned public sources.
5. Build source list and timeline.
6. Compare branding, contact routes, payment routes, and official links.
7. Record alternative explanations.
8. Draft findings with confidence levels.
9. Redact unnecessary personal data.
10. Produce final report and evidence index.
11. Recommend proportionate next steps.
12. Close out retention/deletion decisions.

9. Expected Evidence Pack

- E60-001 Official website homepage.
- E60-002 Official booking/payment page.
- E60-003 Official social account link list.
- E60-004 Questioned public page.
- E60-005 Questioned payment/contact route.
- E60-006 Archive snapshot if available.
- E60-007 Search results showing public confusion if relevant and safe to include.

REFERENCE SECTION

Appendices and Worksheets

Glossary, checklists, rubrics, visual index, and final QC material

Appendix A - Glossary

Attribution: The process of connecting a finding, account, event, or object to a possible person, organisation, place, or cause. Attribution should always be expressed with confidence levels.

Chain of custody: A record showing how evidence was captured, stored, handled, copied, redacted, and reported.

Claim: A statement that can be checked. A claim is not the same as a source.

Confidence level: A careful expression of how strongly the available evidence supports a conclusion.

Correlation: A connection between two or more pieces of information. Correlation does not automatically prove identity, intent, or causation.

Doxxing: Publishing or spreading personal information about a person in a way that can expose them to harm, harassment, or intimidation.

Entity: A person, account, organisation, domain, device, address, event, location, or other object being tracked in an investigation.

Evidence card: A structured note that records a single item of evidence, its source, capture date, relevance, limitations, and confidence level.

False positive: A result that appears to match but is not actually connected to the subject or question.

Finding: A checked and documented answer to part of the investigation question.

Geolocation: The process of identifying where an image, video, object, or event may be located using visible clues and supporting sources.

Hash: A digital fingerprint of a file, used to help show that the file has not changed.

Indicator: A clue that may suggest a pattern, risk, link, or direction for further checking.

Inference: A reasoned interpretation based on evidence. Inferences must be labelled clearly and should not be presented as facts.

Metadata: Data about a file or item, such as creation time, device information, dimensions, author fields, coordinates, or software history.

Open source: Publicly available information that can be accessed lawfully without bypassing controls or using deception.

OSINT: Open-source intelligence; the disciplined collection, assessment, and reporting of information from lawful public sources.

Primary source: A source closest to the original event, record, or object.

Proportionality: The principle that collection should be limited to what is necessary for the legitimate purpose.

Redaction: Removing or obscuring sensitive information before sharing or publishing.

Scope: The agreed boundary of an investigation, including what is included, excluded, and off-limits.

Source reliability: A judgement about whether a source is likely to be accurate, complete, current, and independent.

Verification: The process of checking whether a claim, source, image, event, or link is accurate and sufficiently supported.

Appendix B - Safe Investigation Checklist

Use this checklist before starting any OSINT task.

Purpose

- ■ The purpose is legitimate.
- ■ The investigation question is written down.
- ■ The expected output is known.
- ■ The work is necessary and proportionate.

Scope

- ■ Included subjects are defined.
- ■ Excluded subjects are defined.
- ■ Stop conditions are written down.
- ■ Escalation points are known.

Legal and ethical boundary

- ■ No unauthorised access.
- ■ No impersonation.
- ■ No harassment or doxxing.
- ■ No evasion of platform controls.
- ■ Personal information will be handled carefully.

Evidence handling

- ■ Case folder created.
- ■ Source log created.
- ■ Evidence card template ready.
- ■ Redaction plan ready.
- ■ Original and working copies separated.

Reporting

- ■ Findings will be separated from assumptions.
- ■ Confidence levels will be used.
- ■ Contradictions will be recorded.
- ■ Sensitive information will be redacted.

Appendix C - Source Reliability Rubric

Score each source before relying on it.

Factor	Low	Medium	High
Origin	Unknown or reposted	Identifiable but indirect	Original or official source
Date	Undated or stale	Date known but context unclear	Current and relevant date
Independence	Copies other sources	Partly independent	Independently confirms claim
Evidence	Assertion only	Some supporting material	Clear evidence or records
Incentive	Strong incentive to mislead	Mixed incentive	Low incentive to mislead
Completeness	Missing context	Partial context	Sufficient context

Recommended wording:

- **Low confidence:** The source may be useful as a lead only.
- **Medium confidence:** The source supports the finding but requires confirmation.
- **High confidence:** The source is reliable, relevant, and independently supported.

Appendix D - Confidence Language Guide

Use careful language that matches the evidence.

Avoid

- Proves
- Definitely
- Obviously
- Must be
- Exposed as
- Caught
- Guilty

Prefer

- Indicates
- Suggests
- Is consistent with
- Appears to show
- Supports the assessment that
- Has not been independently confirmed
- Alternative explanations remain possible

Confidence scale

Low confidence: One weak source, unclear context, or unconfirmed lead.

Moderate confidence: More than one source, but with some uncertainty, missing context, or possible alternative explanations.

High confidence: Multiple reliable and independent sources support the finding, and obvious alternatives have been considered.

Never increase the confidence level because a finding feels likely. Increase it only because the evidence is stronger.

Appendix E - Redaction Checklist

Before sharing any report, screenshot, worksheet, or evidence pack, check for sensitive material.

Remove or obscure where not necessary

- ■ Home addresses
- ■ Phone numbers
- ■ Personal email addresses
- ■ Private social handles
- ■ Children or vulnerable people
- ■ Medical information
- ■ Financial details
- ■ Government ID numbers
- ■ Passwords, tokens, or API keys
- ■ Exact private locations
- ■ Faces of uninvolved people
- ■ Vehicle registration details unless necessary

Keep if necessary, but justify

- ■ Public business contact information
- ■ Public company records
- ■ Official public statements
- ■ Published media where use is lawful and proportionate

Redaction log

Record every redaction with:

- Item redacted
- Reason
- Original storage location
- Redacted copy location
- Person approving release

Appendix F - OSINT Report Template

Report Title

Prepared for: Prepared by: Date: Version: Scope reference:

1. Executive Summary

Briefly state what was asked, what was found, what was not found, and the confidence level.

2. Scope

Included: Excluded: Stop conditions: Legal/ethical notes:

3. Method

Describe the public-source methods used. Do not include unnecessary sensitive operational detail.

4. Key Findings

Finding	Confidence	Main Sources	Notes

5. Evidence Summary

Evidence ID	Source	Captured	Relevance	Limitations

6. Contradictions and Alternatives

Record conflicting evidence and possible alternative explanations.

7. Limitations

State what could not be checked and what remains uncertain.

8. Recommendations

Use proportionate, lawful, practical recommendations only.

9. Redaction Notes

Summarise redactions made before sharing.

10. Appendices

Attach evidence cards, timelines, screenshots, and source logs as appropriate.

Appendix G - Tool Category Index

This index groups tool types by purpose. It does not endorse bypassing access controls, violating platform rules, or using tools against people without a legitimate lawful purpose.

Search and discovery

- General search engines
- Specialist search engines
- News search
- Academic search
- Public-register search
- Archive search

Source preservation

- Screenshot tools
- Web archive tools
- PDF capture tools
- Hashing tools
- Evidence note systems

Domain and company research

- Domain registration lookup/RDAP tools
- Certificate transparency search
- Company register portals
- Business directories
- Charity/non-profit registers

Social and community research

- Native platform search
- Public profile review
- Public group/forum search
- Community archive search

Image and geolocation

- Reverse image search
- Metadata inspection
- Map and satellite tools
- Street-level imagery tools
- Weather and sun-position references

Analysis and reporting

- Timeline tools

- Spreadsheet tools
- Diagram/entity-map tools
- Report templates
- Redaction tools

Defensive monitoring

- Search alerts
- Domain alerts
- Brand monitoring
- Impersonation checks
- Breach-notification services

Tool choice should follow the case scope, not curiosity. If a tool collects more information than needed, narrow the use or do not use it.

Appendix H - Visual Index

This appendix mirrors the working visual register so the production designer can build the visual pack later.

OSINT Bible - Visual Register

Style direction:

- Clean dark technical workbook style.
- Gold/amber accents where appropriate.
- Simple diagrams, flowcharts, checklists, evidence cards, and investigation maps.
- No fake law-enforcement branding.
- No images that imply hacking, intrusion, stalking, or illegal access.

Core Visual Set

V01. OSINT lifecycle wheel: question → collect → verify → analyse → report → review. V02. Ethical boundary diagram: public information, consent-based research, restricted data, unlawful access. V03. Evidence card template: claim, source, date captured, URL/reference, reliability, notes. V04. Source reliability pyramid: primary source, official source, reputable secondary source, social claim, anonymous claim. V05. Investigation planning board: objective, scope, exclusions, sources, risks, output. V06. Search operator cheat sheet. V07. Entity relationship map: person, company, domain, location, document, event. V08. Timeline strip: event, source, confidence, contradiction marker. V09. Geolocation clue board: signs, road markings, shadows, weather, architecture. V10. Final report anatomy: executive summary, method, findings, evidence, limitations, appendix.

Volume Visual Allocation

Volume 1: V01, V02, V03, V04, V05. Volume 2: V06 plus source map diagrams. Volume 3: V07 plus identity-match caution graphics. Volume 4: V09 plus geolocation workflow panels. Volume 5: V08, V10 plus report/checklist layouts. Volume 6: defensive audit dashboards and monitoring boards.

Additional Chapter Visuals

V11. Clean OSINT workspace layout: messy desktop vs structured project folder with evidence discipline arrow. V12. Evidence discipline chain: research question → source checked → observation → evidence card → confidence rating → finding → report citation. V13. Search funnel and search log: question → known facts → components → broad search → targeted search → verification → evidence card → finding, with a companion search log table. V14. Source reliability and bias assessment card: source ladder, assessment fields, independence check, contradiction panel, and confidence supported. V15. Entity and attribution map: separate entity cards for person/account/domain/organisation, relationship arrows with confidence badges, and a warning strip: clue ≠ identity. V16. Safe investigation planning board: central investigation plan board with panels for question, scope, exclusions, source plan, evidence method, output, risk controls, and stop points. V17. Complete mini-investigation workflow: question → scope → source plan → capture evidence → evidence cards → analysis → confidence rating → mini report, with case folder and caution markers. V18. Search operator and query-building board: research question → components → variants → query family, with core operators, search log panel, and caution strip: result = lead, captured source = evidence, verified pattern = finding.

V19. News and archive timeline board: live page, archived capture, news article, timeline strip, and caution that archive capture proves page state not truth. V20. Public registry evidence card: official search result, registration/reference number, jurisdiction, evidence card, and redaction strip. V21. Specialist source evaluation board: academic, technical, patent, dataset, and plain-English evidence translation cards. V22. Company and domain relationship map: legal entity, brand, domain, website, public record, archive, and certificate clue with confidence arrows. V23. Social account verification board: handle/display/person separation, website cross-link check, evidence card, privacy strip, and confidence badge. V24. Community source reliability board: forum thread, marketplace listing, review pattern, passive observation shield, and lead-only caution. V25. Monitoring and change detection dashboard: scope panel, alert queries, watchlist, change comparison, triage table, and stop/review marker. V26. Source list matrix: source categories, purpose, reliability, jurisdiction, limitations, review date, and discovery/evidence labels. V27. Complete search workflow case board: research question, source list, query plan, evidence cards, timeline, contradictions, finding, and monitoring footer.

V28. Person research safety gate: purpose, lawful/legitimate check, necessity, proportionality, minimisation, redaction, stop/report. V29. Username correlation matrix: same handle warning, shared indicators, contradictions, confidence, and redaction. V30. Contact clue safety ladder: public role inbox through private contact, with relevance and redaction decisions. V31. Organisation relationship map: company, trading name, product, domain, social profile, officer, document, regulator. V32. Company officer and filing timeline: incorporation, name change, officer appointment, filing, launch, public notice. V33. Public organisational footprint board: jobs, privacy policy, help docs, status page, press, procurement, talks. V34. Community information-flow map: original source, reposts, forum claims, news mention, official response, correction. V35. Scam-risk indicator matrix: identity, contact, payment, domain, reviews, complaints, official warnings, alternatives. V36. Ambiguous match decision tree: identifiers, controlled links, contradictions, confidence, and no-finding endpoint. V37. Complete entity investigation board: scope, evidence log, map, contact review, company check, community map, report.

V38. Reverse image search workflow board: starting image, claim split, preserve original, full search, crop search, text/object search, earlier-use comparison, evidence table, cautious finding. V39. Metadata handling and redaction board: original file, working copy, redacted export, plus EXIF/GPS/timestamp/filename/thumbnail privacy warnings. V40. Visual geolocation clue board: image clue zones, unique/generic markers, hypothesis table, direction-of-view arrow, and privacy shield. V41. Map and street-level comparison panel: public photo callouts alongside map/satellite/street-view checks, imagery date, scale, orientation, and match table. V42. Weather and shadow time-check board: weather, sun/shadow direction, seasonal clues, timezone conversion, and time-confidence meter. V43. Environmental clue stack: region, town, street, viewpoint, and time layers with transport, buildings, signs, language, numbers, and redactions. V44. Video verification timeline: key frames, audio clues, cut markers, reverse-frame search, source context, and limits. V45. Event verification matrix: event/location/time/cause/impact split connected to official, media, platform, map, weather, and timeline evidence. V46. Geolocation report anatomy: summary, callout image, comparison table, confidence meter, limitations, redaction/privacy footer. V47. Complete geolocation case board: source log, image search, metadata note, clue inventory, map comparison, video timeline, event matrix, final finding, redaction decisions.

Volume 5 and 6 Visuals

V48. Clue-to-finding analysis pipeline: raw clue, source, observation, verification, alternative explanation, confidence, finding, report citation. V49. Entity graph workspace: nodes for people/accounts/domains/organisations/events, edge labels, confidence badges, source citations, and privacy redaction layer. V50. Timeline strip: event date, publication date, capture date, source reliability, contradiction marker, and confidence bands. V51. Confidence language ladder: confirmed, high, moderate, low, unsupported, contradicted, with evidence and limitation fields. V52. Alternative explanation matrix: claim, supporting evidence, contradicting evidence, benign explanations, harmful explanations, next checks, conclusion. V53. Final report anatomy board: cover, executive summary, scope, method, findings, evidence table, limitations, redactions, appendix. V54. Redaction workflow: original evidence, working copy, public copy, hidden metadata check, privacy risk flags, and disclosure decision gate. V55. Human-in-the-loop automation board: task, allowed sources, rate limits, logging, review queue, confidence gate, stop switch. V56. OSINT quality-control gate: scope, source, evidence, analysis, privacy, legal, report, and handover checks. V57. Complete report case board: question, scope, evidence pack, timeline, entity graph, contradiction table, findings, redactions, QC sign-off. V58. Personal footprint dashboard: accounts, emails, usernames, images, addresses, documents, breaches, privacy settings, and action tracker. V59. Household and small-business exposure map: people, roles, public contact points, assets, routines, web presence, and mitigation actions. V60. Defensive scam-check matrix: identity, domain, payment, contact method, social proof, complaints, official confirmation, and escalation route. V61. Brand monitoring board: official assets, keywords, lookalike domains, social profiles, marketplaces, alerts, triage, and escalation. V62. Incident evidence preservation flow: detect, preserve, isolate, log, escalate, report, retain, review. V63. OSINT engagement board: request, scope, authority, data handling, communication rhythm, review gates, deliverables, closeout. V64. Legal and escalation decision tree: public source, personal data, safety risk, regulated issue, evidence preservation, specialist review, official report. V65. OSINT toolkit maintenance board: tool register, purpose, version, data handled, update date, risk, replacement, and retirement status. V66. OSINT playbook binder: triggers, scope templates, workflows, checklists, report templates, escalation contacts, and review cycle. V67. Capstone defensive operation board: objective, scope, asset register, monitoring, evidence, analysis, report, escalation, lessons learned.

Appendix I - Final QC Checklist

Use this before releasing a finished OSINT report, worksheet pack, training handout, or book edition.

Content

- ■ Findings are evidence-led.
- ■ Claims and sources are separated.
- ■ Confidence levels are used consistently.
- ■ Alternative explanations are recorded.
- ■ Limitations are visible.

Safety

- ■ No unnecessary personal data.
- ■ No doxxing-enabling details.
- ■ No instructions for unauthorised access.
- ■ No harassment or targeting language.
- ■ Escalation guidance is included where needed.

Evidence

- ■ Source log complete.
- ■ Capture dates recorded.
- ■ Screenshots labelled.
- ■ Originals preserved.
- ■ Redacted copies separated.

Production

- ■ File names are consistent.
- ■ Version number is visible.
- ■ Internal links work.
- ■ Table of contents is current.
- ■ Copyright and disclaimer are present.