COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

OSINT: Open-Source Intelligence in Litigation

Public Data, Lawful Method and Evidence That Holds Up

A vast amount of relevant information sits in plain sight: social-media posts, company filings, property and land records, court and insolvency registers, domain and website data, news, archived pages and the open web. Open-source intelligence, OSINT, is the disciplined gathering and analysis of this publicly available material to answer questions that arise in litigation, who is behind a company, where an asset or a person is, whether an account of events holds together, what a party said publicly before the dispute. Done well, OSINT is powerful, lawful and proportionate. Done badly, it strays into unlawful data-gathering, produces material that cannot be authenticated, or captures evidence in a way that is challenged and excluded. The difference lies in method: capturing public material so it can be authenticated later, respecting the law and platform terms, verifying rather than assuming, and documenting the whole process. This guide sets out for UK lawyers what OSINT covers, how it is gathered and preserved so it survives scrutiny, where its legal and ethical limits lie, and how it is deployed as evidence rather than mere information.

⏱ Estimated reading time: 24 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Its OSINT work gathers publicly available material, social media, company and property records, domain and web data, archives, lawfully and proportionately, and, crucially, captures and preserves it so it can be authenticated and relied on as evidence rather than dismissed as an unverifiable screenshot. The analysis supports asset tracing, due diligence, fact-testing and attribution, and is reported under CPR Part 35 and CrimPR Part 19 with sources, method and limits documented.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | OSINT GATHERING & PRESERVATION | AUTHENTICATED WEB CAPTURE | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: a great deal of relevant evidence sits in plain sight, but public does not mean proven, so OSINT is only useful when the material is captured and preserved so it can be authenticated, gathered lawfully and proportionately, and verified rather than assumed, turning information into evidence that holds up.

The sources (§3): social media, company and property registers, court and insolvency records, domain and website data, news and archived pages, the open web. **Capture and preservation (§4):** the decisive discipline, capturing public material with its metadata, hashes and a documented method so it can be authenticated later, not relied on as a bare screenshot that is trivially challenged. **Verification (§5):** public material is often wrong, stale or fake, so it is corroborated, its source and date established, and any account attributed to a person, not taken at face value. **Legal and ethical limits (§6):** gathering must respect the UK GDPR, platform terms, and the line against unlawful access, deception and harassment, so the method itself does not taint the evidence. **Deployment (§7):** asset tracing, due diligence, testing a party's account against what they said publicly, and attribution, deployed as authenticated, sourced evidence.

- **Much evidence is in plain sight:** social media, registers, domain data, news and archives are open to lawful gathering.
- **Public does not mean proven:** open material can be wrong, stale or fake, so it is verified and corroborated.
- **Capture for authentication:** preserve public material with metadata and hashes, not as an unverifiable screenshot.
- **Respect the limits:** lawful, proportionate gathering within the UK GDPR, platform terms and against deception.
- **Method makes it evidence:** documented sourcing and preservation turn information into evidence that survives challenge.

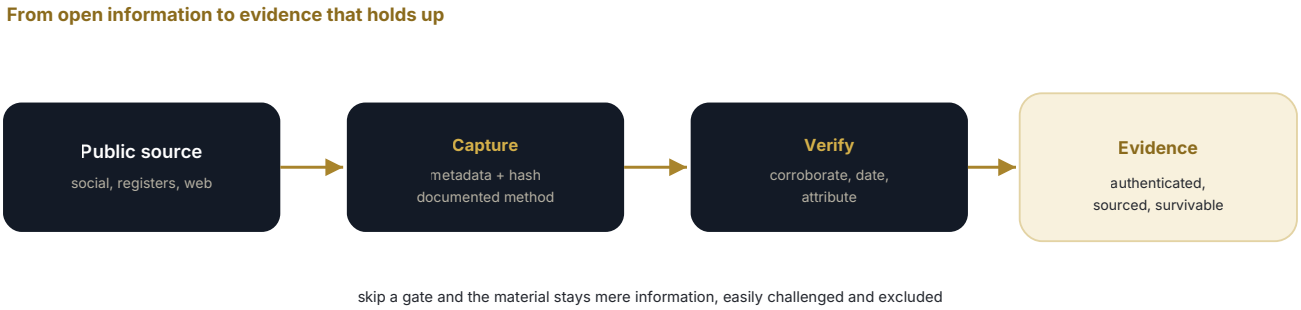

Figure 1 - OSINT becomes evidence only by passing through the gates: lawful capture with metadata, then verification, then documented sourcing; skip one and it is just an unprovable screenshot.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: public does not mean proven

There is an enormous amount of useful information sitting in the open. A party's own social-media posts may contradict their pleaded case; company registers reveal who owns and controls what; property and land records show what someone holds; court, insolvency and sanctions registers carry status and history; domain and website records show who is behind an online operation; news reports and archived versions of web pages preserve what was said and when. Gathering this openly available material to answer a live question is open-source intelligence, and it is often the quickest, cheapest and most proportionate way to learn something that matters to a case.

The trap is to assume that because something is public it is therefore proved. It is not. Public material is frequently wrong, out of date, or deliberately fake: a profile may not belong to the person assumed, a post may be misdated, a screenshot may be fabricated, a record may be superseded. And even genuine, accurate public material becomes useless as evidence if it is gathered carelessly. A screenshot of a social-media post, taken casually and pasted into a statement, is trivially challenged: how do we know it is real, that it says what it appears to say, that it was there on the date claimed, that it has not been edited? The answer is method. OSINT becomes evidence, rather than mere information, only when the public material is captured and preserved so it can be authenticated, with its source, its date, its metadata and its integrity recorded; when it is verified and corroborated rather than taken at face value; when any account is properly attributed to a person; and when the whole process is documented, and stays within the law, the platforms' terms and the bounds of proportionality and privacy. This guide is about doing OSINT so that what it finds actually holds up.

§ 0 3 · THE OPEN SOURCES

What OSINT covers: the open sources

- **Social media and the open web:** public posts, profiles, images, connections and activity across social platforms, and the wider open web, showing what a party said, did and associated with, often before the dispute crystallised (guide 96's timeline discipline): the richest and most contested source.
- **Company and corporate records:** registers of companies, officers, ownership and filings (in the UK and abroad), revealing structure, control and financial history: the backbone of who-is-behind-what analysis (§7).
- **Property, land and asset registers:** land registry, property and, where public, vehicle and other asset records, showing holdings relevant to tracing and enforcement (guide 128's asset context).
- **Court, insolvency and sanctions records:** public registers of judgments, insolvency, disqualifications and sanctions, carrying status and history that bear on credibility and risk (§7).
- **Domain, website and technical data:** domain registration, website archives and technical records showing who operates an online presence and how it has changed, tied to devices and accounts where relevant (guides 125, 126): the digital-footprint layer.

Figure 2 - the principal open sources, from social media to public registers to domain data, gathered together and cross-checked rather than relied on singly.

§ 0 4 · CAPTURE AND PRESERVATION

Capturing and preserving so it can be authenticated

- **Capture for authentication, not just a screenshot:** public material captured with its full context, the live URL, the page source, timestamps and available metadata, and hashed, so its authenticity and its state on the capture date can be proved, not merely asserted (guides 2, 3): the discipline that makes it evidence (§2).
- **Preserve before it changes:** social posts and web pages are edited and deleted, so the relevant material is captured promptly, because a post seen today may be gone tomorrow (guide 95's missing-evidence urgency): capture as preservation.
- **Use archives:** web archives and cached versions preserving prior states of pages, evidencing what a site or post said at an earlier date, captured and authenticated like any other source (§8): the record of what used to be there.
- **Document the method:** the tools, steps, dates and examiner recorded, so the capture is reproducible and its provenance clear, the OSINT equivalent of chain of custody (guide 71's reproducibility): the process that survives challenge.
- **Avoid contaminating the source:** gathering conducted so as not to alter the material, alert the subject or leave a trace that changes behaviour, using appropriate, lawful techniques (§6): the observation that does not disturb what it observes.

§ 0 5 · VERIFICATION AND ATTRIBUTION

Verification, corroboration and attribution

- **Verify, do not assume:** public material tested for accuracy and currency, since it is often wrong, stale or fabricated, and corroborated against independent sources before it is relied on (guide 100's honest-limits discipline): the antidote to public-means-proven (§2).
- **Establish source and date:** the origin and date of each item established, a post's true author and posting time, a record's currency, a page's capture date, so it is placed correctly and not misdated (guide 108).
- **Attribute accounts to people:** a social or online account linked to a real person through corroborating evidence, not assumed from a name or photo, because accounts are impersonated, shared and fake (guides 105, 126): the profile tied to the person, or honestly not.
- **Guard against fabrication:** screenshots and posts tested for authenticity, because fabricated social-media evidence is common (guide 126's provenance discipline), so captured and authenticated material is preferred to a supplied image: the fake screenshot caught.
- **Corroborate across sources:** a finding built from several open sources agreeing, company records with property records with social activity, rather than a single unverified item, so the conclusion rests on convergence (guide 124's convergence discipline).

§ 0 6 · LEGAL AND ETHICAL LIMITS

Legal and ethical limits

- **UK GDPR and privacy:** gathering and using personal data from open sources still engages the UK GDPR, so there must be a lawful basis, necessity and proportionality, and the collection is minimised to what the matter requires, publicly available is not a licence for unlimited processing (guide 20).
- **Lawful access only:** the firm line against unlawful access, no logging into others' accounts, no circumventing access controls, no computer misuse, so the gathering never crosses from open-source into unauthorised access (guide 117's self-help prohibition): public means public.
- **No deception or pretexting:** against creating fake profiles to befriend a subject, deceiving people into disclosing information, or other pretexting that is unlawful or unethical and taints the evidence and the practitioner (relevant SRA and professional duties): honest method only.
- **No harassment or surveillance overreach:** gathering that does not become harassment, stalking or disproportionate surveillance of an individual, staying within the civil and criminal limits on such conduct: observation, not intrusion.
- **Platform terms and admissibility:** the terms of platforms respected where relevant, and the method kept clean so that how the evidence was obtained does not become a ground to exclude or discredit it (guide 20): the method that does not taint the result.

§ 0 7 · DEPLOYMENT

Deployment: asset tracing, due diligence and fact-testing

- **Asset tracing and enforcement:** company, property and corporate records, with social and web data, locating assets, ownership and connections for freezing, tracing and enforcement, alongside device and financial forensics (guides 98, 128): open records turned into recoverable assets.
- **Due diligence and background:** OSINT assembling a lawful, authenticated background picture of a party, counterparty or witness, structure, history, credibility, sanctions and insolvency status, for risk and decision-making (§3).
- **Testing a party's account:** a party's own public posts and records tested against their pleaded case or witness evidence, a claimed injury against holiday photos, a claimed date against a timestamped post, a denial against a public statement (guide 98): the account checked against what they said in the open.
- **Attribution and identification:** OSINT linking accounts, sites and activity to people and entities, corroborating the device and on-chain attribution of other work (guides 105, 128): the open-source strand of naming who is behind something.
- **Presented as authenticated evidence:** OSINT findings deployed with their capture, source, date and verification documented, and their limits stated, so they are evidence a court can rely on rather than unverified assertion (§4, §5): information made into evidence.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: OSINT is itself a way of finding where evidence lives, but each open source is one node, and the same fact is usually recorded in several, which is what allows verification. A social post exists on the live platform, in the platform's own records (reachable by disclosure, guide 105), in web archives, and often in the copies others shared. A company fact exists in the register, in filings, in property and court records, and in news. A person's identity behind an account exists across their posts, their connections, their reused handles and the device and account evidence of other work. The discipline is to corroborate any open-source finding across these, because a single public item may be wrong or fake, and to remember that OSINT complements, rather than replaces, the disclosed and forensic sources: it points to where formal evidence lies and tests accounts against public statements, while the authenticated capture, the platform disclosure and the device forensics supply the proof. When a live post is deleted, the archive or a shared copy preserves it; when an account is denied, corroborating open sources and device evidence attribute it; and when a single record looks decisive, the other registers confirm or correct it.

EVIDENCE	LIVE OPEN SOURCE	WEB ARCHIVES	PLATFORM / REGISTRAR RECORDS	OTHERS' SHARED COPIES	DEVICE / ACCOUNT FORENSICS	DELETED / SUPERSEDED
Social post	Y: live (may change)	Y: prior state	Platform disclosure	Y: reshared	Device artefacts	Archive / disclosure
Company fact	Y: register	Filed history	Registry records	News reports	n/a	Superseded filings kept
Property / asset	Y: register	Prior entries	Registry	n/a	n/a	Historic titles
Account identity	Public profile	Archived profile	Registrar / platform	Connections	Y: device links	Varies
Website / domain	Y: live site	Y: archived site	Domain registration	Cached copies	Hosting records	Archived versions

Fallback strategy in one line: corroborate every open-source finding across live source, archive, register and forensic evidence; when a live post is deleted or an account denied, the archive, the shared copy and the device evidence hold and attribute it.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE HOLIDAY PHOTOS THAT ANSWERED THE INJURY CLAIM

A claimant asserted a debilitating injury confining him at home. His own public social-media activity told a different story, and the §4 discipline made it usable: rather than a casual screenshot, the relevant public posts and photographs, showing him active and abroad during the period of claimed incapacity, were captured with their URLs, timestamps and metadata, hashed and documented, and their §5 dates and authorship verified and the account attributed to him. The material was corroborated against public flight and event information (§8). When the claimant later suggested the posts were old or not his, the authenticated capture, with verified dates and attribution, held, where a bare screenshot would have collapsed. The lesson is §4's: public material becomes evidence only when captured and preserved so it can be authenticated, and the difference between a casual screenshot and a properly captured, dated and attributed record is the difference between something challenged away and something that holds.

EXAMPLE 2 · THE HIDDEN NETWORK BEHIND THE COMPANY

A dispute needed to know who really controlled a web of companies. The §3 and §7 OSINT assembled it: public company registers revealed officers, ownership and cross-directorships; property registers showed linked holdings; domain records tied several websites to common operators; and archived pages (§4) preserved earlier corporate descriptions since removed. Each source was captured and documented, and, per §5, the findings were corroborated across sources rather than resting on any single record, and accounts and entities attributed carefully. The result was an authenticated picture of the real control behind the structure, built entirely from open, lawfully gathered sources and pointing to where formal disclosure should be sought (§8). The lesson is §5's: OSINT is strongest as convergence, several open sources agreeing, captured and corroborated, reveal a structure that no single record shows, and the documented method turns that picture into evidence that supports the next step rather than mere background.

EXAMPLE 3 · THE FAKE SCREENSHOT AND THE CLEAN METHOD

A party produced screenshots of social-media posts said to prove harassment by the other side. Applying §5's guard against fabrication and the provenance discipline of guide 126, the material was tested rather than accepted: the platform's own records and web archives held no trace of the posts, the purported account showed inconsistencies, and the screenshots bore the hallmarks of fabrication. Meanwhile, the party's own lawful OSINT was conducted to the §4 and §6 standard, captured, documented, within the UK GDPR and platform terms, with no fake profiles or deception, so its evidence was clean and admissible while the opponent's fabricated screenshots were exposed. The contrast was decisive: authenticated, lawfully gathered material against unverifiable, fabricated images. The lesson is that OSINT cuts both ways, it exposes fabricated public evidence through verification, and it survives challenge itself only when gathered lawfully and captured for authentication, so method is what separates evidence from an unprovable, or fraudulent, screenshot.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The casual screenshot:** the fundamental error, a screenshot pasted into a statement with no capture, metadata or method, trivially challenged (Example 1, §4).
- **Public-means-proven:** open material taken at face value without verification, when it is often wrong, stale or fake (Example 3, §5).
- **Assuming attribution:** an account attributed to a person from a name or photo, without corroboration (§5).
- **Crossing the legal line:** logging into accounts, creating fake profiles, pretexting or circumventing access, which taints the evidence and the practitioner (§6).
- **Ignoring the UK GDPR:** personal data gathered and used without lawful basis, necessity or proportionality (§6).
- **Not preserving before it changes:** relevant posts and pages lost to editing or deletion because they were not captured promptly (§4).
- **Relying on a single source:** a finding rested on one unverified item rather than corroborated across sources (Example 2, §5).
- **Undocumented method:** the gathering not recorded, so its provenance and reproducibility cannot be shown (§4).

Technical limitations

- **Public data can be wrong or fake:** open material is unverified by nature and requires corroboration: the core limit (§5).
- **Attribution is separate:** an account is not a person without corroborating evidence (§5).
- **Material is transient:** posts and pages change and vanish, so capture is time-sensitive and gaps remain where it was not preserved (§4).
- **Legal limits bound the method:** the UK GDPR, access laws and professional duties constrain what may lawfully be gathered (§6).
- **Access varies:** some records are restricted, paywalled or foreign, so coverage is uneven and stated (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What precise question should OSINT answer, an asset, a person, a control structure, an inconsistency, so the gathering is scoped and proportionate?
- What public material do we already have, and has it been captured properly or only screenshotted?
- Are there sensitivities (privacy, the risk of alerting a subject) that shape how gathering should proceed?

Ask your opponent (where relevant)

- For any social-media or web material relied on, please provide the authenticated capture (URL, date, metadata) rather than a screenshot, and confirm the account and its attribution.
- Please confirm the source and date of any public record relied on, and whether it remains current.
- Please disclose the native or platform-authenticated version of any post or page in issue.

Ask your eDiscovery / forensic provider

- How will the public material be captured and preserved so it can be authenticated later?
- How is each item verified, dated and attributed, and corroborated across sources?
- How do we keep the gathering within the UK GDPR, access laws and platform terms so the method does not taint the evidence?

SUGGESTED WORDING · INSTRUCTION FOR AN OSINT GATHERING AND ANALYSIS

> "We instruct you to conduct open-source intelligence gathering to answer the question(s) at Schedule 1, lawfully and proportionately. Please: (1) identify and gather relevant publicly available material (social media and the open web, company, property, court, insolvency and sanctions records, domain and website data, and archives), scoped to the question and minimised as required by the UK GDPR; (2) capture and preserve each item so it can be authenticated, recording the source URL, date, page source and available metadata, hashing the capture, and documenting the tools and method so it is reproducible; (3) verify each item for accuracy and currency, establish its source and date, attribute any account or online presence to a person or entity with corroboration, and guard against fabricated material; (4) corroborate findings across multiple sources rather than relying on single items, and state confidence and limits honestly; and (5) conduct all gathering by lawful means only, without accessing others' accounts, circumventing controls, using deception or pretexting, or engaging in harassment, and respecting platform terms, so the method does not taint the evidence. Present findings with their sources, capture details and verification documented."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The OSINT checklist

- ☐ The question scoped; gathering proportionate and minimised
- ☐ Each item captured with URL, date, source and metadata, and hashed
- ☐ Material preserved promptly before it changes or is deleted
- ☐ Archives used to evidence prior states
- ☐ Each item verified for accuracy, source and date
- ☐ Accounts attributed to people with corroboration
- ☐ Findings corroborated across multiple sources
- ☐ Gathering lawful: no account access, deception or pretexting
- ☐ UK GDPR, access laws and platform terms respected
- ☐ Method documented, reproducible and reported with limits

Red flags

- A casual screenshot offered as evidence with no capture or method: Example 1.
- Public material relied on at face value without verification: Example 3.
- An account attributed to a person from a name or photo alone.
- Gathering that involved logging in, fake profiles or pretexting.
- Personal data gathered with no regard to the UK GDPR.
- A finding resting on a single unverified source.
- No record of how or when the material was gathered.

When to involve a digital forensic expert

Whenever public material is going to matter as evidence rather than mere background, because the value lies entirely in the method: the expert captures and preserves open material so it can be authenticated, with URL, date, metadata and hash and a documented, reproducible process, so it holds up where a casual screenshot collapses (Example 1, §4); verifies, dates and attributes each item and corroborates across sources, guarding against the fabricated posts that are increasingly common (Example 3, §5); keeps the gathering lawful and proportionate, within the UK GDPR, access laws, platform terms and professional duties, so the method does not taint the result (§6); and deploys the findings, for asset tracing, due diligence, testing a party's account and attribution, as authenticated, sourced evidence under CPR Part 35 or CrimPR Part 19 (§7). Through **cflab.uk** and **e-discovery.uk**, OSINT is practised as evidence-gathering, not web-searching: lawful, documented and verified, so that what is found in plain sight can actually be relied on, and so that an opponent's unverified or fabricated public material is exposed for what it is.

§ 13 · COMMON QUESTIONS

Frequently asked questions

If information is public, can we just use it?

Gather it lawfully, yes, but two cautions apply (§5, §6). First, public does not mean proven: open material is often wrong, stale or fabricated, so it must be verified, dated, attributed and corroborated before it is relied on. Second, gathering and using personal data still engages the UK GDPR and must be lawful and proportionate, and the gathering must stay within access laws and platform terms. Public material is a starting point for evidence, not evidence in itself.

Why is a screenshot not good enough?

Because it proves almost nothing on its own (§4, Example 1). A screenshot can be edited or fabricated, carries no reliable date, and has no verifiable link to a real source. Properly captured OSINT records the live URL, the page source, timestamps and metadata, is hashed, and its method is documented, so its authenticity and its state on the capture date can be proved. That is the difference between evidence that holds and an image that is challenged away.

Can we set up a fake profile to see a private account?

No (§6). Creating fake profiles to befriend or deceive a subject, logging into others' accounts, or circumventing access controls is unlawful or unethical, taints any evidence obtained and exposes the practitioner. OSINT works with genuinely public material gathered by honest means. Where information sits behind access controls, it is obtained by lawful process, disclosure, orders, not by deception or unauthorised access. The line is firm: public means public.

How do we know a social-media account belongs to the person?

By corroboration, not assumption (§5). Accounts are impersonated, shared and fake, so a name or photo is not enough. Attribution is built from corroborating evidence, consistent details across posts, connections, reused handles, and, where available, device and account forensics linking the account to the person (guides 105, 126). The honest position is stated: the account is attributed to the person where the evidence supports it, and left unattributed where it does not.

Can OSINT expose fabricated evidence?

Yes, and it often does (Example 3, §5). Fabricated screenshots of posts or messages are common, and verification, checking the platform's own records and web archives, testing the account, and applying provenance analysis (guide 126), frequently shows that the supposed material never existed. OSINT cuts both ways: it gathers genuine public evidence and it exposes fake public evidence, provided it is done with the same verification discipline in both directions.

Is OSINT a substitute for disclosure and forensics?

No, it complements them (§7, §8). OSINT is often the fastest way to learn something and to find where formal evidence lies, but public material is unverified and limited, so it points to the disclosure to seek, the account to have attributed, the asset to trace, while the authenticated capture, platform disclosure and device forensics supply the proof. Used together, OSINT and the forensic and disclosed sources are far stronger than either alone.

§ 14 · REFERENCE

Glossary

OSINT
Gathering and analysing publicly available information.

Open source
Information available to the public without special access.

Authenticated capture
Public material preserved with metadata and hash to prove it.

Web archive
A stored prior version of a web page.

Attribution
Linking an account or presence to a real person.

Verification
Testing public material for accuracy, source and date.

Corroboration
Confirmation from multiple independent sources.

Pretexting
Deceiving people to obtain information; not permitted.

Company register
A public record of companies, officers and ownership.

Provenance
The documented origin and method of gathered material.

Sources and authoritative references

The OSINT disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (OSINT gathering and authenticated capture, attribution, asset tracing, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 04 · Collection and Phase 06 · Analysis (open-source capture and verification as practised): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- ICO, UK GDPR guidance (lawful basis, necessity and proportionality when processing personal data, including from open sources): ico.org.uk · SRA Standards and Regulations (professional conduct, honesty and integrity): sra.org.uk
- Computer Misuse Act 1990 (the limit against unauthorised access): legislation.gov.uk, CMA 1990 · Forensic Science Regulator, Code of Practice v2: gov.uk, FSR Code
- PD 57AD and CPR Part 31: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

OSINT at the laboratory is practised as evidence-gathering, not web-searching, because the value lies entirely in the method. Relevant public material, social media and the open web, company, property, court, insolvency and sanctions records, domain and website data, and archives, is gathered lawfully and proportionately, scoped to the question and minimised as the UK GDPR requires (§3, §6). Each item is captured and preserved so it can be authenticated, with its URL, date, page source and metadata recorded, hashed, and the method documented and reproducible, so it holds up where a casual screenshot would collapse (Example 1, §4). Every item is verified for accuracy, source and date, accounts are attributed to people with corroboration rather than assumption, findings are corroborated across sources, and fabricated material is exposed through the same verification discipline (Examples 2 and 3, §5). The gathering never crosses into account access, fake profiles, pretexting or harassment, so the method does not taint the evidence (§6). The findings support asset tracing, due diligence, the testing of a party's account against what they said in the open, and attribution, deployed with their sources and limits documented under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding principle is simple: what is in plain sight can be relied on only if it is gathered lawfully, captured for authentication and verified.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace