COMPUTER FORENSICS LAB

London digital forensics · Established 2007

Digital Forensic Evidence: What Every Defence Lawyer Needs to Know

⏱ Estimated reading time: **19 min read · 4,358 words**

A practical guide to digital artefacts, forensic analysis and courtroom strategy, written for solicitors, barristers and litigators handling electronic evidence.

NPCC guidance · ISO 17025 · CPR 35 / CrimPR 19 · cflab.uk

§ ABOUT THE AUTHOR

WRITTEN BY COMPUTER FORENSICS LAB

Computer Forensics Lab is a London-based digital forensics practice established in 2007. Our examiners produce CPR Part 35 and CrimPR Part 19 compliant expert reports for defence solicitors, barristers, in-house counsel and private clients, and give evidence in the Crown Court, County Court, High Court and employment tribunals.

We handle mobile phone and computer examinations, cloud and email analysis, deleted data recovery, image and audio authentication, and e-discovery for civil litigation - with continuity of evidence maintained from seizure to court.

Established 2007 · London | **ISO 17025-aligned procedures** | **ACPO / NPCC digital evidence principles** | **CPR Part 35 expert reports** | **CrimPR Part 19 expert evidence** | **Court-experienced expert witnesses** | **Full chain-of-custody documentation**

§ CONTENTS

IN THIS GUIDE

Every entry is a live link: click to jump straight to that section. Each link updates the page address so you can copy and share a direct link to any section.

§ 01 · THE NEW FINGERPRINTS

1. THE DIGITAL EVIDENCE REVOLUTION

Picture a Crown Court on an ordinary Tuesday. The exhibit under discussion is not a knife or a fingerprint. It is a WhatsApp message, and counsel are arguing about whether the tick marks prove it was read. Down the corridor, a civil trial turns on whether a spreadsheet was really created in 2019 or quietly rebuilt last month. This is now the everyday texture of litigation.

Walk into any courtroom in the UK today and you will find something that would have seemed extraordinary two decades ago: lawyers arguing over pixels, timestamps and metadata. Emails, WhatsApp chats, photographs, browser histories and cloud backups have become the new fingerprints and DNA. They can establish where someone was, who they spoke to, what they knew, and when they knew it.

For defence solicitors and barristers, understanding digital evidence is no longer optional. It is essential. A single forensic artefact can dismantle a prosecution case, corroborate an alibi or expose a forged document. But digital evidence is also notoriously easy to misunderstand, misinterpret or misrepresent. That is where a qualified **digital forensics expert** becomes indispensable.

This guide walks you through the most common types of digital evidence, how forensic experts handle them, and how you can use that knowledge to strengthen your defence strategy. Whether you are dealing with a fraud allegation, a harassment claim or a complex commercial dispute, the principles here will help you ask the right questions and challenge weak evidence effectively.

§ 02 · FIRST PRINCIPLES

2. WHAT IS A DIGITAL ARTEFACT?

At its simplest, a digital artefact is any trace left behind by computer or user activity. Think of it as the digital equivalent of a footprint. Every time someone sends an email, takes a photo, browses a website or plugs in a USB drive, their device quietly records evidence of that action. Some of it is obvious: the email itself, the photo, the downloaded document. Much of it is hidden in plain sight, buried in log files, registry entries and system caches the average user never sees.

Figure 1 · Two families of artefact: what the user sees, and the record kept behind the scenes.

In forensic terms, artefacts serve three critical functions in court:

- **Corroboration:** supporting or contradicting witness testimony, strengthening or undermining a narrative.
- **Attribution:** linking a specific action to a specific person, device or account.
- **Chronology:** establishing a precise sequence of events, often to the exact second.

§ 03 · METHOD

3. THE FORENSIC PROCESS: FROM SEIZURE TO COURTROOM

Before diving into specific types of evidence, it is worth understanding how forensic experts work. The process is methodical, scientific and designed to withstand scrutiny in court. It follows five controlled stages:

Figure 2 · The five-stage laboratory workflow. One wrong move at any stage and the evidence can be challenged as contaminated.

- **Identification:** recognising every potential source of evidence: a laptop, a mobile phone, a cloud account, a USB stick, even a smart home device.
- **Preservation:** securing data before anything is touched, with every step documented.
- **Acquisition:** creating a bit-for-bit forensic image so the original is never put at risk. Hash values, the digital fingerprints of the data, prove the copy is identical.
- **Examination:** using specialist tools such as EnCase, X-Ways, Cellebrite and Magnet AXIOM to recover deleted files, build timelines and reveal hidden connections.
- **Reporting:** presenting findings in a clear, court-compliant format that judges and juries can follow without drowning in jargon.

In the UK, forensic experts operate under the National Police Chiefs' Council (NPCC) Digital Evidence Guidelines, which replaced the older ACPO Principles. These emphasise integrity, reproducibility and accountability. Any expert who cuts corners risks having their entire analysis excluded from evidence.

§ 04 · THE EVIDENCE MAP

4. COMMON TYPES OF DIGITAL EVIDENCE

The sections that follow explore the principal categories of digital evidence arising in civil and criminal cases: what each looks like, why it matters, and how a forensic expert helps you use it effectively.

Figure 3 · Eighteen evidence categories, from the inbox to unallocated disk space.

4.1 EMAILS AND WEBMAIL

Emails remain one of the most common and powerful forms of digital evidence. They reveal communication patterns, agreements, threats and intent. They are also surprisingly easy to forge, manipulate or misattribute.

What forensic experts look for: PST and OST files from Outlook, MBOX files from Thunderbird, webmail caches and, above all, message headers, which trace an email's journey through mail servers and reveal IP addresses, routing and timestamps.

How experts handle it: The mailbox is preserved by forensic imaging or export. The expert reconstructs conversation threads, verifies integrity through hash comparison and validates headers to confirm authenticity. Deleted and draft emails can often be recovered, and metadata can prove whether a message was fabricated, altered or sent at a different time than claimed.

> **For the defence:** *In a fraud case, an expert can show that an email purportedly sent by the defendant actually originated from a completely different IP address, undermining the claim of authorship.*

4.2 INSTANT MESSAGING AND SOCIAL APPS

WhatsApp, Signal, Telegram, Discord, Messenger, Skype, Teams, Slack: each platform leaves its own forensic footprint, and together they are treasure troves of evidence about relationships, intent and coordination.

What forensic experts look for: Chat logs, call logs, media attachments, deletion traces, contact lists and timestamps, extracted from mobile devices, desktop sync folders or cloud backups.

How experts handle it: Tools such as Cellebrite UFED and Magnet AXIOM parse encrypted databases like msgstore.db and app .sqlite files. Even deleted messages may be recoverable from unallocated space or cloud synchronisation data. Chats are reconstructed chronologically, metadata intact, showing exactly who said what and when.

> **For the defence:** *In a harassment case, analysis may reveal that messages were altered after the fact, or that threatening messages originated from a spoofed number or a different account entirely.*

4.3 SMS, MMS AND CALL LOGS

Text messages and call records may seem old-fashioned, but they remain highly relevant: clear records of who contacted whom, when, and for how long. They verify alibis and pin down event timing.

What forensic experts look for: Messages and call logs extracted from iTunes and iCloud backups, Android backups, or directly from the handset.

How experts handle it: Data is extracted using read-only forensic methods, with timestamps retained in UTC and converted accurately for local time zones. Deleted messages can sometimes be recovered through database techniques, and call logs establish whether communication took place exactly as alleged.

> **For the defence:** *A client accused of orchestrating an assault insisted he was asleep when the planning calls supposedly took place. The call log on his handset showed no outgoing activity that night, while the complainant's own records revealed the calls were made to a different number entirely. The timing case collapsed.*

4.4 PHOTOS AND IMAGES

A picture may be worth a thousand words, but in digital forensics the real story often lies in the metadata. Every photograph taken on a modern device carries a hidden payload: when it was taken, on what camera, and often exactly where.

What forensic experts look for: JPEG, PNG, HEIC and RAW files with embedded EXIF metadata, including camera model, timestamp and GPS coordinates.

How experts handle it: The expert extracts EXIF data, verifies image integrity and looks for manipulation such as Photoshop traces. Hash comparison links identical photos across devices, and GPS tags can be plotted on mapping software to demonstrate location patterns.

> **For the defence:** *In one insurance dispute, a claimant submitted photographs of storm damage said to have been taken the morning after the storm. The EXIF data told a different story: the images were captured eleven days earlier, on a different phone, forty miles from the insured property. The claim was withdrawn.*

4.5 AUDIO RECORDINGS AND VOICE NOTES

Audio can be compelling: admissions, threats, corroborative speech. It can also be edited, spliced or taken out of context.

What forensic experts look for: MP3, WAV, AMR and proprietary mobile formats, together with metadata such as creation date and device ID.

How experts handle it: The expert preserves the original file, examines encoding parameters and compares background noise and digital signatures for signs of tampering. Spectrogram analysis reveals edits and splices, and a clean chain of custody keeps the recording admissible.

> **For the defence:** *A voice note produced in a family dispute appeared to capture a threat. Spectrogram analysis showed an abrupt change in room tone mid-sentence and two encoding generations: the file had been assembled from separate recordings. What sounded damning was, forensically, a composite.*

4.6 VIDEOS AND CCTV FOOTAGE

Video provides visual confirmation of events, actions and identities, but it is rarely as straightforward as it first appears.

What forensic experts look for: MP4, AVI and MOV files, plus DVR system exports.

How experts handle it: Experts perform frame-by-frame analysis, extract stills, synchronise timestamps and verify authenticity through codec analysis. Deleted or overwritten clips may be recovered from storage systems. In court, video analysts can clarify motion, enhance low-light imagery or synchronise multiple camera feeds into a complete picture.

> **For the defence:** *In an affray case, the prosecution relied on a single CCTV angle that appeared to show the defendant throwing the first punch. The DVR clock was seven minutes fast. Once corrected and synchronised with a second camera, the footage showed him arriving after the fight had already begun.*

4.7 DOCUMENTS AND SPREADSHEETS

Documents sit at the heart of countless disputes, from contract breaches to fraud. What many lawyers overlook is the hidden metadata that reveals a file's true history.

What forensic experts look for: Microsoft Office files, PDFs and accounting data such as Sage and QuickBooks exports.

How experts handle it: Experts recover deleted and previous versions from shadow copies and temporary files. PDF metadata shows the software used and the creation sequence, while hidden Office metadata reveals origin, author and revision history: powerful evidence of forgery or after-the-fact alteration.

> **For the defence:** *In a commercial dispute, file metadata may show that an agreement was created after its alleged signing date, exposing fraudulent backdating.*

4.8 INTERNET AND WEB ACTIVITY

Browser history reveals interests, intentions and behaviour. It can show preparatory acts, research, or attempts to conceal activity.

What forensic experts look for: Browser history, cookies, cached pages, downloads, search history and saved passwords.

How experts handle it: Forensic tools parse browser databases such as History, Cookies.sqlite and WebCacheV01.dat to reveal URL visits, timestamps and user accounts. Correlation with event logs and the DNS cache confirms authenticity.

> **For the defence:** *An expert may demonstrate that a defendant's device was not used to access a specific website at the relevant time, directly countering prosecution attribution.*

4.9 CLOUD STORAGE AND ONLINE ACCOUNTS

Cloud services have transformed how data is stored, and equally how evidence is hidden, shared and deleted. Google Drive, Dropbox, OneDrive and iCloud all keep detailed logs of user activity.

What forensic experts look for: Upload, sharing and deletion activity, together with sync logs and local cache data.

How experts handle it: Experts retrieve sync logs and cached data to determine what was uploaded, shared or deleted. Cloud metadata can show who accessed a file and from which device. Preservation orders or lawful warrants may be required to obtain provider records.

> **For the defence:** *A departing sales director denied taking anything with him. His work laptop's sync logs showed a folder called 'Personal' shared to an external account two days before resignation, containing the full client pricing book. The sharing timestamp, recipient address and device ID settled the injunction application.*

4.10 SOCIAL MEDIA ACCOUNTS

Social media is increasingly central to both criminal and civil cases. Posts, messages and location tags provide behavioural evidence, demonstrate associations and establish motive.

What forensic experts look for: Facebook, Instagram, X, LinkedIn, TikTok and Snapchat logs.

How experts handle it: Posts, messages and deleted items can be recovered through legal disclosure or device artefacts. Screenshots alone are rarely sufficient: authenticated platform archives or forensic extractions are preferred, with metadata verification to ensure admissibility.

> **For the defence:** *A harassment complaint rested on screenshots of abusive direct messages. A forensic download of the complainant's own account archive showed the messages did not exist in the platform's records, and pixel-level analysis of the screenshots revealed inconsistent font rendering. The images had been fabricated.*

4.11 USB DEVICES AND EXTERNAL MEDIA

USB drives and external disks are common tools of data theft and concealment. Fortunately, they leave unmistakable traces on every computer they touch.

What forensic experts look for: Registry entries, setupapi.dev.log, recent-files lists and drive serial numbers.

How experts handle it: Registry keys identify which devices were connected, their first and last connection times and their assigned drive letters. File-system artefacts such as the MFT and LNK files show which files were accessed from the USB. In data theft cases this confirms, or refutes, allegations of unauthorised copying.

> **For the defence:** *An employer alleged that an engineer had copied CAD drawings onto a USB stick on his final afternoon. The registry showed the stick was indeed connected, but the LNK files told the fuller story: the only files opened from it were his own payslips and a CV. Nothing left the design folder.*

4.12 SYSTEM LOGS AND REGISTRY

The Windows Registry and event logs are a diary the computer keeps about itself: user activity, program execution, device usage and much more.

What forensic experts look for: Windows Registry, Event Logs, Prefetch files, Jump Lists, Amcache and Shimcache.

How experts handle it: Logs are correlated to reconstruct timelines: when an application was opened, which files were accessed, whether a device was in use during a disputed window. These artefacts are crucial for attribution on multi-user systems.

> **For the defence:** *On a family computer used by four people, the prosecution attributed illegal downloads to the father. Event logs showed the downloads occurred while his user account was logged out and a different profile, protected by its own password, was active. Attribution shifted, and the case against him was dropped.*

4.13 VIRTUAL MACHINES AND ENCRYPTED CONTAINERS

Virtual machines and encrypted containers are sometimes used to conceal secondary operating systems or hide incriminating data. Their very existence can be significant.

What forensic experts look for: VMware, VirtualBox and Hyper-V disk images, plus VeraCrypt containers.

How experts handle it: Experts identify virtual disk files, snapshot metadata and potential encryption keys held in memory or configuration files. Decryption may require lawful

compulsion or password recovery, and demonstrating the existence of a hidden container can itself be evidential.

> **For the defence:** *In a fraud investigation, the suspect's laptop appeared clean. A 40 GB file with no extension and high entropy sat in a games folder: a VeraCrypt container. A RAM capture taken at seizure held the mounting key in memory, and the decrypted volume contained the second set of accounts.*

4.14 PASSWORDS AND AUTHENTICATION DATA

Credentials can prove account ownership, enable lawful decryption, or disprove access allegations.

What forensic experts look for: Saved browser passwords, Windows Credential Manager, keychain files and two-factor tokens.

How experts handle it: Credentials are extracted with forensic tools under controlled conditions. Hash cracking or recovery is attempted only under legal authority, and the privacy of unrelated accounts is carefully protected in defence work.

> **For the defence:** *A defendant was accused of sending threats from an anonymous webmail account. His devices held saved credentials for eleven accounts; the anonymous one was not among them, and the account's own login history showed access from an IP range he had never used. Ownership could not be attributed to him.*

4.15 NETWORK AND LOCATION DATA

Wi-Fi logs, GPS coordinates and router histories show where a device was used and which networks it joined.

What forensic experts look for: Wi-Fi logs, GPS coordinates, router connection history and IP logs.

How experts handle it: Timestamps are cross-referenced with system logs and photo metadata to map device movement. In criminal defence this can corroborate an alibi or challenge the prosecution's location-based evidence.

> **For the defence:** *A burglary case put the defendant near the scene based on cell-site data. His phone's own Wi-Fi log showed it joined his sister's home router, three miles*

> *away, six minutes before the alleged entry and stayed connected throughout. The router's records agreed. The cell-site inference did not survive.*

4.16 DELETED AND UNALLOCATED DATA

The idea that deleted means gone forever is one of the biggest myths in digital evidence. Deleted files routinely leave recoverable remnants.

What forensic experts look for: File remnants in unallocated space, shadow copies, Recycle Bin contents and volume snapshots.

How experts handle it: Forensic imaging allows recovery through carving techniques; even partial remnants can confirm a file once existed, whether incriminating or exculpatory. Crucially, experts stress that presence in unallocated space does not by itself indicate user intent: automatic clean-ups and cache rotations happen constantly.

> **For the defence:** *The prosecution presented fragments of an incriminating image found in unallocated space as proof of deliberate downloading and deletion. The defence expert traced the fragments to a browser thumbnail cache, automatically created by a pop-up advert and automatically purged. The user had never seen, saved or deleted anything.*

4.17 FINANCIAL AND ACCOUNTING DATA

In fraud, insolvency and commercial disputes, financial records are often the smoking gun. They can also be manipulated.

What forensic experts look for: Spreadsheets, accounting databases, PDF statements and online banking exports.

How experts handle it: Experts verify metadata, check formula integrity and compare records against original bank statements. File timestamps can expose retrospective adjustments that suggest deliberate falsification.

> **For the defence:** *A creditor produced a spreadsheet said to record loans made over five years. Every worksheet had been created in a single two-hour session the week before proceedings issued, and the 'historic' entries all shared one authoring session ID. The ledger was a reconstruction, not a record.*

4.18 CLIPBOARD AND TEMPORARY DATA

The clipboard and temporary files may seem trivial, yet they can hold fragments of copied messages, passwords or sensitive text that reveal intent or intermediary steps.

What forensic experts look for: Clipboard history, system cache and print spool files.

How experts handle it: RAM capture and pagefile analysis reveal transient data, especially in live acquisitions. Handling must be swift and careful: this data disappears at shutdown.

> **For the defence:** *In an insider trading inquiry, the pagefile preserved a fragment of text copied to the clipboard: the exact wording of an unannounced results statement, captured on the suspect's machine two days before publication. He had never emailed or saved it. The clipboard remembered anyway.*

§ 05 · DEFENCE METHODOLOGY

5. FORENSIC METHODOLOGY FOR DEFENCE CASES

Digital forensics in defence work must prioritise neutrality, data integrity and contextual interpretation. Experts do not act as advocates; their duty is to the court. Even so, a thorough forensic review frequently exposes weaknesses and misinterpretations in the prosecution's evidence. Key aspects include:

- **Validation of evidence integrity:** re-hashing and verifying prosecution images to confirm data has not been altered.
- **Timeline reconstruction:** correlating artefacts across devices and systems, with time zones and clock drift accounted for to prevent misinterpretation.
- **Attribution and user activity:** examining logins, user profiles and behavioural artefacts to test whether the defendant personally carried out the actions attributed to them.
- **Deleted data in context:** recovery of a deleted file does not imply deliberate deletion; many applications clean up automatically, and the expert contextualises this for the court.
- **Alternative explanations:** malware, remote access or shared device usage can all produce artefacts that superficially implicate a user; defence experts explore these to ensure fairness.
- **Reporting and testimony:** reports written in clear, non-technical language, referencing established methodologies (BS EN ISO/IEC 27037:2012 and ISO/IEC 27041:2015), with impartial expert evidence at trial.

§ 06 · CASE STRATEGY

6. EVIDENTIAL VALUE FOR CIVIL AND CRIMINAL LAWYERS

Understanding digital artefacts enables effective cross-examination and case strategy. Before any digital exhibit is accepted at face value, five questions should be asked of it:

Figure 4 · The five-question test for any digital exhibit.

Defence solicitors should instruct digital forensic experts early, ideally before disclosure is finalised, to allow independent analysis of device images and cloud data. A well-qualified expert can identify inconsistencies in police or corporate forensic findings, recover exculpatory material, and clarify technical misconceptions that might otherwise prejudice the defendant.

§ 07 · THE EXPERT IN COURT

7. THE ROLE OF DIGITAL FORENSIC EXPERTS IN COURT

Digital forensic experts play a dual role: scientist and communicator. Their primary responsibility is to the court, but they also serve as interpreters between the technical and legal worlds. In the UK, experts are instructed under Part 19 of the Criminal Procedure Rules or Part 35 of the Civil Procedure Rules, both of which require objectivity and transparency. A well-constructed report typically includes:

- Background and instructions received.
- Devices examined and methodology used.
- Artefacts identified and their interpretation.
- Timeline reconstruction.
- Expert opinion, with its limitations made explicit.

Cross-examination usually targets methodology and interpretation. An expert who can clearly explain how artefacts were recovered and what they do, and do not, signify can decisively influence judicial understanding.

§ 08 · IN PRACTICE

8. REAL-WORLD CASE APPLICATIONS

CRIMINAL DEFENCE

- **Computer misuse and hacking allegations:** logs and IP data may reveal remote access or malware involvement that exonerates the accused.
- **Sexual offence cases:** image metadata is examined for download dates, creation times and false positives that challenge the prosecution narrative.
- **Fraud and forgery:** metadata in documents and emails can disprove alleged authorship or timing.
- **Harassment and threats:** message logs and call records demonstrate the authenticity, or manipulation, of communications.

CIVIL LITIGATION

- **Employment disputes:** email and chat records clarify alleged misconduct or intellectual property breaches.
- **Family law:** mobile and cloud data reveal communication patterns and financial evidence relevant to custody or disclosure.
- **Commercial disputes:** forensic examination of contracts, spreadsheets and deleted documents exposes fabrication or concealment.

§ 09 · PRESERVATION

9. PRESERVING DIGITAL EVIDENCE: BEST PRACTICES

Lawyers should advise clients and instruct experts promptly to avoid inadvertent data loss. Prompt preservation maximises evidential recovery and heads off arguments over contamination and spoliation:

- Do not power on or alter suspect devices; request forensic imaging instead.
- Retain all relevant devices and accounts, including cloud credentials where lawfully accessible.
- Record the chain of custody meticulously.
- Protect client confidentiality and comply with the UK GDPR when handling personal data.

§ 10 · WHY IT MATTERS

10. WHY EXPERT FORENSIC HANDLING MATTERS

Digital artefacts are powerful evidential tools, but only when properly interpreted. Misunderstood metadata or incomplete logs can mislead the court. Defence lawyers benefit from qualified forensic practitioners who can reconstruct timelines objectively, authenticate or challenge digital evidence, recover deleted or overlooked data, and translate complex technical findings into accessible, admissible evidence.

> **Whether the exhibit is an email exchange, a WhatsApp chat, a financial spreadsheet or a registry log, expert digital forensics can mean the difference between conviction and acquittal, or between liability and exoneration.**

§ 11 · QUICK REFERENCE

11. FORENSIC REFERENCE CHART

Use this chart as a rapid lookup when reviewing disclosure: where each evidence type lives, what artefacts it yields, and what it can prove.

EVIDENCE TYPE	TYPICAL FORENSIC SOURCES	COMMON ARTEFACTS	EVIDENTIAL VALUE
Emails	Outlook PST/OST, MBOX, webmail caches	Headers, threads, attachments, deleted items	Authorship, intent, correspondence timelin
Instant messaging	Mobile backups, desktop sync, cloud	Chat and call logs, deletion traces, media	Relationships, coordinat intent
SMS / MMS	iTunes, iCloud and Android backups	Message text, numbers, timestamps, status	Contact and timing of communication
VoIP & call logs	Skype, Teams, Zoom, WhatsApp, handsets	Call logs, durations, participants	Proof and timing of discussions
Photos / images	Camera roll, cloud, social media	EXIF data, GPS, hashes, editing traces	Location and time verification, authenticity
Videos & CCTV	Phones, DVR systems, exports	Metadata, codecs, frame timestamps	Chronology, identificati scene context
Audio / voice notes	Phones, recorders, messaging apps	Waveform, metadata, creation time	Spoken admissions, thre meetings
Documents	Local storage, attachments, cloud drives	Author metadata, revision history, timestamps	Authorship, hidden or revised content
Archives (.zip, .rar)	File system, cloud storage	File names, timestamps, password evidence	Concealment, exfiltratio file grouping
Web browsing	Chrome, Edge and Firefox databases	URLs, searches, downloads, cookies, autofill	Intent, research, preparatory acts

EVIDENCE TYPE	TYPICAL FORENSIC SOURCES	COMMON ARTEFACTS	EVIDENTIAL VALUE
Social media	Browser cache, mobile data, API exports	Posts, messages, uploads, profile data	Behaviour, associations, motive
Cloud storage	Sync folders, sessions, provider logs	Upload and share history, file versions	Transfer, sharing, collaboration evidence
System logs / Registry	Windows Registry, Event Logs, plists	Logins, USB connections, executed programs	User activity and corroborating timelines
USB / external media	Registry, setupapi.dev.log, LNK files	Serial numbers, connection times, labels	Data transfer, unauthori copying
Virtual machines	VMware, VirtualBox, Hyper-V folders	VM configs, snapshots, guest artefacts	Hidden environments, concealment
Credentials	Browser stores, keychains, managers	Saved passwords, hashes, tokens	Account ownership, acc identity
Encryption keys	TPM, BitLocker metadata, PGP keys	Key files, recovery keys, certificates	Encryption identificatior decryption
Network / Wi-Fi	OS logs, router logs, event logs	SSIDs, IPs, MACs, connection times	Location inference, devi presence
Location data	EXIF, GPS logs, cell towers, Wi-Fi	Coordinates, timestamped positions, routes	Position verification, eve correlation
Deleted files	Unallocated space, shadow copies	Fragments, filenames, timestamps	Recovery of concealed material
Clipboard / temp	System memory, app caches, spool files	Copied text, images, passwords	Intent, intermediary data movement
Financial data	Banking apps, spreadsheets, statements	Transaction logs, account metadata	Motive, fraud analysis, payment proof
Mobile backups	Computer backups, iCloud, Google Drive	Contacts, messages, photos, app data	Full device and timeline reconstruction
Forensic suite logs	EnCase, X-Ways, Cellebrite, AXIOM	Processing logs, case notes	Chain of custody, proces verification

§ 12 · COMMON QUESTIONS

12. FREQUENTLY ASKED QUESTIONS

The questions solicitors ask us most often when digital evidence first lands in a case. Click a question to expand the answer.

When should a defence solicitor instruct a digital forensics expert? –

As early as possible, ideally before disclosure is finalised. Early instruction allows independent verification of prosecution images, preservation of volatile data such as cloud accounts and RAM, and time to develop alternative explanations before trial strategy hardens.

Can deleted messages and files really be recovered? –

Often, yes. Deleted files leave remnants in unallocated space, shadow copies, backups and cloud synchronisation data. Recovery depends on the device, how much time has passed and how heavily the storage has been reused. Equally important, an expert can explain when recovered fragments do not indicate deliberate deletion by the user.

Are screenshots of messages or social media posts admissible evidence? –

Screenshots alone are weak evidence because they are trivially easy to fabricate. Courts give far more weight to authenticated platform archives, forensic extractions with intact metadata, and hash-verified copies whose integrity can be independently checked.

What standards govern digital evidence handling in the UK? –

The National Police Chiefs' Council (NPCC) Digital Evidence Guidelines, together with ISO 17025 laboratory accreditation and the methodologies in BS EN ISO/IEC 27037:2012 and ISO/IEC 27041:2015. Expert reports are prepared under Part 19 of the Criminal Procedure Rules or Part 35 of the Civil Procedure Rules.

Does finding an artefact on a device prove the owner put it there? −

No. Attribution is a separate forensic question. Malware, remote access, shared logins, automatic downloads and background processes can all create artefacts without any deliberate act by the device owner. A defence expert tests attribution rather than assuming it.

COMPUTER FORENSICS LAB

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ
cflab.uk (https://cflab.uk) · 0207 164 69 15 · London digital forensics since 2007
NPCC guidance · ISO 17025 · ICO ZB395023

Visit our E-Discovery Website - e-discovery.uk

← Back to cflab.uk home