COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

# macOS Spotlight and Metadata Deep-Dive

## The Index That Remembers Files the Mac No Longer Has

Spotlight is the search system built into every Mac, and behind it sits a rich metadata store that indexes the files on the machine: their names, kinds, sizes, and a wealth of dates and attributes, when a file was created, downloaded, last opened, where it came from, and much more. For the lawyer, two things make this powerful. First, the metadata answers questions the file's own content cannot: not just what a document says, but where it came from, when it was downloaded, and when it was last used. Second, and more striking, the Spotlight index can retain records of files that are no longer on the Mac, so an entry describing a file that has since been deleted or removed to an external drive may survive in the index, evidencing that the file once existed, and often when and where it came from. This guide sets out for UK lawyers how Spotlight and macOS metadata work, what the metadata reliably shows, how index remnants evidence files that have gone, and how this material is recovered and interpreted honestly.

⏱ 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. Spotlight and metadata analysis is a productive strand of its Apple work: reading the rich per-file metadata the Mac maintains, dates, origins and attributes, and mining the Spotlight index for records of files that have since been deleted or moved off the machine. The analysis evidences where files came from, when they were used, and that they once existed, interpreted with an understanding of what each attribute means, and reported under CPR Part 35 and CrimPR Part 19.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | SPOTLIGHT INDEX ANALYSIS | FILE-ORIGIN & METADATA DATING | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

# In this guide

§ 0 1 · ORIENTATION

# Executive summary

The headline point: Spotlight indexes the files on a Mac with rich metadata, dates, origins and attributes, that answers questions content cannot, and its index can retain records of files no longer on the machine, so an index entry may evidence that a deleted or removed file once existed, and where it came from.

**How it works (§3):** Spotlight maintains a metadata index of the files on the Mac, recording names, kinds, sizes and a wide range of dates and attributes, updated as files change. **What it shows (§4):** per-file metadata evidences when a file was created, downloaded, last opened and modified, where it came from (the download source), and other attributes, richer than the file's content alone. **Index remnants (§5):** the index can retain entries for files since deleted or moved to external media, so a remnant evidences that a file once existed on the Mac, often with its origin and dates. **Interpretation (§6):** attributes are read for their precise meaning, origin data interpreted carefully, and findings stated honestly. **Deployment (§7):** proving where a file came from, when it was used, and that a now-absent file was once present, corroborated across the estate.

- **The index outlives the file:** Spotlight can retain records of files no longer on the Mac.
- **Metadata answers origin and use:** where a file came from, when downloaded, created and last opened.
- **Richer than content:** the metadata shows things the document's text does not.
- **Read attributes precisely:** each date and attribute means a specific thing, not a general one.
- **Corroborate honestly:** index and metadata findings confirmed across artefacts and the estate.

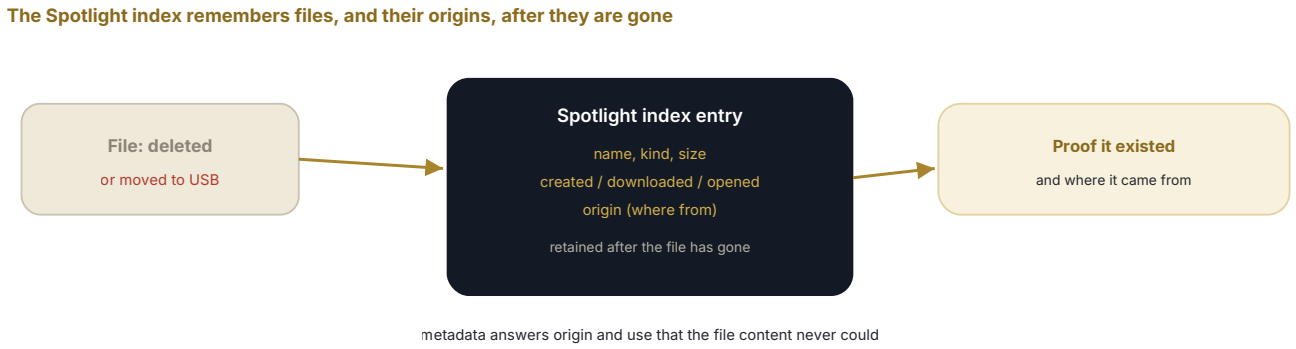


*Figure 1 - even after a file is deleted or moved to external media, a Spotlight index entry may survive, evidencing that the file once existed on the Mac, with its dates and its origin.*

§ 0 2 · FIRST PRINCIPLES

# The problem in plain English: the index outlives the file

To make search instant, a Mac does not scan every file each time; it maintains an index, a catalogue of the files on the machine and information about them, that Spotlight consults. That index, and the metadata behind it, records far more than file names. For each file it can hold the kind, the size, a set of dates, when the file was created, last modified, last opened, and, for downloaded files, when and from where it was obtained, and a range of other attributes drawn from the file and from how it was handled. This is metadata, data about the data, and it frequently answers the questions that matter most in a dispute, questions the file's own content cannot: not what a document says, but where it came from, when it arrived, and when it was last used.

There is a further, striking property. Because the index is a catalogue maintained separately from the files themselves, it can lag behind reality, and that lag is evidentially valuable. An entry describing a file may survive in the index after the file itself has been deleted from the Mac, or moved off to an external drive or a USB stick. In other words, the index can remember files the Mac no longer has. A surviving index remnant may therefore evidence that a particular file once existed on the machine, often complete with its origin and its dates, even though the file is gone, and even though other recovery methods have failed. For the lawyer, this makes Spotlight and macOS metadata a double source: a rich record of the origin and use of files that are present, and, through index remnants, evidence of files that have left. Both must be read with care, because each attribute means a specific thing and origin data has to be interpreted, not assumed. This guide sets out how Spotlight and the metadata work, what they reliably show, how index remnants evidence departed files, and how the material is recovered and interpreted honestly.

§ 0 3 · HOW IT WORKS

# How Spotlight and macOS metadata work

- **The metadata index:** Spotlight maintains an index of the files on each volume, recording per-file metadata so search is instant, a catalogue consulted rather than the files themselves scanned each time (§2): the searchable store behind the magnifying glass.
- **Rich per-file attributes:** the index holding a wide range of attributes, names, kinds, sizes, multiple dates, and origins, drawn from the file and from how macOS handled it, far more than the file's visible content (§4): the wealth of metadata.
- **Origin and download data:** macOS recording, for downloaded files, where they came from and when (the "where from" and quarantine information), so a file's provenance on the machine is captured (§4): the origin trail.
- **Extended attributes:** files carrying extended attributes beyond their content, tags, origin markers, and other data, that the metadata analysis reads alongside the index (§4): the hidden per-file annotations.
- **On the decrypted device:** the index and metadata recovered from the acquired, unlocked, decrypted Mac (guides 131, 133), including index remnants and earlier states in snapshots and backups (guides 132, 137), with integrity preserved (guides 2, 3): the sound recovery basis.

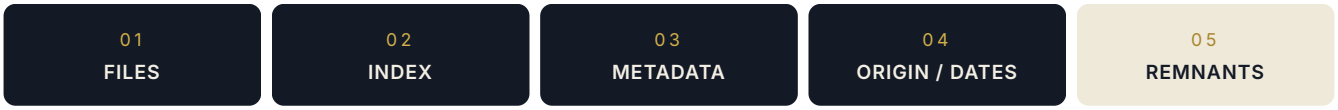


*Figure 2 - Spotlight indexes files into a rich metadata store recording origins and dates, and its remnants can evidence files no longer present.*

§ 0 4 · WHAT THE METADATA SHOWS

# What the metadata reliably shows

- **Origin, the "where from":** for downloaded files, the source they came from and when, so a document's arrival on the machine, from a website, an email, a message, can be evidenced, provenance the content does not carry (guide 129): the where-did-this-come-from answer.
- **The date cluster:** the created, modified, last-opened and added dates recorded per file, so when a file appeared, was changed and was last used can be established, richer than a single timestamp (guides 108, 134): the when answers.
- **Kind, size and identity:** the file's type, size and identifying attributes recorded, so a file can be characterised and matched even where its name or location has changed (§5): the what-is-this answer.
- **Use and access:** last-opened and use-count style attributes evidencing that a file was actually opened, and when, corroborating the activity artefacts (guide 134): the was-it-used answer.
- **Tags and handling:** user tags, quarantine flags and other handling attributes evidencing how a file was treated, so the metadata reflects not just the file but its history on the machine (§6): the how-was-it-handled answer.

§ 0 5 · INDEX REMNANTS

# Index remnants: evidence of files that have gone

- **The index lags the files:** because the index is maintained separately, an entry for a file can survive after the file has been deleted or moved off the machine, so the index remembers files the Mac no longer holds (§2): the remnant that outlives the file.
- **Evidence a file existed:** a surviving index entry evidencing that a particular file was once on the Mac, its name, kind, size, dates and origin, even when the file itself cannot be recovered (guide 4): the proof of past presence.
- **Files moved to external media:** an index entry for a file copied or moved to a USB drive or external disk evidencing that the file was on the Mac and, with device artefacts (guide 134), that it went to that medium, key in exfiltration (guide 110): the departed file traced.
- **Origin of a departed file:** the origin metadata in a remnant showing where a now-absent file came from, so even a deleted file's provenance can be established (§4): the source of the vanished file.
- **Corroborate the remnant:** an index remnant read alongside system artefacts, device-connection logs and the estate (guides 134, 137), so a conclusion about a departed file rests on convergence, not the index alone (guide 130): the remnant confirmed.

§ 0 6 · INTERPRETATION AND HONEST LIMITS

# Interpretation, origin data and honest limits

- **Each attribute means a specific thing:** created, modified, last-opened and origin attributes each carrying a precise meaning, so they are read for what they specifically record, not merged into a vague claim (guides 108, 100): the discipline of precise reading.
- **Origin data interpreted, not assumed:** the "where from" metadata evidencing a recorded source, which is strong but interpreted in context, since it reflects how the file was obtained and can, in unusual cases, be altered (guide 126): the provenance read carefully.
- **Index currency and lag:** the index reflecting the machine as last indexed, which may lag current reality, so a remnant shows past state and the timing of indexing is considered (§5): the lag understood, not ignored.
- **Existence, not intent:** a metadata or index record showing that a file existed, arrived or was opened, not why, so intent is not read into a bare attribute (guides 4, 125): the presence-not-intent limit.
- **Attribution and state honestly:** metadata reflecting account-level activity, attributed to a person only with care, and all findings stated at the confidence the attributes support (guides 105, 100): the honest reading of the metadata.

§ 0 7 · DEPLOYMENT

# Deployment: origin, use and the file that left

- **Proving where a file came from:** the origin metadata establishing that a document was downloaded from a particular source or arrived by a particular route, in IP, fraud and possession matters, provenance the content cannot show (guide 129): the source proved.
- **Proving a file left the machine:** an index remnant, with device artefacts, evidencing that a confidential file was on the Mac and was moved to external media, central to data-theft claims (guide 110): the exfiltration evidenced.
- **Proving a now-absent file existed:** a surviving index entry evidencing that a deleted file was once present, and often when and from where, even where the file itself cannot be recovered (guide 4): the vanished file established.
- **Dating and corroborating use:** the date cluster and last-opened attributes dating a file's arrival and use, corroborating the activity timeline (guides 96, 134): the file placed in the chronology.
- **Corroborated, honest presentation:** the metadata and index findings corroborated across artefacts, snapshots, backups and the estate, and presented at honest confidence under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the metadata evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

# Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the Spotlight index and metadata on a Mac are one record of files, their origins and their history, and the same facts are corroborated across the estate, which both strengthens metadata findings and preserves them where the live index has changed. The live Mac holds the current index, the per-file metadata and index remnants. But APFS snapshots and Time Machine backups (guides 132, 137) hold earlier states of the index and metadata, so a remnant or attribute lost from the live index may survive in a backup; the system artefacts (guide 134) corroborate use and file access; device-connection logs corroborate a file's move to external media; the external medium itself holds the departed file; and the paired devices and iCloud hold their own metadata for synced files. The discipline is to treat the index and metadata as one corroborating source among several, so that a file's origin, use and past presence are confirmed across the estate, and so that a departed file evidenced by an index remnant can be tied, through device logs and the external medium, to where it went. When the live index has moved on, a backup preserves the earlier metadata; when a remnant alone is thin, system and device artefacts corroborate it; and the external medium and the estate complete the story of a file that left.

| EVIDENCE | LIVE SPOTLIGHT INDEX | SNAPSHOTS / BACKUPS | SYSTEM ARTEFACTS | DEVICE-CONNECTION LOGS | EXTERNAL MEDIUM / ESTATE | DELETED / DEPARTED |
|---|---|---|---|---|---|---|
| **File origin** | Y: where-from | Y: earlier index | Download traces | n/a | Source system | Remnant holds origin |
| **File dates** | Y: date cluster | Y: earlier states | Activity times | n/a | Copy on medium | Remnant holds dates |
| **File use** | Last-opened | Earlier metadata | Y: opens (guide 134) | n/a | n/a | Remnant + artefacts |
| **File moved out** | Remnant entry | Earlier index | Copy traces | Y: USB / drive | Y: the medium | Y (converging) |
| **Past existence** | Y: remnant | Y: backup copy | References | n/a | Backup / medium | Y (multiple routes) |

Fallback strategy in one line: corroborate metadata and index remnants across snapshots, backups, system and device artefacts and the external medium; when the live index has changed, a backup preserves the earlier record, and the estate confirms a departed file's origin, use and destination.

§ 0 9 · IN THE WILD

# Worked examples

### EXAMPLE 1 · THE INDEX THAT PROVED THE FILE HAD BEEN THERE

A departing employee denied a confidential file had ever been on his Mac, and the file was indeed absent. The §5 Spotlight index told a different story: a surviving index remnant recorded the file, by name, kind, size and dates, evidencing that it had once been on the machine (guide 4). The §4 origin metadata in the remnant showed where it had come from, and §8 device-connection logs and the activity artefacts (guide 134) showed a USB drive connected shortly before the file left the index, converging on the conclusion that it had been copied to external media (guide 110). The §6 interpretation was careful, existence and origin, corroborated, not intent assumed. The denial did not survive. The lesson is §2's: the Spotlight index can remember files the Mac no longer holds, so an index remnant frequently evidences that a now-absent file once existed, with its origin and dates, and, corroborated by device artefacts, that it was moved off the machine.

### EXAMPLE 2 · THE ORIGIN METADATA THAT FIXED PROVENANCE

A dispute turned on where a document had come from: the party claimed to have authored it, the other side said it had been taken from their systems. The §4 origin metadata settled it: the file's "where from" attribute recorded that it had been downloaded from the claimant's own internal system on a specific date (guide 129), and the §4 date cluster showed it arriving on the Mac at that time, not being created there as authored work. The §6 interpretation read the origin data carefully and in context, and §8 corroboration from the browser and system artefacts (guides 134, 136) confirmed it. The metadata, not the content, revealed the true provenance. The lesson is §4's: macOS records where downloaded files came from, so the origin metadata often establishes a file's true provenance, arrival by download rather than authorship on the machine, answering a question the document's content alone cannot.

### EXAMPLE 3 · THE ATTRIBUTE READ FOR EXACTLY WHAT IT MEANT

An analysis initially treated a file's "created" date on the Mac as the date the document was written, suggesting it predated the events in issue. The §6 precise-reading discipline corrected this: the created date on the Mac reflected when the file arrived on that machine, by copy or download, not when the document was originally authored elsewhere, and the origin and date-cluster attributes, read for their specific meanings, showed the true sequence (guide 108). Conflating the Mac "created" date with authorship would have produced a wrong conclusion. The §6 honest reading, each attribute meaning a specific thing, avoided the error. The lesson is §6's: metadata is powerful but only when read precisely, each date and attribute records a specific event, and treating, say, a file-system "created" date as the moment of authorship is a classic error that careful, attribute-by-attribute interpretation prevents.

§ 10 · WHERE IT GOES WRONG

# Common mistakes and technical limitations

## Common mistakes

- **Ignoring the index for departed files:** concluding a file was never present because it is absent, missing the index remnant that shows it was (Example 1, §5).
- **Reading only content, not metadata:** examining what a file says while ignoring where it came from and when it arrived (Example 2, §4).
- **Misreading attributes:** treating a Mac "created" date as authorship, or conflating distinct dates (Example 3, §6).
- **Assuming origin without interpretation:** reading "where from" data as conclusive without context (§6).
- **Ignoring index lag:** treating the index as perfectly current rather than reflecting the last indexing (§6).
- **Not corroborating remnants:** a departed-file conclusion rested on an index remnant alone without device or system corroboration (§5).
- **Reading intent into an attribute:** a bare metadata record treated as evidence of why, not just that (§6).
- **Overlooking backups:** earlier index states in snapshots and backups not consulted when the live index has changed (§8).

## Technical limitations

- **Metadata records events, not intent:** attributes show that something happened, not why: the interpretive limit (§6).
- **The index reflects last indexing:** it may lag current reality, so timing of indexing matters (§6).
- **Origin data can, rarely, be altered:** "where from" is strong but interpreted in context (§6, guide 126).
- **Remnants may be incomplete:** an index remnant may hold only part of a file's metadata, so corroboration is needed (§5).
- **macOS evolves:** Spotlight, the index format and attributes change across versions, checked per version (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

# Questions to ask · Suggested wording

## Ask your client

- Is the question about a file's origin, its use, or whether a now-absent file was once present, so the metadata and index can be targeted?
- Might relevant files have been deleted or moved to external media, so index remnants should be examined?
- Has the Mac been preserved promptly, so the index and its remnants survive?

## Ask your opponent

- Please preserve and disclose the Spotlight index and file metadata on the device at Schedule 1, including index remnants and the origin ("where from") attributes of the files in issue.
- For any file said never to have been present, please confirm whether the index or a backup records it.
- Please confirm the origin and relevant dates of the documents relied on.

## Ask your eDiscovery / forensic provider

- What do the metadata and index show about the origin, dates and use of the files in issue?
- Do index remnants evidence any now-absent files, and are they corroborated?
- How is each attribute interpreted, and what does it honestly show?

### SUGGESTED WORDING · INSTRUCTION FOR A SPOTLIGHT AND METADATA ANALYSIS

> "We instruct you to examine the Spotlight index and file metadata on the device at Schedule 1, relevant to Schedule 2. Please, on the acquired, decrypted device and preserving integrity: (1) recover the Spotlight metadata index, per-file metadata (including the created, modified, last-opened and added dates), origin ('where from') and quarantine data, extended attributes and tags, and index remnants; (2) establish, for the files in issue, their origin, their relevant dates and their use, distinguishing arrival by download or copy from authorship on the machine, and reading each attribute for its specific meaning; (3) examine index remnants for records of files no longer present, evidencing past existence, origin and dates, and, with device-connection and system artefacts, whether such files were moved to external media; (4) corroborate the findings across snapshots, backups, system artefacts and the estate, and consult earlier index states in backups where the live index has changed; and (5) interpret origin data in context, treat index lag and attribute meaning carefully, read records as evidence of events not intent, attribute to a person only with corroboration, and state confidence honestly."

§ 12 · QUICK CONTROL

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

## The Spotlight and metadata checklist

- ☐ Mac preserved promptly; index and remnants intact
- ☐ Spotlight index and per-file metadata recovered
- ☐ Origin ("where from") and quarantine data read
- ☐ Date cluster (created, modified, opened, added) established
- ☐ Extended attributes and tags examined
- ☐ Index remnants examined for now-absent files
- ☐ Departed files corroborated with device and system artefacts
- ☐ Each attribute read for its specific meaning
- ☐ Earlier index states in snapshots and backups consulted
- ☐ Findings corroborated and stated at honest confidence

## Red flags

- A file said never present when an index remnant shows it was: Example 1.
- Content read but origin metadata ignored: Example 2.
- A Mac "created" date treated as authorship: Example 3.
- Origin data read as conclusive without interpretation.
- Index lag ignored.
- A departed-file conclusion on a remnant alone, uncorroborated.
- Intent read into a bare attribute.

## When to involve a digital forensic expert

Whenever a file's origin, its use, or its past presence matters, because the metadata answers questions the content cannot and the index can evidence files that have gone: the expert recovers the Spotlight index and per-file metadata, establishing where files came from, when they arrived and were used, and reading each attribute precisely so a Mac "created" date is never mistaken for authorship (Examples 2 and 3, §4, §6); and mines index remnants for records of now-absent files, evidencing that a deleted or removed file once existed and, with device and system artefacts, that it was moved to external media (Example 1, §5). Findings are corroborated across snapshots, backups, system artefacts and the estate, origin data is interpreted in context, records are read as evidence of events not intent, and everything is reported at honest confidence under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, Spotlight and metadata work turns the Mac's own catalogue into evidence of where files came from, how they were used, and, through the index that outlives the file, that a document a party denies ever having was once there, and often where it went.

§ 1 3 · COMMON QUESTIONS

# Frequently asked questions

### Can metadata show where a file came from?

Often yes (§4, Example 2). macOS records, for downloaded files, a "where from" attribute capturing the source and, with quarantine data, the circumstances of the download, and the date cluster shows when the file arrived. So the metadata can establish that a document was downloaded from a particular system on a particular date, provenance the content itself does not carry. This is frequently decisive where the question is whether a file was authored on the machine or obtained from somewhere else.

### A file is not on the Mac. Can you still show it was there?

Frequently (§5, Example 1). Because the Spotlight index is maintained separately from the files, an index entry can survive after the file has been deleted or moved off the machine, evidencing that the file was once present, often with its name, kind, size, dates and origin. Corroborated with device-connection logs and system artefacts (guide 134), an index remnant can also help show that a file was copied to external media. So a now-absent file's past presence, and sometimes its destination, is often provable.

### Isn't the "created" date just when the document was written?

Not necessarily, this is a classic trap (§6, Example 3). A file-system or index "created" date on a Mac usually reflects when the file arrived on that machine, by copy or download, not when the document was originally authored elsewhere. Treating it as the authorship date can produce a badly wrong conclusion. Each date and attribute records a specific event, and correct interpretation reads them precisely, using the origin data and the full date cluster to establish the true sequence, rather than conflating distinct timestamps.

### How reliable is the origin ("where from") data?

Strong, but interpreted in context (§6). The "where from" attribute is a genuine record of where a downloaded file came from and is often powerful evidence of provenance. Like any attribute, it is read for what it specifically records and, in unusual cases, can be altered, so it is corroborated with browser, system and estate evidence (guides 134, 136) rather than treated as automatically conclusive. Read carefully and corroborated, origin data is one of the most useful pieces of metadata on the machine.

### Does an index entry prove someone intended to do something?

No, it evidences events, not intent (§6). A metadata or index record shows that a file existed, arrived, was opened or was moved, not why, so intent is never read into a bare attribute. As with browser history (guide 125), the discipline is to distinguish what happened from why it happened, and to keep the metadata evidence to what it actually shows. Intent, where relevant, is inferred only from corroborating evidence and stated at honest confidence, not asserted from a single date or attribute.

### How urgent is preserving the Mac for this?

Promptly (§5, §8). The Spotlight index updates as files change and is reindexed over time, so index remnants for departed files can be lost with continued use, and metadata can change. The sooner the Mac is preserved and acquired, the more of the index and its remnants survive. Where the live index has already moved on, earlier states in APFS snapshots and Time Machine backups (guides 132, 137) can preserve the metadata and remnants, but prompt preservation of the live machine remains the surest course.

§ 14 · REFERENCE

# Glossary

**Spotlight**
The macOS search system and its metadata index.

**Metadata**
Data about a file: dates, origin, kind, size, attributes.

**Index**
The catalogue of files that Spotlight consults.

**Index remnant**
An index entry surviving after the file has gone.

**Where from**
The origin attribute recording a download's source.

**Quarantine data**
Attributes recording how a file was obtained.

**Date cluster**
The created, modified, opened and added dates.

**Extended attribute**
Per-file data held beyond the file's content.

**Provenance**
Where a file came from and how it arrived.

**Reindexing**
Rebuilding the index, which can remove remnants.

## Sources and authoritative references

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

- cflab.uk, digital forensics services (Spotlight index analysis, file-origin and metadata dating, index-remnant recovery, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 06 · Analysis and Phase 05 · Processing (metadata extraction and interpretation as practised): e-discovery.uk/edrm/analysis · e-discovery.uk/edrm/processing
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Apple developer documentation on Spotlight metadata and file metadata attributes: developer.apple.com, file metadata · Apple Platform Security guide: support.apple.com, Platform Security
- Forensic Science Regulator, Code of Practice v2 (interpretation and honest reporting of metadata): gov.uk, FSR Code · ISO/IEC 27037: iso.org, 27037
- PD 57AD and CPR Part 31 · CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

# Working with Computer Forensics Lab

Spotlight and metadata work at the laboratory turns the Mac's own catalogue into evidence of origin, use and past presence. On the acquired, decrypted device (guides 131, 133), the Spotlight index and per-file metadata are recovered, and the files in issue are characterised by their origin ("where from") data, their date cluster and their use attributes, so where a document came from, when it arrived and when it was last opened are established, richer than the content alone, with each attribute read for its precise meaning so a Mac "created" date is never mistaken for authorship (Examples 2 and 3). Index remnants are mined for records of files no longer present, evidencing that a deleted or removed file once existed and, with device-connection and system artefacts (guide 134), that it was copied to external media, evidence that routinely defeats a denial that a file was ever there (Example 1). Everything is corroborated across snapshots, backups, system artefacts and the estate, with earlier index states in Time Machine backups consulted where the live index has changed (guides 132, 137); origin data is interpreted in context, records are read as evidence of events rather than intent, and attribution is handled with care. Findings are reported at honest confidence under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the recurring insight is that the index often remembers what the file itself no longer can, where a document came from, and that it was once there.

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