



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Detecting Backdated or Manipulated Documents

The Forensic Examination of Documents That Claim a Date They Did Not Have

The backdated agreement, the minute written after the meeting it records, the invoice created when the audit loomed, the "contemporaneous" note drafted for the witness statement: document manipulation is the oldest fraud in litigation, and the digital document is both easier to fake and far harder to fake well. A forger controls what the document says and, with effort, what its dates say; what they cannot control is the whole environment in which a genuine document of the claimed date would have existed: the application that would have created it, the fonts and features that would have been available, the platform records that would have captured it, the copies it would have left in other hands, the version history it would have accumulated. Authenticity examination is the systematic comparison of the document as it is with the document as it would have been. This guide sets out the method for UK lawyers, from the internal-evidence tests through the estate's corroboration to the graded finding a court will accept: and the same method's protective use, when a genuine document is wrongly accused.

🕒 Estimated reading time: 25 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. Document authenticity is among its most frequently instructed examinations: backdated agreements, reconstructed records, altered invoices and manufactured notes, in civil fraud, insolvency, family, employment and criminal proceedings: examined from internal evidence and the estate's corroboration, graded honestly, and reported under CPR Part 35 and CrimPR Part 19, for parties alleging manipulation and for parties defending a genuine document against the allegation.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

DOCUMENT AUTHENTICITY EXAMINATION

BACKDATING & ALTERATION DETECTION

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: the forger controls the document, not its world
- 03 Internal evidence: metadata, anachronisms and the drafting signature
- 04 Format-specific examination: Office, PDF, images, scans and email
- 05 External corroboration: the estate the document should have inhabited
- 06 Alteration: detecting changes to an otherwise genuine document
- 07 Grading, reporting and deployment: from finding to consequence
- 08 Source architecture: where else the evidence lives
- 09 Worked examples
- 10 Common mistakes and technical limitations
- 11 Questions to ask · Suggested wording
- 12 Checklist and red flags · When to involve a digital forensic expert
- 13 Frequently asked questions
- 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

Executive summary

THE HEADLINE POINT: A BACKDATED DOCUMENT FAILS ONE OF TWO TESTS: ITS INTERNAL EVIDENCE IS INCONSISTENT WITH THE CLAIMED DATE, OR THE ESTATE IT SHOULD HAVE INHABITED DOES NOT CONTAIN IT: AND THE EXAMINATION RUNS BOTH, GRADES THE RESULT, AND STATES THE ALTERNATIVES

Internal evidence (§3-§4): a document carries the fingerprints of the environment that made it: the application and build version, the template, the fonts and features used, the metadata fields (creation, last-saved, author, revision count, editing time), and format-specific structures (Office's internal XML and relationships, PDF's producer and object history, an image's EXIF and compression signature, an email's header hops). A genuine document of the claimed date is consistent with the environment available on that date; a backdated one frequently is not: the 2019 agreement carrying a 2023 application build, the "contemporaneous" minute with a revision count of one and four minutes' editing time, the scanned "original" whose scanner did not exist at the claimed date, the PDF whose producer string postdates its own creation field. **External corroboration (§5):** a genuine document leaves traces in its world: a first rung in a version ladder (guide 102), an upload event in an audit log (guide 105), copies in the mailboxes it was sent to (guide 83), a place in the backups of its period, a counterparty's version: guide 95's existence evidence run in reverse: the document that claims a date should exist in the estate of that date, and its absence from every store is itself the finding. **Alteration (§6):** where a genuine document has been changed, the version ladder's diffs, the recovered prior state, the tracked-change residue, the layer and object analysis of PDFs and images, and the counterparty's clean copy localise the change to a window and an account. **Grading (§7):** findings run from "consistent with the claimed date" through "inconsistent with the claimed date" to "created no earlier than [date]" and, where the evidence supports it, "fabricated": each with its basis and the alternatives addressed: because forgery is a grave allegation, and because guide 108's innocent rewrites explain most anomalies before manipulation does.

- **Anachronism convicts:** the build, font, feature or format that did not exist at the claimed date: the forger controls the date field, not the tool.
- **The drafting signature tells:** revision counts, editing time and version bursts distinguish a document that was drafted from one that was manufactured.
- **The estate should contain it:** a genuine document of the claimed date has a ladder, an upload, a recipient, a backup: absence from all is the finding.
- **Counterparts are the control:** the other side's copy, the clean earlier version: the altered document's own witness.
- **Grade before alleging:** "inconsistent with the claimed date" is earned by evidence; "fabricated" by more: and innocent explanations are excluded first.

The problem in plain English: the forger controls the document, not its world

To backdate a paper document, a forger needed period paper, a period typewriter and a steady nerve. To backdate a digital document, they need to change a date field, and many do exactly that and stop. The document then says what they want and dates when they want, and looks, to the untrained reader, complete. What the forger has overlooked is that the document is not a self-contained object but a node in a web: created by an application whose version is recorded inside it, using fonts and features whose availability is dated, saved to a platform that logged the save, sent to people whose mailboxes kept it, captured by backups on their schedules, and: if genuine: accumulating a history of drafts, versions and copies that a manufactured document has no time to acquire.

Authenticity examination therefore has two halves. The internal half reads the document for consistency with its claimed date: does everything inside it belong to that time? The external half reads the estate for the document: is it where a genuine document of that date would be? A backdated document usually fails one half; a well-made one may pass the internal half and still fail the external, because the forger cannot retroactively insert a document into last year's backups or a counterparty's inbox. And the same two halves, run on a genuine document wrongly accused, clear it: which is why the method matters more than the suspicion.

Internal evidence: metadata, anachronisms and the drafting signature

- **Application and build anachronism:** the creating and last-saving application's version, recorded in Office XML, PDF producer strings and image software tags, compared to that version's release date: a document cannot have been saved by software released after its claimed save date: the single most decisive internal test, and the one forgers most often fail.
- **Font, feature and format anachronism:** fonts embedded or referenced that were not available on the claimed date; features (Office functions, PDF structures, compression methods, emoji sets) introduced later; format versions that postdate the claim: each a dated element the forger did not think to age.
- **Metadata field consistency:** creation, last-saved and last-printed fields against each other and against the file-system stamps (guide 108's families); author and last-saved-by against the claimed drafting history; revision count and total editing time against the document's length and complexity: the four-minute, one-revision "long-standing" document exposed by its own counters.
- **The drafting signature:** genuine documents accumulate history: multiple saves, edits over days, versions in a ladder (guide 102); manufactured ones are created in a single session, often with the content pasted from elsewhere (paste artefacts, inherited styles from another document): the shape of the making, read from the file.
- **Residue and relationships:** Office files' internal relationships and orphaned parts, embedded objects from other documents, retained tracked changes and comments, hidden text and revision identifiers: the traces of how the document was assembled, frequently naming the source it was assembled from.

Format-specific examination: Office, PDF, images, scans and email

- **Office documents:** the package structure (XML parts, relationships, content types) carrying application version, revision identifiers, style lineage and edit-session traces; document-level and paragraph-level revision IDs that can date content relative to other documents from the same environment; embedded and linked objects with their own metadata.
- **PDFs:** producer and creator strings, creation and modification dates, incremental-update history (a PDF's appended revisions preserving prior states), object and xref structure, embedded font subsets and their versions, form-field and annotation histories, and digital-signature validity and timestamps where present: a PDF frequently contains its own earlier version.
- **Images and scans:** EXIF capture data (device, software, time, GPS), compression signatures and quantisation tables identifying the producing software, error-level and noise analysis for compositing, and, for scans of "original" paper, the scanner's identity and settings against the claimed date: guide 127's deepfake methods at the document scale.
- **Email:** header hops with their server timestamps (guide 87), message identifiers with embedded time and host components, client and encoding signatures, and the message's presence in server-side stores versus the sole copy in a produced mailbox file: a manufactured email typically exists in one place and never travelled.
- **Handwriting and signatures on digital documents:** pasted or traced signature images with their own metadata, inconsistent resolution and compression against the surrounding page, and, where a questioned-document examiner is warranted, guide 100's specialism-matching for the physical-document discipline.

External corroboration: the estate the document should have inhabited

- **The version ladder and the first rung:** where the document lives on a versioned platform, its ladder either starts at or before the claimed date, or it does not (guide 102 §7): the platform's own record of when the document came into being, subject to the flattening and migration explanations of guide 102 §4.
- **Audit and upload events:** platform logs recording the document's first appearance, uploads, shares and edits (guide 105): a document claimed for 2021 whose first platform event is 2024 has a question to answer that the log has already asked.
- **Transmission and recipients:** a genuine agreement was sent to the counterparty; a genuine minute was circulated to the board; a genuine invoice reached the customer: the recipients' mailboxes, the counterparties' files and the sent-items of the period either hold it or do not (guide 83, guide 95 §3): the strongest external test, because the forger cannot reach other people's stores.
- **Backups and archives of the period:** the earliest backup that should contain the document: if it does, the document existed by that date; if backups of the claimed period exist and lack it, the document did not: bracketing the true creation date between the last backup without it and the first with it.
- **Contextual consistency:** the document's references to events, people, prices, addresses and other documents against what was true on the claimed date: the agreement citing a company number allocated later, the minute referring to a decision not yet taken: content anachronism, read alongside the technical kind.

Alteration: detecting changes to an otherwise genuine document

- **Version diffs:** where the ladder survives, the change is localised to a rung with an account and a time (guide 102 §6, guide 107 §4): the altered clause, the changed figure, the deleted paragraph, dated and attributed.
- **Recovered prior states:** PDF incremental updates preserving the pre-alteration content; Office autorecovery and temporary files; earlier copies in mailboxes, backups and counterparts' hands (§5): the document before the change, recovered and compared.
- **Internal inconsistency within the document:** a page or paragraph in a different font subset, style lineage or revision ID from its neighbours; a PDF page with a different producer or compression from the rest; an image region with mismatched noise or compression: the graft showing its seam.
- **Cross-copy comparison:** hash and content divergence between copies that should be identical (guide 82 §7, guide 98 §6): the counterparty's executed copy against the claimant's "same" document, the difference localised and its custodian identified.
- **Signature and execution evidence:** digital signatures whose validity breaks on the altered content; e-signature platform audit trails recording what was signed, by whom, when, with its hash; wet-signature pages whose scan metadata differs from the body pages: execution as the anchor against which alteration is measured.

Grading, reporting and deployment: from finding to consequence

- **The grades:** consistent with the claimed date (nothing internal or external contradicts it, and corroboration exists); unverifiable (nothing contradicts, nothing corroborates); inconsistent with the claimed date (specific anomalies identified, innocent explanations addressed); created no earlier than a demonstrated date (anachronism or absence bracketing the true origin); fabricated or altered (the finding the evidence supports beyond the alternatives): each reached on stated evidence.
- **Innocent explanations first:** guide 108 §4's rewrites (copies, migrations, save-as resets), template inheritance (guide 107 §7), platform flattening (guide 102 §4), scanner and conversion artefacts: each considered and excluded on the record before manipulation is found: the report that skips this step is the report cross-examination dismantles.
- **Reporting to the allegation's weight:** forgery allegations carry professional and reputational consequences and, in criminal contexts, evidential standards: the report is drafted under CPR Part 35 or CrimPR Part 19 with methods, tools, limitations and alternatives explicit (guide 100 §6), and the FSR Code declaration where criminal work in England and Wales is concerned.
- **Deployment:** the graded finding supports strike-out and dishonesty findings in civil fraud, insolvency clawback and director-disqualification proceedings, employment and regulatory outcomes, criminal referral (guide 98 §7's sequencing), and: on the other side: the exoneration of a genuine document with the same rigour (Example 3 below).
- **Preservation of the evidence of examination:** the questioned document imaged write-blocked and hashed before any test (guide 108 §7); the examination reproducible from the record; the original's integrity provable if the finding itself is challenged.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: authenticity is decided by the relationship between the document and its world, so the map is the world. The document itself (internal metadata, structure, anachronisms, drafting signature) is the first source and, for a careless forgery, sufficient. The platform layer (ladder, audit log, upload events) records when the document entered the estate. The transmission layer (sent-items, headers, recipients' copies) records when it left the author's hands. The backup layer brackets its existence in time. The counterparty layer holds the version the forger could not edit. The environment layer (software deployment records, font installations, template histories, the device's own configuration) establishes what was available when. And the contextual layer (the events, people and documents the questioned document refers to) tests its content against the claimed date. When one layer is unavailable: the ladder flattened, the backups rotated, the counterparty uncooperative: the table names the others; and when all the external layers are silent about a document that claims to have been important, the silence is a finding of its own.

QUESTION	THE DOCUMENT ITSELF	PLATFORM LAYER	TRANSMISSION + COUNTERPARTY	BACKUP LAYER	ENVIRONMENT RECORDS	CONTEXTUAL LAYER
Could it have been made on the claimed date	Y: build, font, feature, format	n/a	n/a	n/a	Y: what was deployed when	Y: content anachronisms
When did it actually come into being	Drafting signature, revision IDs	Y: first rung, first event	Earliest send	Y: first capture	Device-config timeline	n/a
Did it exist where it should	n/a	Presence in the period's stores	Y: recipients' copies	Y: period backups	n/a	References by other documents
Has it been altered	Y: seams, incremental updates, residue	Version diffs	Y: the clean copy	Prior state	n/a	Inconsistency with events
Is the anomaly innocent	Save-as, template inheritance	Migration, flattening	n/a	Pre-migration originals	Y: deployment explains builds	n/a

Fallback strategy in one line: read the document for what it could not have been, then read the estate for where it should have been: a forgery fails at least one; a genuine document, properly examined, passes both.

Worked examples

EXAMPLE 1 · THE SIDE LETTER WITH A 2023 PRODUCER STRING

An insolvency dispute turned on a side letter said to have been signed in November 2019, varying a loan's repayment terms in the director's favour. The document was produced as a PDF with a November 2019 creation date. The §4 examination read the PDF's producer string: an office suite build first released in March 2023; its embedded font subset carried a version shipped with that build; and its internal creation date sat four years before the software that wrote it existed. The §5 search found no trace of the side letter in the lender's files, in the director's own 2019 sent-items, in the company's period backups, or in the solicitors' completion bundle for the loan. The §7 grade was "created no earlier than March 2023, inconsistent with the claimed date, and absent from every store in which a genuine document of that date would be expected": with the innocent explanation (a 2023 re-scan of a 2019 original) addressed and excluded: no original was produced, and the PDF's structure showed native generation, not scanning. The liquidator's claim proceeded on the finding.

EXAMPLE 2 · THE MINUTE THAT WAS ASSEMBLED FROM THREE LATER DOCUMENTS

A shareholder produced a board minute recording a 2021 resolution authorising a disputed transaction. The Office file's application build was consistent with 2021 and the creation date plausible. The §3 examination went deeper: the document's paragraph-level revision identifiers matched, in sequence, identifiers found in three other documents from the same author's environment dated 2024; its style lineage inherited from a 2024 template; and its revision count of one and editing time of eleven minutes were inconsistent with a minute claimed to have been drafted, reviewed and approved. The §5 corroboration was empty: no version ladder before 2024, no circulation to the other directors in 2021, no presence in the 2021-2022 board-pack archive, and the company secretary's minute book (physically bound, contemporaneously numbered) had no gap where it would have sat. The §7 finding: inconsistent with the claimed date; assembled in 2024 from content originating in three identified 2024 documents. The build had been aged; the fingerprints had not.

EXAMPLE 3 · THE GENUINE INVOICE THAT WAS ACCUSED

A customer resisting payment alleged that a supplier's invoice had been fabricated after the dispute, citing a file-system creation date in 2025 on the produced PDF. The supplier instructed an examination expecting vindication and got it: the created date was a copy artefact (guide 108 Example 1's pattern: the PDF exported from the accounting system for disclosure); the accounting system's own audit table recorded the invoice's creation on the claimed 2023 date with the original numbering sequence intact; the customer's own accounts-payable mailbox (obtained by disclosure) held the invoice as received in 2023 with server header hops to match; and the period backup of the accounting database contained it. The §7 grade was "consistent with the claimed date, corroborated by four independent sources". The allegation failed with costs. The method that convicts forgeries is the method that clears genuine documents, and the supplier who ran it first controlled the hearing.

Common mistakes and technical limitations

Common mistakes

- **Forgery alleged from a date field:** Example 3's accusation: guide 108's innocent rewrites never considered.
- **Internal evidence only:** the document examined, the estate never searched: the well-aged forgery passing §3 and never meeting §5.
- **External evidence only:** absence pleaded without the internal tests that show why: the "we could not find it" finding, weaker than the "it could not have existed" one.
- **The original never demanded:** a PDF examined when the native source (with its far richer §3 evidence) was obtainable.
- **Handling before imaging:** the questioned document opened, re-saved or converted before write-blocked acquisition: the evidence altered by the examination.
- **Grades inflated:** "inconsistent with the claimed date" reported as "fabricated" without the alternatives excluded: the finding that fails under cross-examination and damages the true one.
- **Counterparties unasked:** the clean copy in the other side's hands never requested: §6's control missing.
- **Specialism mismatched:** a digital examiner opining on wet-ink signatures, or vice versa: guide 100 §3's error.

Technical limitations

- **A careful forger can age the internals:** period software in a virtual machine, period fonts, a rolled-back clock: the internal tests can be passed; the external ones remain, and the report says which were run.
- **External layers expire:** ladders prune, logs rotate, backups cycle, counterparties lose files: the corroborating world shrinks with time, and the examination is stronger the earlier it runs.
- **Unverifiable is a real outcome:** a document with no anachronism and no corroboration is neither cleared nor convicted: the honest grade, reported as such.
- **Scanned paper flattens evidence:** a scan carries the scanner's metadata, not the original's drafting history: the paper original, where it exists, examined by the appropriate specialist.
- **Content anachronism needs domain knowledge:** the company number, the address, the price that was not yet true: found by lawyers and clients as often as examiners: the examination is a joint exercise.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Where is the native original, on which platform, and can it be imaged write-blocked before anyone else opens it?
- Who else received the document on or around the claimed date, and which backups of that period exist?
- What software, templates and devices were in use on the claimed date: the environment records the examination will test against?

Ask your opponent

- Please produce [document] in its native format from the location in which it was originally created, together with its complete version history, platform audit events, and file-system and document metadata, and confirm the software and device used to create it.
- Please disclose all transmissions of [document] on or after its stated date, with recipients and times, and identify the earliest backup or archive in which it is contained.
- Please confirm whether [document] has been converted, re-saved, scanned or copied since its stated date, with the records of each such operation.

Ask your eDiscovery / forensic provider

- Which internal tests were run, what did each show, and which innocent explanations were considered and excluded?
- Which external layers were searched for the document, and what was found in each?
- What grade does the evidence support, and what would move it up or down?

SUGGESTED WORDING · INSTRUCTION FOR AUTHENTICITY EXAMINATION

"You are instructed to examine [document], which purports to have been created on or about [date], and to report on whether its internal characteristics and its presence in the associated data sources are consistent with that date. Please acquire the document write-blocked and hash-verified before examination; examine its internal metadata, structure, application and build identifiers, fonts, features and drafting indicators for consistency with the claimed date; examine the sources at Schedule 1 [platform version histories and audit logs, mailboxes and transmission records, backups, counterparty copies, environment and deployment records] for the document's presence and history; identify any indications of alteration and localise them where possible; consider and address innocent explanations for any anomaly; and grade your conclusion on a stated scale, distinguishing unverifiable from inconsistent and inconsistent from fabricated. Please report in a form suitable for CPR Part 35 [/ CrimPR Part 19, including the Forensic Science Regulator's Code declaration]."

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

The authenticity checklist

- ☐ Native original located; imaged write-blocked and hashed before examination
- ☐ Application, build, font, feature and format dated against the claim
- ☐ Metadata fields cross-checked; revision and editing counters read
- ☐ Drafting signature assessed: single session or accumulated history
- ☐ Format-specific structures examined: Office parts, PDF updates, EXIF, headers
- ☐ Version ladder and audit events searched for the first appearance
- ☐ Transmission records and counterparty copies obtained
- ☐ Period backups checked; existence bracketed in time
- ☐ Content tested for contextual anachronism with the legal team
- ☐ Innocent explanations excluded on the record; finding graded

Red flags

- Producer strings and builds newer than the claimed date: Example 1's 2023.
- Revision IDs and style lineage shared with later documents: Example 2's assembly.
- Single-session creation of documents claimed to have been drafted and reviewed.
- No version ladder, no transmission, no backup presence before the dispute.
- Documents produced only as PDFs or scans when natives should exist.
- Content referring to facts not yet true on the claimed date.
- Forgery allegations resting on a file-system date alone: Example 3's accusation.

When to involve a digital forensic expert

The moment a document's date or content is doubted, in either direction: before anyone opens or converts the original; while the external layers (ladders, logs, backups, counterparties) still hold the corroboration; and before the allegation is pleaded, so it is pleaded at the grade the evidence earns (Examples 1-2) or not pleaded at all (Example 3). Reports run under CPR Part 35 and CrimPR Part 19, with the FSR Code declaration for criminal work in England and Wales. Through **cflab.uk** and **e-discovery.uk**, authenticity examinations run from write-blocked acquisition through both halves of the method to a graded finding: because the forger controls the document, and the examination controls everything else.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can a backdated document really be detected if the forger changed all the dates?

Usually: the dates are the easy part; the application build, fonts, features, revision identifiers and drafting signature inside the file (§3-§4), and the ladder, logs, recipients and backups outside it (§5), are the hard part, and forgers rarely manage all of them: Example 1 failed on its producer string, Example 2 on its revision IDs and empty world. The careful forger who ages the internals still cannot insert the document into last year's backups.

The other side says our document is fabricated because its file date is recent. What now?

Run the examination yourself, first: the recent date is usually a copy or export artefact (guide 108 §4, Example 3 here), and the platform record, the recipients' copies and the period backups will corroborate the true date: the party that proves authenticity holds the hearing. Demand the native and the corroboration through §11's requests if the accuser has them.

What if the document only exists as a scan or a PDF?

The scan carries the scanner's metadata and the PDF its producer's, both dateable (§4), and the external tests (§5) apply in full: where was the document sent, backed up, referenced? The absence of a native original where one should exist is itself a red flag; the paper original, if claimed, is examined by a questioned-document specialist under guide 100's matching.

How confident can an expert be that a document is forged?

As confident as the graded evidence allows (§7): "created no earlier than [date]" from an anachronism is near-certain; "absent from every expected store" is strong but circumstantial; "fabricated" combines both and excludes the alternatives. Honest reports state the grade and its basis; overclaimed ones are dismantled by the first innocent explanation the examiner failed to address.

Can we tell whether a genuine document was altered after signing?

Frequently: version diffs localise changes to rungs (§6), PDF incremental updates preserve prior states, digital-signature validity breaks on altered content, e-signature platforms record what was signed with its hash, and the counterparty's executed copy is the control: the alteration dated, localised and attributed where the evidence allows.

Does this apply to emails and messages as well as documents?

Yes, with format-specific tests (§4): header hops and message identifiers date an email's true transit; presence in server-side stores versus a lone copy in a produced file distinguishes the sent from the manufactured; and messaging platforms' server records (guides 63-66) corroborate or contradict the produced screenshot: guide 87's authenticity work, extended to every format the estate contains.

§ 1 4 · REFERENCE

Glossary

Anachronism

An element that did not exist on the document's claimed date.

Authenticity grade

Consistent, unverifiable, inconsistent, no-earlier-than, or fabricated.

Bracketing

Fixing true creation between the last store without and first with the document.

Drafting signature

The revision, session and version pattern of a document's making.

Incremental update

A PDF's appended revision preserving the prior state.

Producer string

The PDF field naming the software and version that wrote it.

Revision identifier

Office's per-paragraph ID, traceable across documents from one environment.

Seam

The internal inconsistency where altered content meets original.

Style lineage

The template ancestry a document's formatting inherits.

World test

Whether the estate of the claimed date contains the document.

Sources and authoritative references

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

- cflab.uk, digital forensics services (document authenticity, backdating and alteration examination, 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 07 · Analysis (native collection, corroboration searches and authenticity analysis 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
- Forensic Science Regulator, Code of Practice version 2 (declarations for criminal work): gov.uk, [FSR Code v2](https://gov.uk/fsr-code-v2) · CrimPR Part 19: justice.gov.uk, [CrimPR 19](https://justice.gov.uk/crimpr-19)
- CPR Part 35 and PD 35: justice.gov.uk, [Part 35](https://justice.gov.uk/part-35) · CPR Part 32 (notice to prove documents, r.32.19): justice.gov.uk, [Part 32](https://justice.gov.uk/part-32) · PD 57AD: justice.gov.uk, [PD 57AD](https://justice.gov.uk/pd-57ad)
- ISO/IEC 27037 (acquisition and preservation): iso.org, [27037](https://iso.org/27037) · ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about detecting backdated and manipulated documents as at August 2026. Application, format and platform behaviour change; forgery is a grave allegation carrying legal and professional consequences; verify the current position and take advice before any allegation is made. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Authenticity examinations at the laboratory run both halves of the method from a write-blocked, hash-verified original: the internal tests for build, font, feature and format anachronism, metadata consistency, drafting signature and format-specific structure (Example 1's producer string, Example 2's revision identifiers); the external search across ladders, audit logs, transmission records, counterparties and period backups for the document's true first appearance (the world test that clears Example 3 and convicts the others); alteration localised through version diffs, incremental updates and cross-copy comparison; and every anomaly's innocent explanation considered and excluded on the record before a grade is reached. Reports run under CPR Part 35 and CrimPR Part 19 with the FSR Code declaration for criminal work, and the same rigour defends genuine documents against accusation. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a document's date is doubted today, the instruction is guide 108's: stop opening it, and let the examination read it as it is.



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