

Detecting Backdated Or Manipulated Documents

Detecting backdated or manipulated documents involves forensic examination of internal evidence, such as metadata and anachronisms, and external corroboration from the document's expected environment. This guide details methods for identifying alterations and provides insights into grading findings and common pitfalls.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
<https://e-discovery.uk/library/detecting-backdated-or-manipulated-documents>

DOCUMENT AUTHENTICITY · A GUIDE FOR UK LAWYERS Detecting Backdated or Manipulated Documents The Forensic Examination of Documents That Claim a Date They Did Not Have COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
BACKDATING & ALTERATION DETECTION CPR PART 35 EXPERT REPORT S 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 in at i on: 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

§ 01 · ORIENTATION 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,
GRADE THE RESULT, AND STATE THE ALTERNATIVES

§ 02 · FIRST PRINCIPLES The problem in plain English: the forger controls the document, not its world

§ 03 · INTERNAL EVIDENCE Internal evidence: metadata, anachronisms and the drafting signature

§ 04 · FORMAT - SPECIFIC EXAMINATION Format-specific examination in at i on: Office, PDF, images, scans and email

§ 05 · EXTERNAL CORROBORATION External corroboration: the estate the document should have inhabited

§ 06 · ALTERATION Alteration: detecting changes to an otherwise genuine document

§ 07 · GRADINGANDDEPLOYMENT Grading, reporting and deployment: from finding to consequence

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION
DOCUMENT THE ITSELF PLATFORM TRANSMISSION + BACKUP ENVIRONMENT
CONTEXTUAL LAYER COUNTERPART Y LAYER RECORDS LAYER

§ 09 · IN THE WILD Worked examples EXAMPLE1 ·
THESIDELETTERWITHA2023PRODUCERSTRING EXAMPLE2 ·
THEMINUTETHATWASASSEMBLEDFROMTHREELATERDOCUMENTS EXAMPLE3 ·
THEGENUINEINVOICETHATWASACCUSED

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes
Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask
your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED
WORDING · INSTRUCTIONFORAUTHENTICITYEXAMINATION

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The
authenticity checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Can a backdated document really be
detected if the forger changed all the dates? The other side says our document is fabricated
because its file date is recent. What now? What if the document only exists as a scan or a PDF?
How confident can an expert be that a document is forged? Can we tell whether a genuine
document was altered after signing? Does this apply to emails and messages as well as
documents?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab
Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB
NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

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 exam in at i on 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. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915
Page 15 of 17

Source: <https://e-discovery.uk/library/detecting-backdated-or-manipulated-documents>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.