COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Building a Digital Timeline for Litigation

From Scattered Timestamps to a Chronology the Court Can Trust

Most disputes are, at bottom, arguments about sequence: who knew what before signing, whether the file was copied before or after resignation, whether the meeting preceded the trade, which draft came first. Digital estates answer sequence questions with extraordinary precision when the work is done properly: and mislead catastrophically when it is not, because timestamps arrive in mixed time zones, drift-prone clocks, and fields that mean different things on different systems. A litigation timeline is therefore a forensic construction: events extracted from every source this series has mapped, normalised to one temporal frame, corroborated across independent systems, presented with confidence levels, and defensible line by line under cross-examination. This guide explains the method for UK lawyers: what makes a chronology evidence rather than argument, and how to build, test and deploy one.

⏱ 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. Timeline construction is among its most-instructed disciplines: chronologies for fraud trials, employment exits, contract disputes and criminal defence, built from device, cloud, network and communications sources, normalised and corroborated by examiners, and presented under CPR Part 35 with every line traceable to its artefact.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | MULTI-SOURCE TIMELINE CONSTRUCTION | CLOCK & TIMEZONE ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: A LITIGATION TIMELINE IS BUILT, NOT COMPILED: EVENTS FROM INDEPENDENT SOURCES, ONE TEMPORAL FRAME, CORROBORATION PER LINE, CONFIDENCE STATED: SO THE CHRONOLOGY IS EVIDENCE THE OTHER SIDE MUST ANSWER, NOT ARGUMENT THEY CAN DISMISS

The method has four stages. **Harvest (§3):** events extracted from every relevant source this series has mapped: communications (email headers per guide 87, messages per guides 63-66), documents and their version ladders (guide 75), platform audit logs (guides 51-58, 105-107), device artefacts (system logs, USB records, browser history), network and location data, and the financial and structured records of guides 72-74: each event carried with its source artefact and native timestamp. **Normalise (§4):** every timestamp converted to one frame (UTC as the working standard, presented in local time with the conversion stated), with time zones resolved per field, clock drift measured against reference events (the seven-minutes-fast DVR problem), DST transitions handled, and field semantics respected: created, modified, sent and logged mean different things per system, per guide 87's disciplines. **Corroborate (§5):** load-bearing events supported by independent systems: the email's server header against the client's copy, the file operation against the platform log, the badge swipe against the login: with each line graded (corroborated, single-source, inferred) so the timeline's confidence is visible and honest. **Deploy (§7):** the master timeline maintained as a working instrument, filtered views produced for pleadings, witness preparation and trial, and every line traceable to its exhibit: because a chronology that cannot answer "where does that time come from?" is not evidence, and one that can ends arguments.

- **One frame, stated:** UTC underneath, local time on top, conversions explicit: the mixed-zone muddle solved once, at the base.
- **Semantics before sequence:** what each timestamp field measures is established before any two are compared: guide 87's rule, industrialised.
- **Independence is the currency:** two systems that could not have copied each other beat ten fields from one: corroboration by design.
- **Confidence on every line:** graded entries let the strong carry the case and the weak be defended proportionately.
- **Traceability is the test:** line to exhibit to artefact: the chronology deposed as evidence, per CPR Part 35 where an expert speaks to it.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: sequence is the case, and clocks lie politely

Ask what a dispute is really about and the answer is usually an ordering: the director traded *after* the briefing or before it; the design file left *before* the resignation letter or after; the "concluded" agreement was drafted *before* its date or on it. Digital estates seem built to answer such questions: everything is timestamped. The trap is that the timestamps are plural, inconsistent and semantically slippery: a single email carries client times, server times and header hops in different zones; a file's "created" date changes meaning across copies (guide 87's rewrites); a CCTV clock drifts uncorrected for years; a phone logs in local time that changed when its owner flew.

Naive compilation: pulling visible dates into a spreadsheet: produces chronologies that are confidently wrong, and opposing experts dismantle them by finding one impossible ordering and inviting the court to distrust the rest. The forensic construction of this guide exists to prevent that: normalise before comparing, corroborate before relying, grade before presenting. Done properly, the timeline becomes the case's spine: pleadings reference it, witnesses are examined against it, and the other side must either adopt it or build a better one: which, if yours is sound, they cannot.

§ 0 3 · THE RAW MATERIAL

The raw material: event sources across the estate

- **Communications:** email with full headers (server hops as independent clocks, per guide 87), messaging platforms with their databases and server records (guides 63-66), call logs and voicemail metadata: the who-spoke-to-whom layer, densest and best-timestamped.
- **Documents and versions:** file-system dates read with guide 87's caution, DMS and cloud version ladders (guide 75, guides 102, 107) recording every save with account attribution: drafting history as chronology.
- **Platform audit logs:** M365, Google and SaaS audit trails (guides 51-58, 105-107): logins, access, downloads, shares, deletions: server-side clocks with the best semantics in the estate.
- **Device artefacts:** system event logs, USB connection records, browser history, application execution traces, and mobile artefacts (the guide 59-66 set): the at-the-keyboard layer that attribution questions need.
- **The physical-world joins:** location data (guide 124's sources), badge and access-control systems, CCTV (clock-corrected per §4), payment and transaction records (guides 72-74): the anchors that tie digital sequence to rooms, roads and money.

§ 0 4 · ONE CLOCK

Normalisation: time zones, clock drift and field semantics

- **The working frame:** all events converted to UTC for construction, presented in the relevant local time with the conversion rule stated: one base, one presentation layer, no silent mixing: the discipline that makes cross-source comparison legitimate at all.
- **Zone resolution per field:** each source's storage convention established (UTC-native server logs, local-time device fields, header offsets): documented in the timeline's methodology annex, because "what zone is this field in?" is the first cross-examination question.
- **Clock drift measured:** free-running clocks (CCTV DVRs, embedded systems, unsynced machines) calibrated against reference events visible on both the drifting and a trusted clock: the offset found, dated and applied, with the calibration evidence kept: the seven-minutes-fast camera corrected, not trusted.
- **DST and travel handled:** transition weekends checked for every spring and autumn event; devices that travelled resolved against their zone-change records: the two classic one-hour errors, caught by procedure.
- **Field semantics respected:** created, modified, accessed, sent, received, logged: each mapped to what the system actually measures (guide 87's families) before any ordering claim is built on it: the semantic table as the timeline's foundation document.

§ 0 5 · THE WEIGHT OF EACH LINE

Corroboration and confidence: making each line defensible

- **Independence sought:** for every load-bearing event, a second source with a different clock and a different failure mode: server header against client copy, platform log against device artefact, badge system against login record: agreement between systems that could not have contaminated each other.
- **The corroboration lattice:** guide 87 §5's method scaled up: events cross-checked until the timeline's critical path is supported at every link: with the lattice diagrammed for the court where the sequence is contested.
- **Confidence grades:** each entry marked: corroborated (independent sources agree), single-source (one reliable artefact), inferred (bounded by surrounding events), approximate (drift-corrected or semantically soft): the grading that lets cross-examination spend itself on lines the case does not need.
- **Conflicts investigated, not averaged:** where sources disagree, the disagreement is diagnosed (zone error, drift, semantics, manipulation per guide 108-109) and resolved on evidence: an unexplained conflict is stated as such: the honest line beats the smoothed one.
- **Manipulation screening:** load-bearing timestamps tested against guide 87's manipulation signatures and guide 109's backdating artefacts: the timeline's own integrity checked before it vouches for anything else.

§ 0 6 · THE BUILD

Construction in practice: from artefacts to the master timeline

- **The event schema:** each entry: timestamp (UTC and presented), event description, actor and account, source artefact and exhibit reference, extraction method, confidence grade, notes: one row, everything a challenge needs answered.
- **Extraction with provenance:** events pulled by forensic tooling from imaged and collected sources (this series' acquisition disciplines), never retyped from screenshots: the chain from artefact to row unbroken and stated.
- **Scale handled by filtering:** the master set may run to hundreds of thousands of events (super-timelines from device images): the litigation instrument is the filtered view: issues-relevant events promoted, the full set preserved and searchable behind it.
- **Iteration with the legal team:** the timeline built in passes: the skeleton from communications and logs, enriched as disclosure lands, revised as issues sharpen: version-controlled per the series' standing record discipline, so every edition is reproducible.
- **Gap honesty:** silent periods marked as such, with guide 95's analysis applied where silence is suspicious: the timeline showing what is absent as visibly as what is present.

§ 0 7 · IN COURT'S HANDS

Presentation and deployment: chronologies that persuade and survive

- **Views per audience:** the pleading chronology (spare, agreed-fact-heavy), the witness-preparation timeline (their events, their documents), the trial chronology (the critical path with exhibit references), and the expert's annexe (methodology, semantics table, calibration evidence): one master, many faces.
- **Visual honesty:** graphics that show confidence (solid versus outlined markers, corroboration links), density without distortion (uniform scales, gaps visible), and the guide 87-style lattice for contested sequences: persuasion by clarity, not decoration.
- **Every line answerable:** the deployment test: any entry challenged in cross-examination is traced to its exhibit and method within a minute: the schema of §6 earning its columns.
- **Expert versus advocacy:** where sequence is genuinely contested, the timeline enters through a CPR Part 35 report with the examiner speaking to method: where it is not, it serves as an agreed working document: the two roles kept distinct, per guide 100's instruction disciplines.
- **Attacking the opponent's chronology:** the same standards applied in reverse: zones unstated, drift uncorrected, semantics mixed, single-source lines carrying the case: the §4-§5 checklist as cross-examination outline.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a timeline's strength is the independence of its sources, so the map is worked for redundancy on every critical event. A single moment: a file leaving, a message sent, a login: is typically recorded in several places with different clocks and different tamper profiles: the device's own artefacts, the platform's server-side audit log, the counterpart system's record, the network layer, and the physical-world systems (access control, CCTV, payments) that bracket it. The construction pursues at least two per load-bearing event, chosen for independence: and when the primary source is unavailable, damaged, or suspect (guide 95's gaps, guide 108's untrusted stamps), the same map supplies the alternates: the server log when the device is wiped, the counterpart copy when the mailbox is purged, the badge system when the login record is contested. The timeline inherits every source guide in this series; its own contribution is the frame that lets them testify together.

EVENT TYPE	DEVICE ARTEFACTS	PLATFORM AUDIT LOGS	COUNTERPART RECORDS	NETWORK LAYER	PHYSICAL-WORLD SYSTEMS	DELETED/ RECOVERABLE
Message sent	Y: client DB + logs	Y: server records	Y: recipient copy	Header hops	n/a	Varies: guide 95's map
File accessed / copied	Y: MFT, LNK, USB records	Y: access + download logs	Destination system	Transfer logs sometimes	n/a	Varies
Login / session	Y: local event logs	Y: sign-in logs + IPs	n/a	VPN + firewall records	Badge + CCTV brackets	Limited
Document edited	Local save artefacts	Y: version ladders	Shared-copy versions	n/a	n/a	Prior versions often
Person present / moving	Device location artefacts	Sign-in geolocation	n/a	Wi-Fi association logs	Y: badges, CCTV, payments	Varies

Fallback strategy in one line: for every event the case stands on, hold two independent clocks: and when one source is gone or contested, the §8 row names its replacements before the argument starts.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE TRADE, THE BRIEFING AND THE FORTY MINUTES

An insider-dealing defence turned on whether the client placed his order before or after a briefing call said to have conveyed the price-sensitive news. Naive reading condemned him: the broker's confirmation (timestamped 14:22) followed the call log's 13:41 entry. The §4 work reversed it: the broker platform stamped confirmations in UTC; the call log was device-local BST; and the order-entry record: the platform's audit log, not the confirmation: showed submission at 13:03 UTC, thirty-eight minutes before the 13:41 BST (12:41 UTC) call began. The corroboration lattice added the client's own banking app session (13:01-13:06 UTC, independent clock) around the order. One zone error had built the prosecution sequence; the corrected, corroborated timeline: methodology annexe attached: dismantled it. The first cross-examination question of §4 is asked because of cases like this one.

EXAMPLE 2 · THE EXIT THAT WAS CHOREOGRAPHED

An employer suspected a departing sales head had taken the client book, but held only fragments: an odd USB record here, a large download there. The §6 build assembled the estate into one frame: platform logs (mass report exports, 21:40-23:15 UTC on the Sunday), device artefacts (USB drive connected 23:02, LNK files opening the exports from it), badge records (office entry 21:31, exit 23:44), CCTV corrected for its eleven-minute drift showing him alone on the floor, and: the choreography: his resignation email drafted at 23:51 and sent at 08:00 Monday. Each event was single-source trivia; the normalised sequence was a narrative no innocent explanation survived. The claim settled on disclosure of the timeline with its exhibit bundle. Sequence, properly built, is the argument.

EXAMPLE 3 · THE CHRONOLOGY THAT FELL TO ITS OWN SPREADSHEET

Opposing solicitors served a 300-line chronology supporting a backdating allegation: visible dates typed from disclosed documents into a spreadsheet. The §7 attack checklist ran against it: no zone methodology (server-UTC and device-local entries interleaved unconverted); the load-bearing line: a file "modified" hours after the agreement's date: resting on a copy's timestamp that guide 87's rewrite rules explained innocently (the file had been moved to a new DMS, rewriting dates estate-wide on migration day, a fact the migration records proved); and three orderings internally impossible once normalised. The examiner's responsive report corrected the frame, re-graded the lines, and the allegation was not pursued. The example is §2's warning made flesh: compilation is not construction, and the difference is discoverable.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Mixed frames:** Example 1's condemnation and Example 3's collapse: zones interleaved unconverted: the field's most common fatal error.
- **Semantics ignored:** created compared with sent, modified with logged: orderings built across fields that measure different things.
- **Drift trusted:** CCTV and DVR clocks read at face value: the seven-minute correction never made.
- **Compilation from screenshots:** dates retyped without artefacts behind them: no provenance, no answer to "where does that come from?".
- **Single-source critical paths:** the case's spine resting on one clock: §5's independence rule, unapplied where it mattered most.
- **Conflicts smoothed:** disagreeing sources averaged or silently dropped: the honest diagnosis traded for a tidy line.
- **DST weekends unchecked:** the one-hour error, twice a year, waiting.
- **The master unversioned:** editions diverging across the team: which chronology the court saw becoming its own dispute.

Technical limitations

- **Resolution varies:** some sources stamp to the second, some to the minute, some to the day: orderings claimed only at the resolution the sources support.
- **Clocks can be unanchorable:** a drifting clock with no reference event yields offsets with stated uncertainty, not false precision: bounded honestly.
- **Timestamps can be forged:** the timeline screens for manipulation (guides 108-109) but inherits the estate's integrity: contested stamps get their own forensic treatment before they carry weight.
- **Logs expire:** audit-trail retention (guide 105's windows) deletes the best clocks first: harvest early or lose the server side.
- **Correlation is not causation:** sequence proves order, not intent: the timeline states what happened when; the inferences remain the advocate's, argued from it.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which orderings does the case actually turn on: so the critical path is defined and its events doubly sourced first?
- What systems hold the §3 layers: platforms, devices, physical-world records: and which retention clocks are running on them now?
- Did the relevant people or devices travel across zones, and are there known clock-quality issues (CCTV, legacy systems) to calibrate?

Ask your opponent

- Please state, for the chronology served, the timezone convention applied to each source, the treatment of clock drift and daylight-saving transitions, and the semantic meaning attributed to each timestamp field relied on.
- Please identify, for each entry in [the contested sequence], the source artefact, its custodian and extraction method, and confirm whether the entry is corroborated by any independent system.
- Please confirm preservation of the audit logs, device artefacts and reference records underlying the events at [dates], including sources subject to rolling retention.

Ask your eDiscovery / forensic provider

- Is the critical path corroborated line by line: and which entries remain single-source or inferred?
- What did the calibration work establish for the drifting clocks: and what uncertainty survives it?
- Can every load-bearing line be traced to exhibit and method inside a minute: the §7 deployment test?

SUGGESTED WORDING · INSTRUCTION FOR TIMELINE CONSTRUCTION

> "You are instructed to construct a chronology of events relevant to [the issues], from the sources listed in Schedule 1 [devices, platforms, logs, physical-world systems]. All timestamps are to be normalised to UTC with local-time presentation and the conversion methodology stated; timezone conventions, clock-drift calibration and daylight-saving handling are to be documented per source, and the semantic meaning of each timestamp field relied upon identified. Events material to the sequence at [the critical issues] are to be corroborated by independent sources where available, with each entry graded for confidence and traceable to its source artefact, exhibit reference and extraction method. Gaps and conflicts are to be stated, not resolved silently. The chronology and its methodology are to be prepared so as to be suitable for exhibition to a report compliant with CPR Part 35 [/ CrimPR Part 19] if required."

§ 12 · QUICK CONTROL

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

The timeline checklist

- ☐ Critical-path orderings defined with the legal team first
- ☐ Source harvest across all §3 layers; retention clocks beaten
- ☐ UTC base; presentation layer and conversions stated
- ☐ Zone convention documented per source and field
- ☐ Drifting clocks calibrated with kept evidence; DST checked
- ☐ Semantic table built before any cross-field comparison
- ☐ Load-bearing events doubly sourced; independence genuine
- ☐ Every line: artefact, exhibit, method, confidence grade
- ☐ Conflicts diagnosed on the record; gaps shown honestly
- ☐ Master version-controlled; views generated, never forked

Red flags

- Chronologies with no timezone methodology: Example 3's spreadsheet.
- Sequences that flip when one field's semantics are questioned.
- CCTV and DVR times presented uncalibrated.
- Critical events resting on a single, party-controlled clock.
- Impossible orderings surviving in a served chronology.
- Screenshots as the only provenance for dates.
- Audit logs expiring while the sequence is argued by letter.

When to involve a digital forensic expert

At case theory, where the critical orderings are named and their §8 source pairs identified while retention windows are open; at construction, where extraction, normalisation and corroboration are done to the standard cross-examination assumes (Examples 1-2's method); at attack, where an opponent's chronology is audited against §4-§5 (Example 3's collapse); and at trial, where the examiner speaks to methodology under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, timelines are built from artefact to exhibit as one engineered product: the sequence the case stands on, made answerable line by line.

§ 1 3 · COMMON QUESTIONS

Frequently asked questions

Why can't we just build the chronology from the documents' visible dates?

Because visible dates mix zones, semantics and drifting clocks: Example 3's spreadsheet did exactly that and fell to its own lines: and because a chronology without artefact provenance cannot answer the first challenge put to it. Compilation makes a working draft; construction (§4-§6) makes evidence.

What does "normalising to UTC" actually involve?

Establishing each source's storage convention, converting every event to one UTC base, then presenting in relevant local time with the rule stated: plus drift calibration and DST checks: §4's procedure. It is bookkeeping, not magic: the point is that after it, any two events can be legitimately compared: and before it, none can.

How precise are digital timestamps really?

As precise as their clock and resolution: synced server logs are excellent to the second; device fields are good when the clock was; free-running DVRs are only as good as their calibration; some sources resolve only to minutes or days: which is why §5 grades confidence and §10 claims orderings only at supported resolution. Precision is per-source, established, never assumed.

The other side's chronology contradicts ours. How is that resolved?

By methodology: the frames, semantics, calibrations and provenance of both are compared, conflicts diagnosed to their cause (zone error, drift, field mix-up, or a genuinely contested stamp needing guide 108-109 treatment): Examples 1 and 3 are both stories of one chronology surviving that audit and one not. Courts follow the timeline that shows its working.

Can a timeline prove who did something, or only when it happened?

The timeline orders events attributed to accounts and devices; attribution to fingers is the separate discipline of guides 105-107, and the two are built together where identity is contested: Example 2's badge, CCTV and device layers doing exactly that join. Sequence plus attribution is the full product; the timeline alone is the when.

When should timeline work start?

With the case: the best clocks (platform audit logs) sit on rolling retention that deletes them while pleadings are exchanged (§10), and the critical path defined early lets preservation and collection target its sources: guide 95's windows apply to time evidence with full force. A timeline started at trial preparation is built from what survived; one started at instruction is built from what existed.

§ 14 · REFERENCE

Glossary

Calibration event
An occurrence visible on both a drifting and a trusted clock.

Clock drift
A free-running clock's accumulating error against true time.

Confidence grade
The stated support level of a timeline entry.

Corroboration lattice
Cross-checked independent sources supporting a sequence.

Critical path
The orderings the case actually turns on.

Field semantics
What a timestamp field actually measures on its system.

Master timeline
The full, version-controlled event set behind all views.

Normalisation
Conversion of all events to one stated temporal frame.

Super-timeline
The exhaustive machine-extracted event set from an image.

UTC
Coordinated Universal Time: the construction base frame.

Sources and authoritative references

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

- cflab.uk, digital forensics services (multi-source timeline construction, clock calibration, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 07 · Analysis (chronology building, corroboration and presentation as practised): e-discovery.uk/edrm/analysis · Phase 02 · Identification: e-discovery.uk/edrm/identification
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- CPR Part 35 and PD 35 (expert chronologies in civil proceedings): justice.gov.uk, Part 35 · CrimPR Part 19: justice.gov.uk, CrimPR Part 19
- PD 57AD: justice.gov.uk, PD 57AD · ISO/IEC 27037: iso.org, 27037 · ICO, UK GDPR guidance: ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Timeline work at the laboratory is engineered end to end: sources harvested across every §3 layer with retention clocks beaten; normalisation, calibration and the semantic table built as the foundation (Example 1's reversal lived in exactly that work); the corroboration lattice constructed for the critical path; and the master maintained under version control with views generated for pleadings, witnesses and trial: every line passing the §7 deployment test. The same standards run in reverse against served chronologies (Example 3's audit), and examiners speak to methodology under CPR Part 35 and CrimPR Part 19 where sequence is fought. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if the case turns on an ordering, the platform logs that prove it are expiring on schedule now: the harvest is this month's task, whatever the timetable says about trial.

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