COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

The Defensible Multi-Source Evidence Bundle

Assembling Devices, Cloud, Network, Media and Open Sources Into One Coherent, Admissible Case

A modern case is rarely proved by one artefact. It is proved by many, a phone, a laptop, a cloud account, network logs, a video, a location record, a public post, each an imperfect witness, brought together so that they corroborate one another on a single timeline. That assembly is where cases are won, and where they most often go wrong. Sources conflict, or seem to; timestamps are in different zones; the same event is recorded five times with five different clocks; attribution rests on one strand where it should rest on several; and a bundle that looks compelling can collapse if its integrity, its method or its honesty is not sound throughout. This guide is the capstone of the series: it sets out for UK lawyers how the many kinds of digital evidence covered in earlier guides are combined into one defensible bundle, how convergence and contradiction are handled, how integrity and provenance are maintained across every source, and how the whole is presented, at honest confidence, as an admissible, coherent case rather than a pile of exhibits.

⏱ 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. Assembling multi-source evidence is the culmination of the laboratory's work: taking the device, cloud, network, media and open-source material examined in individual instructions and building it into one coherent, integrity-assured, honestly-bounded bundle on a single timeline. The result is reported under CPR Part 35 and CrimPR Part 19 as a case a court can follow and rely on, with every source's provenance, method and limits documented.

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

§ CONTENTS

In this guide

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 1 · ORIENTATION

Executive summary

The headline point: cases are proved not by one artefact but by many imperfect sources made to corroborate one another on a single timeline, so the decisive work is assembly, converging the evidence, resolving apparent contradictions, maintaining integrity across every source, and presenting the whole at honest confidence as a coherent, admissible bundle.

The sources (§3): devices, cloud accounts, network and location data, media, financial and on-chain records and open sources, each an imperfect witness contributing a different piece. **The timeline (§4):** the assembly's spine, every source normalised to a common clock and placed on one master timeline so events can be compared moment by moment. **Convergence and weight (§5):** the finding is strong where independent sources agree; apparent contradictions are examined and explained, not smoothed over, and each strand is weighted by its reliability. **Integrity (§6):** the bundle is only as sound as its weakest link, so hashing, chain of custody, provenance and honest limits are maintained across every source without exception. **Deployment (§7):** presenting the result as a coherent case a court can follow, at honest confidence, rather than a pile of unconnected exhibits.

- **Cases are built, not found:** many imperfect sources are assembled into one corroborated whole.
- **The timeline is the spine:** every source is normalised to a common clock and placed on one master timeline.
- **Convergence carries weight:** independent sources agreeing is strong; contradiction is examined, not hidden.
- **Integrity is end-to-end:** the bundle is only as sound as its weakest source, so provenance holds throughout.
- **Present a case, not a pile:** a coherent, honestly-bounded narrative a court can follow and rely on.

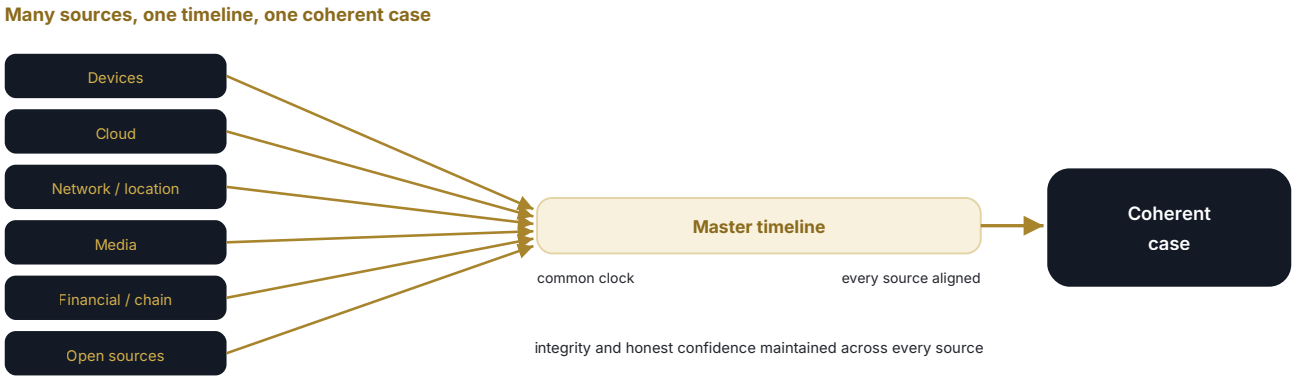

Figure 1 - the assembly: six families of imperfect source normalised to a common clock, aligned on one master timeline, and delivered as a single coherent case with integrity maintained throughout.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: many witnesses, one case

Earlier guides in this series each dealt with a single kind of evidence: how to examine a phone, a cloud account, a video, a location record, a browser, a wallet, a public post. Real cases almost never turn on just one of these. They turn on several at once, and on how those several fit together. A dispute about where a person was at a given moment might draw on the phone's own location, the car's telematics, a wearable's route, a geotagged photograph, a cell-site record and a CCTV frame, six witnesses to the same fact, each with its own accuracy, its own clock and its own gaps. The evidence is not in any one of them; it is in the way they agree, or fail to.

This is where cases are made and unmade. Assemble the sources well, normalise their times, place them on one timeline, let the reliable ones corroborate each other, examine honestly the ones that seem to conflict, and weight each by what it can actually bear, and you have a coherent case that is far stronger than the sum of its parts and very hard to dislodge. Assemble them badly, take timestamps at face value across time zones, rest a conclusion on one strand where several were needed, present a pile of exhibits with no timeline and no narrative, let the integrity of one source lapse and taint the whole, and even a case with genuinely powerful material can collapse under scrutiny. The skill of the multi-source bundle is therefore not forensic examination of any single source, which the earlier guides covered, but integration: making many imperfect witnesses into one honest, coherent, integrity-assured account that a court can follow and rely on. This capstone guide sets out how that integration is done.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 3 · THE SOURCES

The sources and what each contributes

- **Devices:** phones, computers, servers and their storage, contributing the richest first-person record, messages, files, activity, deleted data, but bounded by attribution (which person, not just which device) and by what a single device holds (guides across the series): the core, corroborated by the rest.
- **Cloud accounts:** mailboxes, file platforms, SaaS and backups, contributing the fuller and often longer-lived record that outlasts a wiped device, reached through the account, independent of the hardware (guides 111 to 114): the estate's memory.
- **Network and location data:** logs, Wi-Fi, cell, GPS and app location, contributing place, movement and connection, at varying accuracy, converged rather than relied on singly (guides 124, and network guides): the where and the how-connected.
- **Media, financial and on-chain data:** images, video and audio (authenticated, guides 121, 127), financial records and cryptocurrency (guide 128), contributing depiction, value and flow, each with its own authenticity discipline: the what-happened and the follow-the-money.
- **Open sources:** lawfully gathered, authenticated public material (guide 129), contributing corroboration, context and a party's own public statements, verified and attributed: the plain-sight strand that ties the private record to the public one.

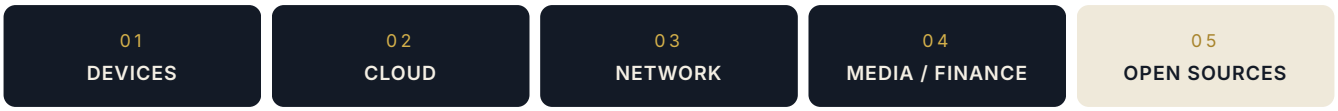

Figure 2 - the six source families of a multi-source case, each contributing a different, imperfect piece that the assembly makes corroborate the others.

§ 0 4 · THE MASTER TIMELINE

Building the master timeline

- **One timeline is the spine:** every relevant event from every source placed on a single master timeline, so the whole case can be read as one sequence rather than as separate exhibits (guide 96): the structure that makes convergence visible.
- **Normalise the clocks:** each source's timestamps converted to a common time base, with time zones, daylight saving and clock drift accounted for, because the same event recorded by six sources can appear at six different times if their clocks are not reconciled (guide 108): the step that prevents false contradiction.
- **Establish each clock's offset:** the DVR that is minutes fast, the server in UTC, the phone in local time, each offset measured and applied, so events align truly rather than apparently (guide 121 §6, guide 108).
- **Label source and confidence:** every event on the timeline tagged with its source and the reliability of that source, so the timeline shows not just what happened when but how well each point is supported (guide 124's confidence discipline).
- **Reconcile with the real-world facts:** the digital timeline married to the known events of the matter, the fraud, the transfer, the incident, so the technical sequence answers the legal question (guide 96): the timeline made to serve the case.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 5 · CONVERGENCE AND WEIGHT

Convergence, contradiction and weight

- **Convergence is strength:** where independent sources agree on a fact, the phone, the car and the wearable all placing a person at home, the finding is robust because no single source carries it alone (guide 124): the whole exceeding the parts.
- **Contradiction is examined, not hidden:** where sources conflict, the conflict is investigated, a clock offset, a device left behind, a stale record, and explained honestly, because a suppressed contradiction is a case waiting to collapse (guides 124, 100): the honesty that holds up.
- **Weight follows reliability:** each strand weighted by what it can bear, a precise GPS fix over a coarse cell record, a typed search over an auto-loaded URL, a key on the device over a clustering inference, so the bundle rests most on its strongest points (guides 124, 125, 128): the calibrated case.
- **No single point of failure:** the central attribution or timing supported by more than one source wherever possible, so the case does not fall if one strand is undermined (guide 105): resilience by corroboration.
- **Honest confidence overall:** the assembled conclusion expressed at the confidence its weakest necessary link allows, and stated as such, so the bundle claims only what it can prove (guide 100): the survivable whole.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 6 · INTEGRITY ACROSS EVERY SOURCE

Integrity and provenance across every source

- **The weakest link governs:** a bundle is only as defensible as its least sound source, so integrity is maintained across all of them without exception, one mishandled exhibit can taint the whole (guides 2, 3): the end-to-end standard.
- **Hashing and chain of custody throughout:** every source acquired, hashed and its custody documented from collection to court, so each strand is verifiably unaltered and its journey accountable (guide 2): the integrity backbone.
- **Provenance for each strand:** where each source came from, how it was collected and by what method recorded and reproducible, so any strand can be explained and, if needed, re-created (guides 71, 126): the accountable origin.
- **Consistent method and standards:** the same disciplined standards, ISO/IEC 27037, the FSR Code, applied across device, cloud, media and open-source collection, so the bundle is uniform in quality (guide 2): no weak corner.
- **Data protection across the whole:** the UK GDPR observed across every source, with collection scoped and minimised and sensitive and third-party data protected throughout the bundle, not just source by source (guide 20): proportionality over the whole.

§ 0 7 · DEPLOYMENT

Deployment: presenting a coherent, admissible bundle

- **A narrative, not a pile:** the bundle presented as a coherent account, the timeline, the convergence, the weight of each strand, so the court reads a case rather than sorting through disconnected exhibits (§4, §5): the story the evidence tells.
- **Honest limits stated:** the confidence of each conclusion, the contradictions examined, and what the evidence does not show, all set out plainly, because a bundle that overclaims invites collapse and one that is honest invites trust (guide 100).
- **Admissibility and disclosure:** the whole prepared to the standards of admissibility and disclosure, integrity, provenance, relevance, proportionality, so the bundle survives challenge and complies with PD 57AD, CPR Part 35 and, in criminal work, CrimPR Part 19 and the disclosure regime.
- **Expert evidence that unifies:** the expert report drawing the sources together into one explanation the tribunal can follow, translating technical detail into a clear, impartial account under CPR Part 35 or CrimPR Part 19 (guide 100): the interpreter of the whole.
- **Ready for challenge:** the bundle built to withstand cross-examination on any single source and on the assembly itself, because the opponent will probe the weakest strand and the joins, and a well-built bundle has neither (§6): the resilient case.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 8 · THE WIDER MAP

Source architecture: the whole estate at a glance

Per this series' source-architecture discipline, of which this guide is the summation: no single source is the case, and the estate is the case. Every earlier guide identified where its evidence also lived, on the device, in the cloud, in backups, on counterpart devices, in logs, in deleted space. The multi-source bundle is the point at which those individual maps are combined into one estate-wide picture, so that the weakness or absence of any single source is covered by the others. The discipline is to map, for the central facts in issue, every source that bears on each, and to assemble them so that presence corroborates and absence is explained. When a device is wiped, the cloud and counterpart hold the record; when a clock is wrong, another source's clock corrects it; when one strand of attribution is weak, another strengthens it; and when a source is missing, the estate map shows what should have been there and, often, why it is not. The table below is the estate at a glance: the central fact types against the families of source that can prove them.

CENTRAL FACT	DEVICES	CLOUD	NETWORK / LOCATION	MEDIA	FINANCIAL / CHAIN	OPEN SOURCES
Who (attribution)	Y: accounts, keys	Y: account identity	Device presence	Faces / voices	KYC, key control	Profile links
What (the act)	Y: files, messages	Y: records	Connections	Y: depiction	Transactions	Public statements
When (timing)	Y: timestamps	Y: server times	Y: log times	Capture times	Y: ledger times	Post dates
Where (place)	Device location	Sync location	Y: GPS/cell/WiFi	EXIF / CCTV	n/a	Check-ins
Value / flow	Wallet, records	Account data	n/a	n/a	Y: on-chain	Company records

Fallback strategy in one line: prove each central fact from more than one family of source, so that no wiped device, wrong clock or weak strand can defeat the case, and the estate as a whole answers what no single source can.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE SIX-SOURCE ALIBI THAT HELD

A defendant's alibi, that he was at home during a narrow window, could have rested on his phone alone, a §5 single-point-of-failure risk, since a phone can be left behind. Instead the §3 sources were assembled: the phone's location, the home router's connection log, his car's telematics showing it parked at home, his wearable's continuous sleep record, a geotagged photograph, and a neighbour's public post placing an event at the house. On the §4 master timeline, with each clock normalised, all six converged on the same conclusion for the same window. When the prosecution suggested the phone had been left at home by someone else, the §5 convergence answered it: the car, the wearable and the photograph could not all have been left behind too. The §6 integrity of every strand was documented, so none could be picked off. The lesson is §5's: an alibi on one source is fragile, but six independent sources converging on one timeline, each with its integrity assured, is a case that cross-examination cannot dislodge.

EXAMPLE 2 · THE CONTRADICTION THAT WAS REALLY A CLOCK

An assembled bundle appeared to contain a fatal contradiction: the CCTV showed the defendant arriving after the incident, while a witness account and a door-access log placed him there before. Rather than suppress the conflict or abandon a source, the §5 discipline of examining contradiction was applied. The §4 clock analysis found the answer: the DVR clock was eleven minutes fast (guide 121 §6) and the access-control server was running in UTC while the witness spoke in local summer time. Once every clock was normalised to a common base, the apparent contradiction dissolved and all three sources agreed. Had the contradiction been hidden, the opponent would have exposed it; had a source been dropped to avoid it, the case would have been weaker and less honest. The lesson is §4 and §5's: most contradictions between well-collected sources are clock artefacts, and normalising the timeline resolves them, which is why the master timeline is the spine of the bundle and why contradictions are examined, never buried.

EXAMPLE 3 · THE STRONG CASE UNDONE BY ONE WEAK EXHIBIT

An opponent presented an otherwise powerful multi-source bundle, device data, cloud records, financial trails, that pointed clearly to their conclusion. It failed on the §6 weakest-link principle. One central exhibit, a key screenshot of a message relied on for attribution, had been captured casually, with no native original, no hash, no provenance and no capture method (guides 125, 129), and its authenticity could not be established. Because that unsound exhibit carried a load-bearing part of the attribution, its collapse under challenge undermined confidence in the assembly as a whole, and the §5 case, lacking a second strand for that attribution, had no fallback. A bundle that was strong in most of its sources fell on its weakest. The lesson is §6's: the bundle is only as defensible as its least sound source, integrity must be end-to-end, and a single load-bearing exhibit that is not properly collected can bring down an otherwise compelling case, which is why every strand is held to the same standard and why load-bearing facts are corroborated.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **No master timeline:** the sources presented as separate exhibits with no common timeline, so convergence and contradiction are invisible (§4).
- **Unnormalised clocks:** timestamps compared across sources without reconciling time zones and drift, creating false contradictions (Example 2, §4).
- **Single point of failure:** a load-bearing fact rested on one source where corroboration was available (Examples 1 and 3, §5).
- **Hiding contradictions:** a conflicting source suppressed rather than examined, leaving the bundle exposed (§5).
- **Uneven integrity:** most sources sound but one casual exhibit undermining the whole (Example 3, §6).
- **Overclaiming confidence:** the bundle asserting more certainty than its weakest necessary link supports (§5).
- **A pile, not a case:** exhibits dumped without a narrative the court can follow (§7).
- **Data protection ignored across the whole:** minimisation applied source by source but not to the assembled bundle (§6).

Technical limitations

- **Sources are individually imperfect:** each has its own gaps and accuracy, which is why the bundle depends on convergence, not any single source (§2, §5).
- **Clocks never quite agree:** reconciliation reduces but rarely perfects alignment, so residual uncertainty is stated (§4).
- **Some facts have only one source:** where corroboration is genuinely unavailable, the single-source limit is acknowledged, not disguised (§5).
- **Integrity gaps cannot be repaired retrospectively:** a source collected badly usually cannot be rehabilitated later (§6).
- **Complexity has cost:** assembling many sources is resource-intensive, so scope is proportionate to the matter (guide 20).

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What are the central facts in issue (who, what, when, where, value), so we can identify every source that bears on each?
- Which sources do we already have, and is each one's integrity and provenance sound, or does any load-bearing exhibit rest on a casual capture?
- Where are the corroborating sources for each key fact, so no conclusion rests on a single strand?

Ask your opponent

- For any multi-source case advanced, please provide the master timeline, the clock offsets applied to each source, and the provenance and integrity record of every exhibit.
- Please identify, for each central fact, the sources relied on, and disclose any source that qualifies or contradicts the conclusion.
- Please confirm the collection method and hash of each source and the attribution basis for each strand.

Ask your eDiscovery / forensic provider

- Does every central fact rest on more than one source, and where is any single point of failure?
- Are all clocks normalised, and are any apparent contradictions clock artefacts or real?
- Is integrity and provenance sound across every source, and what is the honest confidence of the whole?

SUGGESTED WORDING · INSTRUCTION FOR A MULTI-SOURCE ASSEMBLY

> "We instruct you to assemble the digital evidence in this matter into a single, defensible, multi-source bundle. Please: (1) identify, for each central fact in issue (attribution, act, timing, place, value), every source across the estate (devices, cloud, network and location, media, financial and on-chain, and open sources) that bears on it, and ensure each load-bearing fact is supported by more than one source where available; (2) build a master timeline placing every relevant event from every source on a common clock, establishing and applying each source's offset and reconciling time zones and drift, and labelling each event with its source and reliability; (3) identify where sources converge and where they contradict, examining and explaining every apparent contradiction rather than suppressing it, and weight each strand by its reliability; (4) maintain and document integrity, hashing, chain of custody, provenance and method, across every source to a consistent standard, and apply data minimisation across the whole; and (5) present the result as a coherent, honestly-bounded account at the confidence its weakest necessary link supports, prepared to withstand challenge on any single source and on the assembly itself."

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 12 · QUICK CONTROL

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

The multi-source bundle checklist

- ☐ Central facts identified; sources mapped to each
- ☐ Every load-bearing fact corroborated by more than one source
- ☐ Master timeline built with all events on a common clock
- ☐ Each source's clock offset established and applied
- ☐ Events labelled with source and reliability
- ☐ Convergence identified; contradictions examined and explained
- ☐ Each strand weighted by its reliability
- ☐ Integrity, hashing and provenance sound across every source
- ☐ Data minimisation applied across the whole bundle
- ☐ Presented as a coherent case at honest confidence

Red flags

- Exhibits with no master timeline or common clock: §4.
- An apparent contradiction left unexamined: Example 2.
- A load-bearing fact on a single, un-corroborated source: Examples 1 and 3.
- One casually captured exhibit among otherwise sound sources: Example 3.
- Confidence asserted beyond the weakest necessary link.
- A pile of exhibits with no narrative.
- Contradictions suppressed rather than explained.

When to involve a digital forensic expert

Whenever a case rests on more than one kind of digital evidence, which is to say almost always, because the assembly is a discipline in itself, distinct from examining any single source: the expert maps every source to each central fact and ensures load-bearing facts are corroborated (Example 1, §5); builds the master timeline that normalises every clock and turns apparent contradictions back into agreement (Example 2, §4); maintains integrity and provenance end-to-end so no weak exhibit can taint the whole (Example 3, §6); and presents the result as a coherent, honestly-bounded case under CPR Part 35 or CrimPR Part 19, built to withstand challenge on any strand and on the joins. This capstone draws together the whole series: the individual guides examine the sources, and this one assembles them. Through **cflab.uk** and **e-discovery.uk**, multi-source work turns many imperfect witnesses into one honest, coherent, defensible case, because in modern litigation the evidence is rarely in a single artefact, it is in the way the whole estate fits together.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 13 · COMMON QUESTIONS

Frequently asked questions

Why not just rely on the strongest single source?

Because a single source, however strong, is a single point of failure (§5, Examples 1 and 3). A phone can be left behind, a screenshot can be challenged, one clock can be wrong. Corroborating a central fact across several independent sources makes the case far more resilient: if one strand is undermined, the others hold. The strength of a modern case is in convergence, so the assembly rests load-bearing facts on more than one source wherever it can.

Our sources seem to contradict each other. Is the case lost?

Usually not, examine the contradiction rather than fear it (§5, Example 2). Most apparent contradictions between well-collected sources are clock artefacts: different time zones, daylight saving, a DVR running fast, a server in UTC. Normalising every source to a common clock on the master timeline resolves the great majority of them (§4). Where a contradiction is real, it is examined and explained honestly, which is far safer than hiding it and having the opponent expose it.

Why does the timeline matter so much?

It is the spine of the whole bundle (§4). Placing every event from every source on one timeline, with all clocks normalised, is what makes convergence visible and contradiction resolvable. Without it, the sources are just separate exhibits and the court cannot see how they fit; with it, the case reads as one coherent sequence. Most of the work, and most of the errors, in a multi-source case are in building the timeline correctly.

Can one weak exhibit really undermine a strong bundle?

Yes, if it is load-bearing (§6, Example 3). A bundle is only as defensible as its least sound source, and if a casually captured, un-provenanced exhibit carries a central part of the case, its collapse under challenge can undermine confidence in the whole and leave that fact unsupported. That is why integrity, hashing, provenance and method, is maintained to the same standard across every source, and why load-bearing facts are corroborated so no single exhibit is indispensable.

How is confidence stated for a whole bundle?

At the level its weakest necessary link supports, and stated plainly (§5, guide 100). A conclusion that depends on a chain of sources is only as strong as the weakest link in that chain, so the bundle does not claim more certainty than that. Where convergence is strong, confidence is high; where a fact rests on a single or weaker source, that is acknowledged. Honest, calibrated confidence is what lets the whole survive cross-examination.

Isn't assembling all this disproportionate for a smaller case?

It can be, so scope is matched to the matter (§10, guide 20). Not every case needs six sources for every fact; the principle is that load-bearing facts should be corroborated and the whole should be coherent and sound, at a scale proportionate to what is at stake. For a smaller matter that may mean two well-chosen sources on a clean timeline; for a substantial one it may mean the full estate. The discipline scales; the standards do not drop.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 14 · REFERENCE

Glossary

Multi-source bundle
Evidence from several source families assembled into one case.

Master timeline
A single sequence of all events from all sources on a common clock.

Normalisation
Converting all timestamps to a common time base.

Clock offset
A source's difference from true time, measured and applied.

Convergence
Independent sources agreeing on a fact.

Single point of failure
A fact resting on one source with no fallback.

Weakest link
The least sound source, which governs the bundle's strength.

Provenance
The documented origin and method of each source.

Weight
The reliability accorded to a strand of evidence.

Honest confidence
The stated certainty the weakest necessary link supports.

Sources and authoritative references

The multi-source assembly 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 case assembly, timeline and convergence analysis, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, the EDRM lifecycle end to end (identification through production, as the frame for multi-source assembly): e-discovery.uk/edrm · analysis and production: 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 v2 (integrity, method and interpretation across evidence types): gov.uk, FSR Code · ISO/IEC 27037 (identification, collection, acquisition and preservation): iso.org, 27037
- CPR Part 35 and PD 35 (expert evidence and the overriding duty to the court): justice.gov.uk, Part 35 · Attorney General's Guidelines on Disclosure 2024: gov.uk, AG Guidelines
- PD 57AD and CPR Part 31: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31

DISCLAIMER

This publication provides general information about assembling multi-source digital evidence as at August 2026. Every case differs, and the reliability of a bundle depends on the integrity, provenance and honest interpretation of each source and on the soundness of the assembly; conclusions should be stated at the confidence the weakest necessary link supports. 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

This capstone is where the laboratory's work across the series comes together. Individual instructions examine the sources, a phone, a cloud account, a video, a location record, a wallet, a public post, and the multi-source assembly turns them into one case. The central facts in issue are mapped to every source that bears on each, and load-bearing facts are corroborated so nothing rests on a single point of failure (Example 1). A master timeline is built with every event normalised to a common clock, each source's offset established and applied, so convergence becomes visible and apparent contradictions, usually clock artefacts, are resolved rather than hidden (Example 2). Integrity and provenance are maintained end-to-end, to a consistent standard, because the bundle is only as defensible as its weakest source and one casual exhibit can undo an otherwise strong case (Example 3). The whole is weighted by reliability, bounded at honest confidence, minimised for data protection across the bundle, and presented as a coherent account a court can follow, prepared to withstand challenge on any strand and on the joins, under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding principle is the one running through the whole series: the evidence is rarely in a single artefact, it is in the way the whole estate fits together, honestly assembled.

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