



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

Coordinating Forensic Collection Across Multiple Offices and Countries

One Methodology, Many Sites: Consistency, Local Law and the Campaign Plan

A dispute that spans a group spans its geography: offices in three cities, subsidiaries in four countries, custodians in every time zone the business trades in. Collecting from that estate is a campaign, not a visit: one methodology executed consistently everywhere, local teams and local law accommodated without fragmenting the standard, evidence moving across borders on a lawful basis, and a single command structure that can answer, months later, for every site as if it had been one. This guide sets out how to plan and run multi-site and multi-country collections: the hub-and-spokes model, methodology packs, local counsel and local personnel, transfer and blocking-statute analysis, synchronisation against tip-off risk, and the consolidated record that holds it all together.

© Estimated reading time: 28 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. Its examiners plan and run multi-site collection campaigns across the UK and internationally, combining laboratory teams, remote acquisition and vetted local personnel under a single methodology and a single evidential record. Its eDiscovery arm, **e-discovery.uk**, consolidates the outputs of distributed collections into one processing and review pipeline.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

ISO 27001-ALIGNED SECURITY

ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES

MULTI-SITE CAMPAIGN COORDINATION

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: many sites, one standard
- 03 The campaign model: hub, spokes and the methodology pack
- 04 Who collects where: laboratory teams, remote agents, local personnel
- 05 The legal terrain: transfers, blocking statutes and local process
- 06 Synchronisation, sequencing and tip-off risk
- 07 Moving and consolidating the evidence
- 08 The consolidated record: one campaign, one file
- 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: CONSISTENCY IS THE CAMPAIGN'S PRODUCT

A multi-site collection is judged, later, as a single exercise: one methodology, one hash standard, one custody discipline, one record: however many teams, countries and weeks it actually took. The design that achieves this is hub and spokes. The **hub** is a single coordinating examiner-in-charge and lawyer pairing who own the master protocol, the campaign schedule, the deviation log and the consolidated evidence record. The **spokes** are the site executions: laboratory teams travelling, remote agents deployed (guide 38), or vetted local personnel working to the hub's written methodology pack: the per-site distillation of the protocol: methods, tools and settings, forms, hash and custody standards, contingencies and the hub's decision line. Around this structure sit the two cross-border overlays: **data movement law** (UK GDPR transfer rules for personal data flowing to the UK, plus the exporting jurisdictions' own regimes) and **local process law** (blocking statutes, employment codetermination and works councils, state and professional secrecy, and local employment and privacy rules that shape what may be collected, by whom, with what notice). Neither overlay is usually fatal; both must be answered per jurisdiction before collection, in writing, by counsel qualified there. The campaign that runs this way produces evidence a court can treat as one body; the campaign that fragments (different tools here, different forms there, a spoke that improvised) produces a comparison exercise for the other side's expert.

- **The methodology pack travels; the standard does not flex:** local teams may vary logistics, never method: same imaging and hashing standards, same forms, same custody rules, in every jurisdiction, with translations where needed.
- **Sequence against tip-off:** where custodians talk to each other, sites are collected simultaneously or in tight sequence, communications are controlled, and preservation (holds, agent deployment) lands everywhere before collection lands anywhere.
- **Local counsel are infrastructure:** one short advice per jurisdiction (what may be collected, what consents or notices are needed, how data may leave) is the campaign's legal foundation, obtained before, not after, the first spoke executes.
- **Time zones are an asset and a hazard:** a following-the-sun schedule collects continuously, but the hub's decision line must actually be staffed for every spoke's working day, and every log records its timestamps in a declared convention (UTC plus local) so the consolidated chronology assembles cleanly.
- **Consolidation is a workstream, not an afterthought:** evidence, hashes, logs and custody records from every spoke flow to the hub on a defined cadence and format, reconciled weekly, so the campaign's single file exists throughout rather than being archaeologically assembled at the end.

The problem in plain English: many sites, one standard

Every multi-site campaign faces the same temptation: let each site solve itself. The Manchester office has an IT manager who can export mailboxes; the Frankfurt subsidiary has a local vendor it has used before; Singapore is eight hours ahead and surely fine to run its own show. Six months later the disclosure statement describes "forensic collection across the group", and the reality underneath is four methodologies, three hash standards, two custody regimes and one spoke with no records at all. The other side's expert does not need to find wrongdoing; the inconsistency is the finding: if the group could not run one standard, which spoke's evidence carries the exercise's claimed rigour?

The alternative costs coordination rather than money: a hub that writes the standard once and enforces it everywhere; spokes that execute rather than design; and the cross-border homework (transfers, local process) done jurisdiction by jurisdiction before the first device is touched. The guides before this one supply every component: the protocol (36), the site plan (39), remote methods (38), custody (35), hashing (34). This guide is about the layer above them: making twelve executions of those disciplines read, later, as one.

The campaign model: hub, spokes and the methodology pack

- **The hub:** an examiner-in-charge (methodology, quality, consolidation) paired with a coordinating lawyer (scope, privilege, local-law liaison, client communications), holding the master protocol, the campaign schedule, the credential and access matrix per site, the deviation log, and the decision line staffed across the campaign's time zones.
- **The spokes:** one execution unit per site: a travelling laboratory team, a remote deployment, or local personnel: each with a named lead, a site plan per guide 39, and no design authority: questions go up the line, decisions come down it, and both directions are logged.
- **The methodology pack:** the hub's per-site kit: the master protocol's method matrix filtered to that site's sources; tool and settings specifications; the forms (exhibit, transfer, running log, deviation) in the campaign's single format, translated where working languages require; hashing and custody standards; contingency and escalation rules with the hub's contacts; and the reporting cadence and format for sending results home. The pack is what makes a spoke in Singapore produce paperwork interchangeable with a spoke in Leeds.
- **Versioning discipline at scale:** the master protocol amends through one owner (the hub), and amendments propagate to every pack with version numbers; a campaign where sites run different protocol versions has recreated the fragmentation problem with extra steps.
- **The campaign schedule:** sites, dates, teams, dependencies (preservation before collection everywhere; simultaneous first-wave sites; courier and consolidation legs), maintained as the single live document the hub briefs from.

Who collects where: laboratory teams, remote agents, local personnel

- **Travelling laboratory teams** for the sites that matter most: contested devices, complex estates, ordered executions, and anywhere the campaign's credibility concentrates; the cost of flights is small against the cost of the central site being the weak spoke.
- **Remote acquisition (guide 38)** for corporate endpoints under management, cloud tenancies and server estates: often the majority of a modern campaign's volume, collected from the hub with endpoint verification, hash-at-source and session logs, and no travel at all.
- **Local personnel**, where distance, visas, timing or local-law requirements make them the right hands: chosen by vetting (qualifications, tooling, references, conflicts), contracted to the campaign's confidentiality and standards, trained on the methodology pack, and supervised: first exhibits reviewed by the hub before the spoke continues, sampling verification thereafter, per guide 36's hybrid disciplines. Local hands, hub methodology: the formula that scales without fragmenting.
- **Client IT in support roles only**, per the series' standing rule: access, credentials, logistics; evidential acts only under the hybrid conditions, and never at contested spokes.
- **The mixed campaign is normal**: a typical matter runs all four: the laboratory at the headquarters spoke, agents across the endpoint estate, a vetted local examiner in the jurisdiction with a notice period problem, and IT opening doors everywhere. The record shows who did what at every spoke, and the pack made them do it identically.

The legal terrain: transfers, blocking statutes and local process

- **Data leaving each country:** personal data flowing to the UK hub engages the exporting jurisdiction's transfer regime (EU/EEA GDPR routes to the UK under adequacy while it stands; other jurisdictions' own mechanisms elsewhere) and, for onward flows, UK GDPR's rules; the campaign records the basis per route: adequacy, standard contractual clauses, or the legal-claims derogation where genuinely applicable, assessed by counsel rather than assumed.
- **Blocking and secrecy regimes:** some jurisdictions restrict transferring evidence abroad for foreign proceedings (blocking statutes), impose state or banking secrecy, or protect specific data classes; the answer may reshape the plan: collect and process in-country, produce only reviewed relevant material, or route requests through formal legal-assistance channels. Discovering these regimes after collection is how campaigns create satellite litigation.
- **Local employment and privacy process:** works councils and codetermination (notably in parts of Europe) can require consultation before employee-data collection; local rules shape notice to custodians, the scope of permissible monitoring, and what personal material may be reviewed and by whom. The one-page local-counsel advice per jurisdiction answers: what may be collected, from whom, with what notice or consent, under what conditions, and how it may leave.
- **Privilege travels badly:** what is privileged, and whose privilege it is, varies by jurisdiction (in-house counsel's status being the classic divergence); the campaign's quarantine machinery (guide 36) is applied everywhere, with local review where local privilege law demands it.
- **Sequencing the law before the logistics:** the jurisdictions' answers determine the campaign design (where processing happens, what crosses borders, who may collect), so the legal workstream completes, per jurisdiction, before that spoke's date is fixed: law first, flights second.

Synchronisation, sequencing and tip-off risk

- **Preservation lands everywhere first:** holds issued, deletion mechanisms suspended, agents deployed, leaver-device freezes in place across every site before any spoke collects; the campaign's first wave is invisible.
- **Collect sensitive spokes simultaneously:** where custodians communicate (and in a group, they do), the contested sites execute in the same window: the same morning across Europe, the same twenty-four hours globally: so no custodian learns from a colleague's Tuesday what to do before their own Thursday.
- **Communications discipline:** who is told what, when, per site, on a briefing plan the coordinating lawyer owns; announcements synchronised with execution; and the campaign's existence itself treated as confidential until the first wave lands.
- **Following the sun, staffed:** a global schedule can run continuously (Asia-Pacific spokes handing to Europe handing to the Americas), but only if the hub's decision line genuinely answers in every spoke's business hours: the escalation call that reaches a voicemail eight time zones asleep is the campaign's improvised decision waiting to happen.
- **One clock for the record:** every log timestamps in UTC alongside local time, stated on every form; the consolidated chronology (and any later dispute about who knew what when across time zones) depends on nobody having to guess which noon a log meant.

Moving and consolidating the evidence

- **Encrypted at rest, always:** evidence media leaving any spoke is encrypted and sealed, keys travelling separately through the hub; a couriered drive is a custody object (guide 35's transfer rows, tracking, both-end receipts) and a security object at once.
- **Wire versus courier per spoke:** the guide 38 arithmetic, run per site: verified network transfer for what bandwidth allows, couriered encrypted media for bulk, and the hybrid as standard; customs and import realities (media declarations, the jurisdictions where couriered data attracts inspection) checked with the freight and legal workstreams together.
- **In-country processing where law requires:** for blocking-statute and secrecy jurisdictions, the pattern inverts: evidence stays, processing and first review happen locally (local platform or provider under the hub's specification), and only relevant, reviewed, lawfully transferable material crosses: recorded as such.
- **Receipt and verification at the hub:** every arrival is hash-verified against its spoke's schedule, logged into the central evidence store, and reconciled to the campaign manifest; discrepancies chase the same day, while the spoke team still remembers.
- **One processing pipeline:** consolidated evidence flows into a single processing environment (through **e-discovery.uk** in our practice) with uniform settings, so deduplication, threading and review operate across the whole campaign rather than per-site: the point at which twelve collections finally become one dataset.

The consolidated record: one campaign, one file

- **The campaign manifest:** the master index: every spoke, every source, every exhibit reference, hash values, collection dates, method, personnel, and current location: maintained live by the hub, reconciled weekly against spoke reports, and the single answer to "what was collected across the group?".
- **Uniform paperwork, filed once:** the packs' identical forms mean spoke records file into one structure without translation of format; the deviation log is campaign-wide, so patterns (the same contingency firing at three sites) surface and get fixed mid-campaign.
- **The campaign report:** guide 36's collection report at campaign scale: methodology, per-spoke execution summaries, deviations and resolutions, the legal bases per jurisdiction, transfer routes, and the manifest as its schedule: the document the DRD summarises, the opponent receives on request, and the CPR Part 35 report annexes.
- **Ready for the single question:** the whole apparatus exists so that, at trial, "was the Milan collection done to the same standard as London?" is answered by producing the pack, the logs and the manifest rows: paper, not recollection, in every jurisdiction the campaign touched.

Worked examples

EXAMPLE 1 · THE SYNCHRONISED FIRST WAVE

A group-wide fraud investigation spanned London, Dublin, Rotterdam and Dubai, with three suspected custodians who spoke daily. The campaign preserved silently in week one (holds, agent deployment through endpoint management, leaver freezes), completed local-counsel advices in week two, and executed the first wave at 08:00 local time in all four cities on the same Tuesday: laboratory teams at London and Dubai (the contested spokes), agents harvesting Rotterdam and Dublin endpoints, mailboxes exporting server-side throughout. No custodian had a warning Tuesday; the artefacts later showed one had begun deleting at 08:40, twenty minutes after his machine was already imaged. The campaign report's synchronisation section was quoted in the freezing-order evidence: coordination, functioning as proof of seriousness.

EXAMPLE 2 · THE SPOKE THAT RAN ITS OWN SHOW

A multinational's US parent allowed its German subsidiary to "handle its own collection" through a local IT vendor while the UK campaign ran to protocol. The vendor exported mailboxes with consumer tools, kept no hash schedule, consulted no works council, and copied everything (personal data included) to a US review platform without a transfer assessment. The consequences arrived in sequence: a works-council grievance, a regulator enquiry about the transfer, and, in the English proceedings, an expert report contrasting the German spoke's records with the campaign's own standards: the sharpest exhibit being the group's master protocol, which the subsidiary had simply not been given. The re-collection, done properly with local counsel and a methodology pack, cost more than the entire original campaign's coordination budget.

EXAMPLE 3 · THE BLOCKING-STATUTE PIVOT

A campaign's plan assumed all evidence would consolidate in London. Local counsel in one jurisdiction advised that exporting the subsidiary's data for foreign litigation would breach a blocking regime, with personal criminal exposure for directors. The hub pivoted the spoke rather than the standard: collection proceeded to the methodology pack in-country, processing and first-pass review ran on a local platform to the hub's specification, and only documents reviewed as relevant and lawfully transferable crossed, under a recorded basis, with the balance preserved in-country against future orders. The English court was told exactly this in the DRD; the opponent's complaint about "incomplete consolidation" did not survive the paragraph explaining why, and the campaign's compliance became a point in its favour rather than a hole in its disclosure.

Common mistakes and technical limitations

Common mistakes

- **Federated improvisation:** each site solving itself: Example 2, the campaign killer.
- **Law after logistics:** flights booked, then local counsel asked; the transfer analysis as an afterthought to a collection already sitting in the wrong country.
- **Sequential collection of talking custodians:** the Tuesday spoke educating the Thursday spoke.
- **Unvetted local hands:** "a vendor the office has used" executing evidential acts with no pack, no training and no sampling.
- **The unstaffed decision line:** escalations from Asia landing on a sleeping London phone, answered by the field team's own judgment.
- **Mixed clocks:** logs in unstated local times, and a consolidated chronology that needs a spreadsheet and an apology.
- **Consolidation at the end:** spoke records hoarded locally for months, reconciled archaeologically, gaps discovered when the teams have dispersed.
- **Protocol drift across versions:** sites executing different revisions of the master document, honestly and inconsistently.

Technical limitations

- **Coordination has a floor cost:** the hub, the packs, the legal advices and the synchronised scheduling are real spend; below a certain scale (two friendly UK offices), the full apparatus is disproportionate and a single guide 39 plan with two site annexes does the work.
- **Local law can force real asymmetry:** the in-country processing pivot means some spokes genuinely are handled differently; the answer is that the difference is designed, documented and legally grounded, not that it does not exist.
- **Tool ecosystems vary by region:** local personnel may hold different (legitimate) toolsets; the pack specifies outcomes and standards (formats, hashes, logs) tightly enough that tool variance does not become method variance.
- **Simultaneity is bounded by daylight and hands:** a genuinely global same-hour wave needs teams already in place per region; the schedule is built from available hands backwards, not from the ideal clock forwards.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Map the estate by legal entity and country: which subsidiaries, which sites, which systems are shared versus local, and who controls each? (Group structure is the campaign's terrain.)
- Which custodians communicate across sites, and where does tip-off risk concentrate?
- Which jurisdictions do we need local counsel in, and does the group already have relationships there?

Ask your opponent

- Please confirm the methodology under which each group entity's material was collected, and provide the protocol or pack governing sites outside the UK.
- For each jurisdiction, please identify the legal basis on which data was transferred to the review platform, and any material collected but withheld from transfer on local-law grounds.
- Please provide the consolidated schedule of collections: sites, dates, methods, personnel and hash verification.

Ask your eDiscovery / forensic provider

- Show us the campaign structure: who is the examiner-in-charge, what does the methodology pack contain, and how are local personnel vetted, trained and sampled?
- How is the decision line staffed across our time zones, and what is the reporting cadence from spokes to hub?
- Where will processing happen per jurisdiction, and how do the in-country pivots work if local counsel require them?

SUGGESTED WORDING · CAMPAIGN CLAUSES FOR THE MASTER PROTOCOL

"11. Campaign structure. The collection shall be coordinated by [examiner-in-charge] and [coordinating lawyer] (the Hub), who shall maintain the campaign schedule, the consolidated manifest and the campaign-wide deviation log. Each site shall be executed by the team identified in Schedule E under a Methodology Pack issued by the Hub, which shall apply the methods, forms, hashing and custody standards of this protocol without variation; site teams shall have no authority to vary method, and shall refer all questions to the Hub's decision line, which shall be staffed during each site's business hours. 12. Cross-border. No collection shall commence at any site outside the United Kingdom until the Hub has received and recorded local counsel's confirmation for that jurisdiction addressing (a) the lawful scope and manner of collection, (b) any consultation, notice or consent requirements, and (c) the basis on which collected material may be transferred, together with any requirement for in-country processing. All records shall state times in UTC and local time. 13. Consolidation. Each site team shall deliver its evidence, hash schedules, logs and custody records to the Hub in the Pack's format within [n] days of site completion; the Hub shall verify all received material by hash and reconcile the manifest weekly."

SUGGESTED WORDING · LOCAL PERSONNEL ENGAGEMENT (CORE TERMS)

"You are engaged to execute the collection at [site] strictly in accordance with the attached Methodology Pack (v[n]), which governs methods, tools and settings, forms, hashing, custody and reporting. You shall not vary the Pack; questions and unexpected circumstances shall be referred to the Hub decision line at [contact] before further action. Your first completed exhibit set shall be submitted for Hub review before continuing, and your work is subject to sampling verification. You shall keep all matter information confidential, hold collected material encrypted at all times, transfer nothing except by the routes specified in the Pack, and deliver all records in the Pack's format within [n] days of completion."

§ 1 2 · QUICK CONTROL

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

The multi-site campaign checklist

- ☐ Hub named: examiner-in-charge and coordinating lawyer, with a decision line staffed across campaign time zones
- ☐ Estate mapped by entity, country and system; tip-off risk assessed; campaign schedule built with dependencies
- ☐ Master protocol per guide 36; methodology packs issued per site, translated where needed, version-controlled from the hub
- ☐ Local counsel advice per jurisdiction (collection scope, notice/consent, transfer basis, in-country requirements) before that spoke's date is fixed
- ☐ Hands assigned per spoke: laboratory, remote, or vetted-trained-sampled local personnel; client IT in support only
- ☐ Preservation everywhere before collection anywhere; sensitive spokes synchronised; communications plan owned by the lawyer
- ☐ All records in UTC plus local; forms identical across sites
- ☐ Evidence movement designed: encryption, sealed couriered media, verified wire transfers, in-country processing pivots where required
- ☐ Weekly manifest reconciliation; spoke deliverables on a defined cadence and format
- ☐ Campaign report assembled from the live file, DRD-ready, with legal bases and transfer routes recorded

Red flags

- A subsidiary "handling its own collection".
- No local counsel in a jurisdiction with a works council, a secrecy regime or a blocking statute.
- Contested custodians collected days apart while talking daily.
- Local vendors executing without a pack, training or sampling.
- Logs in four unstated time conventions.
- Evidence media crossing borders unencrypted, or data crossing before the transfer basis exists.
- A "consolidated" record that will be assembled after the teams disband.

When to involve a digital forensic expert

At campaign design, before anything is scheduled: the hub structure, the pack, the hands-per-spoke decisions and the synchronisation plan are the examiner-in-charge's product, built with the coordinating lawyer while local counsel advices come in. Throughout execution, as the hub itself: methodology authority, spoke supervision, sampling, consolidation and the manifest. And at the end, for the campaign report and any CPR Part 35 evidence: including, against an opponent, the review that asks of their group disclosure exactly the questions in §11 and

reports which spokes cannot answer them: because in multi-site litigation, the inconsistent campaign is the one that loses the methodology argument, and the consistent one is the one that never has it.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Do we really need local counsel in every country, or is that gold-plating?

Need one short advice per jurisdiction whose data or personnel the campaign touches: yes, as a rule: the cost is small and the failure modes (works-council grievances, transfer breaches, blocking-statute exposure with personal liability) are not. The proportionate version scales with risk: adequacy-covered European jurisdictions with cooperative subsidiaries may need a page; secrecy-regime jurisdictions need real analysis. What is never proportionate is discovering the requirement from the regulator's letter, per Example 2.

Can one UK laboratory really run a global campaign, or do we need providers in each country?

The hub-and-spokes answer: one laboratory runs the campaign (methodology, coordination, the contested spokes, remote acquisition of managed estates) and engages vetted local hands where geography or local law requires them, under the pack and sampling. What you should avoid is the opposite architecture: independent providers per country, each with their own methodology, coordinated by nobody: that is Example 2 franchised. One standard, many hands; never many standards.

How do we handle a jurisdiction that will not let the data leave?

Example 3's pivot: collect in-country to the campaign standard, process and first-review locally on infrastructure the hub specifies, transfer only reviewed, relevant, lawfully transferable material under a recorded basis, preserve the balance in-country, and say all of this plainly in the DRD. English courts deal with such constraints regularly; what they, and opponents, respond badly to is the constraint asserted vaguely, discovered late, or used as cover: the documented pivot is a compliance credential, the undocumented gap is a disclosure hole.

What does synchronisation actually require: must every site be the same hour?

Only where tip-off risk demands it, and only for the sensitive spokes: the contested custodians' sites in one window (same morning regionally, same day globally), preservation everywhere beforehand, and the announcement synchronised with execution. Friendly spokes (cooperative offices, server estates, cloud tenancies) then proceed on the ordinary schedule. Full-campaign simultaneity is rarely necessary and always expensive; targeted simultaneity, per Example 1, is the discipline that pays.

Who gives the expert evidence about a campaign executed by many hands?

The examiner-in-charge: methodology, supervision, verification and consolidation are theirs to prove, exhibiting the packs, sampling results, logs and manifest; spoke personnel provide statements (or local evidence) about their own executions where specific acts are contested. This is the standard architecture of supervised work, and it is precisely why the hub's records exist: the expert who says "I designed the standard, trained the hands, verified the samples and reconciled the results" is giving evidence, not hearsay, about the campaign as a system.

How much longer does a coordinated campaign take than letting sites run in parallel on their own?

Usually none: the spokes still run in parallel; what the campaign adds is a planning phase up front (the packs, the legal advices, the schedule: typically two to four weeks for a multi-country matter) and a consolidation rhythm alongside execution. Uncoordinated parallelism only looks faster because its costs land later: the re-collections, the satellite disputes and the methodology cross-examination all post-date the "saved" fortnight, at multiples. Example 2's arithmetic is the standing answer.

§ 1 4 · REFERENCE

Glossary

Blocking statute

A local law restricting transfer of evidence abroad for foreign proceedings; a design constraint, not a footnote.

Campaign manifest

The hub's live master index of every spoke, source, exhibit, hash and location.

Campaign report

The consolidated methodology-and-execution record for the whole exercise; the DRD's foundation.

Decision line

The hub contact staffed across all spokes' business hours for escalations and scope calls.

First wave

The synchronised collection window for tip-off-sensitive spokes, after silent preservation everywhere.

Hub and spokes

One coordinating authority (methodology, record) executing through per-site teams with no design discretion.

In-country pivot

Collecting and processing locally, transferring only reviewed lawful material, where local law requires.

Local counsel advice

The per-jurisdiction confirmation of collection scope, notice requirements and transfer basis, obtained before execution.

Methodology pack

The per-site distillation of the master protocol: methods, forms, standards, contingencies, reporting.

Sampling verification

Hub re-checking of local personnel's work: first exhibits reviewed, proportions re-verified.

UTC convention

The campaign's single clock: every record in UTC plus stated local time.

Works council

Employee representation whose consultation rights can precede employee-data collection in some jurisdictions.

Sources and authoritative references

The campaign 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-site campaign coordination, on-site, remote and supervised local collection, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Collection and Phase 04 · Processing (consolidating distributed collections into one verified pipeline; "defensibility is built, not retrofitted"): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/processing
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- ICO, UK GDPR guidance including international data transfers: ico.org.uk
- NPCC / College of Policing digital evidence guidance: college.police.uk, [digital devices guidance](https://college.police.uk/digital-devices-guidance) · Forensic Science Regulator Code: gov.uk/forensic-science-regulator
- ISO/IEC 27037:2012 and ISO/IEC 27001: iso.org, [27037](https://iso.org/27037) · iso.org, [27001](https://iso.org/27001)
- CPR Part 35 and PD 57AD (methodology description and the DRD): justice.gov.uk, [Part 35](https://justice.gov.uk/part-35) · justice.gov.uk, [PD 57AD](https://justice.gov.uk/pd-57ad)

DISCLAIMER

This publication provides general information about coordinating multi-site and cross-border forensic collection as at August 2026. The worked examples are fictional and the clause wording illustrative. Cross-border collection engages the law of each jurisdiction involved, on which advice from counsel qualified there is essential; nothing here describes the law of any non-UK jurisdiction. 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. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Campaign coordination is a defined laboratory service: we act as the hub. The examiner-in-charge designs the master protocol and methodology packs with your team, plans hands per spoke (our travelling teams, our remote practice, vetted local personnel under training and sampling), sequences preservation and the synchronised first wave against tip-off risk, and staffs the decision line across your time zones. We work alongside your local counsel network (or help identify one), build the transfer and in-country processing routes their advices require, run consolidation weekly, and deliver the campaign report and manifest DRD-ready, supported under CPR Part 35 where the matter warrants. Through **e-discovery.uk**, the consolidated evidence flows into a single processing and review pipeline, so twelve collections litigate as one dataset. Conflicts checks, confidential scoping discussions and fixed-fee campaign estimates are routine.



I N S T R U C T T H E L A B

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