COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

The First eDisclosure Meeting

50 Questions Lawyers Should Ask

The first meeting with the client about electronic evidence sets the trajectory of the whole exercise: what is preserved, what quietly dies, and what the disclosure certificate will one day have to say. This guide provides a structured 50-question interview covering IT architecture, custodians, devices, cloud services, deleted data, retention, preservation, privacy, privilege and third parties, with what to listen for in every answer and what to do the moment the meeting ends.

⏱ Estimated reading time: 27 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 eDiscovery arm, **e-discovery.uk**, opens every matter the way this guide does: with structured questioning of the client's people and systems, logged as the first entries in the chain of custody, before anything is collected. The 50 questions here are the distillation of that opening discipline, and they are asked, in some form, at the start of every matter the practice takes.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ISO 27001-ALIGNED SECURITY | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | PD 57AD / DRD EXPERIENCE | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: WHY FIFTY STRUCTURED QUESTIONS

The first eDisclosure meeting is the cheapest hour in the whole exercise and the one with the longest consequences: what is asked (and not asked) in it determines what is preserved before the timers run, which sources reach the data map, and whether the disclosure certificate is eventually signed over records or over hope. A structured 50-question interview guarantees coverage of the ten areas that decide those outcomes (architecture, custodians, devices, cloud, deleted data, retention, preservation, privacy, privilege and third parties), produces a signed record that becomes identification evidence, and surfaces the red-flag answers that need forensic escalation while escalation is still cheap.

- **The instrument is the point.** §§4 to 13 provide the fifty questions verbatim, five per area, each with a "listen for" note explaining what the answer changes. Ask them in order, record answers against the numbers, and the meeting note becomes a filing, not a memory.
- **Some answers trigger same-day action.** Retention timers, leaver pipelines, disappearing messages and scheduled migrations do not wait for the follow-up letter; §14 maps each answer type to its action and §15 lists the answers that stop the meeting's ordinary flow entirely.
- **This meeting is strategic, not exhaustive.** It scopes the estate through the people in the room; the written questionnaires and individual custodian interviews (companion guides *Finding the Evidence* and *Identifying the Right Custodians*) follow it and go deeper. The fifty questions are what the lawyer must know by the end of day one.
- **The record does double duty.** Confirmed meeting notes evidence the identification process behind the DRD and certificate, and they anchor the PD 57AD requirement to obtain written confirmation that preservation steps have been taken.

§ 0 2 · FIRST PRINCIPLES

Why the first meeting matters, practically and legally

Practically, the first meeting is where the exercise's information asymmetry is at its worst and its options are at their widest. The client knows things the lawyer needs within hours (what deletes this week, who is leaving, where the WhatsApp deals live) and the lawyer knows things the client needs immediately (that the duties are already live, that IT's helpfulness is dangerous, that the storeroom laptop matters). Fifty structured questions move both directions of that knowledge in one sitting.

Legally, the meeting discharges and evidences live obligations:

- **Preservation duties are already running.** PD 57AD's duties attach once proceedings are contemplated, and legal representatives must take reasonable steps to ensure the client preserves, including notifying employees, former employees and third parties, and must obtain written confirmation that steps have been taken. The meeting is where those steps are specified and the confirmation is set up.
- **Identification underwrites everything.** The reasonable search (CPR 31.7), the DRD's source descriptions and the eventual certificate all assume the sources were competently found; the meeting record is the first and best evidence that they were.
- **Early candour is protective.** The questions about deletion, prior self-help and departed staff are asked now precisely because problems disclosed to your own lawyer in week one are manageable, while the same facts discovered by an opponent in month nine are conduct.
- **Costs and strategy start here.** Volumes, custodian counts and accessibility answers from this meeting seed the assessment, the budget and the settlement judgment; a meeting that skips them defers every number the case needs.

§ 0 3 · METHOD

How to run the meeting

- **Who attends:** the client's decision-maker (GC or instructing director), the person who actually runs IT (in-house head or the MSP's lead engineer, not the account manager), and one operationally senior person close to the events. Keep it under six people; individual custodian interviews come later and are deliberately separate, because people disclose side channels alone that they will not volunteer in front of the IT director.
- **Before:** send the agenda (wording in §16) with a short document request: org chart, systems list or asset register if one exists, retention policy, BYOD policy, and the leaver process. What arrives (and what cannot be found) is itself the first data point.
- **During:** ask the fifty questions in order, numbering the answers; park detail rabbit-holes into follow-ups rather than losing coverage; flag every §15 red-flag answer aloud as it lands, with its same-day action agreed in the room; and close by agreeing the single IT point of contact and the written-confirmation mechanism.
- **Immediately after:** execute the day-one actions (hold, suspensions, leaver freeze, third-party notices) before the note is even typed; then circulate the numbered note for correction and confirmation, and convert it into the outputs table in §14.
- **Format notes:** ninety minutes is realistic for the fifty questions at strategic depth; run it in person or on video with screens shared (the IT lead pulling live admin consoles answers half the architecture questions with evidence rather than recollection); and if a provider or examiner is already engaged, have them attend the architecture, deleted-data and retention sections, where technical follow-ups land immediately.

§ 0 4 · QUESTIONS 1–5

IT architecture

1 · Walk me through where the organisation's data lives: email platform, file storage, chat and collaboration tools, business systems, and anything else with company information in it.

Listen for: the platform names and tenancy structure (one Microsoft 365 tenancy or several; Google alongside; legacy servers still running). This is the spine of the data map; everything else hangs off it.

2 · Who administers those systems, and are any managed by an outside IT provider? Who holds global administrator rights?

Listen for: the MSP relationship (a third party who needs a preservation notice today) and admin control (which determines who can suspend timers, export data, and whose fingers must not wander through evidence).

3 · Is there a systems inventory, asset register or data map, however informal? Can we have it?

Listen for: whether one exists at all. If yes, it accelerates everything; if no, the identification exercise starts from interviews and the cross-checks (finance records, SSO application lists) described in our companion guide *Finding the Evidence*.

4 · What has changed in the estate over the relevant period: migrations, new platforms, decommissioned systems, mergers or rebrands with old domains?

Listen for: where the older data went. Migrations strand mail in legacy archives, old domains mean extra custodian identities, and a decommissioned system may survive only in a backup someone must now find.

5 · Which business systems record the transactions or events this dispute is about (CRM, ERP, finance, quality, sector systems), and who understands each one?

Listen for: the named system owners. Structured systems are scoped through reports and audit trails, not document collection, and the person who understands the schema is an identification asset to book now.

§ 0 5 · QUESTIONS 6–10

Custodians

6 · Who was actually involved in the events behind this dispute: who negotiated, decided, approved, performed and recorded? Not the org chart; the people who did the work.

Listen for: the doers below the seniority line (the project coordinator, the assistant who ran the inbox). Participation, not rank, makes a custodian, and this answer seeds the tiered list.

7 · For each of those people: have they changed role, been absent for periods, or does anyone else send from their mailbox or manage their diary?

Listen for: delegation and cover arrangements, which split one identity across several humans and complicate attribution; the predecessor in a role is a custodian too.

8 · Who among them has left, is leaving, or is likely to leave? What happens to a leaver's accounts and devices here, and on what timetable?

Listen for: the leaver pipeline and anyone already in it. This is a same-day action answer: reissues stop and deletions freeze before this meeting ends, and PD 57AD's former-employee notices follow.

9 · Are there shared or team mailboxes and group channels the relevant work ran through (info@, sales@, a project channel)? Who has access to each?

Listen for: the non-custodial sources that individual custodians' collections will not cover, each needing a system owner and, later, an access-history for attribution.

10 · Did any contractors, consultants or agency staff work on these matters? On our systems, theirs, or both?

Listen for: the outside identities (their accounts in your tenancy are yours; their own systems raise control questions under their contracts, covered in our companion guide on control).

§ 0 6 · QUESTIONS 11–15

Devices

11 · What devices do the relevant people use for work: issued laptops and phones, and, honestly, personal devices too?

Listen for: the BYOD reality as against the policy. Work material on personal devices is inside the exercise via structured requests and protocols; silence about it is the one indefensible position.

12 · Is there an asset register or mobile device management system, and does it match reality? What would it miss?

Listen for: the reconciliation gaps: devices in mailbox-access logs that appear in no register are exactly the unmanaged endpoints that get missed.

13 · What happens to devices when they are replaced, repaired or upgraded? Where are the old ones now?

Listen for: the drawer of old phones and the storeroom shelf of laptops awaiting reissue: often the only place deleted-era evidence still exists, and days from being wiped.

14 · Have any relevant devices been lost, reset, repaired, reimaged or disposed of since the dispute arose (or in the months before)?

Listen for: answered honestly, this is triage gold: any yes routes the device (or its remnants: backups, replacement) to the forensic path, and the fact pattern into the file note now rather than a witness statement later.

15 · Do people use removable media (USB drives, external disks) or connect personal storage to work machines?

Listen for: exfiltration surfaces and orphan copies. USB usage plus a departing employee equals a same-week forensic question, not a month-three one.

§ 0 7 · QUESTIONS 16–20

Cloud services

16 · Beyond the main platforms, what cloud and SaaS services does the business use: file sharing, e-signature, HR, project tools, sector applications, anything paid by subscription?

Listen for: the unlisted estate. Follow up with the two cross-checks that find what memory misses: twelve months of accounts payable filtered for software, and the SSO provider's connected-application list.

17 · Do staff use personal cloud accounts (personal Gmail, Dropbox, iCloud) for anything work-related, officially or not?

Listen for: the shadow channel where candid material lives. Personal accounts are request-and-protocol territory, and auto-forwarding rules from corporate mail are the tell to check in the admin console.

18 · What messaging apps are used for business: WhatsApp, Signal, Telegram, iMessage? By whom, with whom, and are disappearing-message settings on anywhere?

Listen for: disappearing timers, which are a same-day, in-writing action: settings off and handsets scheduled for extraction. Chat evidence is central in modern disputes and dies fastest.

19 · For the main tenancy: what licence tier are we on, and do we know what that means for audit logs, retention controls and export capability?

Listen for: the tier answer (or the blank look that means the MSP must answer). Log windows of 30 to 180 days are running now; what the tenancy can preserve and produce is a fact to establish this week.

20 · Who are the cloud accounts actually registered to? Any business accounts on a founder's or employee's personal email, or a personal number running WhatsApp Business?

Listen for: the ownership tangles that complicate both control and preservation: the company Instagram on a personal login, the domain registered to an ex-director. Untangle holder, credentials and rights per account.

§ 0 8 · QUESTIONS 21–25

Deleted data

21 · Has anyone deleted, cleaned up, exported or reorganised anything potentially relevant since this dispute arose, or in anticipation of it? This is a safety question, not an accusation.

Listen for: anything other than a clean no. Framed properly, this question surfaces the routine tidy-up, the panicked deletion and the well-meant export alike, and every yes routes to forensic assessment while recovery windows are open.

22 · Has anyone already investigated internally: IT looking through a laptop, HR reviewing a mailbox, a manager checking a leaver's files?

Listen for: the informal look that changes artefacts. If it happened, stop further access now and record exactly who did what, when, with what tools; the candid access log limits the damage.

23 · Where does deleted material go on each platform, and how long does it survive: recycle bins, recoverable-items folders, retention holds?

Listen for: the recovery windows (typically 30 to 180 days) that are closing as you speak. In-platform litigation holds and deleted-item exports are this week's work.

24 · Is there any reason to think the other side, or a departed employee, deleted or took anything? What makes you think so?

Listen for: the suspicion and its evidence. It shapes the preservation letters going out, the specific-disclosure strategy, and whether the client's own sources (logs, backups) need forensic attention to prove someone else's deletion.

25 · If we needed to see what a mailbox or drive looked like on a specific past date, could we? What would that involve here?

Listen for: whether the organisation can time-travel (holds, versioning, snapshots) or only remember. The answer previews the backup questions and tells you whether deletion disputes are provable or merely arguable.

§ 0 9 · QUESTIONS 26–30

Retention and backups

26 · What retention and auto-deletion policies are configured right now on email, chat and drives: the actual settings, not the policy document?

Listen for: the live timers (90-day Teams chat expiry is the classic) whose suspension is a day-one action with a named person and a written confirmation.

27 · What automatic deletion or archiving jobs are scheduled to run in the next 90 days, on anything?

Listen for: the calendar of destruction: mailbox purges, log rotations, archive jobs, scheduled disposals. Each either pauses or is documented as out of scope, decision by decision.

28 · Describe the backup regime: what is backed up, to where, on what rotation, and who operates it?

Listen for: the rotation schedule, because the snapshot covering the critical period may be next to be overwritten; pausing rotation for in-scope systems is cheap and reversible.

29 · How far back could we actually restore if we had to, and what would it cost and involve? Any legacy formats (tapes, old systems) needing special handling?

Listen for: the accessibility economics that PD 31B makes part of reasonableness: preserve first, restore on demonstrated need, and park the tape library openly with the cost evidence.

30 · Have retention settings, hold policies or backup schedules been changed by anyone since the dispute arose?

Listen for: post-dispute changes, which are either innocent housekeeping to document now or a serious problem to escalate now; both are better known today.

§ 10 · QUESTIONS 31–35

Preservation actions

31 · What preservation steps, if any, have already been taken, by whom, and is there anything in writing?

Listen for: the baseline. Whatever exists gets absorbed into the formal hold; whatever was assumed ("we told people to keep things") gets replaced by the written notice with acknowledgment tracking.

32 · Who needs to receive the legal hold: which people, and which system operators, including the MSP? Who will acknowledge on behalf of IT operations?

Listen for: the distribution list built in the room, expressly including the operators (deletion is mostly done by systems and administrators, not by notice recipients).

33 · Can litigation holds be applied inside the platforms today (Purview, Vault, or equivalents), and who will do it?

Listen for: the named person and the today. In-platform holds catch what notices cannot: the recoverable items, the timer-bound chat, the custodian who ignores email.

34 · Is anything volatile enough that it should be forensically preserved this week: suspect devices, key handsets, CCTV, a leaver's laptop?

Listen for: the triage list. The asymmetry rule decides doubtful cases: a forensic image now preserves every later option, ordinary handling forecloses some, so uncertainty resolves toward preservation.

35 · Who will be the single point of contact for all IT actions from today, and who will give the written confirmation that preservation steps have been taken?

Listen for: one name for each. The single channel prevents the parallel helpfulness that destroys evidence, and the written confirmation is a PD 57AD requirement, not a courtesy.

§ 11 · QUESTIONS 36–40

Privacy and data protection

36 · What personal data will the exercise inevitably touch: employees' communications, customers' information, special-category data in HR or health contexts?

Listen for: the sensitivity profile, which shapes minimisation (targeted trees rather than whole servers), redaction planning and the lawful-basis record the exercise should carry.

37 · What do staff-facing policies say about monitoring and the company's access to work communications, and what have staff actually been told?

Listen for: the transparency baseline. Collection from staff systems is lawful and expected, but the employment-law fairness and ICO guidance around it are easier honoured from existing policies than improvised.

38 · Where personal devices hold work material, are the individuals likely to cooperate with a targeted, privacy-protective extraction? Any relationships already strained?

Listen for: the consent landscape. The structured request with an independent extraction protocol works with cooperative custodians; identify the difficult ones now so the approach (and any fallback) is planned, not reactive.

39 · Is any relevant data outside the UK: foreign subsidiaries, overseas servers, custodians abroad? Any jurisdictions with strict local rules?

Listen for: the cross-border map: transfer mechanisms, local advice needs, and in-country processing options are planned before collection, not litigated after.

40 · Is there a live data-protection dimension already: a breach, an ICO interaction, subject access requests from the opponent or departing staff?

Listen for: parallel proceedings by another name. SARs from adversaries and breach timelines interact with disclosure strategy and deadlines, and the same evidence often serves both.

§ 12 · QUESTIONS 41–45

Privilege

41 · Which lawyers have touched these matters: external firms, in-house counsel, and in-house lawyers wearing commercial hats?

Listen for: the privilege domains and names for screening, and the mixed-role individuals whose material will need judgment rather than rules (in-house legal advice attracts privilege; commercial input does not).

42 · Was there an internal investigation, review or report into these events? Who commissioned it, who conducted it, and for what stated purpose?

Listen for: the documents whose privilege status is genuinely contestable. Purpose, authorship and circulation determine the position, and finding the report in month one beats explaining it in month nine.

43 · How does advice travel internally: is legal advice forwarded into business threads, summarised in board packs, pasted into chat?

Listen for: the dissemination habits that put privileged content inside otherwise disclosable families, which sizes the privilege-review burden and argues for early clawback terms in the DRD.

44 · Is there any joint, shared or common-interest dimension: co-defendants, insurers, group companies sharing advice, prior transactions with shared counsel?

Listen for: the multi-party privilege architecture that determines who may see what during the exercise itself, and which consents or protocols must exist before hosting and review start.

45 · Has anything privileged possibly already gone out: to the opponent pre-action, to a regulator, to an auditor or adviser?

Listen for: waiver risk to assess now, calmly: what went, to whom, on what terms, and whether limited or inadvertent disclosure positions need protecting before anyone else raises them.

§ 13 · QUESTIONS 46–50

Third parties

46 · Which outside organisations hold or process company data: the MSP, hosting and backup providers, payroll, accountants, records storage?

Listen for: the preservation-notice list. Data held on the client's behalf is within its control; the notices go today, and the contracts (access, assistance, exit clauses) get gathered this week.

47 · Have any providers changed during the relevant period: a switched MSP, a migrated host, an ended contract? Where did the data go at exit?

Listen for: the exit data sets and the old provider's residual holdings, both on contractual retention clocks that a prompt notice can stop.

48 · Who on the other side of these events (counterparties, agents, brokers, joint venturers) holds the other half of the correspondence?

Listen for: the preservation-letter targets beyond the opponent itself: cheap letters now that found later spoliation arguments and frame CPR 31.17 applications if cooperation fails.

49 · Are there carriers, banks or platforms whose records may matter: call records, payment flows, platform accounts and their logs?

Listen for: the true third parties needing court-assisted routes with lead times (third-party disclosure, witness summonses, *Norwich Pharmacal*, letters of request), planned early because their clocks (carrier retention especially) run short.

50 · Is any other proceeding, regulator or authority already touching this data: police, a regulator, an insurer's investigators, parallel litigation?

Listen for: the parallel demands that constrain and complicate: seized devices, regulator undertakings, insurers' access, and the coordination (and criminal-standard handling) they may require from day one.

§ 14 · CONVERSION

After the meeting: converting answers into actions

ANSWER CLUSTER	IMMEDIATE OUTPUT	FEEDS INTO
Q1–5 architecture; Q16–20 cloud	Data map v0; MSP notice; licence-tier and log-window checks tasked	Identification and the written questionnaires (*Finding the Evidence*)
Q6–10 custodians	Candidate custodian list with leaver flags; shared-source list with owners	Tiering and interviews (*Identifying the Right Custodians*)
Q11–15 devices; Q21–25 deleted data; Q34	Forensic triage list; stop-access instructions; same-week acquisition schedule	The triage discipline (*eDisclosure or Digital Forensics?*)
Q26–33, Q35 retention and preservation	The hold issued; timers suspended with confirmations; rotation paused; SPOC named; written-confirmation request sent	The hold register and PD 57AD compliance
Q36–40 privacy; Q41–45 privilege	Minimisation and transfer notes; privilege screen list; clawback and protocol points for the DRD	Review protocol and DRD drafting
Q46–50 third parties	Preservation letters out; contract-gathering tasked; court-route lead times diarised	Control schedule (*Control of Electronic Documents*)

Then the record: the numbered note circulated for correction, the client's confirmation obtained, and the whole filed as identification evidence. Within the fortnight, the meeting's outputs flow into assessment and search design, and the strategy document assembles them, as set out in the companion guide *How to Build a Defensible eDisclosure Strategy*.

§ 15 · ESCALATION TRIGGERS

Red-flag answers

Some answers change the meeting from scoping to incident response. Flag them aloud when they land, and leave the room with the action agreed:

THE ANSWER	THE SAME-DAY ACTION
"IT already had a look through his laptop." (Q22)	All access stops; who-did-what-when recorded; device to forensic assessment
"Her mailbox is due for deletion Friday." / "That laptop is being reissued." (Q8, Q13)	Pipeline frozen in writing before the meeting ends; device pulled and shelved
"We cleared some old chats to be tidy." (Q21)	No judgment, full detail, forensic recovery assessment while windows are open; candid file note
"Disappearing messages are on in that group." (Q18)	Timers off in writing today; handsets scheduled for extraction
"The retention policy changed a few weeks ago." (Q30)	Change history exported; who, when, why documented; escalate if post-dispute
"The old MSP still has everything, contract ended in spring." (Q47)	Preservation notice to the old provider today; exit data set located
"The police took two phones last month." (Q50)	Coordination strategy before anything else moves; criminal-standard handling assumed
"We sent the investigation report to the insurer / the regulator." (Q45)	Waiver analysis now; circulation mapped; positions protected before the opponent raises it

§ 16 · WHERE IT GOES WRONG & DRAFTING AIDS

Common mistakes · Suggested wording

Common mistakes

- **The meeting without the operator.** The GC attends, IT does not, and every systems answer is "I would have to check": half the fifty questions deferred a week they cannot afford.
- **Coverage sacrificed to depth.** Forty minutes on the first juicy topic, sections H to J never reached, and the privilege and third-party landmines found later by standing on them.
- **Accusatory framing.** Q21 and Q22 asked like cross-examination, producing defensiveness instead of the candour that protects the client; the safety-question framing exists for a reason.
- **Actions deferred to the follow-up letter.** The timer suspension "confirmed in writing next week" while the timer runs; day-one actions are agreed in the room with names and today attached.
- **No numbered record.** Rich discussion, prose note, and six months later nobody can say whether backups were actually asked about. Number the answers to the questions.
- **Treating this as the only interview.** The strategic meeting scopes; the individual custodian interviews (separately, later) surface what nobody says in front of the IT director.

Suggested wording · Meeting request to the client (core paragraphs)

> "We need to hold an initial meeting about the electronic evidence in this matter within the next [2] working days. Duties to preserve relevant data are already in force, and some data types are at risk of automatic deletion, so timing matters. Please ensure attendance by: [decision-maker]; the person with day-to-day administrative control of your IT systems (in-house or your IT provider's lead engineer); and [operational lead]. If available, please bring or send in advance: an organisation chart, any systems list or asset register, your document retention policy, any BYOD or IT use policy, and a note of your leaver process. Until the meeting, please ensure that no devices are reissued, repaired, reset or disposed of, no accounts are deleted, and no one reviews or tidies potentially relevant material."

Suggested wording · Post-meeting confirmation request (core paragraphs)

> "Further to today's meeting, we attach: (1) the numbered note of the meeting, for correction and confirmation; (2) the legal hold notice for distribution to the individuals and system operators listed; and (3) the schedule of preservation steps agreed, with the responsible person and date for each. Please confirm in writing by [date] that each step in the schedule has been implemented, or tell us immediately if any cannot be. Please also confirm that [name] will act as the single point of contact for all IT actions in this matter, and that no changes will be made to systems, retention settings, accounts or devices relevant to this matter without our prior agreement."

§ 17 · QUICK CONTROL

Checklist · When to involve a digital forensic expert

The first-meeting checklist

- ☐ Meeting held within days of instruction; duties explained at the top
- ☐ Right people in the room: decision-maker, systems operator (or MSP lead), operational lead
- ☐ Agenda and document request sent ahead; arrivals (and gaps) noted
- ☐ All fifty questions asked; answers numbered against the questions
- ☐ Red-flag answers flagged aloud with same-day actions and named owners
- ☐ Day-one actions executed before the note is typed: hold, suspensions, leaver freeze, timer changes, third-party notices
- ☐ Single IT point of contact named; written-confirmation mechanism agreed
- ☐ Numbered note circulated, corrected, confirmed and filed as identification evidence
- ☐ Outputs converted per §14: data map v0, custodian candidates, triage list, notice schedule, privilege screens
- ☐ Follow-ups diarised: written questionnaires, custodian interviews, assessment kickoff

When to involve a digital forensic expert

Bring an examiner into the meeting itself where the matter plainly carries forensic weight (departed employees under suspicion, disputed documents, regulatory or criminal colour): the architecture, deleted-data and retention sections then generate scoped technical follow-ups in real time. Otherwise, the meeting's escalation outputs go to the laboratory the same week: every Q14, Q21, Q22 and Q34 answer that is not a clean no, every red-flag row in §15, and every source whose recovery window is measurably closing. The triage principles are in the companion guide *eDisclosure or Digital Forensics? Choosing the Correct Approach*.

§ 18 · COMMON QUESTIONS

Frequently asked questions

Who should attend the first meeting?

Three roles, ideally under six people: the client's decision-maker (GC or instructing director), whoever actually administers the systems (the in-house IT head or the MSP's lead engineer, specifically not just the account manager), and one operationally senior person close to the events. Individual custodians come later, separately and deliberately so: the strategic meeting and the custodian interviews surface different things.

What if IT is fully outsourced?

Then the MSP is in the meeting (under confidentiality cover), because half the fifty questions are theirs to answer, and the MSP also receives a preservation notice as a third party holding client data. Establish in the meeting who at the provider will implement holds and suspensions, on whose instruction, and confirm the contract's access and assistance terms are being gathered.

What if the client cannot answer many of the questions?

Expect it, and treat the gaps as findings: every "we would have to check" becomes a numbered follow-up with an owner and a date, and the gap pattern itself tells you how much identification support the matter needs. What must not happen is unanswered questions silently becoming unasked ones; the numbered record prevents exactly that.

How long does this take, and can it be split?

Ninety minutes covers the fifty questions at strategic depth with a disciplined chair. Splitting works if the split is by section with the urgent ones first: architecture, custodians, devices, deleted data, retention and preservation (Q1 to 35) cannot wait; privacy, privilege and third parties (Q36 to 50) can follow within days if they must. What cannot be split off is the day-one action list.

Should we run this meeting pre-action?

Yes, whenever a dispute is realistically contemplated: the preservation duties are already live, the volatile data is already dying, and pre-action versions of the fifty questions improve the letter of claim or response as well as the eventual disclosure. The only adjustment is emphasis: pre-action, questions 21 to 35 (deletion, retention, preservation) carry even more weight because more time remains to act on the answers.

Is this meeting privileged, and does the note get disclosed?

The meeting and its note are litigation-privileged legal work in the ordinary way. What the exercise later deploys is derived material: the data map, the hold register, the DRD descriptions and, where identification methodology is probed, the fact that a structured process was followed on stated dates. Structure the note so the factual answers are severable from strategic commentary, and deployment stays clean.

§ 19 · REFERENCE

Glossary

BYOD
Bring your own device: personal hardware used for work, addressed through structured requests and protocols.

Day-one actions
The preservation steps executed the day of instruction: hold, timer suspensions, leaver freeze, third-party notices.

Disappearing messages
Auto-delete settings in chat applications; a same-day, in-writing suspension wherever relevant.

Hold register
The dated record of hold recipients, acknowledgments, suspensions and confirmations.

Leaver pipeline
The IT process deleting accounts and reissuing devices after departure; frozen before this meeting ends.

MSP
Managed service provider: outsourced IT holding the client's estate, and a day-one preservation-notice recipient.

Numbered note
The meeting record with answers keyed to question numbers, circulated, confirmed and filed as identification evidence.

Recovery window
The period during which deleted material survives in recycle bins, recoverable-items stores or provider retention.

Red-flag answer
An answer converting scoping into incident response, with a same-day action owned in the room.

Single point of contact
The one named client-side channel for all IT actions, preventing parallel helpfulness.

Tenancy
The organisation's instance of a cloud platform, administered through its admin accounts.

Written confirmation
The client's PD 57AD-required confirmation that preservation steps have been implemented.

Sources and authoritative references

The interview discipline in this guide draws on materials published by our e-discovery practice and laboratory, referenced here as sources:

- e-discovery.uk, EDRM Phase 01 · Identification (custodians, repositories and scope logged as the chain of custody's first entries) and Phase 02 · Preservation: e-discovery.uk/edrm/identification · e-discovery.uk/edrm/preservation
- e-discovery.uk, the practice's method statement ("Bring us in early. Defensibility is built, not retrofitted"): e-discovery.uk
- e-discovery.uk, Knowledge Centre practice notes, including mobile and disappearing-message evidence: e-discovery.uk/knowledge
- cflab.uk, digital forensics services (same-week preservation, device and cloud acquisition under chain of custody, the destination for this meeting's escalations): cflab.uk/digital-forensics-services
- cflab.uk, guides for lawyers, including preservation best practice and what informal access does to artefacts: cflab.uk/guides
- Practice Direction 57AD (preservation duties, including notification of employees, former employees and third parties, and written confirmation): justice.gov.uk, PD 57AD
- CPR Part 31 and PD 31B (reasonable search; the Electronic Documents Questionnaire): justice.gov.uk, PD 31B
- ICO, UK GDPR guidance, including employment practices and monitoring: ico.org.uk
- Data Protection Act 2018: legislation.gov.uk/ukpga/2018/12 · Data (Use and Access) Act 2025: legislation.gov.uk/ukpga/2025/21
- Attorney General's Guidelines on Disclosure (rev. 2024): gov.uk, AG's Guidelines

DISCLAIMER

This publication provides general information about early-stage electronic disclosure practice in the United Kingdom as at August 2026. It 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. Rules, guidance and legislation change; always check the current text. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

We are frequently in the room for exactly this meeting, and it is the cheapest point at which to involve us: an examiner or e-discovery consultant attending the architecture, deleted-data and retention sections converts uncertain answers into scoped technical follow-ups on the spot, and the same-week actions the meeting generates (in-platform holds, timer suspensions verified, leaver devices acquired, handsets extracted before recovery windows close, DVR footage exported) are executed under laboratory chain of custody from the first hour. From there, the meeting's outputs flow into the practice's standard machinery through **e-discovery.uk**: identification support and questionnaires, early data assessment, defensible collection, processing, hosted review and production, with the forensic laboratory receiving every escalation the fifty questions surface. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine, and attendance at a first meeting can usually be arranged within two working days.

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