Planning An On Site Digital Evidence Collection

Planning an on-site digital evidence collection requires careful consideration of access, authority, credentials, and equipment. This guide details the necessary pre-visit reconnaissance and execution steps to ensure a successful collection day, minimising disruption and securing evidence properly.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/planning-an-on-site-digital-evidence-collection

ON - SITE COLLECTION · A GUIDE FOR UK LAWYERS Planning an On-Site Digital Evidence Collection Access, Equipment, Credentials, Disruption and the Day That Goes to Plan COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES ON-SITE & LABORATORY ACQUISITION CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: why site days go wrong 03 The pre-visit reconnaissance 04 Access, authority and the people question 05 Credentials, encryption and the keys to the estate 06 Equipment: what the kit list actually contains 07 The day itself: sequence, disruption and logging 08 Departure: sealing, transport and the site left behind 09 Worked examples 10 Common mistakes and technical limitations 11 Questions to ask · Suggested wording 12 Checklist and red flags · When to involve a digital forensic expert 13 Frequently asked questions 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: THESITEVISITISWONINTHEWEEKBEFOREIT

§ 02 · FIRST PRINCIPLES The problem in plain English: why site days go wrong

§ 03 · THEWEEKBEFORE The pre-visit reconnaissance

§ 04 · DOORSANDPEOPLE Access, authority and the people question

§ 05 · KEYS Credentials, encryption and the keys to the estate

§ 06 · THEVAN Equipment: what the kit list actually contains

§ 07 · EXECUTION The day itself: sequence, disruption and logging

§ 08 · LEAVINGWELL Departure: sealing, transport and the site left behind

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEQUESTIONNAIRETHATFOUNDTHESECONDSERVERROOM EXAMPLE2 · THEQUARTER - ENDCOLLISIONTHATPLANNINGDISSOLVED EXAMPLE3 · THEKITLISTVERSUSTHE2011RAID

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

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent (for agreed or supervised visits) Ask your e Discovery / forensic provider SUGGESTED WORDING · CLIENT SITE - PREPARATION INSTRUCTION SUGGESTED WORDING · DAY- PLANHEADER (THEONE - PAGE VERSION THE TEAM CARRIES)

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The on-site planning checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions How long does an on-site collection take? Can the business keep working while we collect? Should devices be imaged on site or taken to the laboratory? What if we find devices on site that are not on the schedule? Do we need to tell staff what is happening? What does the client get after the visit?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

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

Questions and answers

How long does an on-site collection take?

The arithmetic answer: total scheduled storage divided by parallel imaging throughput, plus the fixed costs (walk- through, powered-on work, sweeping, sealing): typically a day for a handful of machines, two to three for a small office, and a planned campaign for anything larger, with servers often taken in overnight windows. The planning answer: however long the reconnaissance says, plus margin: because the schedule that assumed the questionnaire was complete meets §2's cupboard eventually.

Can the business keep working while we collect?

Largely, if planning made it so: user machines lifted in batches against loaners or d own time windows, servers imaged from snapshots or out-of-hours, and the sequence built around the business calendar. The honest exceptions: the specific machine being imaged is unavailable while it images (unless live-acquired), and contested devices leave immediately and stay gone. Example 2 is the model: disruption is a negotiation the week before, not a discovery on the day.

Should devices be imaged on site or taken to the laboratory?

Per device, by plan: on-site imaging suits healthy, standard hard w are the business needs back and uncontested contexts; seizure to the laboratory suits contested devices (custody strength), failing or exotic media (§10), encrypted machines pending key recovery, and anything the volume arithmetic cannot fit into the site window. The protocol's method matrix records which, and the site plan books transport and loaners accordingly; "we'll decide at the desk" is the answer this guide exists to delete.

What if we find devices on site that are not on the schedule?

The standard contingency: record them (photograph, location, description), preserve them in place or seize per the protocol's unexpected-source clause, and refer the scope question to the decision number the same hour: guide 36's stop-preserve-call, which converts the surprise into a documented decision. What the team never does is silently image them (scope without authority) or silently ignore them (the omission cross-examination finds): the corridor of guide 36's first example runs through every site.

Do we need to tell staff what is happening?

A lawyer's decision made in planning, balancing UK GDPR transparency, employment-relations reality, tipping-off risk in fraud contexts, and the practicalities of lifting machines from desks. Options run from full announcement through need-to-know framing to covert out-of-hours collection where the risk analysis and legal basis support it; each has different sequencing and different paper work, and the examiner executes which ever was chosen: the kitchen is not where this gets decided.

What does the client get after the visit?

The deliverable set the protocol promised: the evidence schedule (every exhibit, reference, seal and location), the hash schedule, the collection report reconciling plan against execution with the running and deviation logs, photographs, and the custody records: plus the practical outputs: retained-device list, return timetable, and the named contact for the morning-after

questions. If the matter proceeds, the same set is what makes the collection exchangeable and defensible; it is written once, for both audiences. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915