Forensic Image Logical Extraction Or Targeted Collection

This guide for UK lawyers addresses the critical decision of forensic collection methods: forensic image, logical extraction, or targeted collection. It defines each approach, compares them, and provides a framework for matching the method to evidential need, considering cost, proportionality, and risk.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/forensic-image-logical-extraction-or-targeted-collection

COLLECTION METHOD S · A GUIDE FOR UK LAWYERS Forensic Image, Logical Extraction or Targeted Collection? Choosing the Right Depth of Acquisition, Source by Source COMPUTER FORENSICS LAB · E-DISCOVERY. UK

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: a false binary 03 The three methods, properly defined 04 The comparison table 05 Matching method to evidential need 06 Cost and proportionality: the chain consequences 07 The decision tree 08 The honest risk register of each method 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: DEPTHISCHOSENPERSOURCE, ANDTHEOPTIONTOGODEEPER ISPRESERVED

§ 02 · FIRST PRINCIPLES The problem in plain English: a false binary

§ 03 · TERMSOFART The three methods, properly defined Forensic (physical) image Logical extraction Targeted collection

§ 04 · SIDEBYSIDE The comparison table FORENSIC IMAGE LOGICAL EXTRACTION TARGETED COLLECTION

§ 05 · FIT Matching method to evidential need

§ 06 · THEMONEY Cost and proportionality: the chain consequences

§ 07 · THEDECISION The decision tree

§ 08 · HONESTLEDGER The honest risk register of each method Forensic image

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEHYBRIDTHATFITTEDTHECASE EXAMPLE2 · THEBLANKETINSTRUCTION EXAMPLE3 · THETRIGGERTHATFIRED

§ 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 Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTION PA R AG RAPH (METHOD PER SOURCE WITH TRIGGERS) SUGGESTED WORDING · DRD / CORRESPONDENCE PA R AG RAPHEXPLAININGAMIXED APPR OAC H

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

§ 13 · COMMON QUESTIONS Frequently asked questions Is targeted collection defensible, or will we be criticised for not imaging? Can we start light and upgrade to imaging later if needed? Do we need to image every custodian's laptop? How do phones fit this framework? Roughly what does each method cost? What should we do when the other side chose the wrong method for a contested source?

§ 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

Is targeted collection defensible, or will we be criticised for not imaging?

Targeted collection is not merely defensible but the proportionate default in most civil disclosure, provided the discipline travels with it: a scope derived from interviews and the data map, forensic execution (hashes, manifests, logs), preservation behind it, and a recorded rationale. Criticism attaches not to the method but to its casual version: undocumented scope, no preservation, no reason. The question "why did you not image?" is answered in one sentence when the answer was written at the time.

Can we start light and upgrade to imaging later if needed?

Only if the source still exists in a meaningful state: continued use overwrites deleted material daily, and reissue or disposal ends the question. That is exactly why the framework separates preservation from collection: sequester or image the plausible-risk sources now (cheap, no processing), collect light, and the upgrade later is a decision, not a resurrection. Starting light with no preservation is the version that fails.

Do we need to image every custodian's laptop?

Almost never. In a typical matter the laptops that justify imaging are the small set connected to contested conduct; the remaining custodians' evidential contribution is their communications and documents, which live in server-side and cloud repositories reachable by targeted collection without touching the devices at all. The nineteen-laptop reflex buys volume, cost and grievances, not evidence: Example 2 is its biography.

How do phones fit this framework?

Awkwardly, which is why they get their own guide: mobile acquisition levels (logical, file system, physical where possible) are constrained by device, OS version and lock state rather than free choice, and access opportunities are fragile. The practical rule: when a phone matters and is accessible, take the fullest extraction the device supports at that moment, because the marginal cost is small and the opportunity may not recur; the depth decision is made by the device as much as the examiner.

Roughly what does each method cost?

Orders of magnitude, honestly: imaging a single computer typically runs from several hundred pounds to low four figures including verification and handling; logical and targeted collections often less per source, with server and cloud collections priced by scope and logistics. But acquisition prices mislead: the dominant difference is downstream, where an imaged-and-promoted estate can cost ten times a targeted one through processing, hosting and review. Price the chain per method, per source, and the comparison becomes real; the companion costs guide supplies the arithmetic.

What should we do when the other side chose the wrong method for a contested source?

Establish it in correspondence (method, tools, scope, whether the source survives), then act on what remains: if the device exists, seek preservation and deeper acquisition by agreement or application, promptly, before further use degrades it; if it was reissued or wiped after the dispute arose, the questions become preservation-duty questions, and the artefacts of the

destruction itself may be examinable. Either way, an examiner's statement of what the chosen method cannot show about the contested issue converts a methodological quibble into a submission with teeth. 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 Page 16 of 19

Source: https://e-discovery.uk/library/forensic-image-logical-extraction-or-targeted-collection. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.