What Happens During EDiscovery Processing

E-discovery processing is the critical, often overlooked, stage between data collection and document review. This guide demystifies the process, explaining how decisions about exceptions, de-NISTing, and filters shape the final document set, ensuring defensibility and accuracy in electronic disclosure.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/what-happens-during-ediscovery-processing

EDISCOVERY PROCESSING · A GUIDE FOR UK LAWYERS What Happens During e Discovery Processing? The Black Box Between Collection and Review, Opened for Lawyers COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES EDRM PROCESSING PRACTICE EXCEPTION & RECONCILIATION REPORTING CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: PROCESSINGTURNSDATAINTODOCUMENTSTHROUGHRECORDED DECISIONS: THERECORDISWHATMAKESYOURDISCLOSUREDEFENSIBLE

§ 02 · FIRST PRINCIPLES The problem in plain English: the stage nobody watches

§ 03 · THEPIPELINE The pipeline: from collected data to reviewable documents

§ 04 · THEDECISIONS The decisions that matter: exceptions, de NISTing and filters

§ 05 · THEARITHMETIC Reconciliation: making the numbers add up

§ 06 · THEAWKWARDINPUTS Special formats: mobile data, chat, cloud exports and structured sources

§ 07 · WHENCOUNTSARECONTESTED Processing disputes: challenging and defending the counts

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EXCEPTION SOURCE RE- COUNTERPART CREDENTIALS T YPE PULL COPIES & KEYS OTHER VERSIONS / BACKUPS NET RESULT RENDERS

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEEXCEPTIONTHATWASTHECASE EXAMPLE2 · THE400GBTHATBECAME41, 000DOCUMENTS, DEFENSIBLY EXAMPLE3 · THEFAMILIESTHATCAMEAPART

§ 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 · PROCESSING PA R AG RAPHFORTHEDISCLOSUREPROTOCOL

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

§ 13 · COMMON QUESTIONS Frequently asked questions Why did 400 GB of data become only 40,000 documents? What actually happens to files that cannot be processed? Is it safe to remove "system files" from the review set? Our opponent's production has emails whose attachments are missing. Innocent? Can we change processing decisions after review has started? Does processing alter the underlying evidence?

§ 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

Why did 400 GB of data become only 40,000 documents?

Because volume and count measure different things: containers expand into items, then de NISTing removes the operating system's furniture, date and scope filters remove the out-of-range, and deduplication collapses the copies: each step with a recordable count. The right response to the question is Example 2's table; suspicion is only warranted when no table exists.

What actually happens to files that cannot be processed?

They become exceptions: logged by category (encrypted, corrupt, unsupported, empty), triaged, and either resolved through the §8 routes: credentials, source re-pulls, counterpart copies, specialist tooling: or consciously accepted and listed. What must never happen is silent disappearance: the exception list is disclosure work- product, and Example 1 is why.

Is it safe to remove "system files" from the review set?

Almost always: de NISTing removes known-hash operating system and application files with no user content, and doing so is standard, published-list, recorded practice. The caveat is the matter where system artefacts are the evidence: user-activity and exfiltration cases per guides 41 and 61: which opt out of the cull for the relevant sources, knowingly and in writing.

Our opponent's production has emails whose attachments are missing. Innocent?

Sometimes (source-side stubbing, genuine transmission failures): but it is exactly what broken family handling looks like, and the question is answerable: ask for their family reconciliation and unitisation settings per §11. A producing party that preserved families can say so in a sentence; one that cannot has Example 3 ahead of it.

Can we change processing decisions after review has started?

Yes, with discipline: new ranges, scopes or unitisation are run as documented deltas: reprocessed, reconciled, overlaid: never silently merged, so the workspace's arithmetic stays coherent and prior review work maps cleanly onto the corrected set. Example 3's fix is the model; its costs are the argument for getting settings instructed the first time.

Does processing alter the underlying evidence?

No: it derives from preserved originals: text, images, normalised fields: while the collected sources stay sealed and hashed, and any produced native is traceable back to them. What processing does alter is visibility: which is the whole point of governing it, since a document invisible to search and review is, functionally, undisclosed. cflab. u k · e-disc ove r y. u k