File Wiping Anti Forensics And The Evidence They Leave Behind

Anti-forensics actions, such as file wiping or device resets, are acts that leave behind examinable traces. This guide details the techniques, the evidence they create, and what survives, helping practitioners understand the consequences of deliberate data destruction.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/file-wiping-anti-forensics-and-the-evidence-they-leave-behind

ANTI - FORENSICS · A GUIDE FOR UK LAWYERS File Wiping, Anti-Forensics and the Evidence They Leave Behind When the Attempt to Destroy Evidence Becomes the Evidence COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES ANTI-FORENSICS EXAM IN AT I ON

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: destruction is an act, and acts are recorded 03 The techniques: wiping, cleaning, encryption, resets and obfuscation 04 The traces: installation, execution, patterns and the negative space 05 Mobile, cloud and platform anti-forensics 06 What survives: the honest limits of recovery and the estate's redundancy 07 Deployment: timing, intent and the consequences of proven destruction 08 Source architecture: where else the evidence lives 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: ANTI - FORENSICSDESTROYSCONTENTANDCREATESEVIDENCE OFDESTRUCTION: THEEXAMINATIONREADSTHETOOL, THEEXECUTION, THEEXTENT ANDTHETIMING, STATESHONESTLYWHATISGONE, ANDLETSTHECOURTDRAWTHE INFERENCETHATDELIBERATEDESTRUCTIONAFTERADUTYAROSEINVITES

§ 02 · FIRST PRINCIPLES The problem in plain English: destruction is an act, and acts are recorded

§ 03 · THETECHNIQUES The techniques: wiping, cleaning, encryption, resets and obfuscation

§ 04 · THETRACES The traces: installation, execution, patterns and the negative space

§ 05 · MOBILE, CLOUD AND PLATFORM AN TI-FORENSICS Mobile, cloud and platform anti-forensics

§ 06 · WHATSURVIVES What survives: the honest limits of recovery and the estate's redundancy

§ 07 · DEPLOYMENT Deployment: timing, intent and the consequences of proven destruction

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION AUDIT

+ + PHYSICAL + SHADOW DEVICE ESTATE WIPED / ARTEFACTS REDUNDANCY UNRECOVERABLE PLATFORM BEHAVIOURAL JOURNALS RECORDS LAYER COPIES

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEFREE - SPACEWIPEANDTHESEARCHTHATPRECEDEDIT EXAMPLE2 · THEPHONERESETTHENIGHTBEFOREHANDOVER EXAMPLE3 · THECLEANERTHATWASROUTINE, ANDTHEALLEGATIONTHATFAILED

§ 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 · ANTI - FORENSICS PA R AG RAPHFORAHOLDNOTICE

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

§ 13 · COMMON QUESTIONS Frequently asked questions The other side's laptop is completely empty. Can anything be recovered? Can an expert tell the difference between routine clean-up and deliberate destruction? A phone was factory-reset before h and over. Is the evidence gone? What if the data was encrypted rather than wiped? How should we warn a client not to do any of this? Is running a wiping tool a criminal offence?

§ 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

The other side's laptop is completely empty. Can anything be recovered?

From wiped regions, honestly, no (§6); from what the tool missed (journals, shadow copies, alternate streams) and from the estate the party did not control (syncs, backups, counterparts), frequently a great deal (Example 1's 1,100 files). And the wipe itself, dated and scoped from the tool's artefacts, is often worth more than the content: courts infer against destroyers.

Can an expert tell the difference between routine clean-up and deliberate destruction?

Usually: routine tools run on schedules with long histories, target predictable locations and pre-date the dispute (Example 3); deliberate destruction is installed recently, executed in bursts, targets the disputed material selectively, and clusters around the duty date (Example 1): §7's timing and selectivity, with the journal showing whether bulk deletion preceded the run.

A phone was factory-reset before h and over. Is the evidence gone?

The device's contents, largely; the case, rarely: the reset is timestamped in firm w are and re-enrolment records, pre-reset cloud backups often survive (Example 2), counterparties hold their copies of every message, and the platform logged the account's activity. The reset becomes the exhibit; the backup becomes the evidence.

What if the data was encrypted rather than wiped?

Encryption conceals rather than destroys: the enablement is dated (§5), the data exists, and the with hold in g of keys after an order is a conduct question with serious consequences (guides 117-118): distinct from the technical impossibility of decryption, which the examiner states honestly. The court is told when, and asked to draw the conclusion.

How should we warn a client not to do any of this?

Explicitly, in the hold notice, naming the acts (cleaning tools, resets, reinstalls, encryption, account deletion, clock changes), stating that they are traceable, and setting out the consequences: §11's paragraph. Clients under hold destroy evidence far more often from ignorance of the traces than from calculated risk; the warning removes the ignorance.

Is running a wiping tool a criminal offence?

It can be, where it is done to pervert the course of justice in criminal proceedings, and in regulated contexts destruction of records may breach statutory duties: the civil consequences (adverse inference, strike-out, contempt where an order is breached) arise far more commonly and are severe in themselves (§7). The finding is evidenced the same way which ever track it reaches, and specialist advice is taken on the criminal edge. cflab. u k · e-disc ove r y. u k