SAMPLE DIGITAL FORENSIC REPORT

Was the laptop altered after it was handed back, and what can be recovered?

SCENARIO	**Integrity of a returned laptop used by the employer before imaging, and recovery of deleted files**
INSTRUCTED BY	**A financial advice firm (anonymised)**
DEVICE	**Windows 11 business laptop, 512 GB NVMe drive, BitLocker enabled**
PERIOD EXAMINED	**1 April to 29 May 2026**
METHOD	**Full forensic image of the drive, analysed with our forensic software**

Sample report: anonymised, details changed. This is an example of our reporting, based on real casework. Names, dates, file names and identifying details have been changed. It is not a live case file.

CONTENTS

01 Summary of findings
02 Instructions and scope
03 How to read this report
04 Evidence and method
05 Lawful basis and proportionality
06 Limitations
07 The boundary: 8 to 12 May
08 The firm's handling after return
09 The seven disputed files
10 Could the clock have been changed?
11 Recovery of deleted files
12 Alternative explanations considered
13 Conclusions
14 What we would also ask for
15 Glossary of records relied on
16 About this sample report

Easy Data Recovery
Forsyth House, Cromac Square, Belfast, BT2 8LA

028 9002 0144
easyrecovery.co.uk
Mon–Fri 9am–5:30pm

01 Summary of findings

The former employee alleges that files found on the laptop were placed there by the firm after the laptop was returned. The records show a clear boundary between the employee's use and the firm's later handling, and every file the firm relies on was created before that boundary. Times are UK time (BST).

- **The boundary.** The employee's last session ended with a shutdown at 17:22 on 8 May 2026. The laptop was next started at 10:04 on 12 May, after it had been returned.
- **The firm's handling.** The laptop was used on 12, 13 and 20 May under the firm's administrator account and, on 13 May, under the employee's account after its password had been reset. In total, 214 files were opened, 6 folders were copied to a USB stick and no user file was created, changed or deleted in the employee's profile.
- **The disputed files.** The seven files the firm relies on, among them a client export and two draft letters to clients, were created between 21 April and 7 May. Their creation is recorded in four independent places, none of which the firm's later sessions touched.
- **System changes after return.** Windows installed updates on 12 May and restarted twice. Some system records were overwritten as a result, and they are listed below.
- **Deleted files.** The employee deleted 118 files on 8 May. Ninety-one were recovered in full and nine in part. Eighteen had been overwritten, and at least six of those were overwritten by the 12 May update.
- **Not supported.** No evidence was found that any date on the laptop had been altered, that the clock had been changed or that files had been copied onto the laptop after 8 May.

The records support the conclusion that the disputed files were created during the employee's use of the laptop and not by the firm (confidence: high). The firm's handling reduced what could be recovered, and did not alter what is relied on.

02 Instructions and scope

The client is a financial advice firm. An adviser resigned on 24 April 2026 and returned the laptop on 11 May. The firm's office manager and its outsourced IT technician then looked through the laptop before deciding to instruct a forensic examination. In correspondence, the adviser's representative alleged that incriminating files had been "planted" during that period. The client asked five questions.

NO.	QUESTION	SHORT ANSWER
1	When did the employee last use the laptop?	8 May, ending 17:22
2	Who used it afterwards, when, and what did they do?	The firm, on 12, 13 and 20 May. Files were opened and copied out. Nothing was added
3	Were the seven disputed files created before or after return?	Before, between 21 April and 7 May
4	Could dates have been manipulated?	No evidence of it, and several records that would expose it
5	What deleted material can be recovered?	91 of 118 files in full, 9 in part

This report was commissioned by the firm. The examiner's duty is to report what the records show, including findings that are unhelpful to the firm. Several are.

03 How to read this report

Every finding in this report is labelled so that a reader can see at once how much weight it carries.

LABEL	MEANING
Observed fact	Something recorded on the laptop itself. The source record is named, and another examiner working from the same image would find the same thing.
Inference	What the examiner concludes from one or more observed facts. Each inference carries a confidence level.
Unresolved	A question the laptop cannot answer. Where another source could answer it, that source is named.

Confidence levels are used as follows. **High**: several independent records agree and no reasonable alternative fits them. **Medium**: the records support the conclusion, but an alternative explanation remains open. **Low**: the records are consistent with the conclusion and no more. Findings describe actions recorded under a user account. They do not, by themselves, identify the person at the keyboard or the reason for an action.

04 Evidence and method

Exhibit. One Windows 11 Pro laptop with a 512 GB NVMe solid-state drive, protected by BitLocker. It was received on 29 May 2026 with the recovery key. The firm supplied written accounts from the office manager and the IT technician of what each had done.

Imaging. The drive was removed, connected through a hardware write-blocker and imaged in full, including unallocated space. The image was verified by MD5 and SHA-256 hash, with the values held on the case file. All analysis was carried out on a verified working copy.

Analysis. The image was unlocked and processed in our forensic software. File system records were also parsed with a second tool, and the two sets of results were compared for the seven disputed files.

Sources used.

- The System and Security event logs: starts, shutdowns, logons, password changes and clock changes.
- The NTFS master file table, which holds two independent sets of dates for every file, and the USN change journal.
- Volume shadow copies. Windows had kept three earlier snapshots of the drive, dated 14 April, 28 April and 6 May.
- Jump Lists, LNK files, Office recent lists and the documents' own internal properties.
- USB device history, Recycle Bin records, and a deleted-file search of unallocated space.

Times. Converted from UTC to UK time, BST (UTC+1) throughout.

05 Lawful basis and proportionality

The laptop is the client's property and was examined on the client's written instruction for the specific questions listed above. The examination was limited to the stated period and to material relevant to those questions. Personal content found on the laptop was not read beyond what was needed to classify it, and is reported by category and count, not reproduced. The client was advised to record its lawful basis for the examination and to keep this report confidential to those who need it, in line with the Information Commissioner's guidance on monitoring workers. The individual concerned may be entitled to request a copy of personal data held about them, including in this report.

06 Limitations

- **The laptop was used before imaging.** Three sessions and a Windows update took place after return. Each is documented below. Their effect is that some deleted data was overwritten and some log entries were replaced by newer ones.
- **Solid-state storage.** A solid-state drive clears deleted data in the background whenever it is powered. Every hour the laptop was switched on after 8 May reduced what could be recovered.
- **Open, not read.** The records show that a file was opened. They do not show how long it was read for or what was noticed.
- **The USB stick.** The stick used by the IT technician on 13 May was supplied and examined. It holds copies only, and it has not been treated as evidence of the employee's activity.
- **A person is not identified.** Sessions are attributed by account, password events and the written accounts supplied.

07 The boundary: 8 to 12 May

DATE AND TIME (BST)	EVENT	SOURCE
8 May, 16:48 to 17:05	118 files deleted from Documents, Desktop and Downloads	Recycle Bin records; USN journal
8 May, 17:06	Recycle Bin emptied	USN journal
8 May, 17:22	Shutdown, started by the user	System event log
11 May	Laptop handed in at reception	Firm's asset log
12 May, 10:04	Laptop started	System event log
12 May, 10:06	Administrator account logged on	Security event log

OBSERVED FACT

The System event log records no start, wake or logon of any kind between 17:22 on 8 May and 10:04 on 12 May. The daily uptime counter restarts from zero on 12 May.

INFERENCE

The employee's use of the laptop ended at 17:22 on 8 May. Every record dated after that time belongs to the firm's handling. Confidence: high.

08 The firm's handling after return

SESSION	ACCOUNT	WHAT WAS DONE	EFFECT ON THE EVIDENCE
12 May, 10:04 to 11:30	Administrator, by the IT technician	Windows updates installed, two restarts. Employee's password reset at 11:12	About 4 GB of system files replaced. Unallocated space partly overwritten. Older event-log entries displaced
13 May, 09:20 to 10:45	Employee's account, by the office manager and IT technician together	214 files opened or previewed. Six folders copied to a 64 GB USB stick	"Recently opened" lists and file access dates updated. No file created, modified or deleted in the profile
20 May, 14:10 to 14:25	Administrator, by the IT technician	BitLocker recovery key exported. Laptop shut down for dispatch	None of significance

OBSERVED FACT

The Security log records the password reset of the employee's account at 11:12 on 12 May, made from the administrator account. Until that moment only someone who knew the employee's password could log on to that account.

OBSERVED FACT

The change journal for the employee's profile between 12 and 20 May contains entries for access-date updates and for Windows' own housekeeping files. It contains no entry creating, renaming or overwriting any document, spreadsheet, PDF or email file.

OBSERVED FACT

The written accounts of the office manager and the IT technician match the records in every respect except one. The office manager's account does not mention opening the employee's personal folder, `Documents\Private`, in which 31 files were previewed on 13 May.

INFERENCE

The firm's sessions were limited to looking and copying out. Confidence: high. The preview of the personal folder went beyond what was needed, and it is reported here because the employee is entitled to know of it.

09 The seven disputed files

FILE	CREATED	RECORDED IN
`Client_list_export.csv`	21 April, 18:14	File table (both date sets); change journal; browser download record; 28 April snapshot
`Clients_to_contact.xlsx`	22 April, 08:40	File table; change journal; Office recent list; document properties; 28 April snapshot
`Letter_draft_1.docx`	29 April, 12:55	File table; change journal; document properties; 6 May snapshot
`Letter_draft_2.docx`	30 April, 13:10	File table; change journal; document properties; 6 May snapshot
`New_firm_terms.pdf`	5 May, 19:02	File table; change journal; browser download record; 6 May snapshot
`Fee_comparison.xlsx`	6 May, 08:15	File table; change journal; document properties; 6 May snapshot
`Transfer_forms_pack.zip`	7 May, 17:48	File table; change journal

OBSERVED FACT

Six of the seven files are present, with identical content, inside snapshots that Windows made on 28 April and 6 May. A snapshot is a frozen copy of the drive as it was on that date. The firm had no access to the laptop on either date.

OBSERVED FACT

For every file, the two independent sets of dates in the file table agree with each other and with the change journal. Tools that alter file dates change one set and leave the other, and such a mismatch is the usual sign of tampering. No mismatch exists.

OBSERVED FACT

The change journal numbers its entries in sequence. The entries creating the seven files sit in sequence among thousands of ordinary entries from the same days in April and May. Entries cannot be inserted into the past without breaking the sequence, and the sequence is unbroken.

INFERENCE

All seven files were created on the dates shown, during the employee's use of the laptop, and were not placed there after return. Confidence: high.

UNRESOLVED

`Transfer_forms_pack.zip` was created the day after the last snapshot, so it rests on two sources and not four. Its contents, 14 PDF forms, were downloaded individually on 7 May according to the browser's download record.

10 Could the clock have been changed?

OBSERVED FACT
Windows logs every change to the system clock. The log shows only automatic adjustments of less than one second, made by the internet time service. No manual change is recorded in the period.

OBSERVED FACT
Times recorded by outside systems agree with the laptop's own. The download records for two of the files carry the web server's time, and the snapshots carry their own creation times.

INFERENCE
The laptop's clock was accurate throughout and was not set back. Confidence: high.

11 Recovery of deleted files

OUTCOME	FILES	NOTES
Recovered in full	91	Verified by opening each file. Supplied to the client on encrypted media
Recovered in part	9	Fragments only. Mostly large PDFs
Not recoverable	18	Space reused. For six, the reuse is by files installed in the 12 May update
Total deleted on 8 May	118	Names, sizes and original locations known for all 118

OBSERVED FACT
Of the 118 deleted files, 64 were personal: photographs, household documents and a CV. They have been listed for the client by category and count and were not opened.

OBSERVED FACT
Among the 54 work-related files were earlier versions of the two draft letters and a spreadsheet named `Who_is_coming.xlsx`, which was recovered in full.

INFERENCE
Had the laptop been left switched off after 11 May, more would have been recovered: at least the six files overwritten by the update, and probably others cleared by the drive while it was powered. Confidence: high.

A note on Apple laptops

The position differs on a modern Mac. An Apple silicon MacBook's storage is encrypted by hardware and cannot be imaged in full, and space released by a deleted file is cleared at once. The names and times of deletions can usually be reported. The contents of deleted files generally cannot be recovered. Clients with a Mac should expect a report of what was deleted and when, and should not expect the files back.

12 Alternative explanations considered

- **Files were copied onto the laptop from the USB stick.** The stick was first connected at 09:31 on 13 May. All seven files pre-date that by between six and 22 days, and the journal for 13 May shows data moving to the stick only.
- **Dates were forged with a tool.** Addressed above. The two date sets agree, the journal sequence is unbroken and six files exist in earlier snapshots.
- **Someone else used the employee's account before 8 May.** The account was protected by a password known only to the employee until the reset on 12 May. Remote-access software was not installed.
- **The firm's handling destroyed evidence that would have helped the employee.** The handling did overwrite some deleted data. The 18 unrecoverable files are known by name. None appears from its name to bear on the dispute, although that cannot be confirmed without the contents.

13 Conclusions

QUESTION	FINDING	CONFIDENCE
When did the employee last use the laptop?	8 May, ending 17:22	HIGH
What did the firm do afterwards?	Updated Windows, reset a password, opened 214 files, copied six folders out	HIGH
Did the firm add or alter any user file?	No record of it, and records that would show it	HIGH
Were the disputed files created before return?	Yes, all seven	HIGH
Was the clock or any date manipulated?	No evidence of it	HIGH
What was recovered?	91 of 118 deleted files in full, 9 in part	HIGH

14 What we would also ask for

WHAT WE WOULD ASK FOR

The firm's client-management system audit log for 21 April, to confirm the export that produced `Client_list_export.csv` and the account that made it.

WHAT WE WOULD ASK FOR

A fuller written account from the office manager covering the personal folder previewed on 13 May, so that the firm's disclosure is complete.

WHAT WE WOULD ASK FOR

The firm's backup of the laptop, if one exists from before 8 May. It is a further independent copy against which the seven files can be checked.

The lesson of this case applies to every employer. When a concern arises about a returned laptop, do not switch it on, do not let IT "have a look", and do not install updates. Seal it, note who has handled it, and have it imaged first. Looking afterwards, on a copy, loses nothing.

15 Glossary of records relied on

RECORD	WHAT IT IS	WHAT IT CAN AND CANNOT SHOW
Jump Lists and LNK files	Shortcuts Windows creates when a file is opened	The file's path, the times it was opened and the serial number of the volume it was on. Not what was done with the file.
ShellBags	Windows' memory of folders viewed in File Explorer	That a folder existed and was browsed, including on drives no longer attached. Not the folder's contents.
USB device history	Registry keys and the Partition/Diagnostic event log	Make, model and serial of a storage device and each time it was connected. Not what was copied to it.
USN change journal	The file system's own log of changes	Files created, renamed and deleted, with times, until the journal wraps round.
Recycle Bin records	A small index file for each deleted item	Original path, size and deletion time, even after the bin is emptied in some cases.
Prefetch and UserAssist	Program-launch records	That a program ran, when, and how often.
Browser history	History, downloads and saved-login databases	Sites visited, files downloaded, and the accounts signed in. Not what was typed into a page.
Event logs	Windows' system and security logs	Power on and off, logons, and remote-desktop connections. Older entries are overwritten.

16 About this sample report

This document is a sample. It is based on employment casework carried out by our forensic team and shows the structure, depth and wording a client receives. Names, dates, file names, device identifiers and other identifying details have been changed, and findings have been adapted so that no real person or organisation can be recognised. It is not a live case file and should not be relied on as evidence of any event.

Where a report is to be used in court or tribunal proceedings, it is finalised on the instruction of the client's solicitor with the examiner's qualifications and the declaration required in that jurisdiction: Part 35 of the Civil Procedure Rules in England and Wales, the duties of a skilled witness in Scotland, and the expert's declaration required by the High Court's practice directions in Northern Ireland.

Our work follows the four principles of the ACPO Good Practice Guide for Digital Evidence and the handling guidance in ISO/IEC 27037: the original is not altered where that can be avoided, any unavoidable change is recorded and explained, a full record of the work is kept so that another examiner can repeat it, and one named examiner is responsible for the case.

To discuss an examination, call **Easy Data Recovery** on **028 9002 0144** or visit easyrecovery.co.uk. Forsyth House, Cromac Square, Belfast, BT2 8LA.

End of sample report. Easy Data Recovery, Forsyth House, Cromac Square, Belfast, BT2 8LA. 028 9002 0144. easyrecovery.co.uk