Leeds Data Recovery
Professional data recovery and digital forensics

0113 322 3083
leedsdatarecovery.co.uk

SAMPLE DIGITAL FORENSIC REPORT

Were company files copied to an external hard drive?

SCENARIO	Suspected copying of project files to removable storage before leaving
INSTRUCTED BY	An engineering design consultancy (anonymised)
DEVICE	Windows 11 workstation laptop, 1 TB NVMe drive
PERIOD EXAMINED	1 June to 3 July 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 Devices connected
08 The session on 22 June
09 Files opened from the hard drive
10 Other routes checked
11 Attribution
12 Alternative explanations considered
13 Conclusions
14 What we would also ask for
15 Glossary of records relied on
16 About this sample report

01 Summary of findings

A 1 TB portable hard drive that does not belong to the company was connected to the laptop on three evenings in the design engineer's final fortnight. During the longest session, folders with the same names as the company's project folders were created on the drive within seconds of the originals being browsed. Times are UK time (BST).

- **The device.** A Seagate portable hard drive, 1 TB, was connected on 16, 22 and 25 June 2026 for a total of 4 hours 51 minutes. Windows recorded its serial number, so the drive can be matched if it is produced. The serial number is held on the case file.
- **The 22 June session.** Between 18:07 and 20:44 a folder named `Backup\Projects` was created on the drive, followed by 14 sub-folders whose names match 14 of the 31 client project folders in `C:\Projects`. Each source folder was opened in File Explorer in the same minute its namesake appeared on the drive.
- **Files opened from the drive.** Six files were later opened directly from the drive, including two assembly drawings and a costing workbook. Windows recorded the drive's volume serial number in each shortcut, which ties the files to that drive.
- **A second device.** A 32 GB USB stick was also used on most working days. The records show it carrying plot files to the office plotter, which is routine, and it is not a concern.
- **No copy log exists.** Windows does not record which files are copied to a USB drive. The conclusion that project files were copied rests on the matching folder names and timing, not on a single record.

The records support the conclusion that 14 project folders were copied to a personally owned drive on 22 June (confidence: high for the folders, medium for their full contents). What the drive holds now can be established only by examining the drive.

02 Instructions and scope

The client is an engineering design consultancy. A design engineer gave notice on 12 June 2026 and left on 26 June. A colleague reported seeing a portable drive attached to the engineer's laptop after hours. The client asked four questions.

NO.	QUESTION	SHORT ANSWER
1	Which external storage devices were connected, and when?	Two: a 1 TB hard drive on three evenings, and a USB stick on most days
2	Were company files copied to them?	The records support copying of 14 project folders to the hard drive
3	Which projects are affected?	The 14 listed in this report
4	Was any other route used to remove data?	None found

The examination was limited to 1 June to 3 July 2026 and to the engineer's Windows profile and the `C:\Projects` working folder.

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 workstation laptop with a 1 TB NVMe solid-state drive. It was received on 6 July 2026 in a sealed bag. The client stated that the laptop had been locked in a cabinet since the engineer's last day and had not been switched on.

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 against the source, and the values are held on the case file with the chain-of-custody record. All analysis was carried out on a verified working copy.

Analysis. The image was processed in our forensic software, and the USB findings were checked by reading the underlying registry keys and event log directly.

Sources used.

- USB device history: the registry's device records and the Partition/Diagnostic event log, which adds an entry each time a storage device is connected or removed.
- ShellBags, which record folders viewed in File Explorer, including folders on drives that are no longer attached.
- LNK shortcut files and Jump Lists, which record files opened and the serial number of the volume they were on.
- The NTFS master file table and USN change journal for the laptop's own drive.

- Browser history and installed-program records, to check for other routes.

Times. Windows stores these records in UTC. This report converts to UK time, BST (UTC+1) throughout the period.

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

- **No list of copied files.** Neither Windows nor macOS keeps a log of files copied to removable storage. Copying is established here by correlating several records. This is standard practice, and its limits are stated with each finding.
- **Folder records, not file records.** ShellBags record folders that were displayed in File Explorer. They show that a folder existed on the drive and when it was first seen there. They do not list the files inside it.
- **The drive has not been examined.** The drive itself would show exactly what was copied, when, and whether it has since been opened on another computer.
- **Event log retention.** The connection log on this laptop reaches back to 2 March 2026. Earlier connections of the same drive, if any, are not recorded there.
- **A person is not identified.** The records show activity under the engineer's Windows account. Attribution is addressed separately below.

07 Devices connected

Two USB storage devices were connected in the period. Phones, keyboards and other non-storage devices are excluded.

DEVICE	CONNECTED	ASSESSMENT
Seagate portable hard drive, 1 TB, volume label `BACKUP_HD`	16 June 17:52 to 18:31; 22 June 18:07 to 20:44; 25 June 17:40 to 19:15	Not a company asset. First ever connection to this laptop was 16 June, four days after notice was given
USB stick, 32 GB, volume label `PLOTS`	19 of 20 working days, usually for under ten minutes mid-morning	Company stick used to carry plot files to the large-format plotter. Routine

OBSERVED FACT

The registry records the hard drive's first installation on this laptop at 17:52 on 16 June 2026. The connection log contains no earlier entry for its serial number.

OBSERVED FACT

The client's asset register, supplied for comparison, lists the `PLOTS` stick and does not list any Seagate drive.

INFERENCE

The hard drive is a personally owned device that was first used with this laptop after notice was given. Confidence: high.

08 The session on 22 June

The office closes at 17:30. The door-access record supplied by the client shows the engineer leaving at 20:51 on 22 June.

TIME (BST)	EVENT	SOURCE
18:07:22	Hard drive connected; assigned drive letter E:	Connection log; registry
18:09	`E:\Backup` and `E:\Backup\Projects` first displayed	ShellBags
18:10 to 18:58	Six project folders opened in `C:\Projects`; a folder of the same name appears under `E:\Backup\Projects` within 60 seconds of each	ShellBags (both volumes)
19:02 to 19:20	No folder activity. Laptop awake, mains power	Event log
19:21 to 20:36	A further eight project folders opened in `C:\Projects`, each followed by a matching folder on E:	ShellBags (both volumes)
20:38	`E:\Backup\Standards` and `E:\Backup\Templates` first displayed	ShellBags
20:44:05	Hard drive removed	Connection log
20:46	Laptop shut down	Event log

OBSERVED FACT

Fourteen folder names under `E:\Backup\Projects` are identical, character for character, to 14 folder names in `C:\Projects`. Each name combines a client code and a project number, so a chance match is not credible.

OBSERVED FACT

The 14 source folders hold 9,860 files totalling 61 GB. At typical speeds for this type of drive, copying 61 GB takes between one and two hours. The session lasted 2 hours 37 minutes.

INFERENCE

The 14 project folders were copied from the laptop to the hard drive during this session. The matching names, the one-for-one timing and the time available all point the same way. Confidence: high that the folders were created on the drive; medium that every file inside them was copied, because folder records do not list files.

UNRESOLVED

Whether the copies were complete, and whether any files were later removed from the drive. Only the drive can show this.

09 Files opened from the hard drive

On 25 June, the third session, six files were opened directly from the hard drive. Opening a file from a location proves the file was there.

TIME (BST)	FILE OPENED FROM E:	SOURCE
17:48	`Backup\Projects\[client code]-2291\GA-2291-014_revC.dwg`	LNK file; Jump List
17:53	`Backup\Projects\[client code]-2291\GA-2291-015_revB.dwg`	LNK file; Jump List
18:05	`Backup\Projects\[client code]-2304\Costing_2304_v7.xlsx`	LNK file; Office recent list
18:22	`Backup\Standards\Weld_procedure_library.pdf`	LNK file
18:40	`Backup\Templates\Titleblock_master.dwt`	LNK file
19:02	`Backup\CV and references\CV_June2026.docx`	LNK file; Office recent list

OBSERVED FACT

Each shortcut records the volume serial number of the drive the file was opened from. All six carry the same volume serial number, and it matches the volume recorded when the Seagate drive was connected. The drive type is recorded as "fixed", which is how Windows describes portable hard drives.

OBSERVED FACT

The drawing and costing files above have the same names, sizes and last-modified times as files still present in `C:\Projects` on the laptop.

INFERENCE

Copies of company drawings, a costing workbook, the weld procedure library and the drawing template were on the hard drive by 25 June. Confidence: high. The presence of a CV folder on the same drive supports the view that the drive is a personal one.

10 Other routes checked

The client asked whether data left by any other route. The following were examined and nothing of concern was found.

ROUTE	WHAT WAS CHECKED	RESULT
Cloud storage	Installed programs, sync-client folders, browser history for storage and file-transfer sites	Company OneDrive only. No personal cloud storage or transfer site used
Webmail	Browser history for personal mail services	A personal mailbox was read on nine days. No compose page was open on 16, 22 or 25 June
Messaging apps	Installed apps and their transfer folders	Microsoft Teams only
Printing	Print-job history	Normal volumes. No large print runs in the final fortnight
The `PLOTS` stick	Folders seen and files opened on it	Plot files only, matching the plotter's job log
Deletion	Recycle Bin, change journal, cleaning tools	No bulk deletion and no cleaning tool run

OBSERVED FACT

No attempt to conceal the hard-drive sessions was found. Nothing was deleted in bulk, no history was cleared and no cleaning tool was run.

11 Attribution

- The laptop was unlocked with the engineer's password at 18:05 on 22 June and was not locked again until shutdown.
- During the 19:02 to 19:20 gap, the engineer's company mailbox was open in the browser and two emails were sent from it, according to the page titles.

- The door-access record places the engineer in the building until 20:51, five minutes after the laptop shut down. The client states that no other member of staff was present after 18:15.

INFERENCE
The engineer was the person using the laptop during the 22 June session. Confidence: high.

12 Alternative explanations considered

- **An authorised backup.** Some firms ask staff to back up work before leaving. The client states that no such instruction was given, that project data is backed up centrally, and that personal storage devices are prohibited by its IT policy, which the engineer signed.
- **Personal files only.** The drive held a CV folder, and removing personal files is reasonable. The folder names and the six opened files show that company material was also on the drive.
- **Folders created but nothing copied.** It is possible to create empty folders. Fourteen empty folders with exact project names would serve no purpose, and files were later opened from two of them.
- **Work taken home to finish.** The engineer's remaining tasks, listed by the client, concerned three projects. Fourteen were copied, including four that had been closed for more than a year.

13 Conclusions

QUESTION	FINDING	CONFIDENCE
Which devices were connected?	A personal 1 TB hard drive on 16, 22 and 25 June; a company USB stick daily	HIGH
Were company files copied to them?	Fourteen project folders, two library folders and named files were on the hard drive	HIGH
Was every file in those folders copied?	Likely, given the time taken, but not shown by the laptop	MEDIUM
Was another route used?	No evidence of one	HIGH
Who was using the laptop?	The engineer	HIGH

14 What we would also ask for

WHAT WE WOULD ASK FOR
The hard drive itself. If it is produced, we can image it, list every file on it with dates, and report whether it has been connected to other computers since 25 June. The serial number recorded by the laptop will confirm it is the same drive.

WHAT WE WOULD ASK FOR

The file server's access log for the 14 projects, if the server keeps one, to show whether the same projects were also opened from elsewhere.

WHAT WE WOULD ASK FOR

A list of the 14 projects' clients and commercial value, which the client's solicitor may need in order to assess the seriousness of the loss.

Recovering the drive from a former employee is a legal step. The client's solicitor can advise on a request for delivery up or an undertaking, and this report is written so that it can support such a request.

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 in England and Wales, it is finalised on the instruction of the client's solicitor with the examiner's qualifications, a statement of the instructions received and the declaration and statement of truth required by Part 35 of the Civil Procedure Rules.

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 **Leeds Data Recovery** on **0113 322 3083** or visit leedsdatarecovery.co.uk. 17th Floor, The Pinnacle, Albion Street, Leeds, LS1 5AA.

End of sample report. Leeds Data Recovery, 17th Floor, The Pinnacle, Albion Street, Leeds, LS1 5AA. 0113 322 3083. leedsdatarecovery.co.uk