NEWCASTLE DATA RECOVERY

SAMPLE DIGITAL FORENSIC REPORT

Did the laptop connect to company systems after the employee left?

SCENARIO	Suspected remote access to company servers after termination of employment
INSTRUCTED BY	A logistics and distribution company (anonymised)
DEVICE	Windows 11 business laptop, 256 GB NVMe drive
PERIOD EXAMINED	1 February to 16 March 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 Remote access during employment
08 Connections after 20 February
09 What the sessions showed
10 How access remained possible
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

Newcastle Data Recovery
Rotterdam House, 2nd Floor, 116 Quayside, Newcastle, NE1 3DY

0191 406 1051
newcastle-datarecovery.co.uk
Mon–Fri 9am–5:30pm

01 Summary of findings

The laptop made remote-desktop connections to two company servers on three dates after the IT administrator's employment ended on 20 February 2026. The laptop was still in the former employee's possession on those dates. Times are UK time (GMT).

- **Connections after leaving.** The remote-desktop client connected to the company's finance server on 23 February and 2 March, and to its file server on 2 and 9 March. The company's VPN client connected first on each occasion.
- **What was on screen.** Windows keeps small cached image tiles of remote sessions. Tiles recovered from the 2 March session show part of a file-browser window on the finance server and a folder named `Payroll 2026`.
- **Saved credentials.** The laptop held saved remote-desktop credentials for both servers under a shared administrator account name, not the former employee's own account.
- **Files brought back.** Three files were saved to the laptop during the 2 March session: two spreadsheets and a PDF, in a folder named `tmp_srv`. They were deleted on 10 March and two were recovered.
- **Before leaving.** Remote connections to the same servers were routine during employment, at 61 sessions in the three weeks examined. That is consistent with the role.
- **What the laptop cannot show.** The laptop proves that it connected and that a session was displayed. Proof of a successful logon, and of what was opened or changed on the servers, comes from the servers' own logs.

The records support the conclusion that the former employee's laptop was used to open remote sessions on company servers on three dates after employment ended (confidence: high), using a shared administrator account that had not been disabled.

02 Instructions and scope

The client is a logistics company. Its IT administrator was dismissed on 20 February 2026 and returned the company laptop by courier on 12 March. During that period the finance team reported that a payroll folder had been reorganised. The client asked five questions.

NO.	QUESTION	SHORT ANSWER
1	Did this laptop connect to company systems after 20 February?	Yes, on 23 February, 2 March and 9 March
2	Which systems?	The finance server and the file server, through the VPN
3	What was done during those sessions?	Partly shown: a payroll folder was on screen, and three files were saved to the laptop
4	How was access possible after dismissal?	A shared administrator account and a VPN profile were still valid
5	Was anything hidden?	Three files were deleted before the laptop was returned

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 256 GB NVMe solid-state drive, not encrypted. It arrived at the client's office by courier on 12 March 2026 and was forwarded to us unopened, in the courier's packaging, on 16 March.

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, and the values are held on the case file. All analysis was carried out on a verified working copy.

Analysis. The image was processed in our forensic software. Remote-desktop cache tiles were extracted and reassembled with a specialist tool, and each reassembled image is exhibited on the case file with the tiles it was built from.

Sources used.

- The remote-desktop client's registry records, which list servers connected to and the user name last used for each.
- The remote-desktop client's event log, which records each connection attempt with the destination and time.
- The remote-desktop bitmap cache, which holds small image tiles of what was displayed.
- The VPN client's log file and Windows' network connection history.
- Windows Credential Manager, which lists saved credentials. Passwords were not extracted.
- Jump Lists, LNK files, the USN change journal, Recycle Bin records and a deleted-file search.

Times. Converted from UTC. GMT applied throughout the period, so UTC and UK time are the same.

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

- **A connection is not a logon.** The laptop's records show that the remote-desktop client reached a server and, where cache tiles exist, that a desktop was displayed. The definitive record of a successful logon, its account and its duration is on the server.
- **Cache tiles are fragments.** The cache holds small squares of the screen, without times, and overwrites the oldest. Reassembly is partial. A tile can be tied to a session only where the cache file's own dates allow it.
- **Server-side actions are not recorded here.** Files opened, moved or changed on a server during a remote session leave no trace on the laptop unless they were copied back to it.
- **The laptop was out of the client's control.** Between 20 February and 12 March the laptop was at the former employee's home. Anyone with access to it there could have used it. Attribution is addressed below.

- **Passwords were not tested.** We did not attempt to use any saved credential against the client's live systems.

07 Remote access during employment

To judge the later sessions fairly, the three weeks before 20 February were examined first.

MEASURE	1 TO 20 FEBRUARY
Remote-desktop sessions to the finance server	22, on 12 working days
Remote-desktop sessions to the file server	39, on 14 working days
Typical time of day	08:30 to 17:45, with four evening sessions for patching
Account name used	The employee's own administrator account in 58 sessions; the shared administrator account in 3
VPN used	Only when working from home, on 5 days

OBSERVED FACT
Remote administration of both servers was a normal part of the role, and nothing in the pattern before 20 February is unusual.

OBSERVED FACT
The employee's own administrator account was disabled by the client at 16:10 on 20 February, according to the client's IT provider. The shared administrator account and the VPN profile were not changed until 11 March.

08 Connections after 20 February

DATE AND TIME (GMT)	EVENT	SOURCE
23 Feb, 19:42	VPN connected from a home broadband address	VPN client log
23 Feb, 19:44	Remote-desktop connection to the finance server, user name: shared administrator account	RDP event log; registry
23 Feb, 19:51	VPN disconnected	VPN client log
2 Mar, 20:15	VPN connected	VPN client log
2 Mar, 20:17 to 21:03	Remote-desktop connection to the finance server	RDP event log
2 Mar, 20:31 to 20:38	Three files created in `C:\Users\…\Documents\tmp_srv`	USN journal
2 Mar, 21:05 to 21:20	Remote-desktop connection to the file server	RDP event log
2 Mar, 21:22	VPN disconnected	VPN client log
9 Mar, 07:58	VPN connected	VPN client log
9 Mar, 08:00 to 08:06	Remote-desktop connection to the file server	RDP event log
9 Mar, 08:07	VPN disconnected	VPN client log
10 Mar, 18:30	`tmp_srv` folder and its three files deleted; Recycle Bin emptied	Recycle Bin records; USN journal

OBSERVED FACT

The remote-desktop client's event log records a connection to each server's internal address at the times shown, and the VPN log shows the tunnel up for the whole of each session. Internal addresses cannot be reached without the VPN.

OBSERVED FACT

The registry records the shared administrator account as the user name last used for both servers. Before 20 February it recorded the employee's own account.

INFERENCE

On three dates after dismissal, this laptop established VPN and remote-desktop connections to company servers using an account that still worked. Confidence: high.

09 What the sessions showed

The bitmap cache file was last written at 21:20 on 2 March and again at 08:06 on 9 March. Tiles could be reassembled into 14 partial screen images.

IMAGE	WHAT IS LEGIBLE	SESSION IT IS TIED TO
1 to 4	The finance server's desktop and a file-browser window. Address bar text ending `\Finance\Payroll\2026`	2 March, by cache file date
5	Part of a file list with names beginning `Payrun_Feb` and `Payrun_Mar`	2 March
6 to 9	A spreadsheet window. Column headings legible; cell contents are not	2 March
10 to 12	The file server's desktop and a window listing shared folders	2 or 9 March. Cannot be separated
13 and 14	A system window titled "Computer Management", showing a list of user accounts	9 March, by cache file date

OBSERVED FACT

The three files saved to `tmp_srv` on 2 March were `Payrun_Feb_2026.xlsx`, `Staff_list_current.xlsx` and `Contract_template.pdf`. The first two were recovered from unallocated space. They have been returned to the client and are not reproduced here because they contain personal data.

INFERENCE

During the 2 March session the payroll folder on the finance server was browsed and at least three files were copied from the server to the laptop. Confidence: high.

INFERENCE

The 9 March session included a view of user accounts on the file server. This is consistent with checking whether access was still available. Confidence: low, because two tiles are a thin basis.

UNRESOLVED

Whether the payroll folder was reorganised from this laptop. Moving folders on the server leaves no record on the laptop.

10 How access remained possible

ITEM	STATE ON THE LAPTOP	RELEVANCE
VPN profile	Installed in 2024, certificate valid to 2027	Allowed the laptop onto the company network from anywhere
Shared administrator credential, finance server	Saved in Credential Manager on 6 January 2026	Allowed logon without typing a password
Shared administrator credential, file server	Saved in Credential Manager on 6 January 2026	As above
Employee's own administrator credential	Saved; rejected after 20 February	Two failed attempts are logged on 23 February at 19:43

OBSERVED FACT

On 23 February the remote-desktop client first tried the employee's own account, which was refused twice, and one minute later connected with the shared account.

INFERENCE

The person using the laptop found that their own account had been disabled and switched to the shared account. Confidence: high.

11 Attribution

The laptop was at the former employee's home, so this question matters more than usual.

- Each session began with a Windows logon using the former employee's password. The account has no other credential.
- On 2 March, between the two remote sessions, the former employee's personal webmail was opened in the browser for two minutes.
- The home broadband address in the VPN log is the same on all three dates and matches the address from which the employee worked from home during employment.
- No evidence was found of another person's accounts or files on the laptop.

INFERENCE

The former employee was the person using the laptop on 23 February, 2 March and 9 March. Confidence: medium to high. The password logon and the personal webmail point to the former employee. Use by another member of the household who knew the password cannot be excluded from the laptop alone.

12 Alternative explanations considered

- **Finishing or handing over work.** The client states that no handover was requested after dismissal, and none of the sessions was followed by any communication to the client.
- **Automatic reconnection.** The remote-desktop client does not connect by itself. Each session required the VPN to be started by hand and the client to be launched, and both launches are recorded.
- **Retrieving personal documents.** The files copied were a payroll run, a staff list and a contract template, taken from company servers.
- **Checking that access had been removed.** This could explain the short sessions on 23 February and 9 March. It does not explain the 46-minute session on 2 March or the copied files.

13 Conclusions

QUESTION	FINDING	CONFIDENCE
Did the laptop connect to company systems after 20 February?	On 23 February, 2 March and 9 March	HIGH
Which systems?	The finance server and the file server, through the VPN	HIGH
What was done?	The payroll folder was browsed and three files were copied to the laptop on 2 March	HIGH
Were server files changed?	Not determinable from the laptop	LOW
How was access possible?	A shared administrator account and VPN profile remained valid until 11 March	HIGH
Was anything hidden?	The copied files were deleted on 10 March, two days before the laptop was returned	HIGH

14 What we would also ask for

WHAT WE WOULD ASK FOR

The Security and remote-desktop logs from both servers for 20 February to 11 March. They record each successful logon, the account, the source address and the session length, and are the definitive record. Server logs overwrite themselves, so they should be exported now.

WHAT WE WOULD ASK FOR

The VPN gateway's connection log for the same period, to confirm the home address and to show whether any other device connected with the same profile.

WHAT WE WOULD ASK FOR

File-server audit records or shadow copies for the payroll folder, to show when it was reorganised and by which account.

Unauthorised access to a computer after permission has ended may be a criminal matter as well as a civil one. Whether to report it is for the client and its advisers. If a report is made, this laptop and its image should be kept unchanged, and we can provide a statement of continuity.

The findings also carry a practical lesson. Shared administrator accounts and long-lived VPN profiles should be changed on the day a system administrator leaves.

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 **Newcastle Data Recovery** on **0191 406 1051** or visit newcastle-datarecovery.co.uk. Rotterdam House, 2nd Floor, 116 Quayside, Newcastle, NE1 3DY.

End of sample report. Newcastle Data Recovery, Rotterdam House, 2nd Floor, 116 Quayside, Newcastle, NE1 3DY. 0191 406 1051. newcastle-datarecovery.co.uk