SAMPLE DIGITAL FORENSIC REPORT

Was the client list taken before the resignation?

SCENARIO	**Suspected removal of a client database by a departing account manager**
INSTRUCTED BY	**A recruitment agency (anonymised)**
DEVICE	**Windows 11 business laptop, 512 GB NVMe drive, BitLocker enabled**
PERIOD EXAMINED	**1 August to 18 September 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 export on 1 September
08 What happened to the archive
09 Contact with the new employer
10 Attribution
11 Alternative explanations considered
12 Conclusions
13 What we would also ask for
14 Glossary of records relied on
15 About this sample report

01 SUMMARY OF FINDINGS

The laptop records show that the agency's client and contact database was exported from the web-based CRM on the evening of 1 September 2026, two days before the account manager resigned. The export was saved, opened, renamed and placed in a compressed archive within 25 minutes. Times are UK time (BST).

- **Export.** Two files were downloaded from the CRM in the Edge browser at 18:42 and 18:44: `Client_Export_2026-09-01.csv` (4.1 MB) and `Contacts_All_Active.xlsx` (2.7 MB). The CRM's export page was not visited at any other time in the 90 days of browser history that survive.
- **Handling.** Both files were opened in Excel, then moved from Downloads to a new folder, `Documents\Personal\Misc`. At 19:06 they were added to an archive named `house_docs.zip`, and the two originals were deleted.
- **Personal webmail.** A personal Outlook.com mailbox was open in a second browser profile from 18:55 to 19:14. The message-compose page was open at 19:08, two minutes after the archive was created. The laptop does not record what, if anything, was attached.
- **No removable media.** No USB storage device was connected between 20 August and the date the laptop was returned. No personal cloud-storage app was installed.
- **Competitor contact.** The careers page of a named competitor and a LinkedIn message thread with one of its directors were viewed on 12 occasions between 24 August and 2 September.
- **After the resignation.** The archive `house_docs.zip` was deleted on 17 September, the last working day, and the Recycle Bin was emptied. The archive was recovered from the image and contains the two export files.

The records support the conclusion that the export was made and packaged under the account manager's Windows account for a purpose other than normal work (confidence: high). Whether the archive left the laptop by email is a medium-confidence inference that the CRM and mail providers' own logs can confirm or exclude.

02 INSTRUCTIONS AND SCOPE

The client is a recruitment agency. An account manager resigned on 3 September 2026 and left on 17 September to join a competitor. The client asked five questions.

NO.	QUESTION	SHORT ANSWER
1	Was client or candidate data exported from the CRM before the resignation?	Yes, on 1 September at 18:42 and 18:44
2	What was done with any exported data?	Opened, moved, archived, originals deleted
3	Did it leave the laptop, and how?	Not by USB or cloud app. Email is possible and unconfirmed
4	Was there contact with the new employer during employment?	Yes, from 24 August
5	Was anything deleted before the laptop was handed back?	Yes, on 17 September

The examination was limited to the period 1 August to 18 September 2026 and to the account manager's Windows profile.

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 business laptop with a 512 GB NVMe solid-state drive, protected by BitLocker. It was received sealed on 21 September 2026, and the client's IT provider supplied the BitLocker recovery key. The client confirmed in writing that the laptop had not been switched on since it was collected from the account manager on 18 September.

Imaging. The drive was removed and connected through a hardware write-blocker. A full bit-for-bit image was taken, including unallocated space, and verified by MD5 and SHA-256 hash against the source. The hash values and the chain-of-custody record are held on the case file. All analysis was carried out on a verified working copy.

Analysis. The image was unlocked with the recovery key and processed in our forensic software. Key findings were checked against a second parser so that no finding rests on one tool's reading of a record.

Sources used.

- Edge and Chrome history, download records and saved-login lists, for both browser profiles.
- Jump Lists, LNK shortcut files, Office recent-document lists and ShellBags.
- The NTFS master file table and USN change journal, which between them record file creation, renaming, moving and deletion.
- Recycle Bin index records, Prefetch program-launch records and the USB device history.
- A deleted-file search of unallocated space.

Times. Windows stores most times in UTC. This report converts them to UK time, which was BST (UTC+1) throughout the period. The laptop's clock was checked against the image metadata and was accurate to within a few seconds.

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 download is not a row count.** The laptop shows that two export files were downloaded and how large they were. The number of records exported, and the filters applied, are recorded by the CRM itself.
- **Webmail content is not stored locally.** Browser history shows which pages of a webmail service were open and when. It does not record the recipient, the text or the attachments of a message.
- **Browser history is limited to 90 days.** Edge discards older visits. Activity before mid-June 2026 cannot be assessed from history, although downloads and saved logins go back further.
- **Other devices are out of scope.** A phone photograph of a screen, or a CRM login from a home computer, would leave no trace on this laptop.

- **A person is not identified.** The records show activity under one Windows account, protected by a password and a fingerprint. They do not prove who was at the keyboard. Attribution is addressed as a separate finding below.

07 THE EXPORT ON 1 SEPTEMBER

The account manager's diary, supplied by the client, shows the last client meeting of 1 September ending at 17:30. The laptop was then idle until 18:38.

TIME (BST)	EVENT	SOURCE
18:38	Laptop unlocked by fingerprint	Security event log
18:40	CRM opened in Edge; page title "Reports: Data export"	Edge history
18:42:17	`Client_Export_2026-09-01.csv` downloaded to Downloads, 4.1 MB	Edge downloads; USN journal
18:44:03	`Contacts_All_Active.xlsx` downloaded to Downloads, 2.7 MB	Edge downloads; USN journal
18:45 to 18:53	Both files opened in Excel	Office recent list; Jump List
18:55	Second Edge profile opened; personal Outlook.com inbox loaded	Edge history
18:58	Folder `Documents\Personal\Misc` created; both files moved into it	USN journal; ShellBags
19:06:41	`house_docs.zip` created in the same folder, 1.9 MB	USN journal; Prefetch
19:07	Both export files deleted, bypassing the Recycle Bin	USN journal
19:08	Outlook.com compose page open	Edge history
19:14	Outlook.com tab closed; laptop locked at 19:16	Edge history; event log

OBSERVED FACT

The download records name the CRM's export address as the source of both files, and the USN journal shows each file created in Downloads at the second the download finished. The two records come from different parts of the system and agree.

OBSERVED FACT

The export page appears once in the surviving history. On the 58 other working days in that history, the CRM was used for individual candidate and client records only.

INFERENCE

The export was a deliberate, one-off act and not part of the account manager's routine use of the CRM. Deleting the originals with Shift+Delete, which skips the Recycle Bin, and giving the archive an unrelated name, are both consistent with an intention that the files should not be noticed. Confidence: high.

UNRESOLVED

How many records the two files held when exported. The CRM's audit log records each export, the user, the filters and the row count, and should be requested from the CRM supplier.

08 WHAT HAPPENED TO THE ARCHIVE

The archive remained in `Documents\Personal\Misc` until the last working day. It was not opened again on the laptop.

DATE AND TIME	EVENT	SOURCE
1 Sept, 19:06	`house_docs.zip` created	USN journal
1 Sept, 19:08	Outlook.com compose page open in the personal profile	Edge history
2 Sept, 08:12	Outlook.com "Sent items" page viewed for under a minute	Edge history
17 Sept, 16:31	`house_docs.zip` and the folder `Misc` sent to the Recycle Bin	Recycle Bin index
17 Sept, 16:33	Recycle Bin emptied: 41 items	USN journal
17 Sept, 16:40	Edge history for the personal profile cleared from 16:00 onwards	Edge history gap; USN journal

OBSERVED FACT

A deleted-file search recovered `house_docs.zip` intact from unallocated space. Its SHA-256 hash is recorded on the case file. It contains two files whose names and sizes match the two downloads of 1 September. The recovered files have been supplied to the client separately and are not reproduced here.

OBSERVED FACT

No USB storage device was connected between 20 August and 18 September. The only cloud-storage app installed is the company's own OneDrive, and the archive's folder was outside the synced area. No file-transfer website appears in either browser profile.

INFERENCE

The sequence of archive creation at 19:06, the compose page at 19:08 and a visit to Sent items the next morning is consistent with the archive having been emailed from the personal mailbox. The laptop holds no record of the attachment itself. Confidence: medium.

UNRESOLVED

Whether a message with an attachment was sent at about 19:08 on 1 September. Only the mailbox holder or the mail provider can show this. It is a matter on which the client's solicitor can advise.

09 CONTACT WITH THE NEW EMPLOYER

The client asked whether contact with the competitor began during employment. The findings below are limited to that question, and other personal browsing was not reviewed.

DATE	WHAT THE RECORDS SHOW	SOURCE
24 Aug	Competitor's "Careers" page viewed twice in the personal profile	Edge history
25 to 28 Aug	LinkedIn message thread with a director of the competitor opened on four days	Edge history (page titles)
27 Aug	`CV_2026_final.docx` opened from Downloads	Jump List
1 Sept, 12:20	A PDF titled "Offer letter" downloaded from Outlook.com and opened	Edge downloads; Jump List
2 Sept	LinkedIn thread opened twice	Edge history
3 Sept, 09:05	`Resignation.docx` created in Documents	USN journal

OBSERVED FACT

The offer letter was downloaded at 12:20 on 1 September. The CRM export followed at 18:42 the same day, and the resignation letter was created two days later.

INFERENCE

The export was made after an offer of employment had been received from the competitor and before notice was given. Confidence: high. The content of the LinkedIn messages and of the offer letter was not examined.

10 ATTRIBUTION

All of the activity above took place under one Windows account, which is the account issued to the account manager.

- The laptop was unlocked by fingerprint at 18:38 on 1 September. One fingerprint identity is enrolled for the account.
- The personal Outlook.com mailbox and the LinkedIn account used in the second browser profile are in the account manager's own name, according to their page titles and saved-login entries.

- The diary supplied by the client places the account manager in the office until at least 17:30 that day, and no other user account was logged on.

> INFERENCE
> The account manager was the person using the laptop between 18:38 and 19:16 on 1 September. Confidence: high. A fingerprint unlock followed by use of personal accounts in the same session leaves little room for another user.

11 ALTERNATIVE EXPLANATIONS CONSIDERED

- **A legitimate export for work.** Account managers may run reports. This was the only use of the export page in 90 days, it was made outside working hours, and the files were renamed, archived under an unrelated name and deleted. No report, mailshot or handover document using the data was created.
- **A handover file.** A handover would normally be stored where colleagues could find it. The archive was stored in a personal folder and deleted on the last day.
- **Tidying up before returning the laptop.** Removing personal files before handing back a laptop is common and is not in itself suspicious. Here the deleted material included company data, and the browser history of the personal profile was also cleared.
- **Someone else used the laptop.** Addressed under Attribution above.

12 CONCLUSIONS

QUESTION	FINDING	CONFIDENCE
Was data exported from the CRM before the resignation?	Two export files were downloaded on 1 September at 18:42 and 18:44	HIGH
What was done with it?	Opened, moved to a personal folder, archived as `house_docs.zip`, originals deleted	HIGH
Did it leave the laptop?	Not by USB or cloud app. The timing fits an email from a personal mailbox	MEDIUM
Was there contact with the new employer during employment?	From 24 August, with an offer letter on 1 September	HIGH
Was anything deleted before the laptop was returned?	The archive, 40 other items and part of the browser history, on 17 September	HIGH

13 WHAT WE WOULD ALSO ASK FOR

The laptop is one source. Three others would turn the medium-confidence finding into a firm answer.

> **WHAT WE WOULD ASK FOR**
> The CRM supplier's audit log for the account between 1 August and 17 September. It will show each export, the filters used and the number of records, and any logins from addresses other than the office.

> **WHAT WE WOULD ASK FOR**
> The company's Microsoft 365 audit log for the same period, to exclude the company mailbox and OneDrive as routes out, and to confirm the office sign-in times.

> **WHAT WE WOULD ASK FOR**
> Any company phone issued to the account manager. Messaging and photo records on a phone often complete the picture.

The client should also preserve the recovered archive and this laptop unchanged until its solicitor has advised on next steps. Requests to a personal mail provider or to the former employee are legal steps and are outside the scope of a forensic report.

14 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.

15 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 **Manchester Data Recovery** on **0161 871 0788** or visit manchester-datarecovery.co.uk. Peter House, Oxford Street, Manchester, M1 5AN.

End of sample report. Manchester Data Recovery, Peter House, Oxford Street, Manchester, M1 5AN. 0161 871 0788. manchester-datarecovery.co.uk