SAMPLE DIGITAL FORENSIC REPORT

What was deleted from the MacBook on the last morning?

SCENARIO	**Deletion of files, an app and browsing history shortly before a dismissal meeting**
INSTRUCTED BY	**A property management company (anonymised)**
DEVICE	**Apple MacBook Air, Apple silicon, 256 GB, FileVault enabled**
PERIOD EXAMINED	**7 to 10 September 2026, with a focus on the morning of 10 September**
METHOD	**Forensic logical image of the data volume, analysed with our Mac forensic system**

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 morning of 10 September
08 What was in the Trash
09 The renewals tracker
10 The shared folders
11 After 10 September
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

Between about 10:04 and 10:40 on 10 September 2026 the MacBook records a concentrated period of deletion and clearing under the office manager's user account. Times are UK time (BST) and are accurate to the few-minute window of the system log that recorded them.

- **Trash.** The Trash was emptied twice, at about 10:13 (48 items) and about 10:27 (39 items). The names of the deleted items survive. Their contents do not.
- **A company spreadsheet.** `tenancy_renewals_tracker_2026.numbers` was deleted from the company's shared cloud folder at about 10:13, roughly ten minutes before the company's own removal of access reached the laptop. It was not renamed or moved.
- **Browsing history.** Safari's Clear History function ran at about 10:20 and again at about 10:28. About 21,500 cached website files were removed. No browsing history survives for any date.
- **An app.** A messaging app was moved to the Trash at about 10:20 and deleted at the second emptying.
- **USB drive.** A 32 GB USB drive was connected at 09:36 and removed at about 10:34. A file with the same name as the deleted spreadsheet was opened from it. The Mac does not record what was copied to or from the drive.
- **Not attributed to the user.** The shared cloud folders "Lettings" and "Accounts" (41,300 files) disappeared from the laptop between 10:23 and 10:39. The managing director has confirmed that he removed the office manager's access that morning, and the records are consistent with that.

The deletion and clearing were carried out under the office manager's account while that account was in active use (confidence: high). The records do not show why. A person clearing personal material from a work laptop is one explanation, and it does not account for the deleted company spreadsheet.

02 INSTRUCTIONS AND SCOPE

The client is a property management company. Its office manager was dismissed at a meeting on the morning of 10 September 2026. The managing director believed that the office manager had learned of the meeting in advance. The client asked five questions.

NO.	QUESTION	SHORT ANSWER
1	Were files deleted on 10 September, and which?	Yes. 87 items emptied from the Trash, and one spreadsheet deleted from the shared folder
2	Was a USB drive used?	Yes, from 09:36 to about 10:34
3	Were any apps removed?	One messaging app
4	Was browsing history cleared?	Yes, twice
5	Who removed the shared folders?	The company, by withdrawing access

The three working days before 10 September were examined for comparison.

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 Apple MacBook Air with Apple silicon and a 256 GB internal drive, FileVault enabled, with one user account. It was received on 6 October 2026. The client supplied the login password and disclosed two occasions on which the laptop had been handled since 10 September. Both are dealt with below.

Imaging. The storage in an Apple silicon Mac is soldered to the logic board and encrypted by hardware that cannot be bypassed, so the drive cannot be removed and copied as a Windows laptop drive can. A forensic logical image of the data volume was taken instead, with the Mac

running and unlocked. This copies every file and system record that exists on the volume. The image was hashed with SHA-256 on completion, and the value is held on the case file. All analysis was carried out on a working copy.

Analysis. The working copy was analysed with our Mac forensic system, which was also used to verify the image hash and to browse the file system.

Sources used.

- File system event logs (FSEvents), which record files created, renamed, moved and removed. Each event is timed by the log file that holds it, usually a window of a few seconds to a few minutes.
- Recent-document and recent-volume lists, print-job records, saved document versions and the Trash folder's index.
- The Mac's record of cloud-synced files, which shows deletions that arrive from a cloud service.
- Safari and cloud-storage application data.

Times. The tools report UTC. This report converts to UK time, BST (UTC+1). The Mac's time zone was set to London 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

- **Deleted content is not recoverable.** A logical image holds no free space, and an Apple silicon Mac clears and encrypts released storage. The records show that files were deleted and what they were called. They do not show what the files contained.
- **Times are windows, not instants.** FSEvents does not time each event. An event is known to have happened between the closing of one log file and the next. On the morning in question those windows are between 40 seconds and three minutes long.
- **App-usage records had expired.** macOS keeps its minute-by-minute record of which app was in front for about four weeks. The laptop was imaged 26 days after the events and then only part of 10 September remained. Imaging sooner would have preserved more.
- **USB contents are not visible.** The Mac shows when the drive was connected and which of its files were opened, not what was copied.

- **Later handling.** The managing director opened the laptop later on 10 September, and it was put on charge on 28 September. These sessions are identified below and excluded.
- **A person is not identified.** The records show actions under the user account, not who performed them.

07 THE MORNING OF 10 SEPTEMBER

Use began at about 09:05. The dismissal meeting was scheduled for 10:45.

TIME (BST)	EVENT	SOURCE
09:05 to 09:30	Safari browsing; Mail writing data	FSEvents
09:36:19	USB drive "UNTITLED" (32 GB) connected	Recent volumes; FSEvents
09:41 and 09:49	Two scanned invoice PDFs printed from Preview, both opened from the USB drive	Print jobs; recent documents
10:04 to 10:12	Nine scanned PDFs added to the shared folder "Lettings/Invoices 2026". Three files moved from Downloads to the Trash	FSEvents
10:12 to 10:15	`tenancy_renewals_tracker_2026.numbers` removed from the shared folder. Trash emptied: 48 items	FSEvents
10:15 to 10:17	31 screenshots moved from Desktop to the Trash. A personal budget spreadsheet and a holiday booking PDF moved from Documents to the Trash	FSEvents
10:19 to 10:21	Safari Clear History run: about 21,000 cached files, cookies and icon caches deleted	FSEvents (clear-history marker)
10:19 to 10:23	Messaging app moved from Applications to the Trash	FSEvents
10:23 to 10:31	Shared folder "Lettings" removed by the company's withdrawal of access: 29,800 files	FSEvents; cloud-file records
10:26 to 10:27	Trash emptied: 39 items, including the app, the screenshots and the two personal documents	FSEvents
10:27 to 10:28	Safari Clear History run a second time	FSEvents
10:31 to 10:39	Shared folder "Accounts" removed by the withdrawal of access: 11,500 files	FSEvents; cloud-file records
10:34	USB drive removed	FSEvents

OBSERVED FACT

On each of the three previous working days, the Trash was not emptied, Safari history was not cleared, and fewer than ten files were deleted by the user.

INFERENCE

The activity between 10:04 and 10:34 was a deliberate clearing of the laptop and not routine housekeeping. Confidence: high. Whether it was prompted by knowledge of the meeting is not something the laptop can show.

08 WHAT WAS IN THE TRASH

The first emptying removed 48 items. Their names survive in the event log.

CATEGORY	ITEMS	EXAMPLES
Job-application documents	9	CV and covering-letter files, a job description saved as a PDF
Company documents	14	A landlord fee schedule, two tenancy agreement templates, a contractor price list, board-pack PDFs
Images and archives	19	Newsletter images, zip files of scanned documents
Other personal files	6	A utility bill, a parcel label, two photographs

The second emptying removed 39 items: the messaging app, 31 screenshots, the personal budget spreadsheet, the holiday booking PDF and five files from Downloads.

OBSERVED FACT

The 14 company documents in the first emptying were local copies. The same file names exist in the company's shared folders, according to the list supplied by the client.

INFERENCE

Most of what was emptied from the Trash was personal or duplicated company material. Emptying it did not, on the evidence, destroy any company record. Confidence: medium, because file names alone cannot show that a local copy matched the shared version.

09 THE RENEWALS TRACKER

`tenancy_renewals_tracker_2026.numbers` is the client's working list of tenancies due for renewal, with landlord contact details and fee terms. The client regards it as its most commercially sensitive file.

OBSERVED FACT

The file was last saved on 7 September at about 09:30. It was removed from the shared folder between 10:12:18 and 10:15:18 on 10 September, in the same log window as the first Trash emptying.

OBSERVED FACT

The file was not renamed. A rename keeps the same internal file number under a new name, and this file's number ends with a removal. A file named `tenancy_renewals_tracker_2027.numbers` is a separate, older file with a different number, and it was untouched until the company's removal of access reached it at 10:27.

OBSERVED FACT

The file did not pass through the laptop's Trash. It also left no entry in the area macOS uses for deletions that arrive from the cloud service, unlike the 41,300 files removed by the company minutes later.

OBSERVED FACT

The recent-document list for Numbers includes the path `/Volumes/UNTITLED/tenancy_renewals_tracker_2026.numbers`. A file of that name was on the USB drive and was opened from it.

INFERENCE

The tracker was deleted on this laptop, by an action that bypassed the Trash, about ten minutes before the company's withdrawal of access took effect. It was not deleted by the company. Confidence: high.

INFERENCE

A copy of the tracker was on the USB drive. Confidence: high that a file of that name was there; low as to when it was put there, because recent-document lists carry no dates.

UNRESOLVED

Which application or command deleted the file, and whether the copy on the USB drive was made that morning. The cloud service's own activity history would show the deletion and the device it came from.

10 THE SHARED FOLDERS

The client suspected that the office manager had deleted the company's shared folders. The records point the other way.

OBSERVED FACT

The files in "Lettings" and "Accounts" were staged for deletion in the system area macOS uses when a cloud service tells it that files are no longer available. Files deleted by a user go to the Trash or are removed directly. They do not pass through that area.

OBSERVED FACT

The managing director states that he removed the office manager's account from both shared folders that morning, at a time he recalls as about 10:00. The laptop records the removal beginning at 10:23:52.

INFERENCE

The disappearance of the two shared folders from the laptop was caused by the company's own withdrawal of access and not by the office manager. Confidence: high. The folders and their contents remain in the company's account.

11 AFTER 10 SEPTEMBER

No user file activity is recorded between the afternoon of 10 September and the date the laptop was booked in.

DATE	WHAT THE RECORDS SHOW
10 September, 11:00 to 14:10	Light activity in Safari and Mail. The managing director states he opened the laptop that afternoon to see what was on it
11 to 27 September	Automatic app updates only
28 September, about 12:10	Laptop put on charge; an Apple security update installed itself. The managing director states he put it on charge and did not open it
6 October	Laptop received by us. Activity from this date is our handling and is excluded

OBSERVED FACT

Nothing was created, deleted or changed in the user's Documents, Desktop or Downloads folders after 10:40 on 10 September.

12 ALTERNATIVE EXPLANATIONS CONSIDERED

- **Removing personal material.** Most of the deleted items were personal: job applications, screenshots, a budget, a messaging app, browsing history. Removing these before handing back a work laptop is common and understandable. It explains most of the morning's activity.
- **The company deleted the tracker.** The tracker left the laptop ten minutes before the withdrawal of access arrived, by a different mechanism, and on its own. That is not consistent with the company's bulk removal.
- **The tracker was renamed for 2027.** Excluded by the file numbers, as set out above.
- **Someone else used the laptop.** The laptop was unlocked by Touch ID at 09:04, and personal accounts in the office manager's name were in use throughout. No other user account exists.

13 CONCLUSIONS

QUESTION	FINDING	CONFIDENCE
Were files deleted on 10 September?	87 items emptied from the Trash in two batches	HIGH
Was company data destroyed?	One company spreadsheet was deleted from the shared folder. The other company items were duplicates	HIGH
Was a USB drive used?	From 09:36 to 10:34. A copy of the tracker was on it	HIGH
Were apps removed?	One messaging app	HIGH
Was browsing history cleared?	Twice, at about 10:20 and 10:28	HIGH
Who removed the shared folders?	The company, by withdrawing access	HIGH

14 WHAT WE WOULD ALSO ASK FOR

WHAT WE WOULD ASK FOR

The cloud storage service's activity history and deleted-files list for the shared folder. These record who deleted the tracker and from which device, and the file can often be restored. Services keep this history for a limited period, so the request should be made promptly.

WHAT WE WOULD ASK FOR

The 32 GB USB drive, if it can be located. It is the only source that can show what was copied to it.

WHAT WE WOULD ASK FOR

The exact time the meeting invitation was sent and opened, from the company's mail system, if the client wishes to explore whether the meeting was known about in advance.

Clients in a similar position should note the app-usage limitation above. Had the laptop been switched off and sent for imaging in the first week, the record of which apps were used minute by minute on 10 September would still have existed.

15 GLOSSARY OF RECORDS RELIED ON

RECORD	WHAT IT IS	WHAT IT CAN AND CANNOT SHOW
File system events (FSEvents)	macOS's log of files created, renamed, moved and removed	What happened to which path. Each event is timed by the log file that holds it, usually a window of seconds to a few minutes.
Recent-item lists	Each app's list of recently opened documents and volumes	That a file was opened, and from where, including external drives. Most lists carry no time for each entry.
App-usage records (Biome)	Minute-by-minute record of which app was in front	How long each app was in use. Kept for about four weeks only.
Power log	The Mac's record of sleep, wake and lid events	When the laptop was awake. Not who was using it.
Quarantine and download records	A log of files downloaded from the internet	The file, the time and the app that fetched it, and often the web address.
Safari history	Browsing history database	Sites visited with times. If history is cleared, a marker records when.
Trash index	The hidden index inside the Trash folder	Original location of items put in the Trash. Not the time.
Print and version records	Print-job files and saved document versions	What was printed and when; earlier saved versions of documents.

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 **Guildford Data Recovery** on **01483 901310** or visit guildforddatarecovery.co.uk. Building 2, Ground Floor, Guildford Business Park, Guildford, GU2 8XH.

End of sample report. Guildford Data Recovery, Building 2, Ground Floor, Guildford Business Park, Guildford, GU2 8XH. 01483 901310. guildforddatarecovery.co.uk