SAMPLE DIGITAL FORENSIC REPORT

Was source code copied to a personal repository?

SCENARIO	**Suspected removal of proprietary software and research data by a departing developer**
INSTRUCTED BY	**A technology spin-out company (anonymised)**
DEVICE	**Windows 11 developer laptop, 1 TB NVMe drive, BitLocker enabled**
PERIOD EXAMINED	**1 March to 24 April 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 repository
08 The evening of 14 April
09 The archive on 15 April
10 Concealment
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

Oxford Data Recovery
John Eccles House, Oxford Science Park, Robert Robinson Avenue, Littlemore, Oxford, OX4 4GP

01865 593000
oxford-datarecovery.co.uk
Mon–Fri 9am–5:30pm

01 SUMMARY OF FINDINGS

The laptop records show that the company's main code repository was pushed to a second, personal hosting account on 14 April 2026, three days before the developer's last day, and that a compressed archive of the repository and a research dataset was created the following evening. Times are UK time (BST).

- **A second remote.** The local copy of the repository `analysis-engine` was configured with two remote addresses: the company's, and one added on 14 April pointing to a private repository under a personal account on a public code-hosting service.
- **The push.** The repository's own log shows a push of all 23 branches to the personal remote at 21:47 on 14 April. The command history for the same account contains the matching commands.
- **The new repository.** Eleven minutes earlier, the browser shows the hosting service's "Create a new repository" page, followed by a page for a private repository named `ae-backup` under the personal account.
- **An archive.** At 19:12 on 15 April a 3.8 GB archive named `ae_full_2026-04-15.7z` was created in Downloads. It was deleted on 17 April. It was recovered in part: its file listing is intact and names the repository and a 2.9 GB dataset folder.
- **Where the archive went.** No USB storage was connected and no upload site was visited after the archive was made. A personal cloud-storage client was installed on 15 April and removed on 17 April. Its logs were removed with it.
- **AI coding assistant.** A command-line coding assistant kept a prompt history on the laptop. On 15 April it was asked how to remove a remote from a repository's configuration and how to clear command history. Neither was done.

The records support the conclusion that the repository was copied to a personal account on 14 April (confidence: high). Whether the archive left the laptop is unresolved. The hosting service's audit log can confirm the push independently.

02 INSTRUCTIONS AND SCOPE

The client is a spin-out company whose principal asset is an analysis software platform. A senior developer resigned on 20 March 2026 to found a company in a related field and left on 17 April. The client asked five questions.

NO.	QUESTION	SHORT ANSWER
1	Was source code copied outside the company's repositories?	Yes, to a personal private repository on 14 April
2	Was research data copied?	A dataset folder was placed in an archive on 15 April. Its onward movement is unresolved
3	By what route?	A repository push. Possibly also a personal cloud-storage client
4	Was there an attempt to conceal it?	The archive and the cloud client were removed. The repository configuration was left in place
5	Who did it?	The developer's account, in sessions tied to the developer

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 developer laptop with a 1 TB NVMe solid-state drive, protected by BitLocker. It was received on 27 April 2026 with the recovery key. The client confirmed that the laptop was powered off on 17 April and not used again.

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. Repository records were read directly from the working copy with standard version-control tools, without connecting to any network.

Sources used.

- The repository's own records in its `.git` folder: the configuration file, which lists remotes, and the reference logs, which time-stamp each fetch, commit and push made from this copy.
- PowerShell's command history file for the user account.
- Browser history and downloads for Edge and Firefox.
- The code editor's list of recent folders and its terminal history.
- The coding assistant's local prompt history and session transcripts.
- The USN change journal, Prefetch, installed-program records, USB device history and a deleted-file search.

Times. Converted from UTC to UK time. BST (UTC+1) applied from 29 March 2026. Events before that date are GMT.

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 is one end of a push.** The repository log shows that this copy sent its branches to a remote and that the remote accepted them. It does not show what the personal repository contains today.
- **Command history has no times.** PowerShell's history file lists commands in order without dates. The order is reliable. Times are taken from other records.
- **The cloud client's logs are gone.** The personal cloud-storage client was uninstalled, and its folder was deleted and partly overwritten. Its installation, launch and removal are recorded by Windows. What it synchronised is not.
- **The archive is incomplete.** About 60 per cent of the archive's data was recovered. Its internal file listing survived, so the names and sizes of its contents are known. Not every file inside could be extracted.

- **Access to code was authorised.** The developer had full, legitimate access to the repository until 17 April. Cloning, pulling and building are ordinary work and are not treated as findings.
- **A person is not identified.** Attribution is addressed below.

07 THE REPOSITORY

The laptop holds one working copy of `analysis-engine`, at `C:\dev\analysis-engine`.

RECORD	WHAT IT SHOWS
Configuration file	Two remotes: `origin`, the company's hosted repository, and `bk`, a private repository `ae-backup` under a personal account
Configuration file, last modified	14 April 2026, 21:44
Reference log for `origin`	412 fetch and push entries from August 2024 to 17 April 2026, all in a pattern consistent with daily work
Reference log for `bk`	23 entries, one per branch, all time-stamped 14 April 2026, 21:47:10 to 21:47:52, each recorded as "update by push"
Personal account name	An account name incorporating the developer's initials and surname. Held on the case file

OBSERVED FACT
A reference log entry of the type "update by push" is written only when the remote server confirms that it has accepted the branch. Twenty-three such entries exist for the `bk` remote.

OBSERVED FACT
The 23 branches include `main`, the release branches for versions 3 and 4, and `research/calibration-model`, which the client identifies as unpublished work.

INFERENCE
The complete history of all 23 branches was uploaded to the personal repository on 14 April at 21:47. Confidence: high.

08 THE EVENING OF 14 APRIL

TIME (BST)	EVENT	SOURCE
21:22	Laptop woken and unlocked by PIN at a home Wi-Fi network	Event log; network profile
21:31	Personal account signed in to the hosting service in Firefox	Firefox history; saved logins
21:36	Page "Create a new repository"	Firefox history
21:37	Page `ae-backup`, marked private	Firefox history (page title)
21:44	`git remote add bk …`	PowerShell history; configuration file time
21:47	`git push bk --all`	PowerShell history; reference log
21:49	`git push bk --tags`	PowerShell history
21:52	Repository page `ae-backup` reloaded; title now shows the branch `main`	Firefox history
22:05	Laptop put to sleep	Event log

OBSERVED FACT

Firefox was used for the personal account. The developer's company account on the same hosting service was used only in Edge. The two were never signed in within the same browser.

INFERENCE

The use of a separate browser for the personal account kept the two identities apart and is consistent with a planned action. Confidence: medium.

09 THE ARCHIVE ON 15 APRIL

TIME (BST)	EVENT	SOURCE
18:40	Personal cloud-storage client downloaded and installed	Edge downloads; installed programs
18:52	Coding assistant prompt: how to remove a remote from a repository configuration without leaving a trace	Assistant prompt history
18:55	Coding assistant prompt: how to clear PowerShell history	Assistant prompt history
19:03	7-Zip launched	Prefetch
19:12	`ae_full_2026-04-15.7z` created in Downloads, 3.8 GB	USN journal
19:14	Cloud-storage client launched; its sync folder created	Prefetch; USN journal
19:15 to 20:02	Laptop awake on mains power. No other user activity	Event log
20:03	Cloud-storage client closed	Prefetch
17 April, 16:20	Archive deleted. Cloud-storage client uninstalled and its folders deleted	USN journal; uninstall record

OBSERVED FACT

The recovered file listing of the archive names 6,214 files in two top-level folders: `analysis-engine`, 0.9 GB, and `datasets\validation-2025`, 2.9 GB. The client identifies the second as measurement data licensed from a research partner.

OBSERVED FACT

The archive was created in Downloads, not in the cloud client's sync folder. The change journal shows no copy of it being created in the sync folder, although the journal for that folder is incomplete because the folder was later deleted.

INFERENCE

The dataset was gathered into a single archive for transfer. Confidence: high. The installation of a personal cloud client 32 minutes earlier, its launch two minutes after the archive was finished and a 48-minute quiet period are consistent with an upload. Confidence: medium.

UNRESOLVED

Whether the archive was uploaded, and to which account. The cloud provider's records would show this. The laptop's network-usage records, which could have shown the volume of data sent by each program, had been overwritten for that date.

10 CONCEALMENT

The client asked whether steps were taken to hide the activity.

OBSERVED FACT

The coding assistant was asked on 15 April how to remove a remote without trace and how to clear command history. The `bk` remote was still in the configuration file at imaging, and the PowerShell history was not cleared.

OBSERVED FACT

The archive and the cloud-storage client were both removed at 16:20 on 17 April, about 40 minutes before the laptop was handed in. Firefox history was not cleared.

INFERENCE

Some thought was given to removing traces, and the archive and cloud client were removed. The most significant records were left in place. Confidence: medium. The questions put to the assistant are evidence of what was asked, not of what was intended.

11 ATTRIBUTION

- The laptop was unlocked with the developer's PIN at 21:22 on 14 April while connected to a Wi-Fi network that the laptop had joined on 140 previous evenings and weekends.
- The personal hosting account's name incorporates the developer's initials and surname, and the same account appears in saved logins dating from 2023.
- The commits pushed to `bk` are the same commits, with the same author details, that the developer had pushed to the company repository in the course of work.
- The laptop has one user account in regular use. The local administrator account was last used in 2024.

INFERENCE

The developer was the person using the laptop on the evenings of 14 and 15 April. Confidence: high.

12 ALTERNATIVE EXPLANATIONS CONSIDERED

- **A personal backup with no intention to use it.** Developers do keep private copies of their own work. The company's contract assigns the code to the company and forbids copies outside its systems. Whether a copy has been used is not something this laptop can show.
- **Open-source components.** Parts of the platform are open source. The push included every branch, among them unpublished research branches that have never been released.
- **The archive was for handover.** Handover material was placed on the company's shared drive on 16 April and does not include an archive. The archive was deleted, not handed over.

- **The cloud client was installed for personal files.** That is possible, and it is why the upload is reported as a medium-confidence inference. The client was installed after notice, used once and removed.

13 CONCLUSIONS

QUESTION	FINDING	CONFIDENCE
Was source code copied outside the company's repositories?	All 23 branches were pushed to a personal private repository on 14 April	HIGH
Was research data copied?	A 2.9 GB dataset was placed in an archive on 15 April	HIGH
Did the archive leave the laptop?	The timing fits an upload through a personal cloud client	MEDIUM
Was there an attempt to conceal?	Partial: the archive and client were removed, the repository records were not	MEDIUM
Who did it?	The developer	HIGH

14 WHAT WE WOULD ALSO ASK FOR

WHAT WE WOULD ASK FOR

The organisation audit log from the company's code-hosting account, which records clones, fetches and pushes by each member and their network addresses. It shows the developer's access to the company repository in the weeks before 14 April.

WHAT WE WOULD ASK FOR

A preservation request to the hosting service for the repository `ae-backup`, made through the client's solicitor. Hosting services act on such requests in support of legal proceedings.

WHAT WE WOULD ASK FOR

The data licence for the validation dataset, so that the client's advisers can assess whether the research partner must be notified.

This report is written to support an application for delivery up or deletion of the copied material if the client's solicitor advises one. The reference-log entries are the central exhibit, and a certified extract can be supplied.

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 **Oxford Data Recovery** on **01865 593000** or visit oxford-datarecovery.co.uk. John Eccles House, Oxford Science Park, Robert Robinson Avenue, Littlemore, Oxford, OX4 4GP.

End of sample report. Oxford Data Recovery, John Eccles House, Oxford Science Park, Robert Robinson Avenue, Littlemore, Oxford, OX4 4GP. 01865 593000. oxford-datarecovery.co.uk