BDR

BELFAST DATA RECOVERY

SAMPLE DIGITAL FORENSIC REPORT

Who used the shared laptop, and what was sent by messaging app?

SCENARIO	**Attribution of activity on a hand-me-down laptop, and files passed through a desktop messaging app**
INSTRUCTED BY	**A building services contractor (anonymised)**
DEVICE	**Windows 11 business laptop, 512 GB SATA solid-state drive**
PERIOD EXAMINED	**1 July to 28 August 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 laptop and its accounts
08 The messaging app
09 The final week
10 Other routes checked
11 After the last day
12 Alternative explanations considered
13 Conclusions
14 What we would also ask for
15 Glossary of records relied on
16 About this sample report

Belfast Data Recovery
Forsyth House, Cromac Square, Belfast, BT2 8LA

028 9002 0144
belfastdatarecovery.co.uk
Mon–Fri 9am–5:30pm

01 Summary of findings

The laptop had been passed between three members of staff without being reset, so the Windows account in use still carried a previous user's name. The records show that the estimator who left in August 2026 was the person using that account throughout the period, and that tender documents passed through a desktop messaging app in the final week. Times are UK time (BST).

- **Who used it.** Three Windows accounts exist. Only one shows any activity after January 2025. Inside that account, the browser profiles, saved logins, a phone hotspot name and personal documents all belong to the estimator, not to the person the account is named after.
- **Messaging app.** A desktop messaging app linked to a personal phone number was installed on 3 March 2026 and used on most working days. Its transfer folder for the week of 17 to 23 August holds three company files: a tender pricing workbook, a supplier rates list and a bill of quantities.
- **Opened after sending.** The pricing workbook in the transfer folder was opened twice, on 20 and 21 August. The estimator's last day was 21 August.
- **Direction not shown.** The app's transfer folder stores files that were sent and files that were received. The folder alone does not show which. The app's message database on the laptop is encrypted.
- **Other routes.** No USB storage device was connected in August. No personal cloud storage or webmail attachment activity was found.
- **After the last day.** The laptop was used on 24 August for 35 minutes. The client's operations manager states that this was him. One file opened in that session cannot be attributed with confidence.

The records support the conclusion that the estimator used the laptop under a legacy account name (confidence: high) and that three tender documents were sent or received through a personal messaging account in the final week (confidence: high). Whether they were sent out, and to whom, needs the phone or the other party's records.

02 Instructions and scope

The client is a building services contractor. An estimator resigned on 7 August 2026 and left on 21 August. A fortnight later the client lost a tender to a competitor by a narrow margin and learned that the estimator had joined that competitor. The former employee's solicitor then stated that the laptop "was never his" and was shared. The client asked five questions.

NO.	QUESTION	SHORT ANSWER
1	Who used the laptop between 1 July and 21 August?	The estimator, under an account named after a previous user
2	Were tender documents sent outside the company?	Three passed through a personal messaging app in the final week
3	To whom?	Not determinable from the laptop
4	Was any other route used?	None found
5	Was the laptop used after 21 August, and by whom?	Once, on 24 August. Mostly accounted for

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 512 GB SATA solid-state drive, not encrypted. It was received on 14 September 2026. The client disclosed the session on 24 August before we began.

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 processed in our forensic software. Every record type was exported and searched for the client's key terms: the tender reference, the competitor's name and the names of the three files.

Sources used.

- User-account records and the Security and System event logs, for logons, power events and uptime.
- Browser profiles for Chrome, Edge and Firefox: history, saved logins, form entries and profile identities.
- Wi-Fi network history.
- Jump Lists, LNK files and Office recent-document lists.
- The messaging app's local folders, including its dated transfer folders.
- Prefetch program-launch records, USB device history, Recycle Bin records and the USN change journal.

Times. Converted from UTC to UK time, BST (UTC+1) 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

- **The messaging database is encrypted.** The app stores its messages in a database protected by a key held on the linked phone. The names, sizes and dates of transferred files are visible. The messages, and the people they were exchanged with, are not.
- **Sent or received.** The app keeps both outgoing and incoming files in one transfer folder for each week. Direction has to be inferred from other records.
- **Saved passwords.** Passwords stored in one browser were readable by the forensic software. They are held securely on the case file, have not been used and are not reproduced.
- **Shared device.** Attribution rests on the accounts and applications in use around each event. No camera, door or fingerprint record was available.
- **Browser history is partial.** History in the main browser profile survives from 24 May 2026. Saved logins and downloads go back to 2024.

07 The laptop and its accounts

WINDOWS ACCOUNT	LAST ACTIVITY	WHAT IS INSIDE IT
Account A, named after a former contracts manager	24 August 2026. Continuous use from February 2025	A Chrome profile under the estimator's company email address. A Firefox profile with saved logins in the estimator's name. An Edge profile showing Account A's original owner
Account B, named after the operations manager	March 2023	An Edge profile with one saved login for a personal mail service
Account C, a generic "Site" account	January 2025	A Chrome profile under a former site supervisor's company address

OBSERVED FACT

Programs across the system carry the same installation date and hour in October 2024, and several USB devices have "first seen" times that evening. The Windows installation was refreshed on that date, and Account A was kept.

OBSERVED FACT

Inside Account A, saved logins and form entries carry the estimator's name and two personal email addresses for a pension provider, an insurer, a rail booking site, a supermarket and a professional networking site. A Wi-Fi profile is named after the estimator's phone. Three CV files carry the estimator's name. The company mailbox shown in page titles on almost every working day in July and August is the estimator's.

OBSERVED FACT

The Edge browser inside Account A displays the original owner's name. Edge takes its identity from the Windows account's linked work profile, which was never changed. Its activity interleaves with the estimator's Chrome profile within the same minutes on eleven occasions.

INFERENCE

The estimator was the person using Account A from at least February 2025 to 21 August 2026. The account name is a leftover from a previous user and should not be read as that person using the laptop. Confidence: high.

UNRESOLVED

Which fingerprints are enrolled on the laptop's reader. That can be read from the image if attribution is disputed further.

08 The messaging app

RECORD	WHAT IT SHOWS
Installation	3 March 2026, from the Microsoft Store, under Account A
Launches	92 launches between 1 July and 21 August, on 34 of 38 working days
Linked account	A mobile number. The last four digits match the personal number on the estimator's HR record
Transfer folders	One per week. Eleven weeks hold files; eight hold only photographs and voice notes
Week of 17 to 23 August	Seven files, of which three are company documents

The three company documents in the transfer folder for the week of 17 to 23 August:

FILE	SIZE	MATCHING FILE ON THE COMPANY SERVER
`Tender_[ref]_pricing_v6.xlsx`	840 KB	Same name and size, last saved 19 August at 16:52 by the estimator
`Supplier_rates_2026_Q3.xlsx`	310 KB	Same name and size
`BoQ_[ref]_issue2.pdf`	2.4 MB	Same name and size

OBSERVED FACT

The three files' hashes match the copies on the company server, which the client supplied for comparison. They are the company's documents, unaltered.

OBSERVED FACT

The pricing workbook was saved on the server at 16:52 on 19 August. The copy in the transfer folder was created at 17:06 the same day. The messaging app was launched at 17:04.

INFERENCE

The pricing workbook entered the messaging app 14 minutes after its final save, while the app was open. A file that originates on the company server and appears in the transfer folder minutes later is far more likely to have been sent from this laptop than received on it. Confidence: medium to high.

UNRESOLVED

The recipient. It could be the estimator's own phone, as a way of keeping a copy, or a third party. The laptop cannot distinguish the two.

09 The final week

DATE AND TIME (BST)	EVENT	SOURCE
17 Aug, 10:15	Competitor's website, "Our team" page	Chrome history
18 Aug, 12:40	Supplier rates list opened from the server	Office recent list
18 Aug, 12:44	`Supplier_rates_2026_Q3.xlsx` created in the transfer folder	USN journal
19 Aug, 16:52	Pricing workbook saved on the server	Server copy; Office recent list
19 Aug, 17:04	Messaging app launched	Prefetch
19 Aug, 17:06	`Tender_[ref]_pricing_v6.xlsx` and `BoQ_[ref]_issue2.pdf` created in the transfer folder	USN journal
20 Aug, 08:31	Pricing workbook opened from the transfer folder	Jump List
21 Aug, 15:10	Pricing workbook opened from the transfer folder a second time	Jump List
21 Aug, 16:20 to 16:26	64 files deleted from Desktop and Documents; Recycle Bin emptied	Recycle Bin records
21 Aug, 16:41	Laptop shut down	System event log

OBSERVED FACT

The tender was submitted by the client on 26 August. The competitor's winning price was within one per cent of the client's, according to the client.

INFERENCE

The client's final pricing for the tender passed through a personal messaging account two days before the estimator left and a week before the tender closed. Confidence: high. Whether it reached the competitor is not shown by the laptop.

10 Other routes checked

ROUTE	RESULT
USB storage	No storage device connected between 1 and 24 August. A label printer and a laser measure were connected and are not storage
Cloud storage and file-transfer sites	Company OneDrive only. A file-transfer site was last used in January 2026 for drawings sent to an architect
Personal webmail	Read on most days. No compose page open on 18 or 19 August
Printing	The bill of quantities was printed on 19 August at 15:30, which is consistent with normal work
Secure-deletion tools	None installed or run

11 After the last day

The System event log shows a shutdown at 16:41 on 21 August and a start at 09:12 on 24 August. Everything dated after 16:41 on 21 August is therefore separated from the estimator's use by a clear boundary.

TIME ON 24 AUG	EVENT	ATTRIBUTION
09:12	Laptop started; Account A logged on by password	Operations manager, by his own statement. The password was on the handover sheet
09:15 to 09:38	File Explorer: Desktop, Documents and the server's Tenders folder browsed	Operations manager
09:26	Pricing workbook opened from the messaging app's transfer folder	Not attributed
09:41	A search in the estimator's Chrome profile: the competitor's name	Operations manager, by his own statement
09:47	Laptop shut down	Operations manager

OBSERVED FACT

The operations manager's statement says he "had a look through the files and searched the competitor" and does not mention the messaging app's folder.

INFERENCE

The 24 August session was the operations manager's. Confidence: medium to high. It did not create, change or delete any file, and it does not affect the findings above, all of which are dated before 16:41 on 21 August.

UNRESOLVED

Why the workbook was opened from the transfer folder on 24 August. The Jump List makes it one click away for anyone using Account A, which is the likeliest explanation.

12 Alternative explanations considered

- **The laptop was shared, so anyone could have done it.** The other two accounts were last used in 2023 and January 2025. Everything personal inside Account A belongs to the estimator. No other person's accounts appear in the period.
- **The files were received, not sent.** Possible in principle. A received copy of a file that was saved on the company server 14 minutes earlier would first have had to leave the company by some other route, and none was found.
- **The estimator sent the files to his own phone to work from site.** This is a real possibility, and the laptop cannot exclude it. It would still mean the final pricing was on a personal device when the estimator left.
- **The operations manager planted the files on 24 August.** The files were created in the transfer folder on 18 and 19 August, while the estimator was employed and the app was running. Nothing was created on 24 August.

13 Conclusions

QUESTION	FINDING	CONFIDENCE
Who used the laptop from 1 July to 21 August?	The estimator, under a legacy account name	HIGH
Did tender documents pass through a personal messaging app?	Three, on 18 and 19 August	HIGH
Were they sent from the laptop rather than received?	The timing after the server save indicates sent	MEDIUM
To whom?	Not determinable from the laptop	LOW
Was another route used?	No evidence of one	HIGH
Who used the laptop on 24 August?	The operations manager	MEDIUM

14 What we would also ask for

WHAT WE WOULD ASK FOR

The messaging account's own chat export for 17 to 23 August, or examination of the linked phone. Either shows the direction of each file and the other party. If the phone is the estimator's own, this is a matter for the client's solicitor.

WHAT WE WOULD ASK FOR

The company file server's access log for the three files, to confirm that no one else opened them between 17 and 21 August.

WHAT WE WOULD ASK FOR

A signed statement from the operations manager covering each step of the 24 August session, made while his memory is fresh.

Two practical points follow. A laptop passed to a new user should be reset and given an account in that user's name, which would have made the first question in this report unnecessary. And when a concern arises, the laptop should be switched off and left off, because every later session has to be explained.

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 proceedings in Northern Ireland, including before an Industrial Tribunal, it is finalised on the instruction of the client's solicitor with the examiner's qualifications, the sources of all information relied on and the expert's declaration required by the High Court's practice directions.

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 **Belfast Data Recovery** on **028 9002 0144** or visit belfastdatarecovery.co.uk. Forsyth House, Cromac Square, Belfast, BT2 8LA.

End of sample report. Belfast Data Recovery, Forsyth House, Cromac Square, Belfast, BT2 8LA. 028 9002 0144. belfastdatarecovery.co.uk