



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Digital Forensics Investigation Report

Analysis of mobile phone extractions and flash drive artefacts

Module: Digital Forensics Analysis

Assessment: Forensic case report

Submitted By

MD Imran Biswas

Student ID:2436882

University of Wales Trinity Saint David

Table Of Content

1. Introduction.....	3
2. Method and continuity of evidence.....	3
2.1 Acquisition and verification details.....	3
3. Evidence overview.....	3
4. Detailed findings.....	5
4.1 Huawei phone: user identity and accounts	5
4.2 WhatsApp communication with Joe Marsh	5
4.3 Call Log and Email Correlation	6
4.4 Instagram and Facebook escalation.....	6
4.5 Location, travel and meeting context	7
4.6 Flash drive and recovered screenshot evidence	7
5. Timeline of relevant activity	8
6. Evaluation and conclusion	8
7. Limitations and further work	9
References.....	10
Appendix A: Extraction verification screenshots	11
Appendix B: Recovered hidden-message screenshots.....	13
Appendix C: Flash drive screenshot	19
Appendix D: Data files reviewed.....	19

1. Introduction

This report focuses on the pieces of digital evidence provided in the Digital Forensics case file. It contains several mobile phone extraction exports, a flash drive image extraction and a set of screenshots that display recovered strings using either image or file analysis. The aim of the report is to report the relevant findings in a forensic style, outline the linkages between the artefacts and provide a reasoned conclusion from the available evidence, not speculation.

The Huawei phone extraction is the best example of this. The phone number 447917162788 appears several times in the "owner account" as does Peter Dover in the Instagram account peterdover2, the Facebook identifier 61565261156720 and the Gmail account dovp59@gmail.com. In the communications, the topic is the confidential information that ABC Technologies is selling on an AI-based Neuro product, which is discussed. Messages also reference Joe Marsh as an intermediary and Norman Smith as a subsequent contact/potential purchaser. The flash drive and recovered screenshots offer background information, particularly when it comes to messages that have been deleted or carved, and location-style messages.

2. Method and continuity of evidence

This method follows the recognised good practices in digital forensics as outlined in ISO/IEC (2012), Kent et al. (2006) which include identification, acquisition, preservation, analysis and presentation of the digital evidence.

2.1 Acquisition and verification details

Source	Acquisition / verification details
Huawei POT-LX1 P Smart	Android ADB file dump. Extraction started 28/10/2025 16:12:56 and ended 28/10/2025 16:53:34. SHA-256: d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f.
Nokia C2 2nd Edition	Android backup. Extraction started 28/10/2025 16:01:06 and ended 28/10/2025 16:03:26. SHA-256: a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab.
Samsung Galaxy A13	Android backup. Extraction started 28/10/2025 11:57:02 and ended 28/10/2025 12:36:47. SHA-256: 0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195.
Note 14	Android backup. Extraction started 28/10/2025 11:25:18 and ended 28/10/2025 11:27:40. SHA-256: 630724e2f8863adb9c4f7df1ab645e56c19a832d546fe7ab55b0cebf8ea7befd.
Emma Flash Drive E01	Autopsy data source with file-system entries, carved files, orphan files, EXIF metadata and user-content-suspected artefacts.

The image hashes of the extraction screenshots are verified, so the extracted content can be considered as stable for this report. Ensuring and verifying hashes is a common way to provide evidence integrity (ACPO, 2012; SWGDE, 2018).

3. Evidence overview

Device Ownership Table

Evidence ID	Owner / Linked Person	Device / Source	Device Type
E01	Emma / Peter Dover	Huawei POT-LX1 P Smart	Android smartphone
E02	Joe Marsh	Samsung Galaxy A13	Android smartphone
E03	Norman Smith	Nokia C2 2nd Edition	Android smartphone
E04	Unknown / Supporting user	Redmi Note 14	Android smartphone
E05	Emma	Emma Flash Drive E01	USB flash drive / external storage

The purpose of this table is to uniquely identify the owner/user of each of the devices or sources examined, thus enabling the identification of the appropriate evidence item in subsequent findings.

Device / source	Artefact files reviewed	Approximate records
Huawei phone	Chats, contacts, call log, emails, locations, databases, text, archive, cookies and uncategorised data	Over 26,000 exported records across the supplied spreadsheets; most relevant items are in chats, contacts, emails and locations.
Nokia phone	Archive, databases, locations, text and uncategorised data	Approximately 339 records; mainly location and background application artefacts.
Samsung phone	Archive, documents, locations and uncategorised data	Approximately 364 records; useful as supporting device context but not central to the main allegation.
Note 14 phone	Locations, text and uncategorised data	Approximately 305 records; mainly historical location and system artefacts.
Flash drive	File system CSV, orphan files, carved files and archives	Over 9,000 file-system and carved/orphan entries, including user-content-suspected and EXIF-related material.
Screenshots	Recovered strings from file/image analysis	Six screenshot artefacts containing hidden or metadata-style text, locations and dates.
Flash drive	File system CSV, orphan files, carved files and archives, including open.7z	Over 9,000 file-system and carved/orphan entries, including user-content-suspected, EXIF-related material and the compressed archive open.7z, which requires further extraction/password testing before its contents can be confirmed.

The exported material can be considered stable for this report, since the hashes of the images are verified in the extraction. It is a common practice to maintain and verify hashes to provide evidence integrity (Association of Chief Police Officers, 2012; Scientific Working Group on Digital Evidence, 2018).

4. Detailed findings

4.1 Huawei phone: user identity and accounts

The Huawei extraction is connected to the device and Peter Dover. There are multiple entries of Joe Marsh in the contact list, on platforms such as WhatsApp, Facebook and Instagram. This is a cross-platform repetition that fortifies the association of the communications to the same user environment.

Artefact	Relevant value	Interpretation
WhatsApp account	447917162788@s.whatsapp.net	Primary owner account used in the direct messages with Joe Marsh.
Instagram account	peterdover2 / 68515482744	Used for the later contact from Joe, where Joe states that someone in “NSI” is interested.
Facebook account	61565261156720 Peter Dover	Used in the January 2025 messages with Norman Smith.
Gmail account	dovp59@gmail.com	Appears in email and location artefacts, supporting the device-user attribution.

4.2 WhatsApp communication with Joe Marsh

The conversation between Peter Dover and Joe Marsh is highly relevant as it outlines the initial plan on what was to be done with WhatsApp. Peter is considering selling a “highly valuable information from ABC technologies” that is connected to a “new AI based Neuro product” on 21 August 2024. Joe says that this is not a joke and asks who would want to join. Peter responds that he believes that Joe will be able to find the right buyer and that “the competition” were anxious to acquire the technology. This is not a casual discussion, it's a discussion about monetizing the information that is confidential for the company.

This discussion goes on for several months. Joe indicates that he will be meeting with clients in a hotel room about the offer, then mentions Glasgow, Paris and Manchester, and finally reports on 31 Jan 2025, that there is a buyer who requires a sample. Peter states that it's hard to do a demo but not a breakdown, and suggests that they discuss the offshore setup. Joe responds that “5M” is safe and wants to know what is the rest. This series is indicative of an attempted sale with Joe acting as an intermediary and Peter as the source material.

Date/time	Source row	Extract / summary	Forensic relevance
21/08/2024 10:58	Huawei Chats	Peter: access to valuable ABC Technologies AI Neuro product information; considering selling it.	Initial admission of access and intent.
21/08/2024 11:10	Huawei Chats	Peter trusts Joe to find the right buyer; competition may want the technology.	Shows intended recipient market.
21/08/2024 12:13	Huawei Chats	Joe meeting clients in a hotel meeting room.	Shows intermediary activity.
31/01/2025 10:22-10:24	Huawei Chats	Demo sample requested; Peter offers detailed breakdown; offshore arrangement and 5M discussed.	Shows negotiation and payment arrangement.

4.3 Call Log and Email Correlation

Call logs, emails and artefacts of chat were cross referenced with each other to verify consistency of the communication evidence across the seized devices. The call recordings corroborate the larger timeline and the email and messages are more content-rich evidence of intent, file transfer and coordination. This is because call logs only show that contact took place, and were used alongside WhatsApp, Instagram, Facebook Messenger and a USB file to interpret the logs.

Evidence type	What it shows	Forensic value
Call logs	Contact between suspects around the investigation period	Supports communication pattern but does not prove conversation content
WhatsApp / Instagram / Messenger	Message content, arrangements and role links	Strong evidence of intent and coordination
Emails	Possible patent sample transfer or formal communication	Supports file sharing and commercial intent
USB / archive files	Possible storage or transfer of QT-AI-2025 material	Links communication evidence with actual file evidence

4.4 Instagram and Facebook escalation

The 9th September Instagram message is another link in the chain. Joe calls Peter and explains that he found a company in the “NSI” that is interested and asks Peter what sort of information he would share. The term “NSI” is not defined in the export but the message rings true to the previous Whatsapp conversation where Joe seems to be trying to find out where to sell the product and how much information about it Peter is willing to share.

The discussion on Facebook on 31st January 2025 is serious. Norman Smith is told by Peter to start on with him saying that Joe said that Norman was ready to go. Norman wants the blueprint to be sent in parts to avoid the risk of sending it all at once. Peter feels that it ought to be sent all at once. Norman then proposes to begin with the “head” and then says that the first part lets go when “5M offshore” reflects. Peter agrees and lets Norman know he should check his Inbox within 48 hours. The messages are the clearest indication of a covert exchange of sensitive technical information.

Time	Platform	Participants	Meaning
09/09/2024 16:57	Instagram	Joe to Peter	Joe found an interested person and asks what information Peter would share.
31/01/2025 12:47	Facebook	Peter and Norman Smith	Peter says Joe told him Norman was ready to proceed.

31/01/2025 12:49	Facebook	Norman to Peter	Norman asks for the blueprint in chunks.
31/01/2025 12:51	Facebook	Norman to Peter	Norman suggests starting with the “head”.
31/01/2025 12:53	Facebook	Norman and Peter	5M offshore payment and inbox delivery within 48 hours are discussed.

4.5 Location, travel and meeting context

The context (location and message data) is helpful. On 22 August 2024, Joe shares a Google Maps' live-location link. Later on he mentions travelling to and meetings in Glasgow, Paris and Manchester. Huawei location data also reveals travel-related artefacts, such as media coordinates in Wales, Qatar and other foreign coordinates, as well as Gmail-related coordinates. These places are not evidence of what was discussed at the meetings in themselves, they do complement the overall use of travel and external contact during the time period when the sale was under discussion. This doesn't reflect the same direct relationship between the location data and the ABC Technologies information in the Nokia, Samsung and Note 14 datasets as was in the exports provided. For this reason, these artefacts are considered to be supporting evidence and not the primary source of evidence. This is crucial because when evidence provides only background for position or device use, it is important that this evidence is not misrepresented in the report.

4.6 Flash drive and recovered screenshot evidence

The flash drive export is relevant due to the fact that there are a lot of carved files, orphan files and file-system entries in the flash drive. There are a number of EXIF metadata artefacts and user-content suspected artefacts found in autopsy, indicating that there was content that was deleted or embedded on the removable media. There are thousands of carved entries in the CSV file, and an orphanfile listing as well. This does not reveal the specific file(s) that may have been transferred, but it does indicate that there is recoverable data on the flash drive that should be retained and further analyzed. The screenshots are also of crucial significance. They display recovered strings in JPEG/ASCII data, either in it or the other data beside it. There are a number of screenshots that contain text of a message format, dates and locations. In the case of two screenshots, they will have Evidence #1 and Evidence #2, and they will indicate 1 May 2023 times with the Location - Richmond Park, London label. Other strings include: “Are you hungry Now?” (with location - Not McDonalds) and “I’m a Dog with glasses. Bow to me!” (with location - Swansea, Wales) Another screen states that it's “Haha Good Try”. These items appear more like an intentional message or message hidden in the picture than typical picture metadata. As such, they should be considered potential steganographic and/or metadata hiding artifacts. A zip file, called open.7z, was also found on the flash drive. This is important because 7z files often contain multiple files, and can be password protected. So the existence of open.7z indicates that the user might have bundled up, saved or transferred data in the .7z format. The archive should be considered an artefact that might contain relevant material and not evidence of wrongdoing, however, until it can be opened and the items within it are verified, it remains a relevant artefact.

Screenshot evidence	Recovered text	Date / location clue	Interpretation
Evidence #1	Evidence #1	2023:05:01-13:00:00; Richmond Park, London	Possible hidden message or metadata clue.

Evidence #2	Evidence #2	2023:05:01-12:00:00; Richmond Park, London	Second clue pointing to same location with earlier time.
Food clue	Are you hungry Now?	Location - Not McDonalds	Possible misdirection or place clue.
Dog clue	I'm a Dog with glasses. Bow to me!	2021:06:09; Swansea, Wales	Possible hidden message with date and location.
Decoy clue	Haha Good Try	No clear location shown	Likely decoy or challenge artefact.

5. Timeline of relevant activity

Date	Event	Evidence source
21/08/2024	Peter tells Joe he has valuable ABC Technologies AI Neuro product information and is considering selling it.	Huawei Chats
22/08/2024	Joe sends live Google Maps location link.	Huawei Chats
26/08/2024	Joe says a previous meeting did not go as expected and he has more contacts.	Huawei Chats
29/08/2024	Joe says he is flying to Glasgow to meet a contact.	Huawei Chats
09/09/2024	Joe says a person in an "NSI" company is interested and asks what level of information Peter will share.	Huawei Chats
14/10/2024	Joe says he is travelling to Paris to get good deals.	Huawei Chats
20/11/2024	Peter pressures Joe for an update; Joe says he is in final talks and meeting a client in Manchester.	Huawei Chats
31/01/2025 10:15-10:24	Peter and Joe discuss demo sample, detailed breakdown, offshore arrangement and 5M.	Huawei Chats
31/01/2025 12:47-12:53	Peter and Norman discuss blueprint, chunks, "head", 5M offshore and inbox delivery within 48 hours.	Huawei Chats

6. Evaluation and conclusion

The artefacts confirm Peter Dover's involvement in a bid to sell top secret information from ABC Technologies. The main reason is it's consistent and specific on the platforms. The first revelation to Joe Marsh and the scheme for finding a buyer is revealed via WhatsApp. Instagram displays an interest from third party from Joe. Peter goes on to face off against Norman Smith over the blueprint materials, release and payment terms on Facebook. The concept of a "detailed breakdown", the term "blueprint", "head" and "5M offshore" and a 48-hour delivery in the inbox aren't that common in everyday conversation. It seems like Joe Marsh is an intermediary. His emails indicate that he was reaching out to and/or catching up with prospective clients, and keeping Peter informed about client interest. It seems that the later stage would have been the most serious contender for the Norm Smith, who seems to be the best option. The same goes for the flash drive: There is less certainty about its value but the carved material, orphan files and suspected user content makes it a worthwhile medium. The fact that open.7z has been found also indicates that compressed archive files should be further examined, as they may be hiding additional data or data being stored in the compressed file. The hidden message screenshots imply that pictures or file metadata might be employed to hide out clues, areas or communications. In any subsequent investigation they should be analyzed using the special steganography and metadata tools. At this point, however, the best evidence is not just a suspicion of the existence of suspicious files, but that the communications

indicate intent, planning, identification of buyers and discussion of payment. The strongest case is if the chat records are complemented by attribution and timing data for the account. The biggest drawback is that the actual ABC Technologies data file is not named as part of the provided exports. However, the messages are a clear, and, for this purpose, convincing statement of attempts to make an unauthorized disclosure. Since the strongest forensic value is derived from the correlation between communication records, removable storage artifacts, archive evidence, and recovered deleted material, the evidence should be evaluated collectively rather than separately.

7. Limitations and further work

Limitation	Recommended follow-up
The actual confidential file is not directly identified in the supplied exports.	Search extracted file systems for ABC, Neuro, blueprint, head, demo, NSI and related keywords; priorities attachments and deleted files.
Some messages are deleted or sender-deleted.	Recover deleted WhatsApp rows from msgstore.db and correlate with backups if available.
Flash drive carved material is large and not fully interpreted from CSV exports alone.	Export suspected user-content files and run file-type validation, hash comparison, metadata review and string search.
Screenshot strings suggest hidden messages but do not prove the hiding method.	Run EXIF, strings, binwalk/steganalysis and image comparison on original image files where available.
Location artefacts support travel context but not meeting content.	Correlate locations with chat timestamps, travel records and external CCTV or hotel records if authorised.

References

- Association of Chief Police Officers (2012) Good Practice Guide for Digital Evidence. Version 5. Available at: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (Accessed: 11 May 2026).
- ISO/IEC (2012) ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence. Available at: <https://www.iso.org/standard/44381.html> (Accessed: 11 May 2026).
- Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006) Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. Available at: <https://csrc.nist.gov/pubs/sp/800/86/final> (Accessed: 11 May 2026).
- Scientific Working Group on Digital Evidence (2018) SWGDE Best Practices for Computer Forensic Examination. Available at: <https://www.swgde.org/wp-content/uploads/2024/05/2018-07-11-SWGDE-Best-Practices-for-Computer-Fo.pdf> (Accessed: 11 May 2026).

Appendix A: Extraction verification screenshots

Extractions: 1



File System

Huawei POT-LX1 P Smart
File System [Android ADB]

Extraction start date/time
28/10/2025 16:12:56
Extraction end date/time
28/10/2025 16:53:34

Device Info

Image Hash Details

Extraction images are verified.

File Dump

SHA256 d5193dbf8246c09fde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f

Close

Huawei phone extraction verification and hash details.

Extractions: 1



File System

Detected Model Nokia C2 2nd Edition
File System [Android Backup]

Extraction start date/time
28/10/2025 16:01:06
Extraction end date/time
28/10/2025 16:03:26

Device Info

Image Hash Details

Extraction images are verified.

Backup

SHA256 a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab

Close

Nokia phone extraction verification and hash details.

Extractions: 1



File System

Samsung GSM SM-A137F Galaxy A13
File System [Android Backup]

Extraction start date/time
28/10/2025 11:57:02
Extraction end date/time
28/10/2025 12:36:47

Device Info

Image Hash Details

Extraction images are verified.

Backup

SHA256 0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cdef8753a9a3195

Close

Samsung phone extraction verification and hash details.

Extractions: 1



[File System](#)

Detected Model Note 14
File System [Android Backup]

Extraction start date/time
28/10/2025 11:25:18
Extraction end date/time
28/10/2025 11:27:40

Device Info

Image Hash Details

Extraction images are verified.

Backup

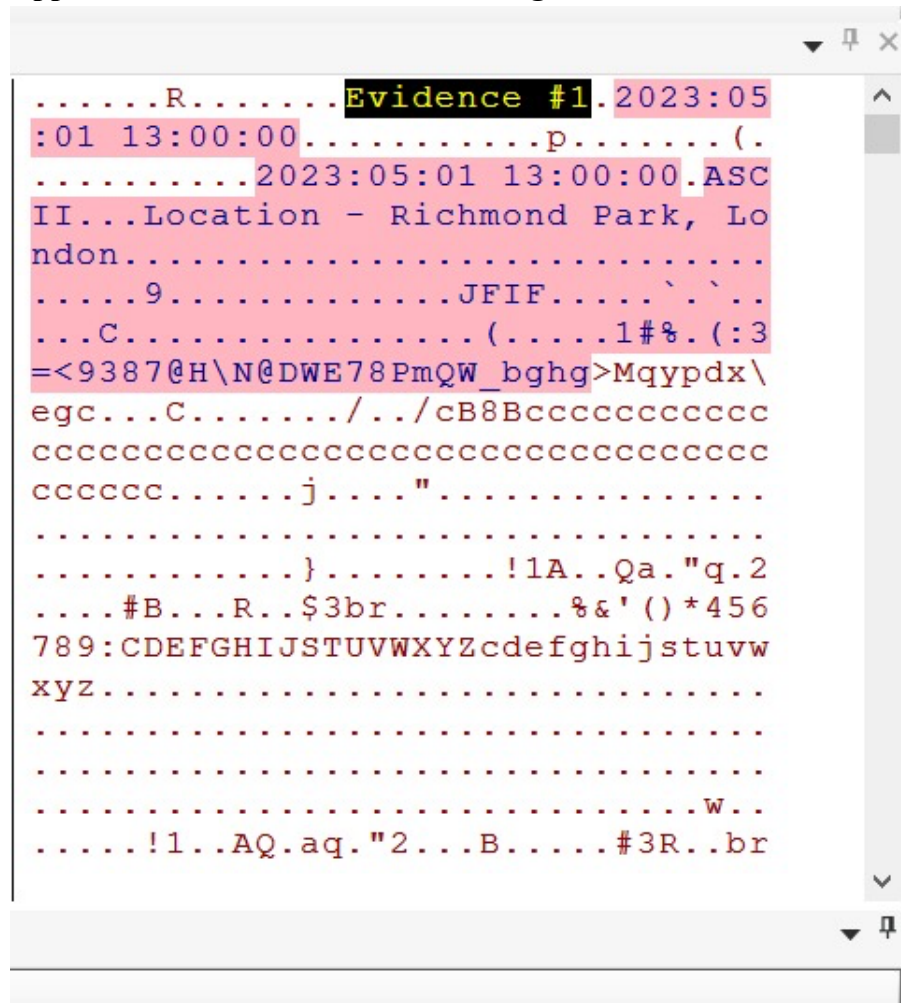
Verified

SHA256 630724e2f8863adb9c4f7df1ab645e56c19a832d546fe7ab55b0cebf8ea7befd

Close

Note 14 phone extraction verification and hash details.

Appendix B: Recovered hidden-message screenshots



Recovered string showing Evidence #1, 2023:05:01 13:00:00, Richmond Park, London.

```
35 .....R.....Evidence #2.2023:05
00 :01 12:00:00.....p.....(
43 .....2023:05:01 12:00:00.ASC
5F II...Location - Richmond Park, Lo
04 ndon.....
00 .....y.....JFIF.....`..`..
33 ...C.....(.....1#%.(:3
5C =<9387@H\N@DWE78PmQW_bghg>Mqypdx\
53 egc...C...../.../cB8Bcccccccccccc
53 ccccccccccccccccccccccccccccccccc
05 ccccccc.....j.....".....
01 .....
32 .....}.....!1A..Qa."q.2
36 ....#B...R..$3br.....%&'()*456
77 789:CDEFGHIJSTUVWXYZcdefghijstuvw
35 xyz.....
3A .....
01 .....
01 .....w..
72 .....!1..AQ.aq."2...B.....#3R..br
```

Recovered string showing Evidence #2, 2023:05:01 12:00:00, Richmond Park, London.

```
..Join us. Become the Darkness!..
.....b.....v.....2023
:06:01 00:00:00.ASCII...Location
- Unknown .....JFIF...
..H.H.....C.....(.....
1#%.(:3=<9387@H\N@DWE78PmQW_bghg>
Mqypdx\egc...C...../.../cB8Bcccc
cccccccccccccccccccccccccccccccc
cccccccccccccc.....j.....".....
.....}.....!1A..
Qa."q.2....#B...R..$3br.....%&
'()*456789:CDEFGHIJSTUVWXYZcdefgh
ijstuvwxyz.....
.....
.....
.....w.....!1..AQ.aq."2...B.....
#3R..br...$4.%.....&'()*56789:CDE
```

Recovered string “Are you hungry Now?” and “Location - Not McDonalds”.

```
.i.....H.....I'm a Dog with g
lasses. Bow to me!.....f....
...!...z.....2021:06:09 00:00:0
0.ASCII...Location - Swansea, Wal
es.....
...Z.....JFIF.....`..`...
..C.....(.....1#%.(:3=
<9387@H\N@DWE78PmQW_bghg>Mqypdx\e
gc...C...../.../cB8Bcccccccccccccc
cccccccccccccccccccccccccccccccccc
cccccc.....j..".
.....
.....}.....!1A..Qa."q.2.
...#B...R..$3br.....%&'()*4567
89:CDEFGHIJSTUVWXYZcdefghijstuvw
xz.....
.....
.....
.....!1..AQ.aq."2...B.....#3R..br.
```

Recovered string “I’m a Dog with glasses. Bow to me!” and “Location - Swansea, Wales”.

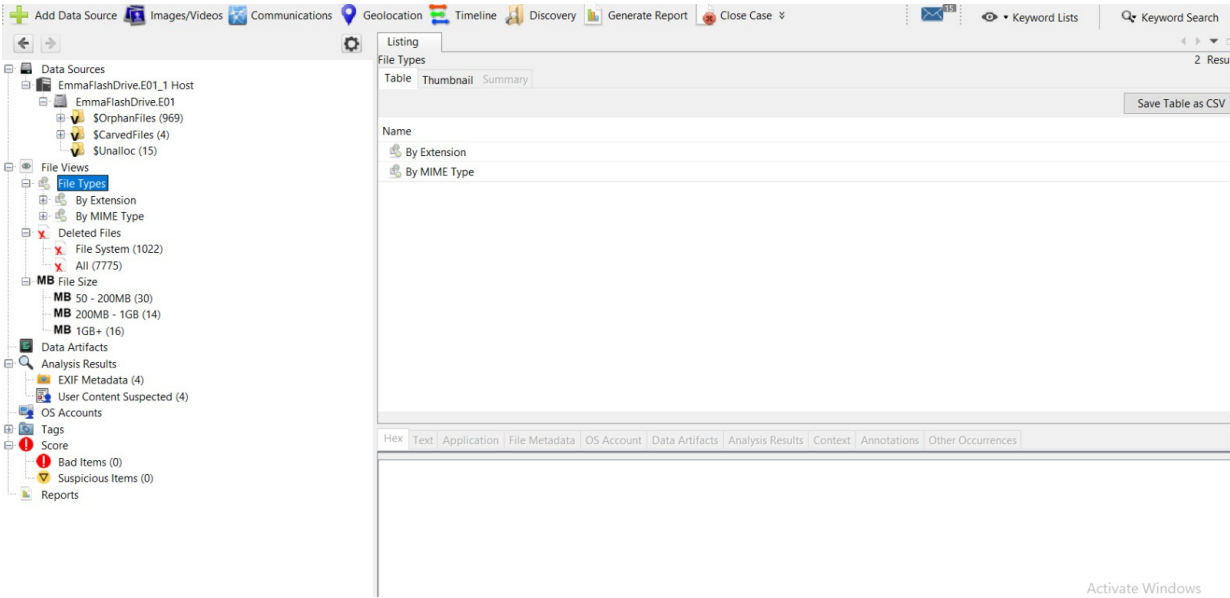
..Are you hungry Now?.....L
.....ASCII...Location - Not Mcd
onalds.....
.....l.....JFIF.....H.H
.....C.....(.....l#%.
:3=<9387@H\N@DWE78PmQW_bghg>Mqypd
x\egc...C...../.../cB8Bcccccccccc
cccccccccccccccccccccccccccccccccc
cccccccc.....j..".
.....
|......}.....!lA..Qa."q
.2....#B...R..\$3br.....%&'()*4
56789:CDEFGHIJSTUVWXYZcdefghijstu
vwxyz.....
.....
.....
.....w
.....!1..AQ.aq."2...B.....#3R..
br...\$4.%.....&'()*56789:CDEFGHIJ
STUVWXYZcdefghijstuvwxyz.....

Recovered string related to hunger / Mcdonalds clue.

```
|.....JFIF.....,.,.....Exif..MM.  
*.....J.....Z..  
.....b.(.....  
....jHaha Good Try. ....,.....,  
.....  
.....JFIF.....,.,..  
...C.....(.....1#%.(:3  
=<9387@H\N@DWE78PmQW_bghg>Mqypdx\  
egc...C...../.. /cB8Bcccccccccccc  
cccccccccccccccccccccccccccccccc  
cccccc.....h....".....  
.....  
.....}.....!1A..Qa."q.2  
....#B...R..$3br.....%&'()*456  
789:CDEFGHIJSTUVWXYZcdefghijstuvw  
xyz.....  
.....  
.....  
.....w..  
.....!1..AQ.aq."2...B.....#3R..br
```

Recovered string “Haha Good Try”, likely a decoy or challenge artefact.

Appendix C: Flash drive screenshot



Autopsy view of EmmaFlashDrive.E01 showing orphan files, carved files, EXIF metadata and user-content-suspected categories.

Appendix D: Data files reviewed

Source	Files / record count summary
Huawei phone	H_Chats 367; H_Contacts 65; H_CallLog 15; H_Emails 71; H_Location 391; H_Database 1,021; H_Text 5,655; H_Uncategories 18,779; plus archive, cookies, autofill and user records.
Nokia phone	N_Locations 30; N_Text 39; N_Database 16; N_Uncategories 253; N_Archive 1.
Samsung phone	S_Locations 283; S_Document 7; S_Uncategories 73; S_Archive 1.
Note 14 phone	Not_Location 49; Note_Text 36; Note_Uncategories 220.
Flash drive	File System 1,022; OrphanFiles 969; Archives 277; Carved_1 1,996; Carved_2 1,998; Carved_3 1,998; Carved_4 761.