Expert Witness Report

Title of the Action: Digital Forensics Analysis Report

Case Reference Number: DFI-JS04

Dated: 26th January 2024

Specialist Field: Digital Forensics Analyst

On behalf of Claimant: Jack Shroff

On the instructions of: Detective Chief Inspector Stafford

Subject Matter:

Luke Dawson

P2665421
De-Montfort House,
De Montfort University,
The Gateway,
Leicester LE1 9BH

Summary Background of the case

In August 2023, Mr Jack Shroff imported a batch of branded clothing, this clothing was then stored in a rented container near Fosse Park. Then on the 4th of November 2023, a fire broke out at the storage facility, destroying the merchandise Mr Shroff had stored. During this incident, an individual named Sergo, who was associated with Mr Shroff, was found unexpectedly deceased.

Leicestershire Police have initiated an investigation into the fire and the subsequent death. Mr Shroff, having been away on business at the time of the fire, has since contacted his insurance company to file a claim. The insurance company is awaiting a police report before carrying out the claim. Pieces of metal, thought to be from a fuel can, were later discovered at the site by police. This has caused the police to start treating the cause of the fire and Sergos death as suspicious and have executed a search and seizure warrant at Mr Shroffs house. All of Mr Shroffs electronic devices have been seized and are being forensically analysed to see if there is any implication considering laws including Computer Misuse, murder, fraud etc…

Summary of my conclusions

This report concludes that, based on the evidence analysed, there is a significant suggestion of premeditated actions orchestrated by Mr Shroff and his associates “Job” and “Rob”, leading up to the events at the storage unit and the death of Sergo. The communications on Mr Shroffs mobile phone activities, particularly with his associates, align with the timeline of the incident and suggest a deliberate effort to alter circumstances at the storage container, as indicated by text messages detailing the movement and storage of a “can” and plans to remove items.

Additionally, the discovery of images on Mr Shroffs phone, which show a jerry can and petrol station, further support the theory of intentional planning. The analysis of the SSD and USB drive has shown encrypted documents containing explicit instructions that could be constructed as a strategy to create the fire that occurred at the storage container, potentially leading to Sergos death. The presence of these documents, along with a browsing history that includes searches for insurance companies and fuel cans, further implies a motive that may be financially driven.

Furthermore, emails taken from the SSD point towards coordination among Mr Shroff “Rob” and “Joji”, especially concerning the collection and placement of a “CAN” at the storage container, along with the disabling of the fire door and fire alarm, implicating them in the planning process. The evidence taken strongly indicated a level of conspiracy and premeditation that necessitates

further inquiry into the intentions and actions of Mr Shroff and his associates. While the current evidence does not definitively establish guilt, it does create a compelling argument that warrants further investigation. These conclusions are created after looking through digital evidence available at this time, and additional material evidence could potentially affirm or modify this conclusion.

Those involved

1. **Mr Jack Shroff:** Owner of the clothing inventory that was destroyed in the fire. Has filed a claim with his insurance company following the incident.
2. **Sergo (Last Name N/A):** Deceased individual who was found unexpectedly dead and was known to work with Mr Shroff.
3. **Leicestershire Police:** The law enforcement agency conducting the investigation into the fire and Sergos death.
4. **Detective Chief Inspector Stafford:** The officer leading the Major Investigation into the incident.
5. **Home Office Pathologist:** The medical professional chosen to conduct the post-mortem examination of Sergo.
6. **Insurance Company:** The people processing Mr Shroffs claim regarding the damages caused in the fire.

Technical Terms and Explanation

Throughout this report, any and all technical terms related to digital forensic and the investigation will be highlighted in **Bold.** These terms will be defined upon their initial use within the body of the report and will also be included in the appendix for easy reference.

The appendix will also contain extracts from published works and guidelines that were referenced during the investigation analysis, including the ACPO guidelines. For the understanding, the appendix will also feature diagrams and photographs that help aspects of the case.

The purpose of the report

The purpose of this expert witness report is to provide a professional and objective analysis of the evidence obtained during my digital investigation into the fire incident at a storage unit in Leicester and the subsequent death of Sergo, an associate of Mr Shroff.

1. **Crime Scene Visit:** Documentation and analysis of digital evidence discovered at the crime scene.
2. **Data Acquisition and Analysis:** Detailed account of the process, securing and analysing of digital data from Mr Shroffs data
3. **Expert Opinion:** To provide insight into the digital evidence significance without rendering an opinion.
4. **Discussion about the Laws:** Determining whether the digital evidence relates to possible violations of:
    - The Computer Misuse Act
    - Murder
    - The Fraud Act
    - False imprisonment
    - Criminal Damage Act
5. **Assumed Facts:** To list the foundational facts as they are presented and accepted.
6. **Enquires into the facts:** To explain the experts approach and methods.
7. **Documents:** Describe the digital documents and records evaluated during the investigation.

My Investigation

The purpose of this section is to lay a foundation for the analysis and opinions expressed in this report. This is achieved by detailing the observations made during the visit to the crime scene, the methods used in the collection of the evidence, and the chronological record of the investigation process.

Crime Scene Visit

The crime scene was located at Jack Shroff's house, 384 Grasmere Street, LE2 7DA, Leicester. Upon arrival, a thorough investigation of the premises was conducted. The residence consisted of both living space and areas where business activities were apparent, including a home office setup with various digital devices.

- **Location:** The home office is located within the residential premises at 384 Grasmere Street, LE2 7DA, Leicester.
- **Physical Appearance:** The office is moderately spacious with a desk cluttered with various items including digital devices such as monitors, keyboards, and computer mice, suggesting active use.

- **Potential Evidence:** Focus was given to the digital equipment that could potentially harbor relevant data. This includes a desktop computer setup with input devices and a mobile phone, these were all photographed and prepared for forensic analysis
- **Evidence Collection:** The evidence collection process was taken with precision. The evidence collection began at 09:35 on the 16th November 2023 and ended at 10:14 the same day, each device was carefully documented, with serial numbers and model details noted. Forensic imaging of the computers Hard Drives, USBs and other devices were conducted using write-blocking technology to ensure data integrity.
- **Pictorial Evidence:** Photographic evidence was taken including a series of high-resolution images capturing the overall layout of the office, individual close-ups of the digital devices, and their connection setups, allowing for a clear view of the work environment and the condition of potential evidence at the time of the investigation.
- **Appendix:** For Pictorial Evidence and annotations of the forensic imaging done at the crime scene please see Appendix

Data Acquisition and Analysis

Acquisition

Mobile Phone:

- The mobile device, owned by Mr Shroff, was handled following the strict chain of custody protocols to maintain its integrity and security.
- The phone was isolated from network connections to prevent remote access and potential data alteration.
- The device was forensically imaged using Cellebrite Reader, ensuring a copy of the data. The imaging process was done on 10/11/23 at 09:15 am, ensuring ACPO guidelines were met.
- Post-imaging, the data's integrity was verified with a hash function, with the results documented for authenticity.

Solid State Drive (SSD):

- After retrieving Mr Shroffs Solid State Drive (SSD), a chain of custody was established to maintain the integrity and security of the evidence.

- The SSD was then attached to a write blocker and inserted in the computer.
- The SSD was taken into FTK imager where a write blocker was used to safely extract an E01 file of data copying a bit for bit version without overriding any important information or alterations occurring.
- After extracting the file, it was taken into the forensic software Autopsy to be forensically imaged and analysed for evidence.
- In order to ensure the data was accurate a hash value was calculated and noted for the forensic image to keep integrity throughout the analysis.

USB:

- The USB device was received and immediately logged to maintain a clear chain of custody.
- To ensure the device was not altered or tampered with a write blocker was used during the acquisition process.
- A forensic image of the USB drive was created on FTK imager to preserve the state of the data for analysis.
- Hash values of the forensic image were then generated and recorded to verify the integrity of the data at all stages of the analysis.

Analysis

Mobile Phone:

- Using Cellebrite software, the forensic image of the phone categorised data into different types, including call logs, text messages, emails, application data, internet history and location data.
- Events and communications were reconstructed around the incident data, focusing on relevant information.
- Data timestamps were cross-referenced with metadata to confirm accuracy.
- Examination of text messages and instant messages revealed conversations with certain people of interest, particularly messages exchanged with individuals named “Job” and “Rob”, indicating potential involvement or knowledge about the incident.
- Photos and videos were also analysed, paying close attention to metadata for creation dates, times, and locations to place the device at specific locations at relevant times.
- Images such as IMG_0006 and IMG_0003 were analysed to establish their relation to the incident.

- The browsing history was reviewed to identify any searches or website visits that could be related to the incident or show preparatory actions.

Images: Multiple images were found in Mr Shroffs camera roll that were relevant to the investigation.

- **IMG_0006:** IMG_0006 is a photo taken on Mr Shroffs phone that appears to be a website selling a Jerry Can, the picture was taken on 23/10/2023.
- **IMG_0003:** IMG_0003 is a photo of what appears to be a wooden container, the image was taken on 10/10/2023.
- **IMG_A:** IMG_A is a photo in a text exchange between Mr Shroff and Job that shows an address, number and website for a Shell petrol station.

Text Messages: Various text chains were found between Jack Shroff and a new individual called “Job”.

- **Text_A:** From Mr Shroff to Job “Come here around 2:30pm”- the text is then followed by a link to a picture (See appendix …)
- **Text_B:** From Job to Mr Shroff “Thumbs up emoji”
- **Text_ C:** From Mr Shroff to Job “Rob will come to see you this afternoon. Handover the can to Rob.”
- **Text_D:** From Job to Mr Shroff “I have moved electricity Generator to the storage.”
- **Text_E:** From Job to Mr Shroff “Tonight we will try to remove things. Yesterday we couldn’t.”

Solid State Drive (SSD):

- The forensic image was examined using Autopsy, allowing for a comprehensive review of all the different files and directories, including any hidden or deleted files.
- The internet browsing history was analysed to uncover any relevant searches or website visits, with attention focused on to the time frame around the incident.
- Documents and multimedia files were reviewed for content that could be pertinent to the case. Metadata for these files was also examined for creation dates, modification dates, and author information.
- A key focus was made into email archives that were searched for communications related to the incident, with a focus on senders, recipients, dates, and email content.

Emails: after looking through Mr Shroffs emails, multiple exchanges between Mr Shroff

and two different people (Rob and Joji). See Appendix … for more information.

- **Email_A:** From Jack Shroff to Joji “This seems a good option. Enough capacity. Top Tech 20ltr Petrol metal Jerry Can (Green)… Get it.”
- **Email_B:** From Jack Shroff to Joji “Come to Sports Lounge Oadby (115, LE25DP) at 7:30pm. We need to discuss and finalise a few things.”
- **Email_C:** From Jack Shroff to Rob “Come to Sports Lounge Oadby (115, LE25DP) at 7:30pm. We need to discuss and finalise a few things.”
- **Email_D:** From Jack Shroff to Rob “Collect CAN from Joji when you see him this afternoon. As discussed on 26th Oct. Place it in the storage. Also take Sergo with you as he knows.”
- **Email_E:** From Jack Shroff to Rob “Please find the list of tasks in the attachments. Use the password which I gave you last Thursday.”
- **Email_F:** From Jack Shroff to Rob “Great!!”
- **Email_G:** From Jack Shroff to Rob “Collect CAN from Joji when you see him this afternoon. As discussed on 26th Oct. Place it in the storage. Also take Sergo to the storage with you this Saturday. Have you managed to complete the exit door and alarm task?”

Browsing History: after looking through Mr Shroffs browsing data, various searches for insurance companies and different Jerry Cans were found. See Appendix Number … for more information.

- **BH_A:** Multiple searches for Insurance and Fuel Cans
- **BH_B:** Links to buying options of different Fuel Cans

Encrypted Files: after looking through Mr Shroffs SSD, some encrypted files were found and decrypted in order to find what information Mr Shroff was hiding. See Appendix Number … for more information.

- **EF_A:** Multiple encrypted documents located on Mr Shroffs SSD
- **EF_B:** Rob.docx File decrypted – “As discussed in our meeting on 26th Oct. Sergo knows our intentions… he is not supportive… leave him to complete some tasks (give him anything to complete) … disable the fire alarm and exit door unlocking systems… when things calm down remove these things asap.”

USB:

- The file system on the USB was thoroughly examined for any hidden, deleted, or encrypted system files that could be valid in this investigation.

- Extensive searches were conducted using specific terms relevant to the case.
- A timeline of file creation and modification was constructed to identify any potential activity.

Expert Opinion

Based on the comprehensive forensic evidence found after the investigation was conducted, it is in my professional opinion that there is substantial evidence that suggests premeditated actions leading up to the fire incident at the storage unit and the death of Sergo. The forensic analysis of the mobile phone owned by Mr Shroff revealed a series of communications with associates referred to as “Job” and “Rob”, that coincide with the timing of the incident. The content discussed in these messages, particularly Text_C which instructs the handover of a “can” to Rob, and Text_E discussing the removal of items on a specific night.

The discovery of images such as IMG_0006, which shows a website selling a jerry can dated prior to the incident, coupled with IMG_A, which is a photo in a text exchange indicating a Shell petrol station. These findings, when analysed in conjunction with the text messages, imply that there was a plan involving fuel cans. The examination of the SSD and USB drive also owned by Mr Shroff revealed encrypted documents that, once being decrypted, contained explicit instructions that raise concerns. The contents of EF_B, specifically, hint at intentional sabotage by asking Rob to “disable the fire alarm and exit door unlocking systems”.

Browsing history analysis has also uncovered searches for insurance companies and fuel cans (BH_A and BH_B), which could indicate motives related to financial gain and further planning. Furthermore, the emails, particularly Email_D and Email_G, clearly outline instructions to collect a “CAN” from Joji and to take Sergo to the container; this can be interpreted as implicating both Rob and Joji in the planning of the events as associates to Mr Shroff. It is my professional opinion that the evidence suggests that further investigation into Mr Shroff and his associates is necessary to determine their involvement in the incident. This is based solely on the digital evidence available at this time, and further material evidence may reinforce or alter the conclusions drawn.

Discussion about the Laws

Computer Misuse Act 1990

- **Definition of the law:** This Act makes it an offence to access or modify computer material without authorisation, or to impair the operation of any computer intentionally or recklessly.
- **Who does the law apply to?** This Act can potentially be applied to Mr Jack Shroff and his associates, based on the digital evidence indicating manipulation of digital content.
- **How does it apply?** By accessing and modifying the computer systems and data related to the planning and execution of the incident, both at the physical location of Mr Shroffs office and through online communications.
- **Evidence and References:** Encrypted files on SSD (EF_B), communications regarding actions related to planning (Text_C & Text_E).

Murder - Common Law

- **Definition of the law:** Murder is the unlawful killing of another human being with the ***Intent*** to kill or cause grievous bodily harm to another.
- **Who does the law apply to?** If intent can be established then Mr Shroff and/or his associates can be tried for the murder of Sergo.
- **How does it apply?** Through the planning and execution of actions that led to Sergos death, at the location of the storage unit where the incident took place.
- **Evidence and References:** Communications suggesting premeditation and planning (Text_C & Text_E) actions taken to disable systems (EF_B).

Manslaughter - Common Law

- **Definition of the law:** Manslaughter is similar to Murder but without the intent to kill or cause bodily harm, often resulting from an illegal act or negligence.
- **Who does the law apply to?** Mr Shroff and his associates, if it can be shown that their actions were negligent leading to death.
- **How does it apply?** If the death of Sergo occurred without intentional killing but through negligence or other unlawful acts at the storage unit
- **Evidence and References:** Encrypted files that could lead to a dangerous environment (EF_B) and text message (Text_C & Text_E)

The Fraud Act 2006

- **Definition of the law:** This Act defines fraud as a false representation, failing to disclose information.
- **Who does the law apply to?** Potentially Mr Shroff, if it can be proven that he intended to deceive the insurance company.

- **How does it apply?** Through the intentional setting of a fire to claim insurance money.
- **Evidence and References:** Searches for insurance companies (BH_A), evidence suggesting planning of the fire incident (IMG_0006, Text_C and Text_E)

False imprisonment - Common Law

- **Definition of the law:** False imprisonment occurs when a person is unlawfully restrained against their will
- **Who does the law apply to?** Any involved parties
- **How does it apply?** By disabling safet systems to restrict Sergos freedom of movement within the unit
- **Evidence and References:** instructions found in the decrypted document (EF_B)

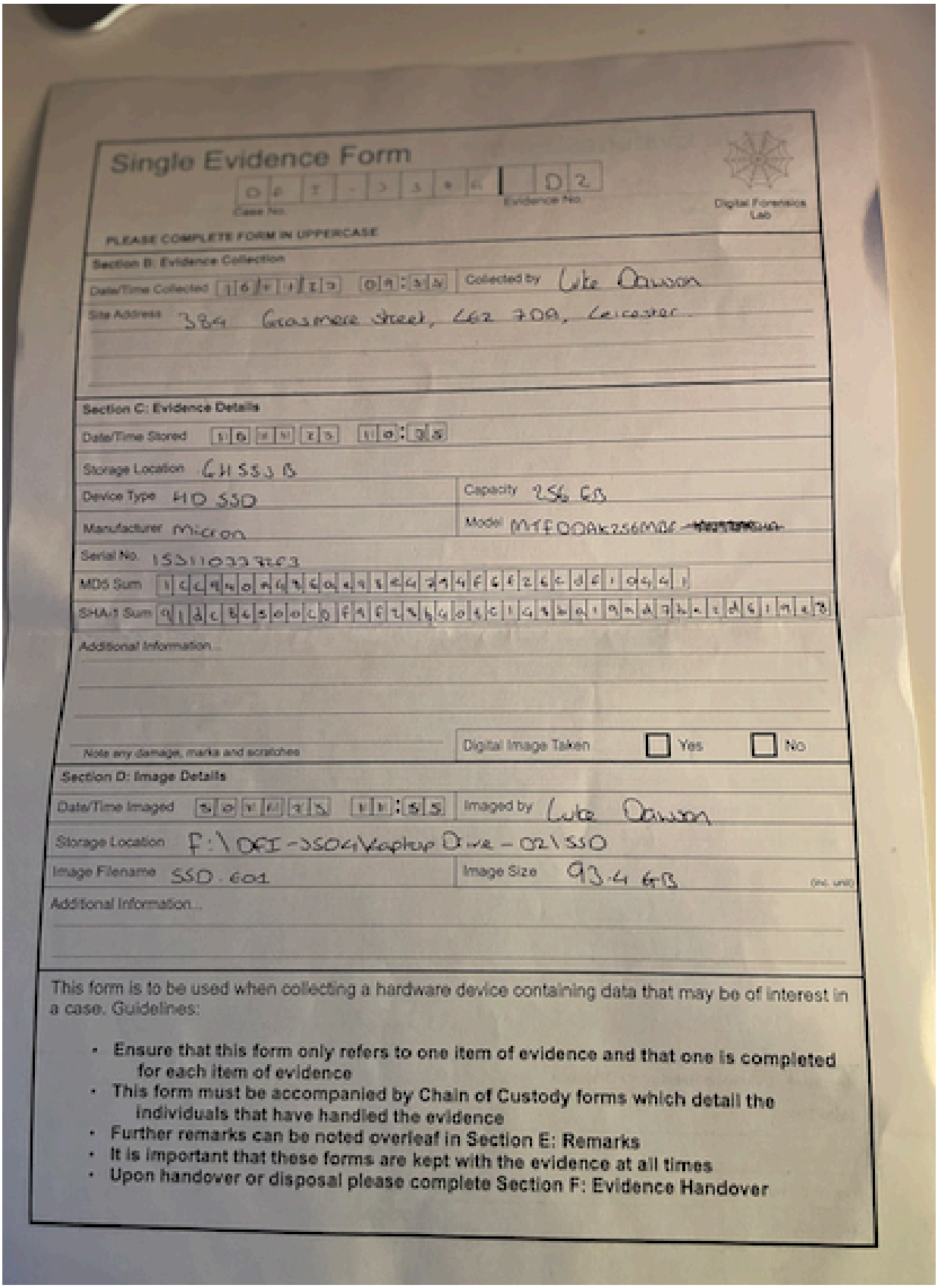
Criminal Damage Act 1971

- **Definition of the law:** This Act makes it an offence to intentionally or recklessly destroy or damage property belonging to another
- **Who does the law apply to?** Mr Shroff and his associates, if they intentionally panned the destruction of the storage unit.
- **How does it apply?** By planning and causing the fire at the storage unit, potentially using a fuel can seen in evidence.
- **Evidence and References:** Images of a website selling a Jerry Can (IMG_0006), messages discussing the procurement and placement of the can (Text_C and Text_E).

Forms

Single Evidence Forms

SSD



Single Evidence Form

Case No: 0[illegible]-[illegible] Evidence No: 02

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 16/12/23 09:55 Collected by Luke Dawson

Site Address 384 Grasmere Street, LE2 7DB, Leicester

Section C: Evidence Details

Date/Time Stored 16/12/23 10:35

Storage Location LH SSD B

Device Type HD SSD Capacity 256 GB

Manufacturer Micron Model MTFDDAK256MDF

Serial No. 153116333263

MD5 Sum [illegible]

SHA1 Sum [illegible]

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☐ Yes ☐ No

Section D: Image Details

Date/Time Imaged 20/12/23 11:55 Imaged by Luke Dawson

Storage Location F:\DFI-3504\Vaptop Drive - 02\SSD

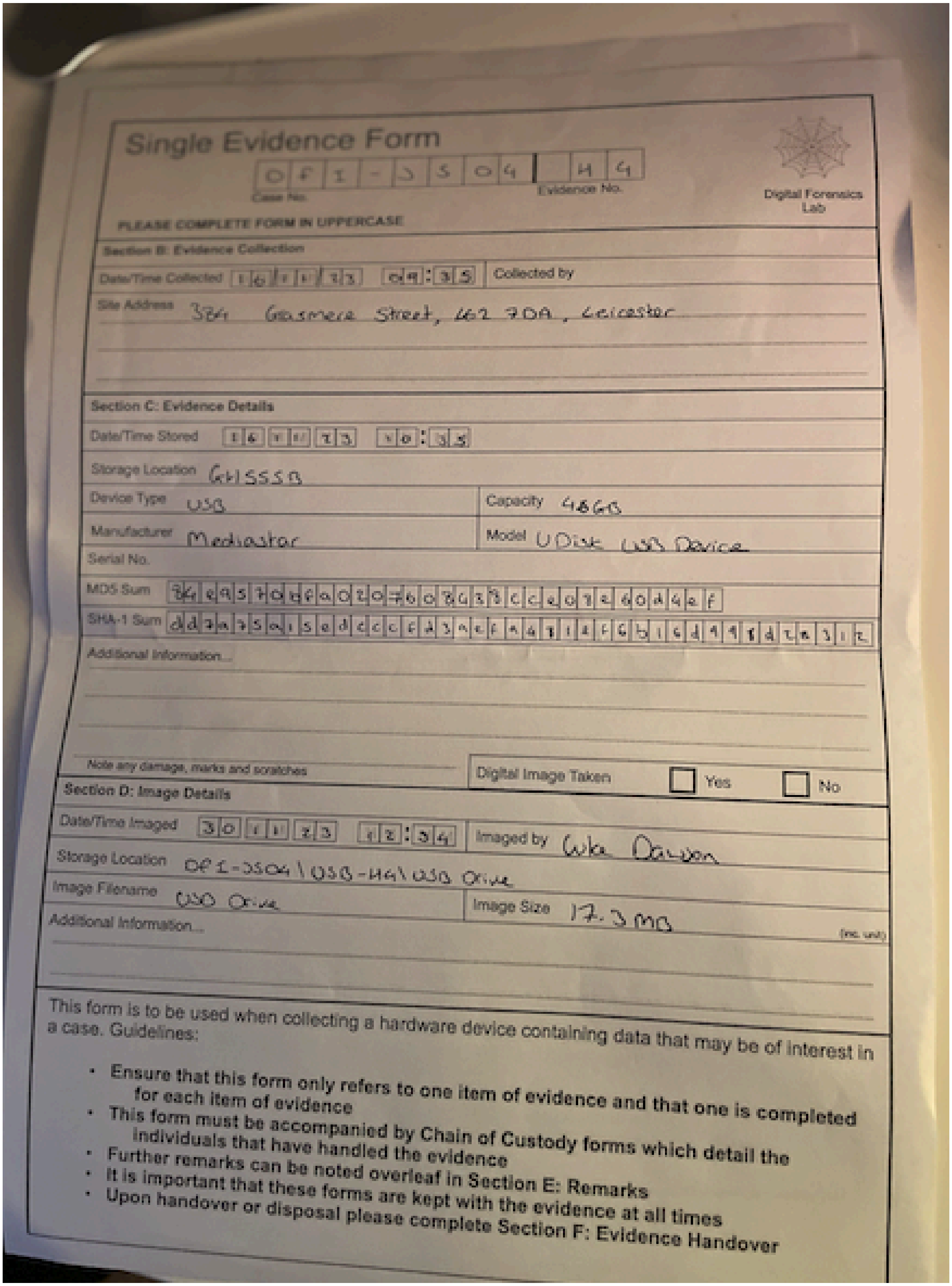
Image Filename SSD.E01 Image Size 93.4 GB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence
- This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence
- Further remarks can be noted overleaf in Section E: Remarks
- It is important that these forms are kept with the evidence at all times
- Upon handover or disposal please complete Section F: Evidence Handover

USB



Single Evidence Form

Case No. OF1-3504 Evidence No. H4

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 16/11/23 09:35

Collected by

Site Address 384 Grasmere Street, LE2 7DA, Leicester

Section C: Evidence Details

Date/Time Stored 16/11/23 10:35

Storage Location GH555B

Device Type USB

Capacity 4GB

Manufacturer Mediastar

Model UDisk USB Device

Serial No.

MD5 Sum [illegible]

SHA-1 Sum [illegible]

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☐ Yes ☐ No

Section D: Image Details

Date/Time Imaged 30/11/23 12:34

Imaged by Luka Dawson

Storage Location OF1-3504\USB-H4\USB Drive

Image Filename USB Drive

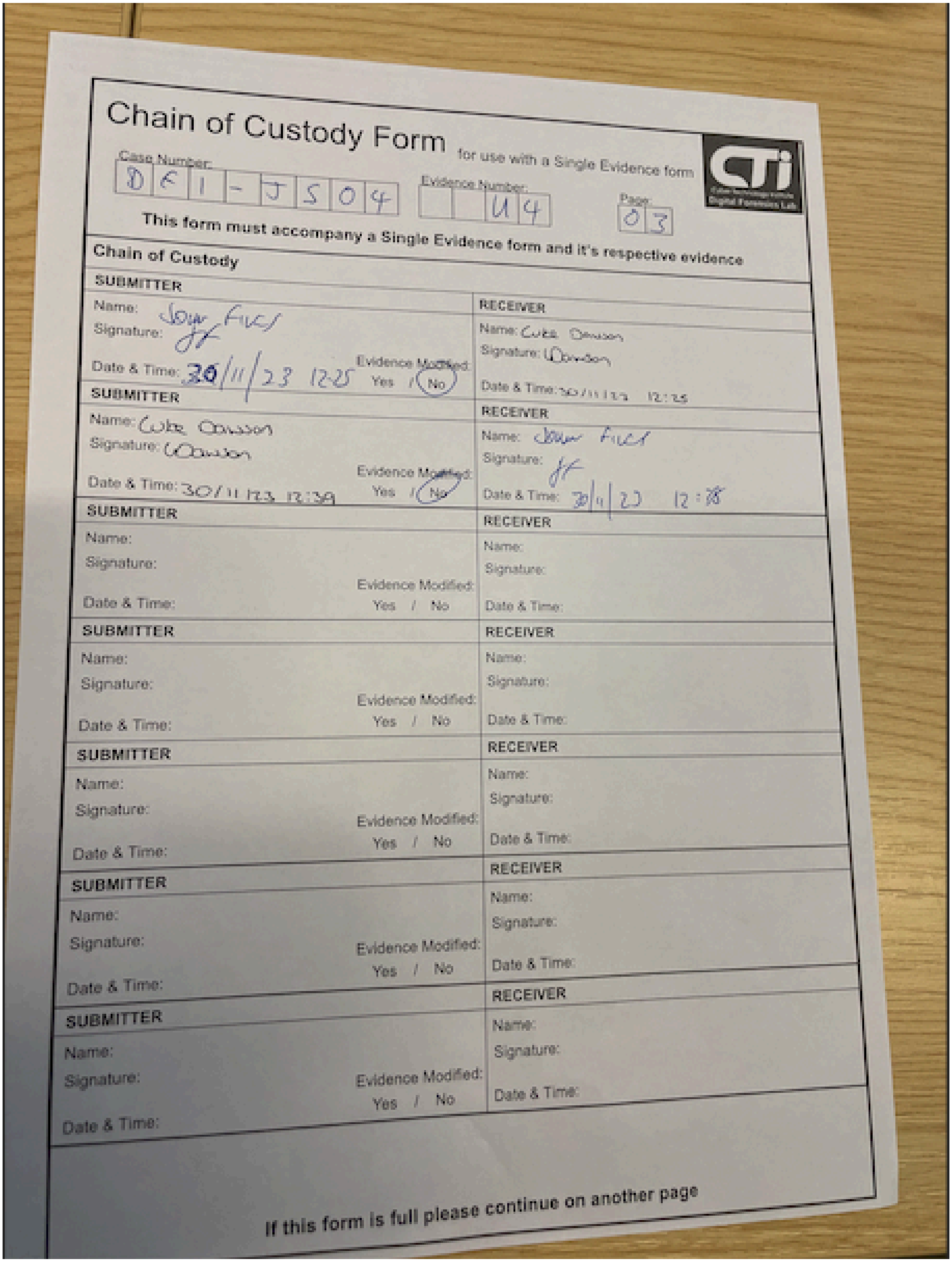
Image Size 17.3 MB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence
- This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence
- Further remarks can be noted overleaf in Section E: Remarks
- It is important that these forms are kept with the evidence at all times
- Upon handover or disposal please complete Section F: Evidence Handover

USB - H4



Chain of Custody Form for use with a Single Evidence form

CTi Cyber Technology Institute Digital Forensics Lab

Case Number: DFI-JS04

Evidence Number: U4

Page: 03

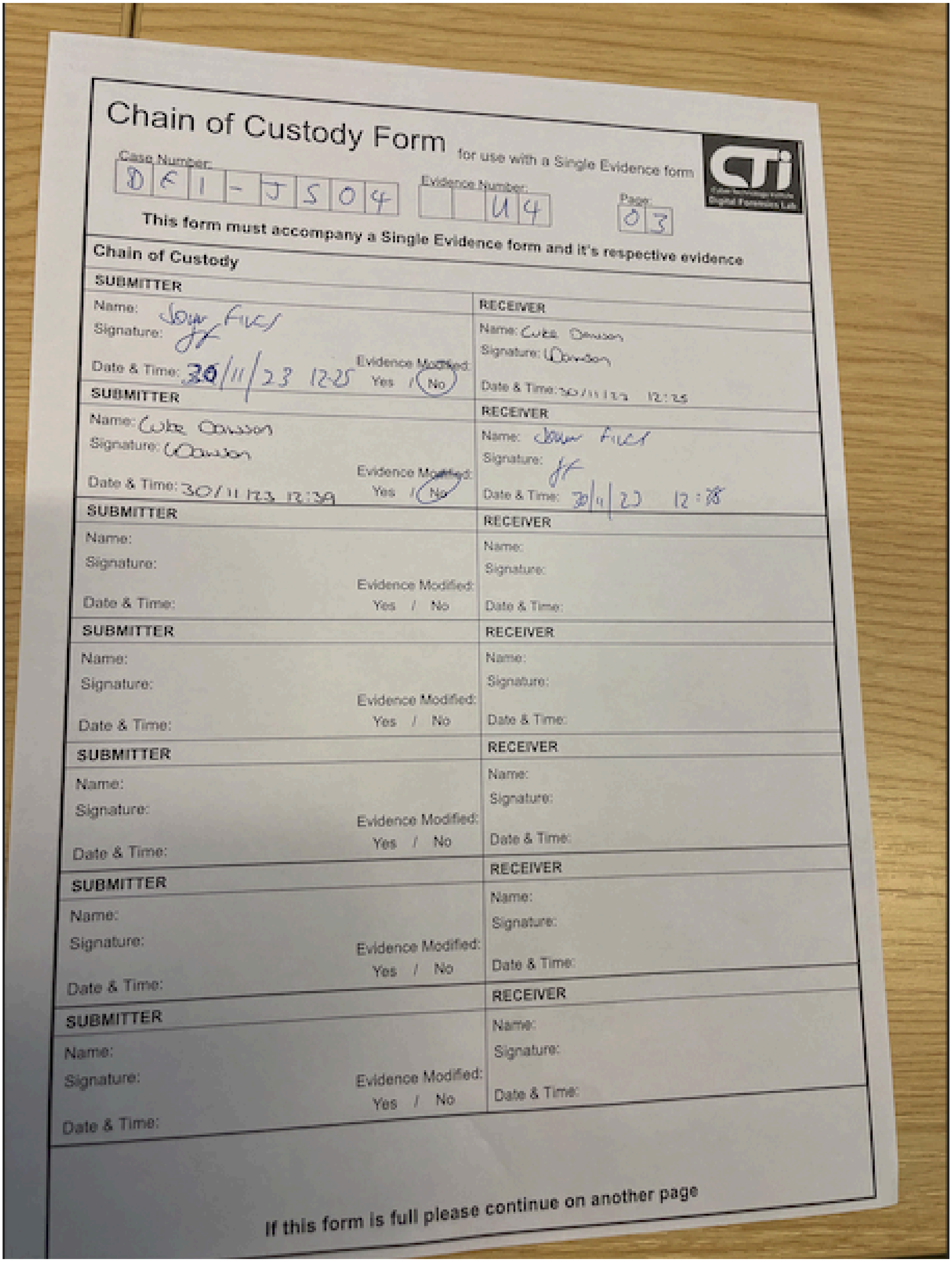
This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Name: John Filer Signature: JF Date & Time: 30/11/23 12:25 Evidence Modified: Yes / No (circled: No)	Name: Luke Dawson Signature: LDawson Date & Time: 30/11/23 12:25
Name: Luke Dawson Signature: LDawson Date & Time: 30/11/23 12:39 Evidence Modified: Yes / No (circled: No)	Name: John Filer Signature: JF Date & Time: 30/11/23 12:38
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

USB - H4



Chain of Custody Form for use with a Single Evidence form

Case Number: DFI-JS04 | Evidence Number: U4 | Page: 03

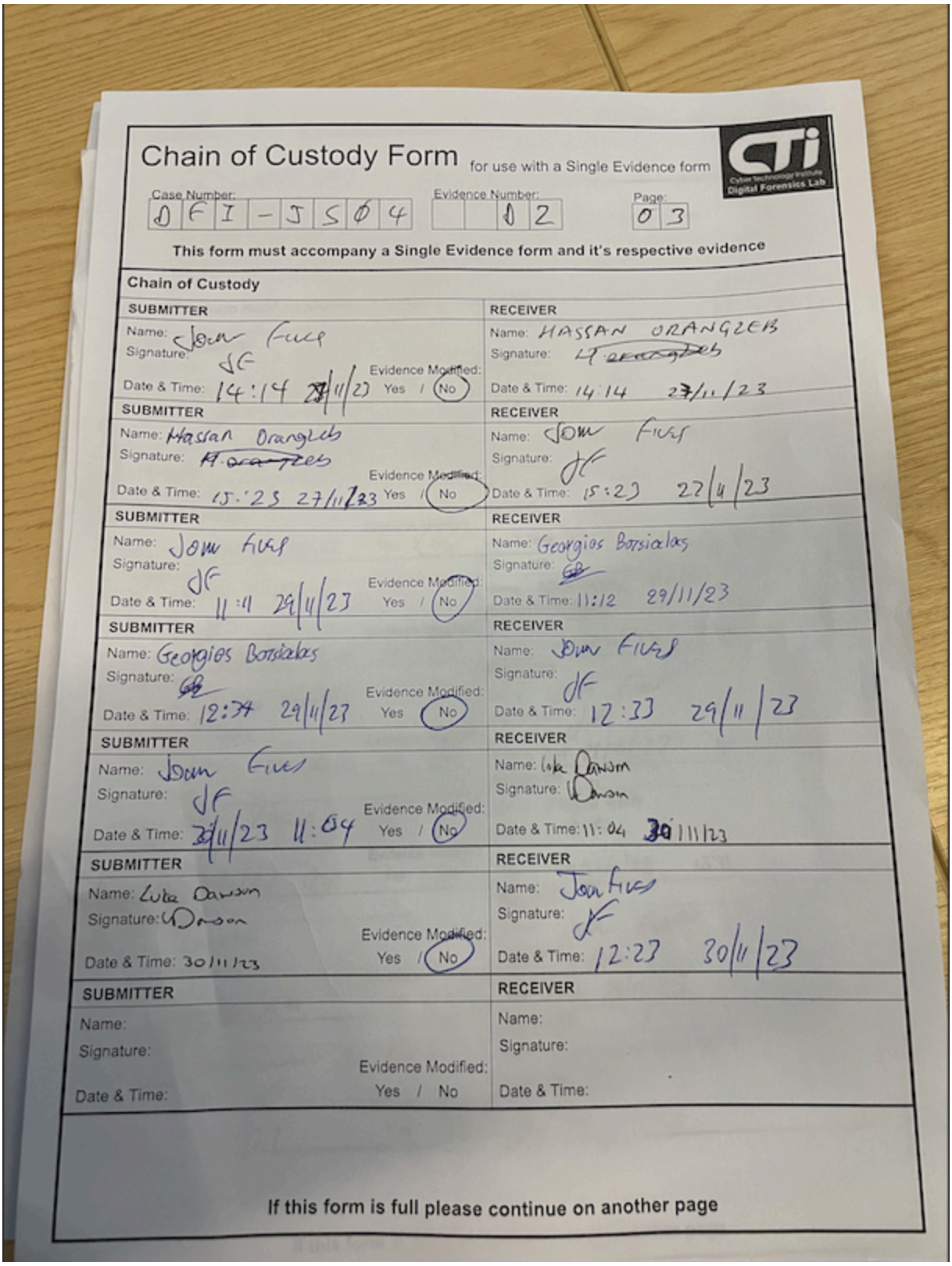
This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Name: John Fuci Signature: Date & Time: 30/11/23 12:25 Evidence Modified: Yes / No	Name: Luke Dawson Signature: Date & Time: 30/11/23 12:25
Name: Luke Dawson Signature: Date & Time: 30/11/23 13:39 Evidence Modified: Yes / No	Name: John Fuci Signature: Date & Time: 30/11/23 12:38
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

SSD - D2



Chain of Custody Form for use with a Single Evidence form

Cyber Technology Institute Digital Forensics Lab

Case Number: DFI-JS04 Evidence Number: D2 Page: 03

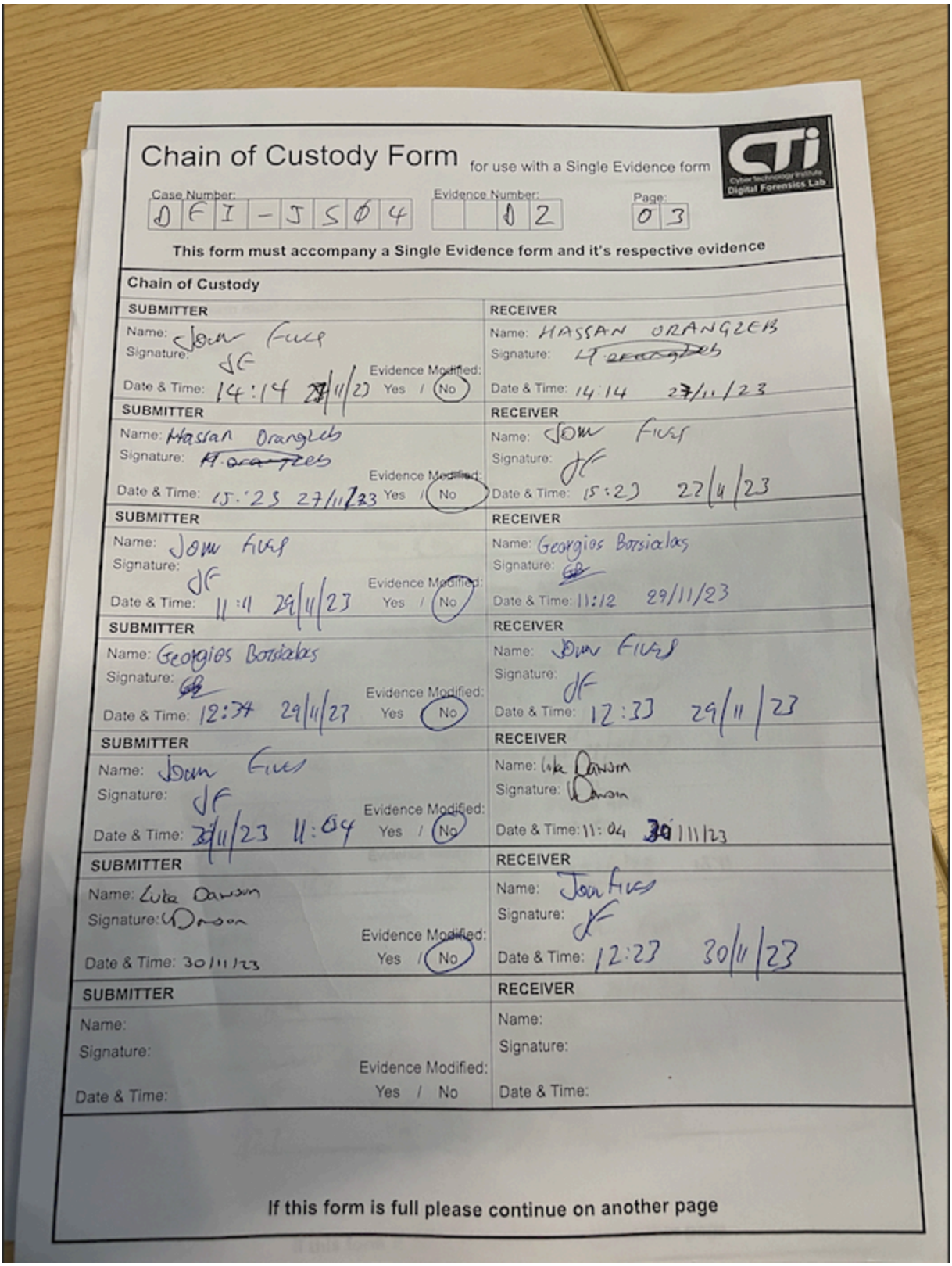
This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Name: John Fives Signature: JF Date & Time: 14:14 27/11/23 Evidence Modified: Yes / (No)	Name: HASSAN ORANGLES Signature: H Orangles Date & Time: 14:14 27/11/23
SUBMITTER	RECEIVER
Name: Hassan Orangles Signature: H Orangles Date & Time: 15:25 27/11/23 Evidence Modified: Yes / (No)	Name: John Fives Signature: JF Date & Time: 15:29 27/11/23
SUBMITTER	RECEIVER
Name: John Fives Signature: JF Date & Time: 11:11 29/11/23 Evidence Modified: Yes / (No)	Name: Georgios Borsiolas Signature: GB Date & Time: 11:12 29/11/23
SUBMITTER	RECEIVER
Name: Georgios Borsiolas Signature: GB Date & Time: 12:34 29/11/23 Evidence Modified: Yes (No)	Name: John Fives Signature: JF Date & Time: 12:33 29/11/23
SUBMITTER	RECEIVER
Name: John Fives Signature: JF Date & Time: 29/11/23 11:04 Evidence Modified: Yes / (No)	Name: Luke Dawson Signature: L Dawson Date & Time: 11:04 30/11/23
SUBMITTER	RECEIVER
Name: Luke Dawson Signature: L Dawson Date & Time: 30/11/23 Evidence Modified: Yes / (No)	Name: John Fives Signature: JF Date & Time: 12:27 30/11/23
SUBMITTER	RECEIVER
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

SSD - D2



Chain of Custody Form for use with a Single Evidence form

Cyber Technology Institute Digital Forensics Lab

Case Number: DFI-JS04 Evidence Number: D2 Page: 03

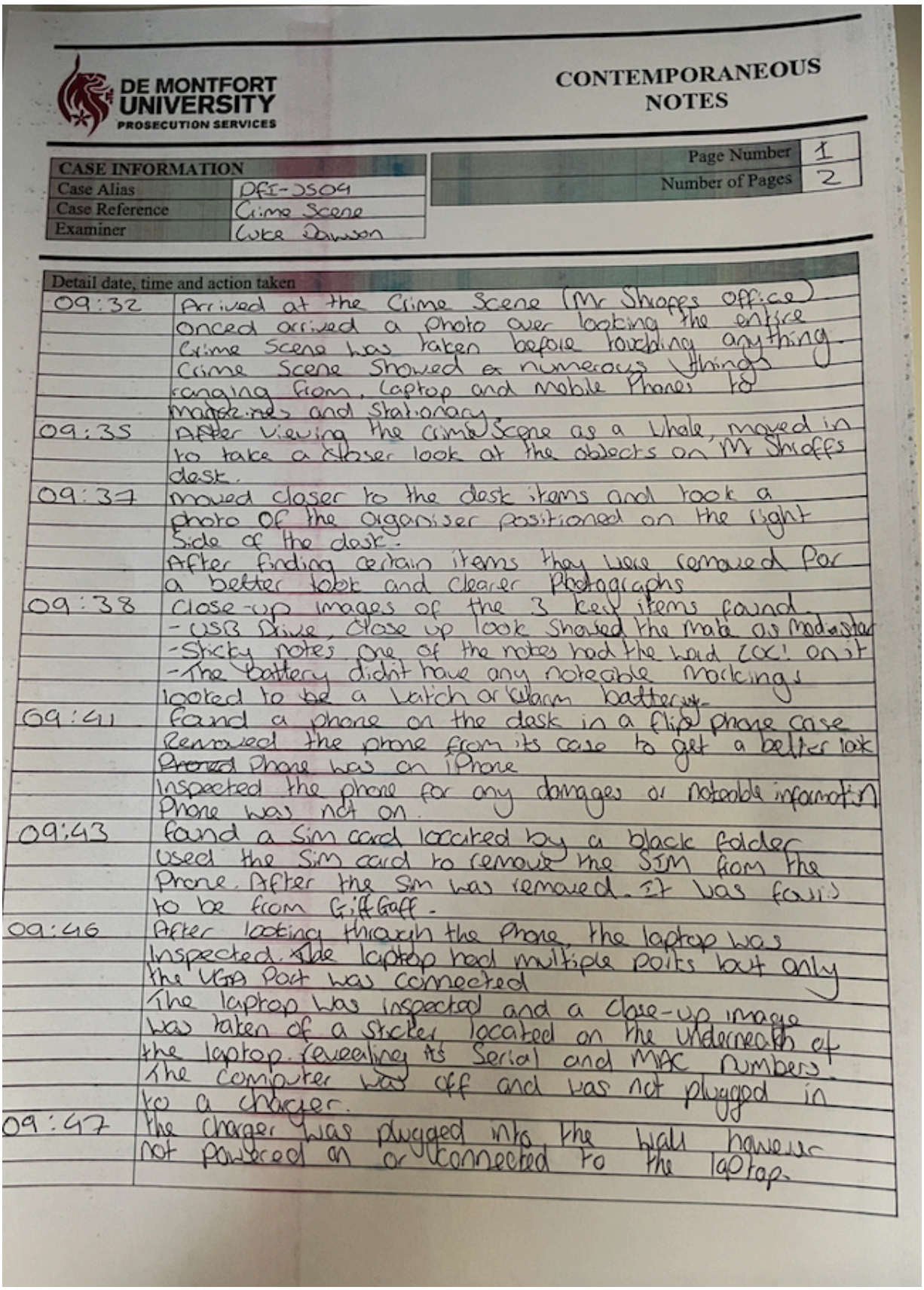
This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Name: John Finn Signature: JF Date & Time: 14:14 27/11/23 Evidence Modified: Yes / (No)	Name: HASSAN ORANGZEB Signature: H. Orangzeb Date & Time: 14:14 27/11/23
SUBMITTER	RECEIVER
Name: Hassan Orangzeb Signature: H. Orangzeb Date & Time: 15:25 27/11/23 Evidence Modified: Yes / (No)	Name: John Finn Signature: JF Date & Time: 15:25 27/11/23
SUBMITTER	RECEIVER
Name: John Finn Signature: JF Date & Time: 11:11 29/11/23 Evidence Modified: Yes / (No)	Name: Georgios Bosiakas Signature: GB Date & Time: 11:12 29/11/23
SUBMITTER	RECEIVER
Name: Georgios Bosiakas Signature: GB Date & Time: 12:34 29/11/23 Evidence Modified: Yes (No)	Name: John Finn Signature: JF Date & Time: 12:33 29/11/23
SUBMITTER	RECEIVER
Name: John Finn Signature: JF Date & Time: 29/11/23 11:04 Evidence Modified: Yes / (No)	Name: Luke Dawson Signature: L Dawson Date & Time: 11:04 30/11/23
SUBMITTER	RECEIVER
Name: Luke Dawson Signature: L Dawson Date & Time: 30/11/23 Evidence Modified: Yes / (No)	Name: John Finn Signature: JF Date & Time: 12:23 30/11/23
SUBMITTER	RECEIVER
Name: Signature: Date & Time: Evidence Modified: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

Crime Scene



DE MONTFORT UNIVERSITY
PROSECUTION SERVICES

CONTEMPORANEOUS NOTES

CASE INFORMATION	
Case Alias	DFI-0509
Case Reference	Crime Scene
Examiner	Cate Dawson

Page Number	1
Number of Pages	2

Detail date, time and action taken	
09:32	Arrived at the Crime Scene (Mr Shoppes office) Onced arrived a photo over looking the entire Crime Scene was taken before touching anything. Crime Scene showed ~~a~~ numerous things ranging from, Laptop and Mobile Phones to magazines and Stationary
09:35	After viewing the crime Scene as a Whole, moved in to take a closer look at the objects on Mr Shoffs desk.
09:37	moved closer to the desk items and took a photo of the organiser positioned on the right Side of the desk. After finding certain items they were removed for a better look and clearer Photographs
09:38	Close-up images of the 3 key items found. -USB Drive, Close up look Showed the make as Modostar -Sticky notes, One of the notes had the word 'Cat' on it -The battery didnt have any noteable markings, looked to be a watch or alarm battery.
09:41	Found a phone on the desk in a flip phone case. Removed the phone from its case to get a better look ~~Phone~~ Phone was an iPhone Inspected the phone for any damages or noteable information Phone was not on.
09:43	Found a Sim card located by a black folder. Used the Sim card to remove the SIM from the Phone. After the Sim was removed. It was found to be from GiffGaff.
09:46	After looting through the Phone, the laptop was Inspected. The laptop had multiple ports but only the USB Port was connected The laptop was inspected and a close-up image was taken of a Sticker located on the underneath of the laptop. revealing its Serial and MAC numbers. The computer was off and was not plugged in to a charger.
09:47	The charger was plugged into the wall however not powered on or connected to the laptop.

DE MONTFORT UNIVERSITY
PROSECUTION SERVICES

CONTEMPORANEOUS NOTES

Page Number	2
Number of Pages	2

CASE INFORMATION	
Case Alias	OF1-3504
Case Reference	Crime Scene
Examiner	Cate Dawson

Detail date, time and action taken	
09:47	The back of the Computer was removed. Close-up images were taken of all the important information and parts found inside the laptop. Images of the Memory were taken detailing Serial and Model numbers. An image was also taken of the Sticker placed on the bottom of the power brick attached to the charger.
09:49	Image was taken of the wall Socket which had two plugs connected (Monitor and Charger) both sockets were powered off at the wall. The Monitor was photographed along with its parts. A further wider image was taken to show all the left side items as a whole.
09:51	Close up images of the 3 Memory Sticks were taken. These were found on the desk and not connected to anything. A blue Memory Stick was revealed to be from a Company called Netgear.
09:53	Close-up images of the Magazines found on the desk. - Private Eye, Amethyst and Info Security.
09:55	Left the Crime Scene.

Mobile Phone & Sim Card

DE MONTFORT UNIVERSITY PROSECUTION SERVICES

Contemporaneous Notes

Cyber Technology Institute Digital Forensics Lab

Case Information	
Case Alias	"SHROFF"
Case Number	DFI - JS04
Examiner	JF

Page Number	1
Number of Pages	2

Date & Time	Details of Actions
10/11/23 09:15	RECEIVED iPHONE - SWITCHED OFF FIGURE 1
	MODEL A1688 FIGURE 2
	REMOVED SIM CARD
	IMEI NUMBER FROM SIM TRAY: 353798080528088
	NOTED CONFIRMING ON DEVICE FIGURE 3
	GIFF GAFF SIM 0066565623328 4Ggg4 FIGURE 4
09:30	SWITCHED PHONE ON - NO PIN
	TURNED WIFI OFF FIGURE 5
	TURNED BLUETOOTH OFF
	SWITCHED AIRPLANE MODE ON
	NOTED APPLE ID IS "JACK SHROFF"
	DISABLED SCREEN LOCK FIGURE 6
	FROM SETTINGS → ABOUT
	IPHONE 6S (A1688)
	IOS 15.7.9
	MODEL NKQN2ZD/A
	SERIAL FRDSR4IWGR49
	IMEI : 353798080528088 (CONFIRM) SIM TRAY
10:00	STARTED UFED 7.66.1.150, PICTURES UFED1 → 12
	SEARCHED USING IMEI TO ID MODEL (A1688)
	SELECT ADVANCED LOGICAL - USE CABLE 210
	FILE SYSTEM SELECTED, CONNECT PHONE WITH HUB/CABLE
10:11:36	ACQUISITION STARTED - TRUST COMPUTER WHEN ASKED
10:17:22	ACQUISITION COMPLETE

DE MONTFORT UNIVERSITY
PROSECUTION SERVICES

Contemporaneous Notes

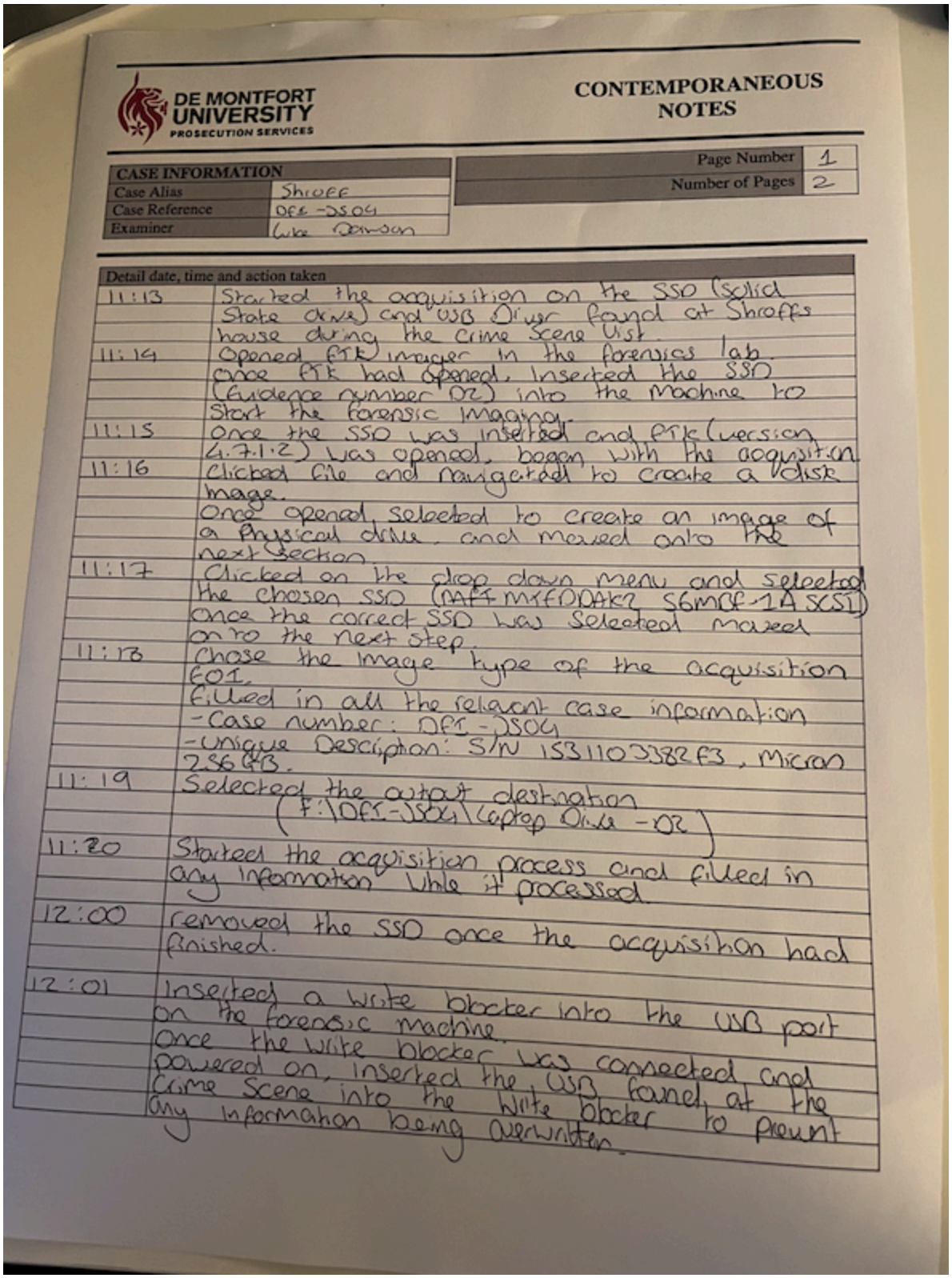
Cyber Technology Institute
Digital Forensics Lab

Case Information	
Case Alias	'SHERFF'
Case Number	DFI - JS04
Examiner	JF

Page Number	2
Number of Pages	2

Date & Time	Details of Actions
10:13:30	ADDITIONAL UFED 7.3 - SELECT ALL (UFED 1.4)
	SELECTED LOGICAL (PARTIAL) - TRUST WHEN ASKED UFED
10:14:52	ACQUISITION STARTED - ENCRYPT - YES 1234 PW= UFED
10:15:44	ACQUISITION COMPLETE
16/11/23 13:00	CONNECTED SIM CARD TO PC USING MULTI SIM
	ADAPTER SIM_FIG1
	STARTED UFED 7.66.1.150 SIM_FIG2
	SELECT SIM + STORAGE DIR SIM_FIG3, 4, 5, 6
13:05:51	ACQUISITION STARTED
13:06:29	ACQUISITION COMPLETE SIM_FIG7
	ACQUISITION STAGE COMPLETED

USB and SSD Acquisition



DE MONTFORT UNIVERSITY
PROSECUTION SERVICES

CONTEMPORANEOUS NOTES

CASE INFORMATION	
Case Alias	Shroff
Case Reference	DFI-0504
Examiner	Luke Dawson

Page Number	1
Number of Pages	2

Detail date, time and action taken	
11:13	Started the acquisition on the SSD (Solid State drive) and USB Driver found at Shroffs house during the crime scene visit.
11:14	Opened FTK imager in the forensics lab. Once FTK had opened, inserted the SSD (Evidence number 02) into the machine to start the forensic imaging.
11:15	Once the SSD was inserted and FTK (version 4.7.1.2) was opened, began with the acquisition.
11:16	Clicked file and navigated to create a disk image. Once opened, selected to create an image of a Physical drive, and moved onto the next section.
11:17	Clicked on the drop down menu and selected the chosen SSD (MTFMXFDAK2 S6MSF-1A SCSI) Once the correct SSD was selected moved on to the next step.
11:18	Chose the image type of the acquisition E01. Filled in all the relavant case information -Case number: DFI-0504 -Unique Description: S/N 153110338283, Micron 256GB.
11:19	Selected the output destination (F:\DFI-0504\Laptop Drive-02)
11:20	Started the acquisition process and filled in any information while it processed.
12:00	removed the SSD once the acquisition had finished.
12:01	Inserted a write blocker into the USB port on the forensic machine. Once the write blocker was connected and powered on, inserted the USB found at the Crime Scene into the write blocker to prevent any information being overwritten.

DE MONTFORT UNIVERSITY
PROSECUTION SERVICES

CONTEMPORANEOUS NOTES

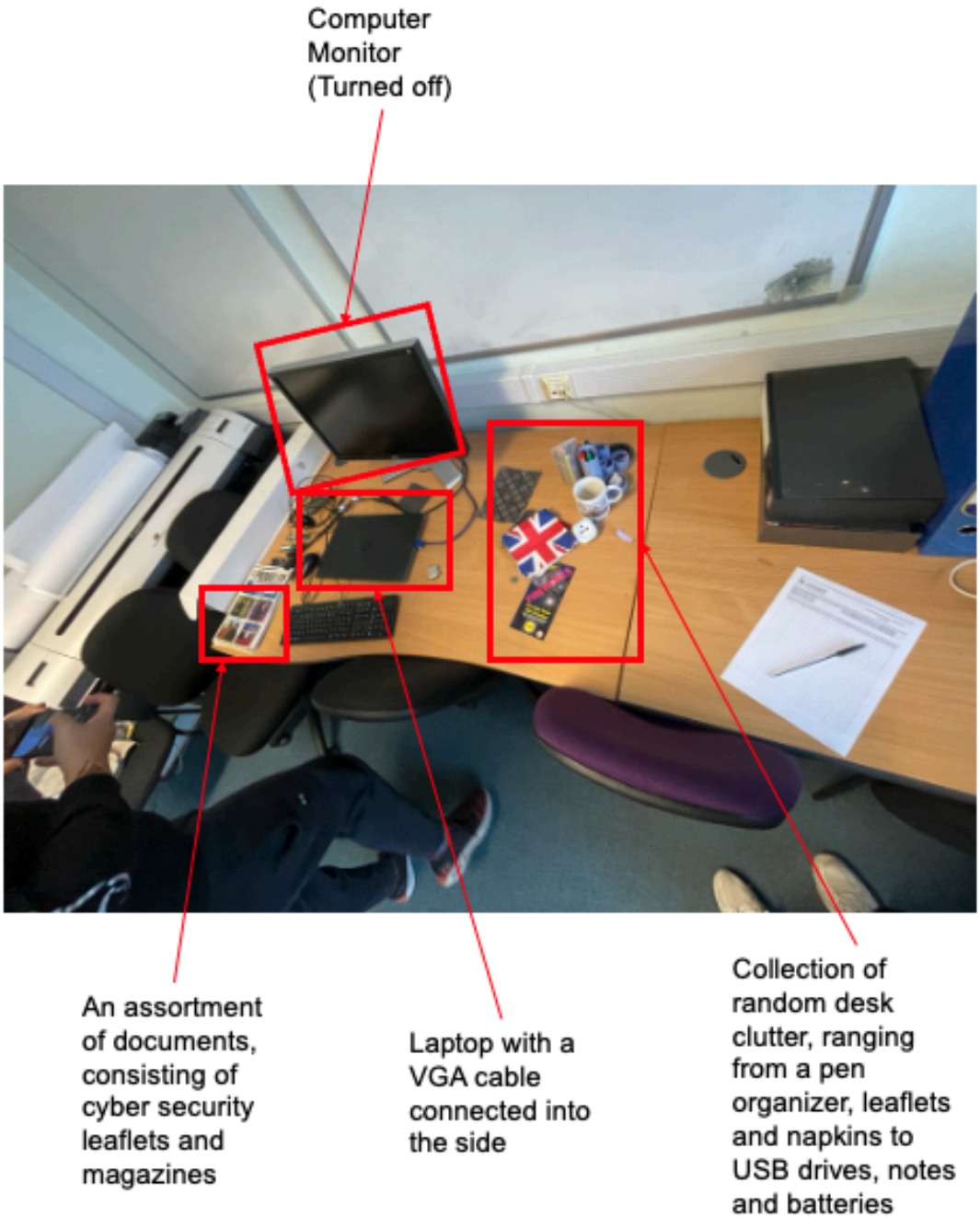
CASE INFORMATION	
Case Alias	Shroff
Case Reference	DFI-JSO4
Examiner	Wke Jackson

Page Number	2
Number of Pages	2

Detail date, time and action taken	
12:03	Once the USB was fully connected, FTK Imager was reopened to start the USB acquisition.
12:04	Clicked onto file create disk image to begin the acquisition of evidence. Once that was open chose the Physical drive option and began the imaging process.
12:05	Selected the inserted USB Drive from the drop down menu (General UDISK USB DEVICE)
12:06	Chose the E01 Selection for the image type and inputted the relevant information. - Case number: DFI-JSO4 - Unique Description: Mediastar 4GB, Silver.
12:08	Selected the output destination folder (F:\DFI-JSO4\USB-M4)
12:10	Started the acquisition process for the USB Drive.
12:24	Finished the acquisition process, removed the write blocker and USB

References

Crime Scene 1 - Overview

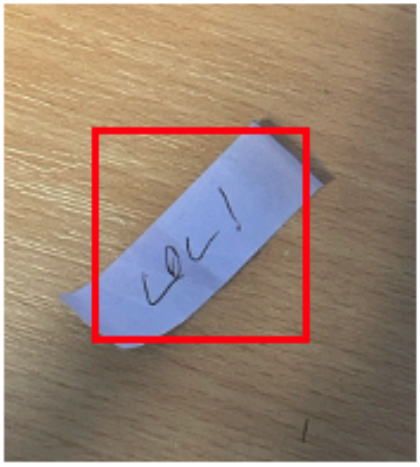


Crime Scene 2 - Desk

CS_2a

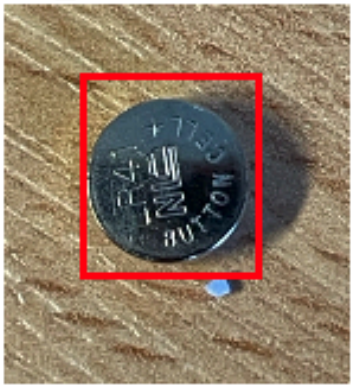
Close up image of the Pen organizer located on the right side of the desk found in Mr Shroffs office, important items like the USB Drive and Notes were removed to get a better image.

CS_2b



Further imaging of the sticky notes with writing on that says "LOL!"

CS_2d



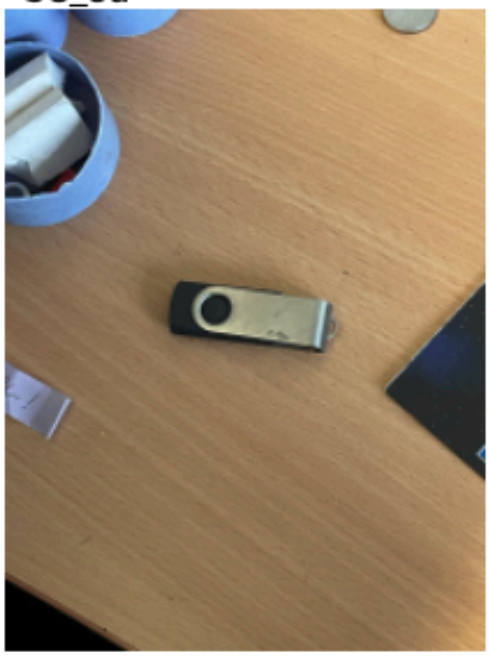
Close up image of a battery found just shy of the pen organiser.

CS_2c

Images of both the notes, battery and USB Drive taken out of the pen organiser for closer up images

Crime Scene 3 - USB

CS_3a



USB drive removed from the pen organiser, will be taken and analysed

CS_3b

Make of the USB Drive is seen as Mediastar

Crime Scene 4 - Phone

CS_4a

CS_4b

Back view of the phone after being removed from the case

CS_4c

CS_4d

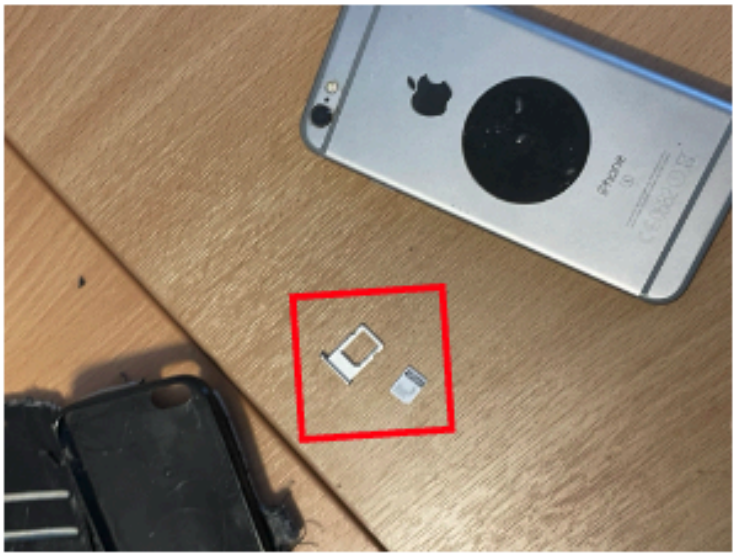
Close up of the back of the phone showcasing all the information

Crime Scene 5 - SIM Card

CS_5a

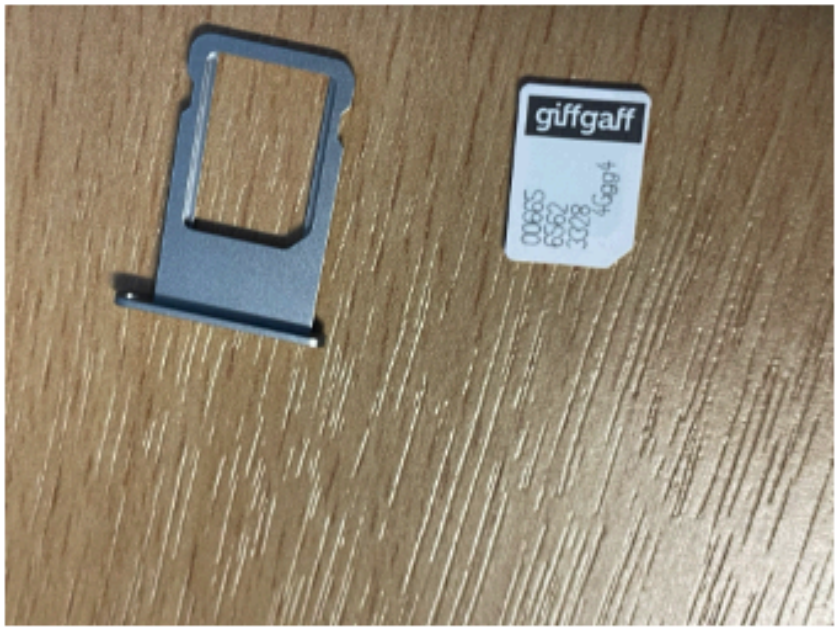
SIM Card remover found on the desk by a black folder

CS_5b



SIM Card remover used to remove the SIM Card from the phone

CS_5c



Close up of the SIM Card, SIM Card is from Giffgaff

Crime Scene 6 - Laptop

CS_6a

Ports on the side of the laptop

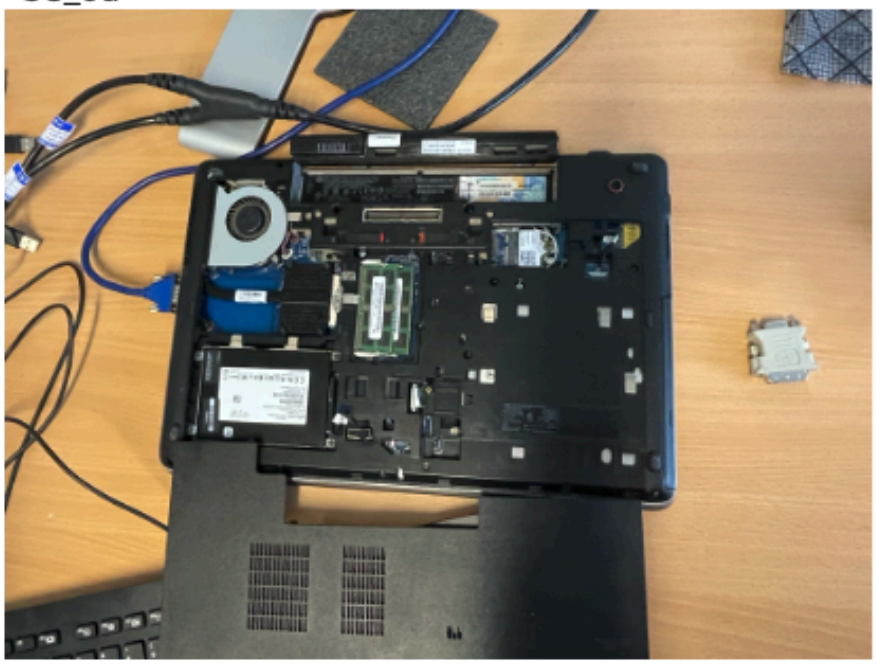
CS_6b

Backside of the laptop

CS_6c

Close up image of the stickers on the bottom of the laptop, showing the serial number and MAC address

CS_6d



CS_6e

Removed the back of the laptop

Close up images of the items found inside the laptop

CS_6f

CS_6g

Close up image of the memory stored inside the laptop

CS_6h

Underside of the power bank connected to the laptop charger

Crime Scene 7 - Accessories

CS_7a

Plugs turned off at the wall

CS_7b

Ports on the side of the monitor

CS_7c

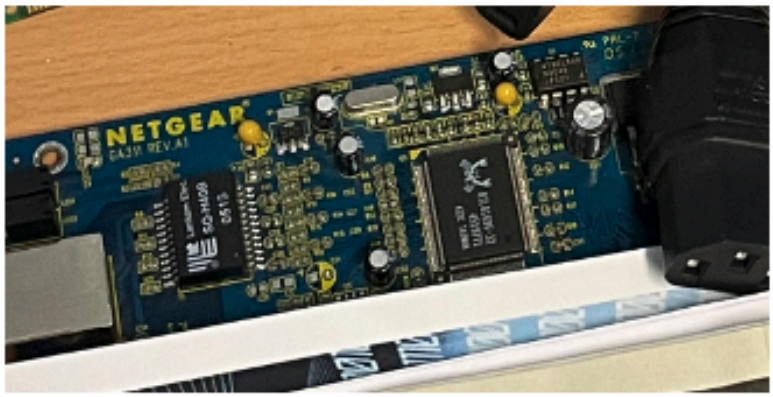
Zoomed out view of the monitor and accessories area

CS_7d

Numerous memory sticks found around the laptop and other computing accessories scattered around the desk

CS_7e

CS_7f



This memory stick is made by the company Netgear

Crime Scene 8 - Desk Items

Technical Report

Title of the Action: Digital Forensics Analysis Report

Case Reference Number: DFI-JS04

Dated: 26th January 2024

Specialist Field: Digital Forensics Analyst

On behalf of Claimant: Jack Shroff

On the instructions of: Detective Chief Inspector Stafford

Luke Dawson

P2665421
De-Montfort House,
De Montfort University,
The Gateway,
Leicester LE1 9BH

Executive Summary

This technical report creates a detailed digital forensic analysis regarding the incident that occurred resulting in the destruction of a storage container and the death of Sergo. Mr Shroff and his associates stored clothing in a rented storage unit near Fosse Park, Leicester, and is now at the centre of this investigation. Procedures were adhered to during the acquisition of the evidence from Mr Shroffs phone, SSD and USB Drive, with a focus on keeping integrity of the data in accordance with the chain of custody protocols and the ACPO guidelines.

The acquired data underwent extensive analysis using leading forensic tools such as Cellebrite, Autopsy and FTK imager. The analysis revealed numerous communications and images that suggest meticulous planning and coordination of involvement potentially leading to the fire. Notable findings included text message communications with Mr Shroffs associates, referred to as "Job", "Rob' and "Joji", and photographs with preparations for the event. Additionally, web browsing history and email communications were combed through, revealing inquiries into insurance companies and purchase of items such as Fuel Cans / Jerry Cans, which could be linked to the incident in question. Decrypted files from Mr Shroffs devices further highlight the suspicious nature of the events leading up to the fire, with instructions that raise concerns.

The evidence presents a complex narrative involving multiple parties and suggests a premeditated conspiracy to commit insurance fraud, potentially leading to arson and the resulting death of Sergo.

Acquisition

Mobile Phone:

Cellebrite:

- To begin with the Acquisition of the mobile phone data, you first need to identify the device. In order to find the make and model name go to: **Settings > General > About.**
- You then need to set **Settings > Display & Brightness > Auto-Lock** to **Never,** once this is done open Cellebrite
- Once open click on **Mobile Device (See Appendix …)**
- Next follow the on screen instructions and click on **Auto Detect**
- It will display all the versions for the same model name, select the version by matching the **model number (See Appendix …)**
- Now select **Logical (Partial)**
- Next select the destination folder where you want to store your extraction and click **Next (See Appendix …)**
- Connect the device to a USB port, once connected click **Continue**

- Now select the sources from where you want to extract the data **(See Appendix …)**
- It will now ask to click on **"Trust"** when it appears on the phone. If a password is applicable you might be asked to input it **(See Appendix …)**
- It may ask for the backup encryption password it is set a default as 1234
- During the file extraction it will ask for the type of multimedia, select **all** and click **OK (See Appendix …)**
- Once the extraction is completed, you will see a summary, review the summary and click **Finish** to complete the process.

Solid State Drive (SSD):

- After retrieving Mr Shroffs Solid State Drive (SSD), a chain of custody was established to maintain the integrity and security of the evidence **(See Forms)**.
- The SSD was then attached to a write blocker and inserted in the computer **(See Appendix …)**.
- The SSD was taken into FTK imager where a write blocker was used to safely extract an E01 file of data copying a bit for bit version without overriding any important information or alterations occurring.

FTK Imager: (Appendix 10A – 10K)

- Picture of the top left corner of the FTK imager software
- Picture shows which version of the FTK imager we are using to acquire the image.
- Go to the File section in the top left-hand corner of the FTK imager software.
- Once in the file heading, navigate to the create disk image **- (Appendix 1A)**
- Once you have opened the Create Disk Image section, it will ask you which type of drive you would like to image.
- For this we will click the Physical Drive option **- (Appendix 1B)**
- Once this is selected click Next
- Now select to image a Physical Drive
- It will now ask which of the available drives you would like to image.
- For this report we will click Evidence number D2 (External SSD) called "MTFDDAK2 56MBF-1A SCSI" **- (Appendix 1C)**
- Once you have selected the drive you want to image, click Finish.
- Now you need to select which type of image you would like to take.
- By default, it should have selected the first option "Raw (dd)"
- Change this and select the E01 file instead, click Next **- (Appendix 1D)**
- Now input all the relevant case information
- Your case & Evidence number can be located on any of your evidence forms if needed.
- For the Unique Description section, include important information such as Serial Numbers, Model Numbers etc.
- Examiner is your name.
- Once all the information is filled click Next **- (Appendix 1F)**
- Now you need to allocate the location for the Forensic image.
- In this case, I have allocated the image to be placed into the Crime Scene folder

(DFI-JS04) and a subfolder (Laptop Drive – D2)
    - Once you have found a location for the drive, give it a name then click Finish **- (Appendix 1G)**
    - Once you have followed all of these steps you should have something that looks like this **(Appendix 1H)** then click Start
- In order to ensure the data was accurate a hash value was calculated and noted for the forensic image to keep integrity throughout the analysis.

USB:

- The USB device was received and immediately logged to maintain a clear chain of custody.
- To ensure the device was not altered or tampered with a write blocker was used during the acquisition process.
- A forensic image of the USB drive was created on FTK imager to preserve the state of the data for analysis.
- Hash values of the forensic image were then generated and recorded to verify the integrity of the data at all stages of the analysis.

FTK Imager: (Appendix 10A – 10K)

- Follow steps 1 through 9 of the above FTK imager guide
- For this report we will click Evidence number D2 (External SSD) called "General UDisk USB Device" **- (Appendix 1)**
- Follow steps 11 through 21 of the above FTK imager guide to finish the process.

Analysis

Mobile Phone:

- Open Cellebrite Reader **(See Appendix 3A)**
- Once Cellebrite reader has opened you may be prompted with the **Activation** window, just click the '**X'** in the upper right corner **(See Appendix 3B)**
- Now click **File** located in the top left corner and **Open UFDR File** that you did in the **Acquisition** steps **(See Appendix 3C)**
- Let the application load and you should be greeted with this **(See Appendix 3D)**
- Next navigate to the contents section and click on the **Chats** heading **(See Appendix 3E)**
- Once in the **Chats** section click on **Number 5** to enter the chat string between Mr Shroff and "Job" **(See Appendix 3F)**
- At the end of the communications string you will find a text from Jack with a link to a **Picture** of a Shell Garage (Evidence IMG_A)
- Now back out from the **Chat** section and navigate back to the home screen, scroll down on the contents section and click onto the **Images** heading (**See Appendix 3I)**
- Once in the **Images** section scroll down to the bottom **(See Appendix 3J)**
- At the bottom of the **Images** section you will find evidence of IMG_0006 and IMG_0003 as well as IMG_A for a second time.

Solid State Drive (SSD):

- Open Autopsy (Either search for the name in the task bar or click the logo)
- Once Autopsy has loaded you will be prompted to either start a new case or open an existing one, either **click "New Case"** or close out of the menu (**See Appendix 4A**)
- If you close out of the menu navigate to the top left corner and click **Case** then **New Case** (**See Appendix 4B**)
- Once you have started your new case you will be asked to input a **Case Name** and the **Directory** you would like to save the Case into. Input and select your information and then click **Next** (**See Appendix 4C**)
- You will now be asked to input the Case **Number** and also your **Examiner Name** once this is filled out click **Finish** (**See Appendix 4D**)
- After the Case has been generated a new window will appear and ask you to **Select Host**
- By default the Generate new host name is selected however **Change** this to the **Specify new host name** heading and type in the name you would like to title it and click **Next** (**See Appendix 4E**)
- Next keep the **Disk Image or VM file** selected and click **Next** (**See Appendix 4F**)
- Now select the path to the **E01** file you generated on the analysis step as the file to be analysed and click **Next** (**See Appendix 4G**)
- Finally in the next section select all the components of the analysis that is required and click **Next** (**See Appendix 4H**)

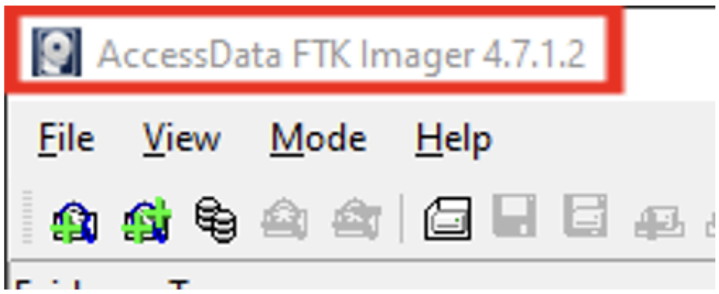
USB Drive:

- Open Autopsy (Either search for the name in the task bar or click the logo)
- Once Autopsy has loaded you will be prompted to either start a new case or open an existing one, either **click "New Case"** or close out of the menu (**See Appendix 4A**)
- If you close out of the menu navigate to the top left corner and click **Case** then **New Case** (**See Appendix 4B**)
- Once you have started your new case you will be asked to input a **Case Name** and the **Directory** you would like to save the Case into. Input and select your information and then click **Next** (**See Appendix 4C**)
- You will now be asked to input the Case **Number** and also your **Examiner Name** once this is filled out click **Finish** (**See Appendix 4D**)
- After the Case has been generated a new window will appear and ask you to **Select Host**
- By default the Generate new host name is selected however **Change** this to the **Specify new host name** heading and type in the name you would like to title it and click **Next** (**See Appendix 4E**)
- Next keep the **Disk Image or VM file** selected and click **Next** (**See Appendix 4F**)
- Now select the path to the **E01** file you generated on the analysis step as the file to be analysed and click **Next** (**See Appendix 4G**)
- Finally in the next section select all the components of the analysis that is required and click **Next** (**See Appendix 4H**)

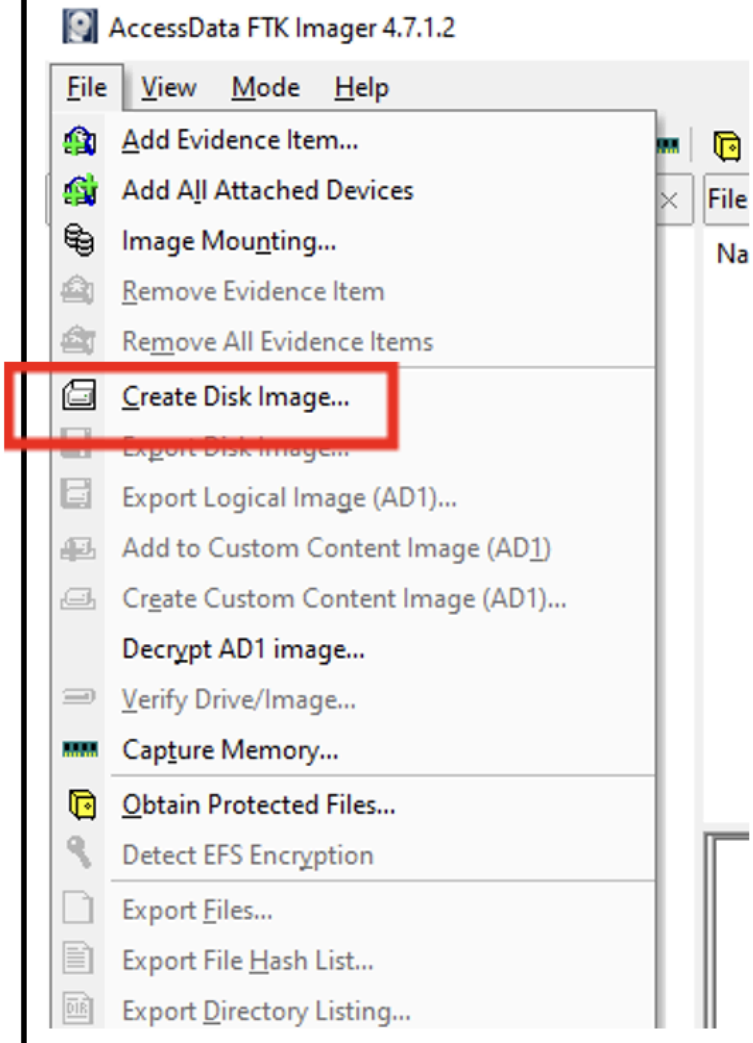
Appendices

1: Acquisition - SSD & USB Drive

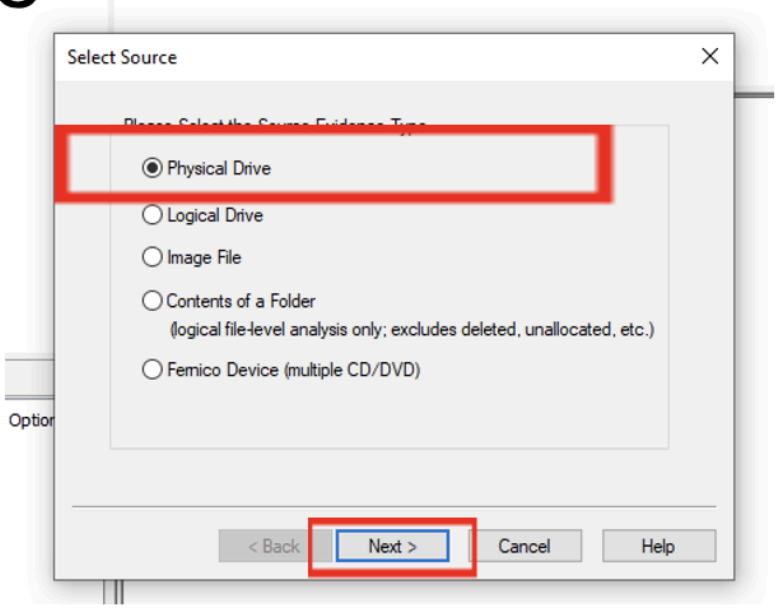
1A



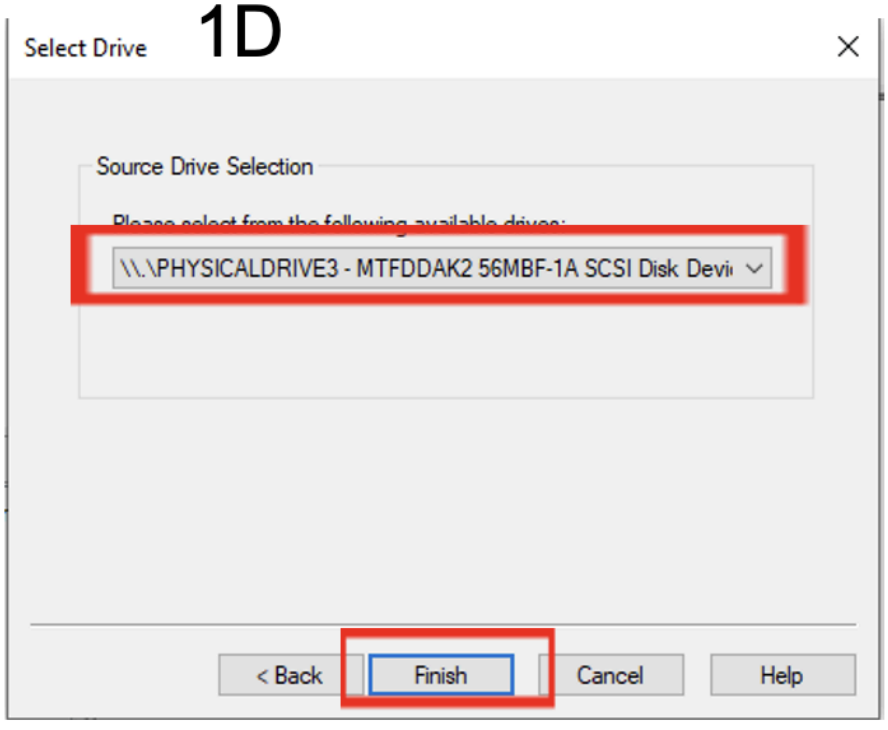
1B



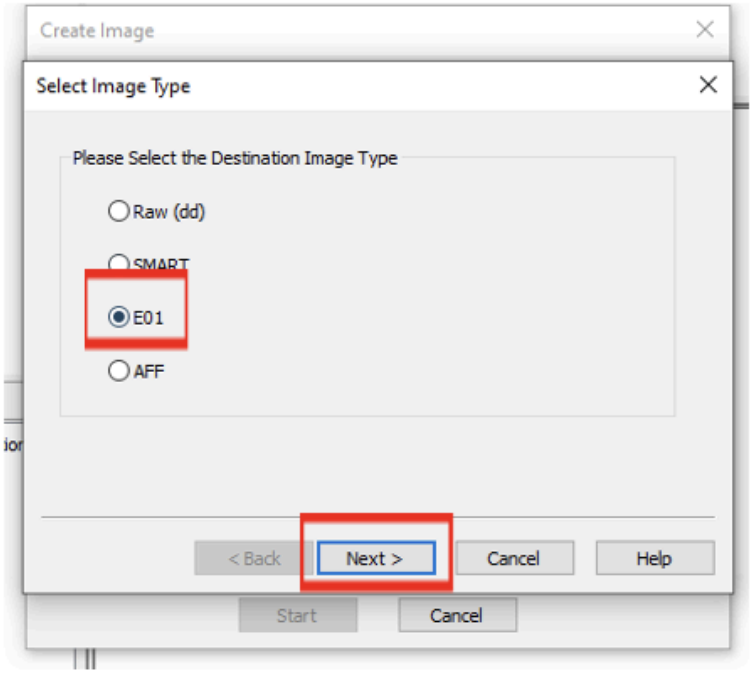
1C


Select Source
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Femico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

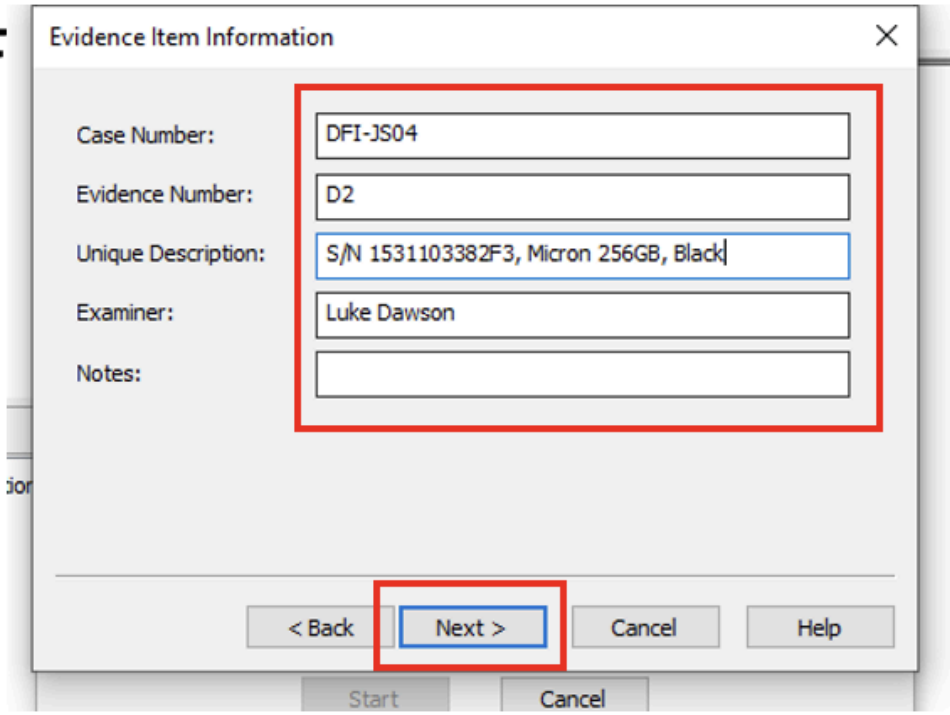
1D


Select Drive
Source Drive Selection
\\.\PHYSICALDRIVE3 - MTFDDAK2 56MBF-1A SCSI Disk Devi
< Back
Finish
Cancel
Help

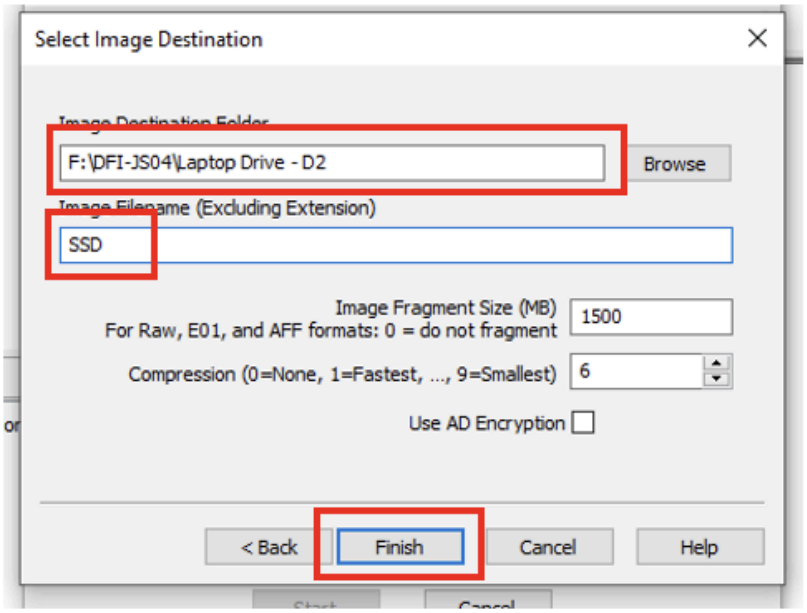
1E


Create Image
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help
Start
Cancel

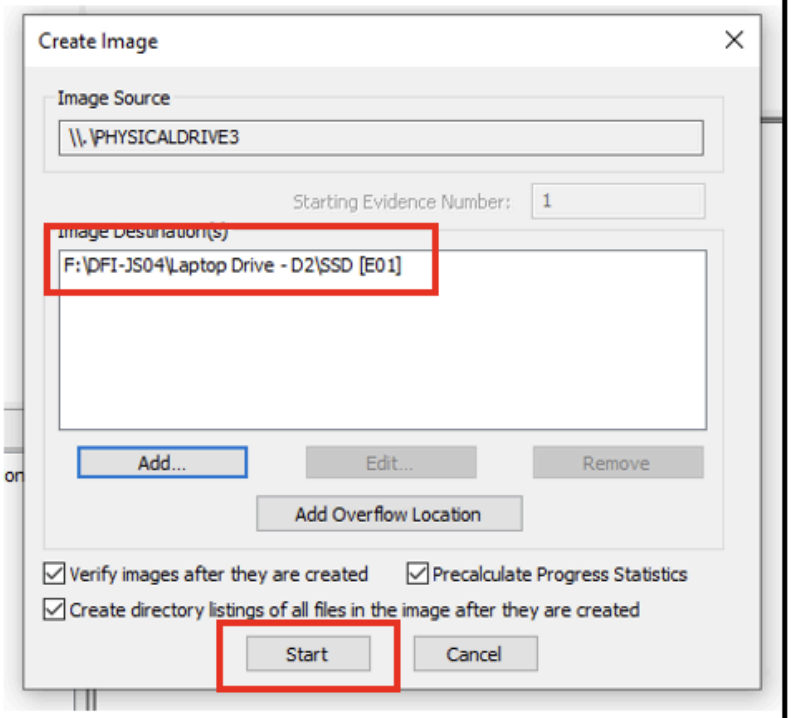
1F


Evidence Item Information
Case Number:
DFI-JS04
Evidence Number:
D2
Unique Description:
S/N 1531103382F3, Micron 256GB, Black
Examiner:
Luke Dawson
Notes:
< Back
Next >
Cancel
Help
Start
Cancel

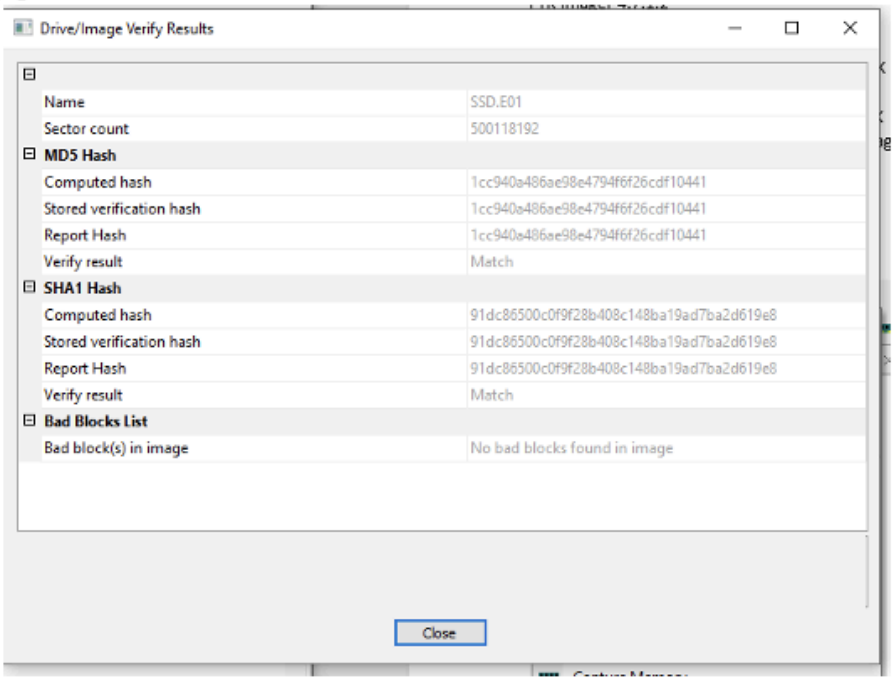
1G


Select Image Destination
Image Destination Folder
F:\DFI-JS04\Laptop Drive - D2
Browse
Image Filename (Excluding Extension)
SSD
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
6
Use AD Encryption
< Back
Finish
Cancel
Help

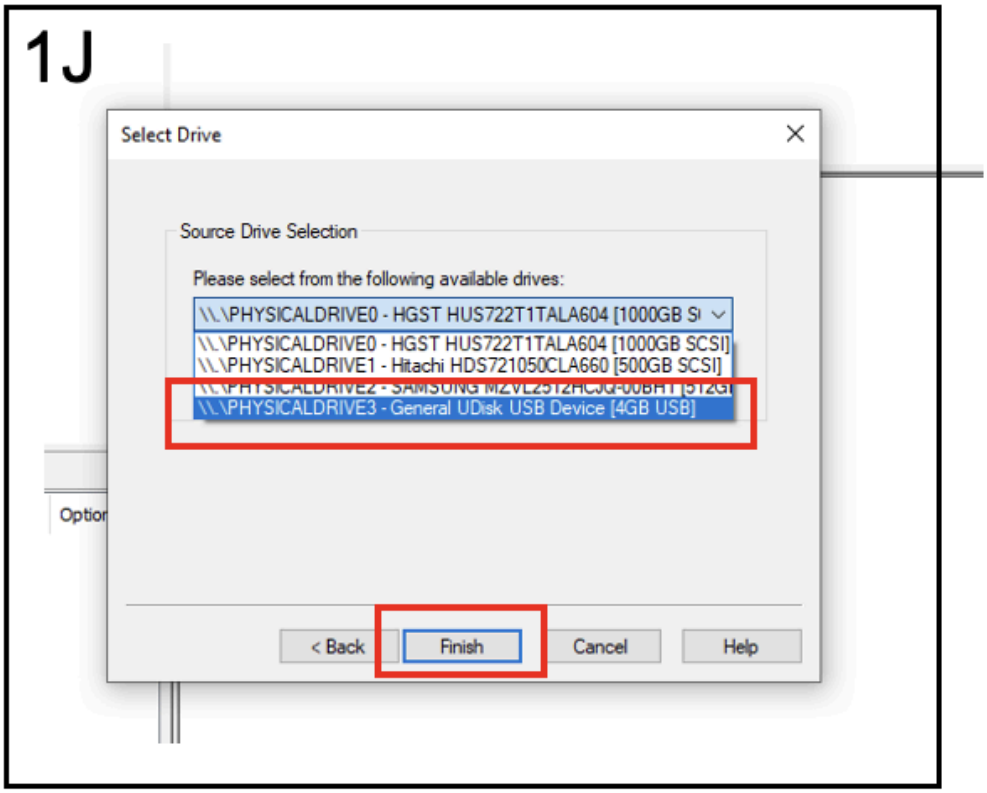
1H


Create Image
Image Source
\\.\PHYSICALDRIVE3
Starting Evidence Number:
1
Image Destination(s)
F:\DFI-JS04\Laptop Drive - D2\SSD [E01]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel

1I


Drive/Image Verify Results
Name
SSD.E01
Sector count
500118192
MD5 Hash
Computed hash
1cc940a486ae98e4794f6f26cdf10441
Stored verification hash
1cc940a486ae98e4794f6f26cdf10441
Report Hash
1cc940a486ae98e4794f6f26cdf10441
Verify result
Match
SHA1 Hash
Computed hash
91dc86500c0f9f28b408c148ba19ad7ba2d619e8
Stored verification hash
91dc86500c0f9f28b408c148ba19ad7ba2d619e8
Report Hash
91dc86500c0f9f28b408c148ba19ad7ba2d619e8
Verify result
Match
Bad Blocks List
Bad block(s) in image
No bad blocks found in image
Close

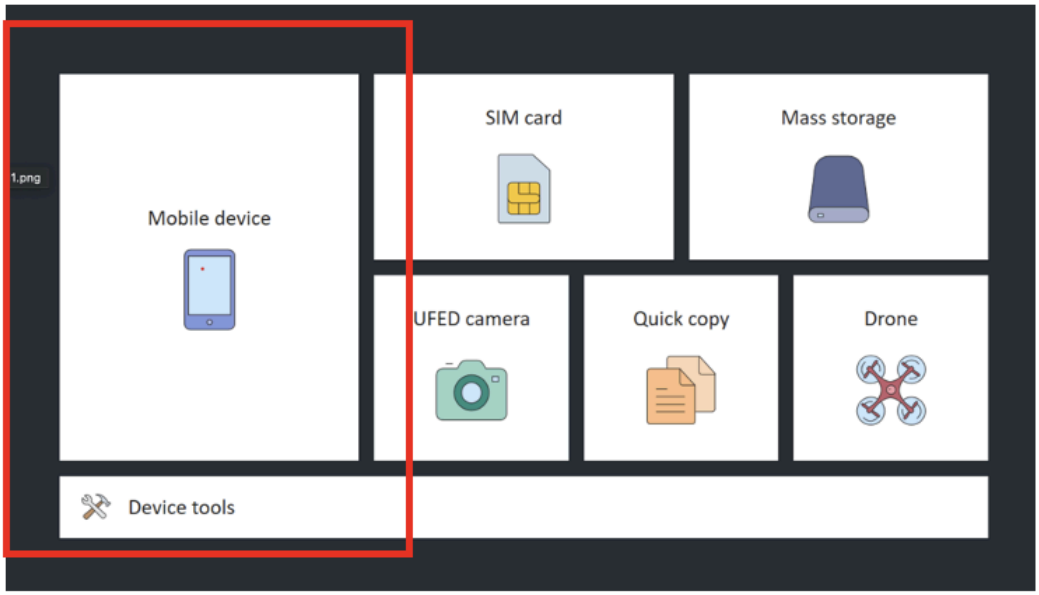
1J


Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE0 - HGST HUS722T1TALA604 [1000GB SCSI]
\\.\PHYSICALDRIVE1 - Hitachi HDS721050CLA660 [500GB SCSI]
\\.\PHYSICALDRIVE3 - General UDisk USB Device [4GB USB]
< Back
Finish
Cancel
Help

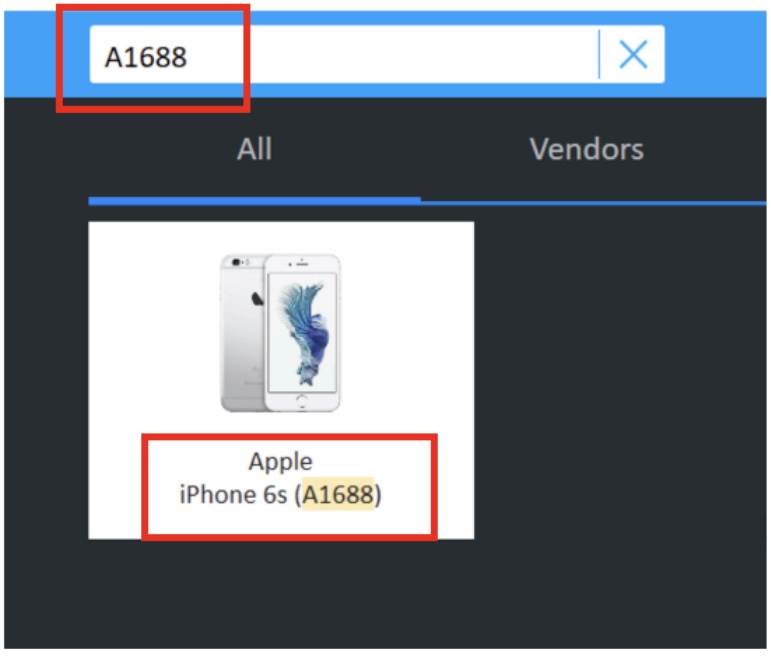
2: Acquisition - Mobile Phone & SIM Card

2A

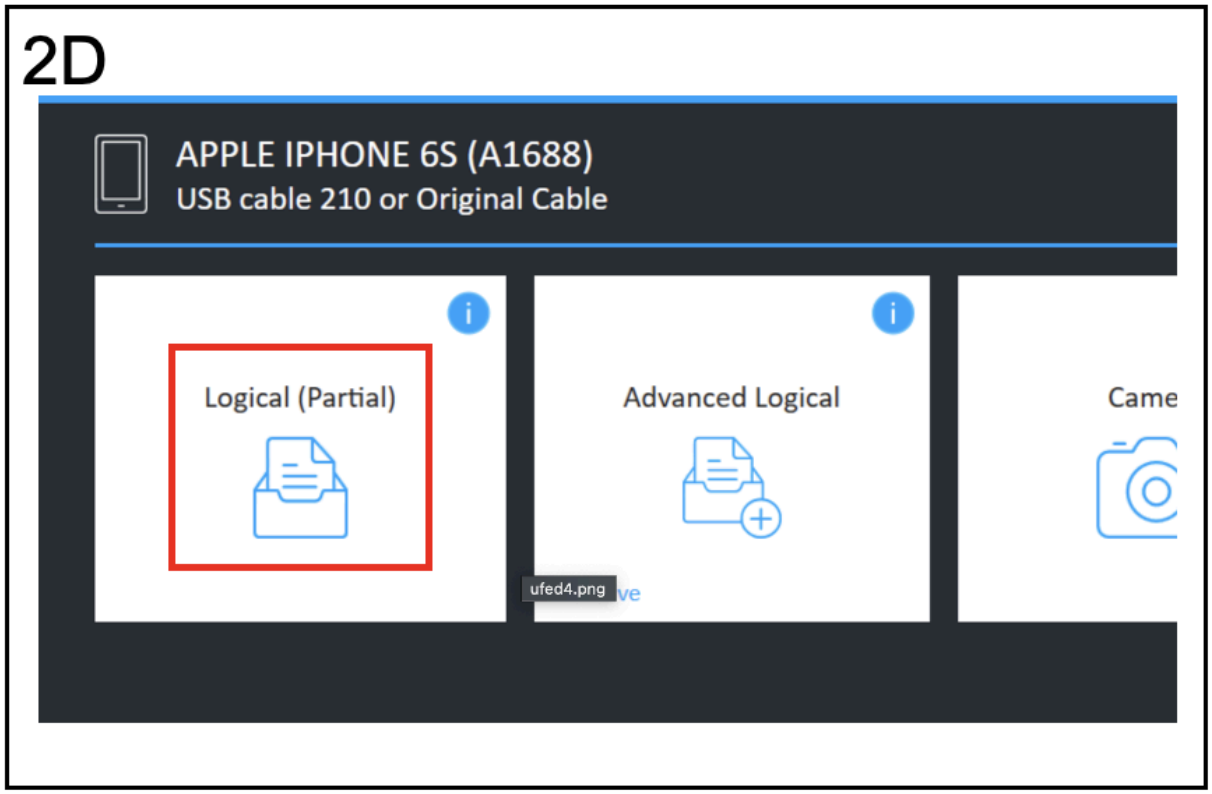
2B


1.png
Mobile device
SIM card
Mass storage
UFED camera
Quick copy
Drone
Device tools

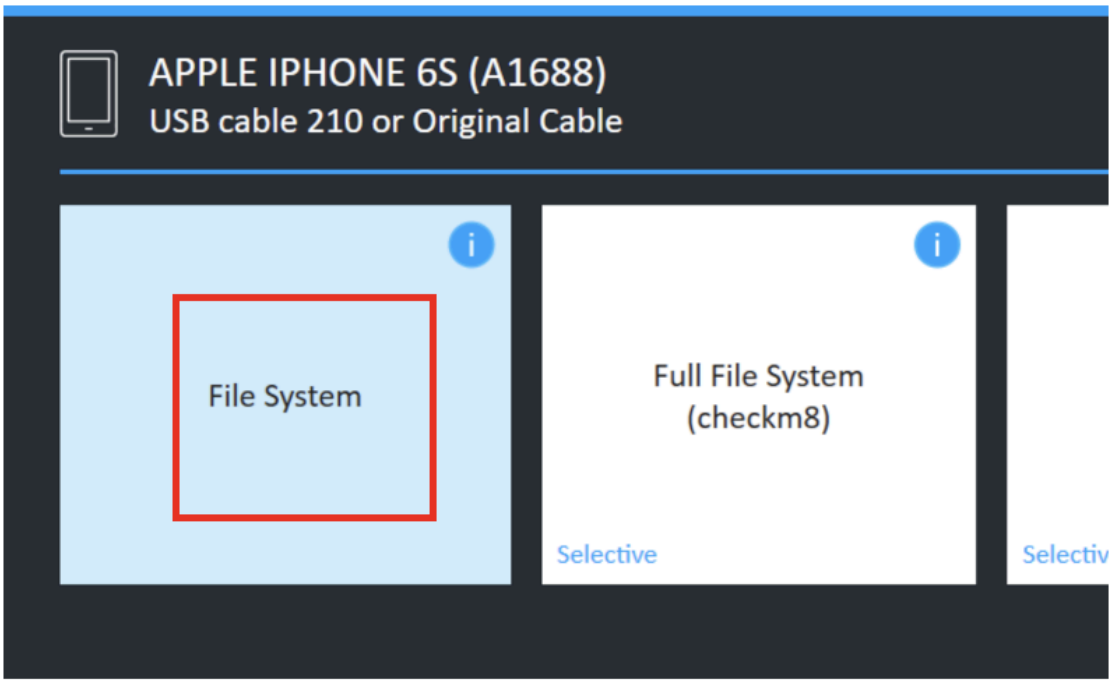
2C


A1688
All
Vendors
Apple
iPhone 6s (A1688)

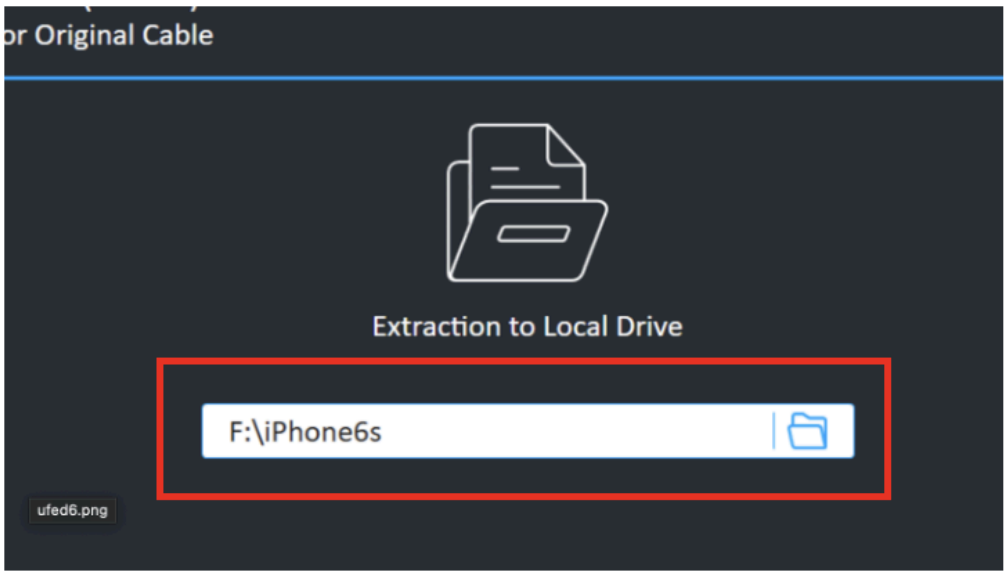
2D

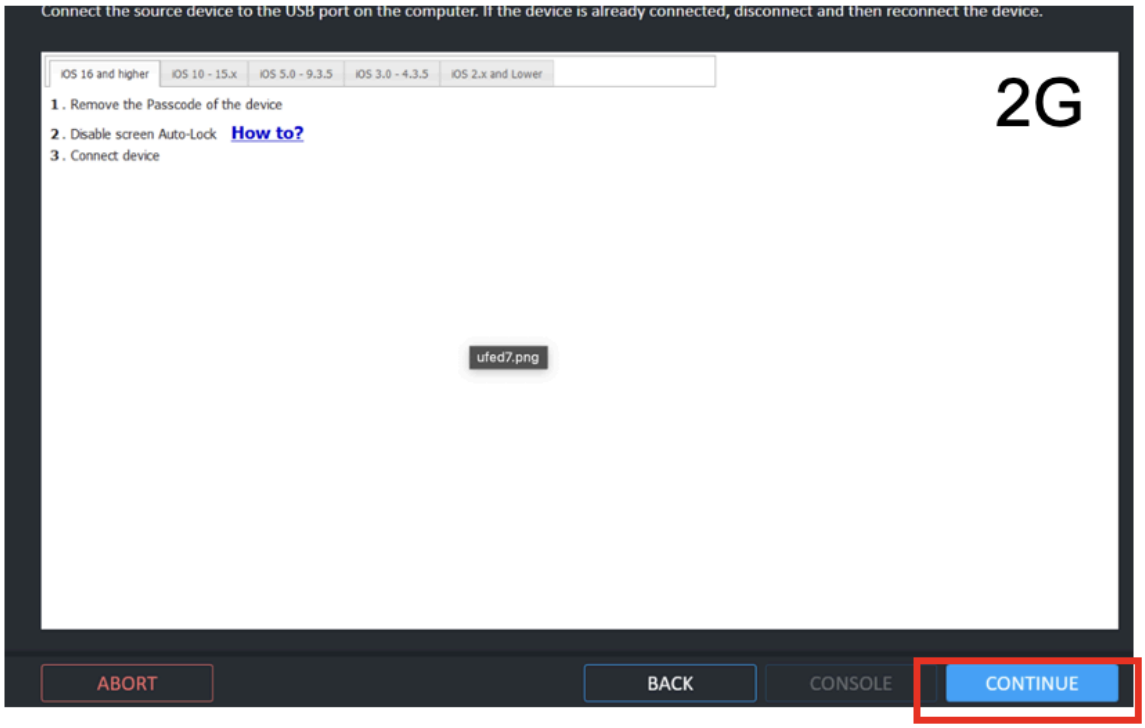

APPLE IPHONE 6S (A1688)
USB cable 210 or Original Cable
Logical (Partial)
Advanced Logical
Came
ufed4.png

2E


APPLE IPHONE 6S (A1688)
USB cable 210 or Original Cable
File System
Full File System
(checkm8)
Selective
Selectiv

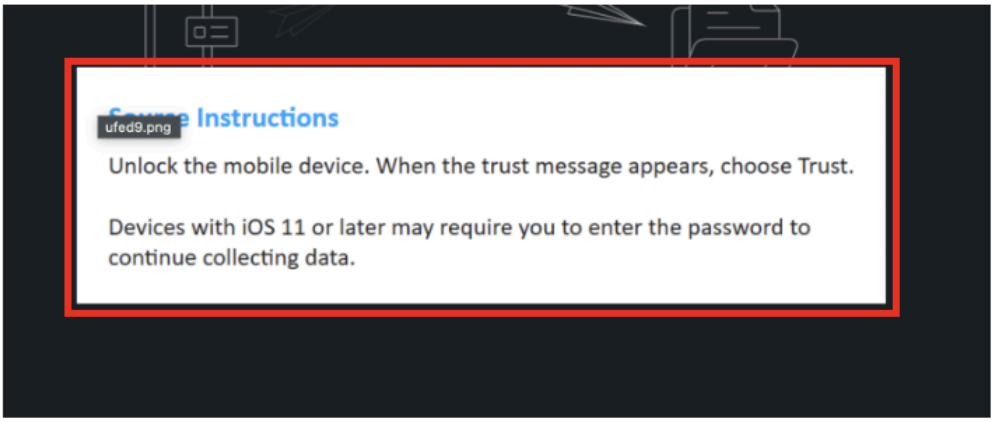
2F


or Original Cable
Extraction to Local Drive
F:\iPhone6s
ufed6.png

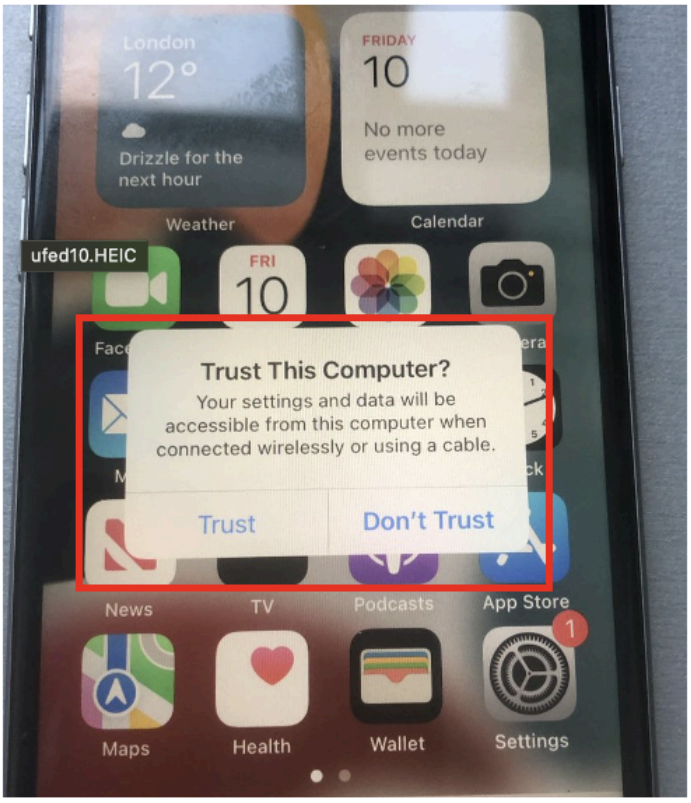

Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
iOS 16 and higher
iOS 10 - 15.x
iOS 5.0 - 9.3.5
iOS 3.0 - 4.3.5
iOS 2.x and Lower
1. Remove the Passcode of the device
2. Disable screen Auto-Lock How to?
3. Connect device
ufed7.png
ABORT
BACK
CONSOLE
CONTINUE

2G

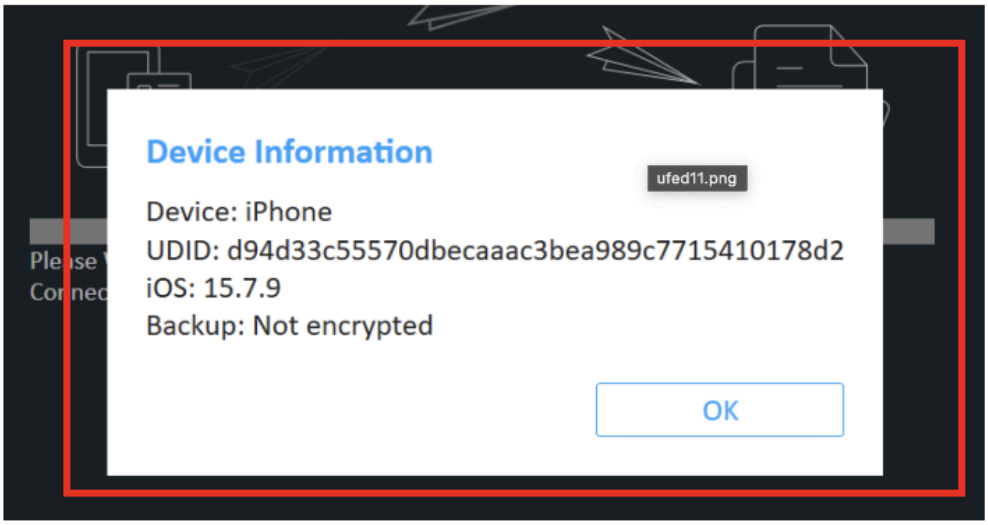
2H


ufed9.png
Instructions
Unlock the mobile device. When the trust message appears, choose Trust.
Devices with iOS 11 or later may require you to enter the password to continue collecting data.

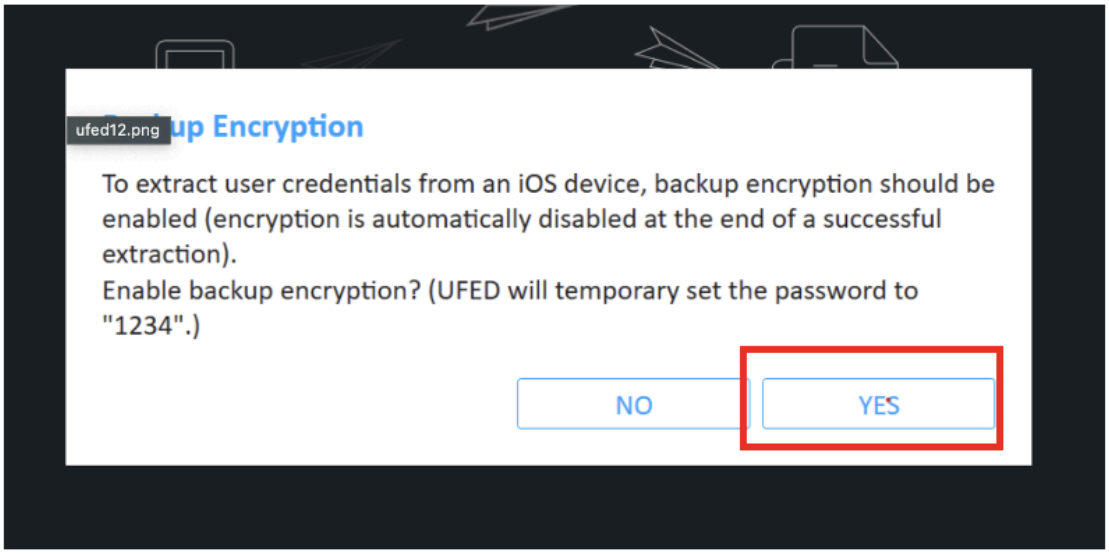
2I


ufed10.HEIC
London
12°
Drizzle for the next hour
Weather
FRIDAY
10
No more events today
Calendar
FRI
10
Trust This Computer?
Your settings and data will be accessible from this computer when connected wirelessly or using a cable.
Trust
Don't Trust
News
TV
Podcasts
App Store
Maps
Health
Wallet
Settings

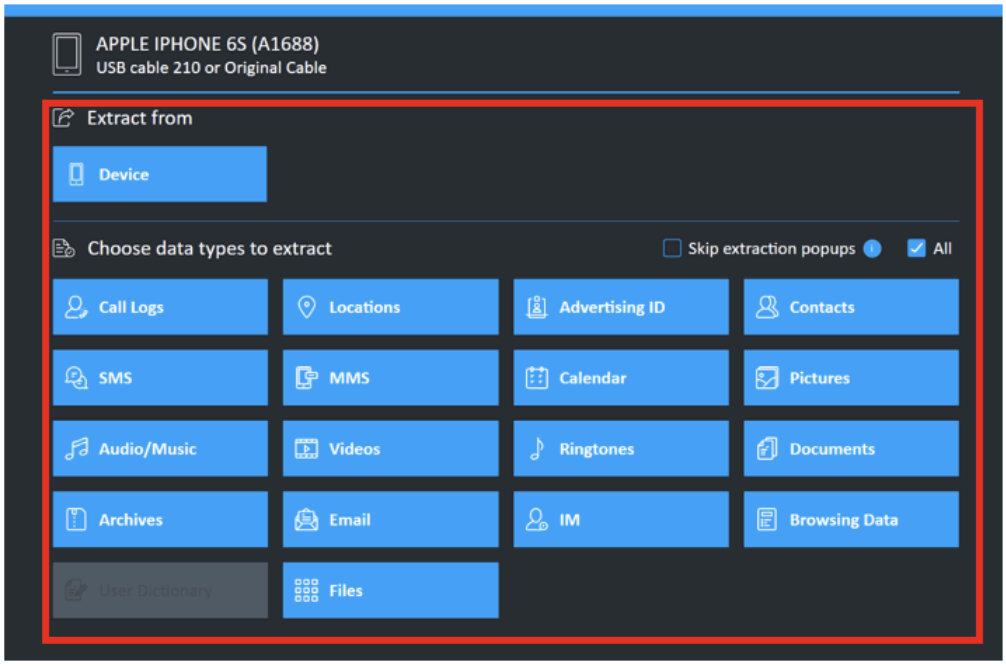
2J


Device Information
ufed11.png
Device: iPhone
UDID: d94d33c55570dbecaaac3bea989c7715410178d2
iOS: 15.7.9
Backup: Not encrypted
OK

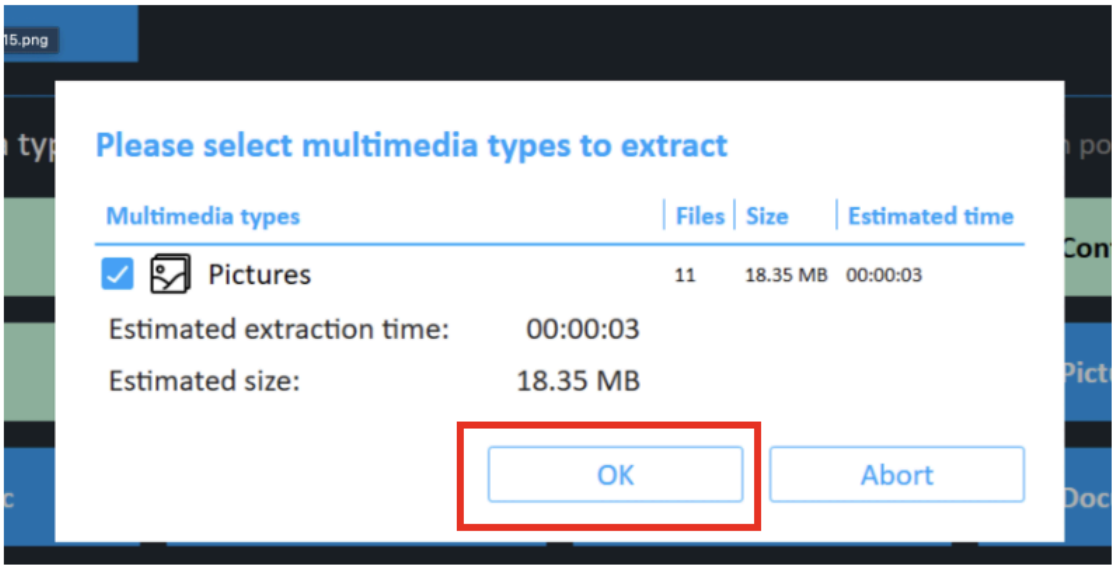
2K


ufed12.png
up Encryption
To extract user credentials from an iOS device, backup encryption should be enabled (encryption is automatically disabled at the end of a successful extraction).
Enable backup encryption? (UFED will temporary set the password to "1234".)
NO
YES

2L

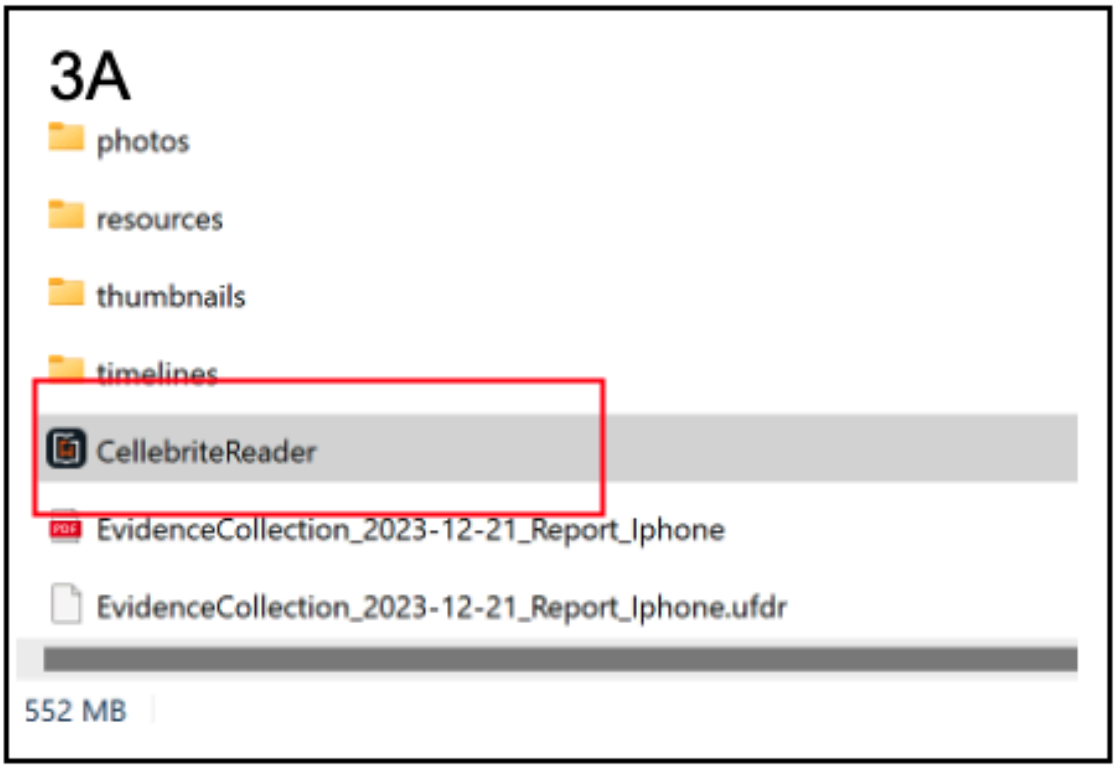

APPLE IPHONE 6S (A1688)
USB cable 210 or Original Cable
Extract from
Device
Choose data types to extract
Skip extraction popups
All
Call Logs
Locations
Advertising ID
Contacts
SMS
MMS
Calendar
Pictures
Audio/Music
Videos
Ringtones
Documents
Archives
Email
IM
Browsing Data
User Dictionary
Files

2J

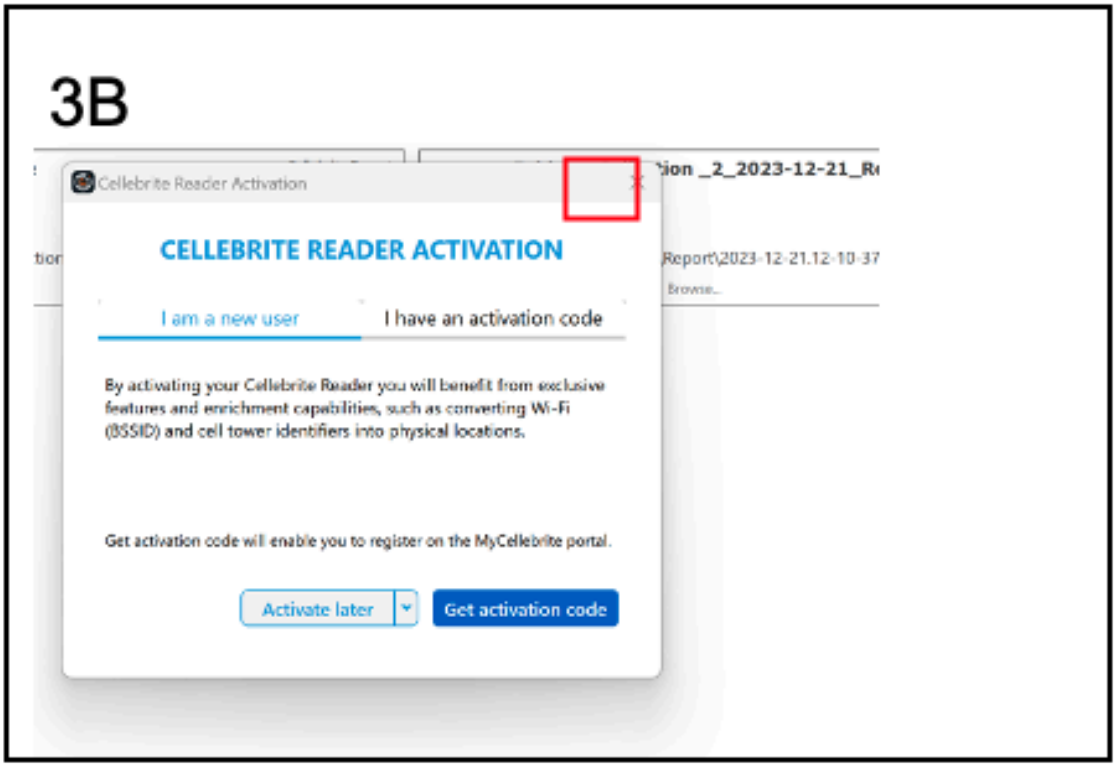

Please select multimedia types to extract
Multimedia types
Files
Size
Estimated time
Pictures
11
18.35 MB
00:00:03
Estimated extraction time:
00:00:03
Estimated size:
18.35 MB
OK
Abort

3: Analysis - Mobile Phone & SIM Card

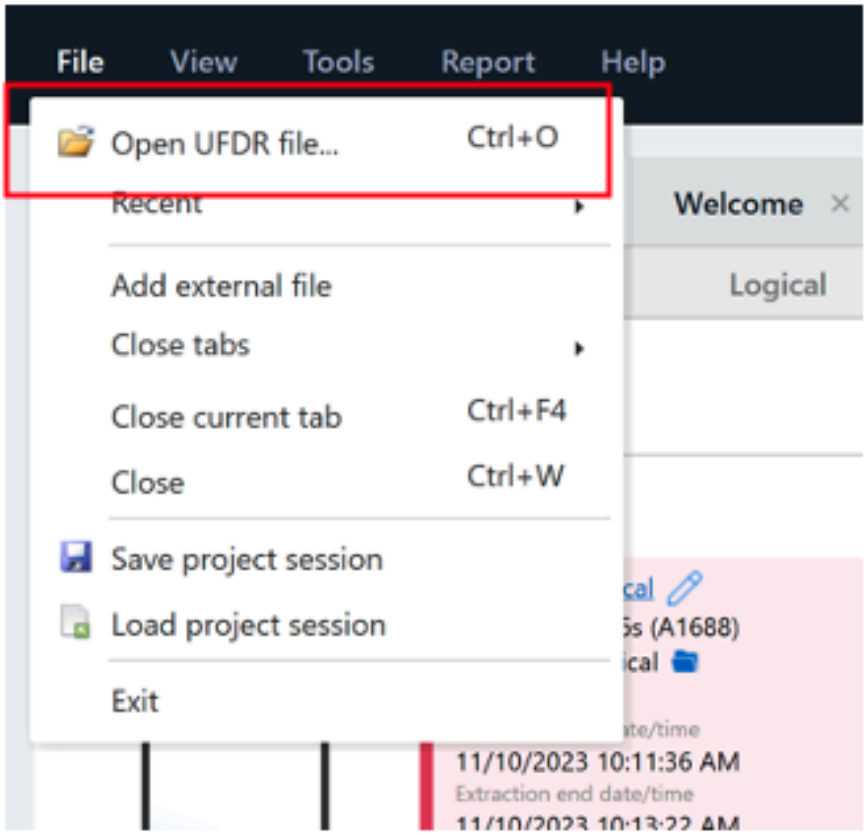
3A



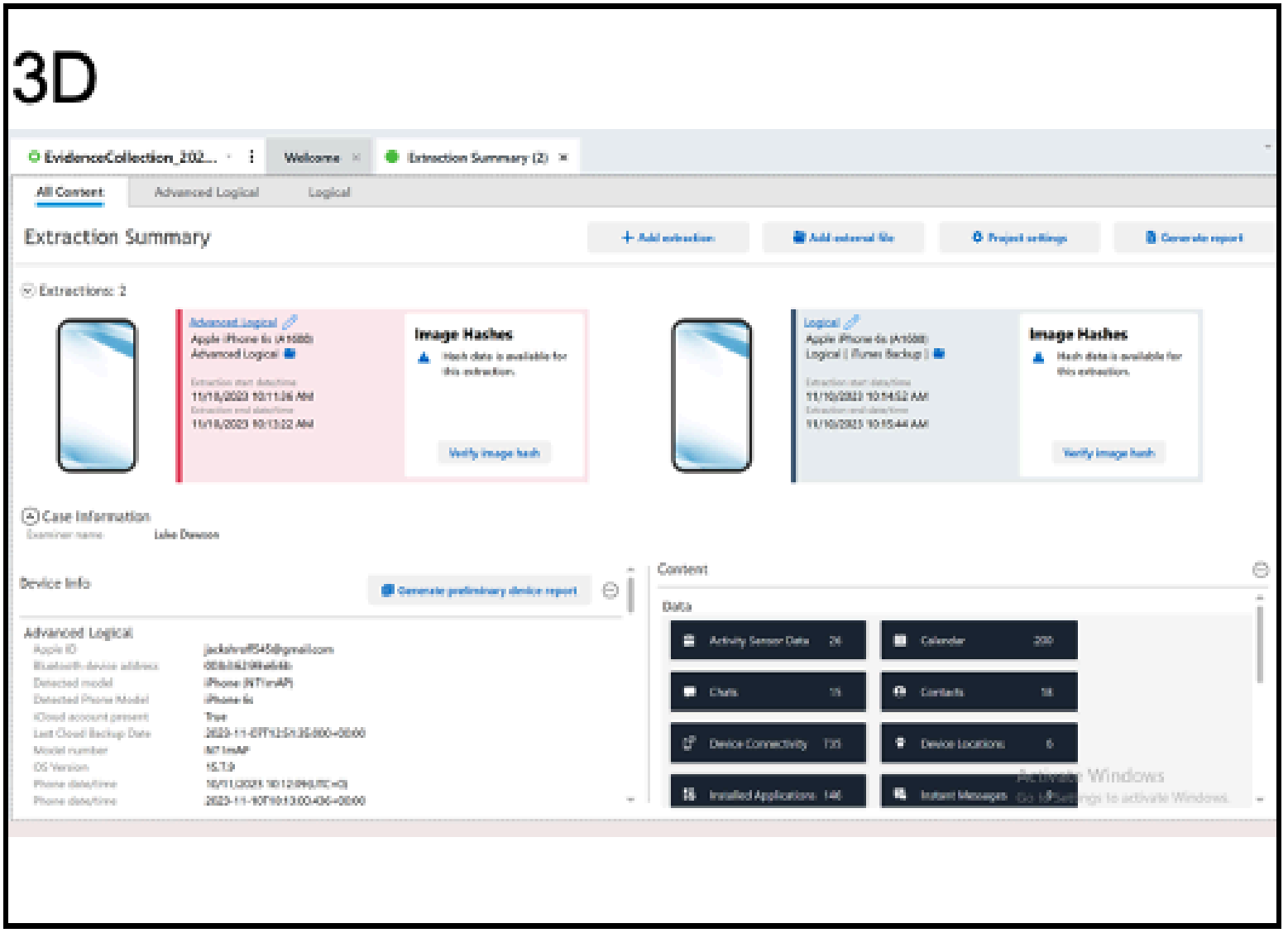
3B



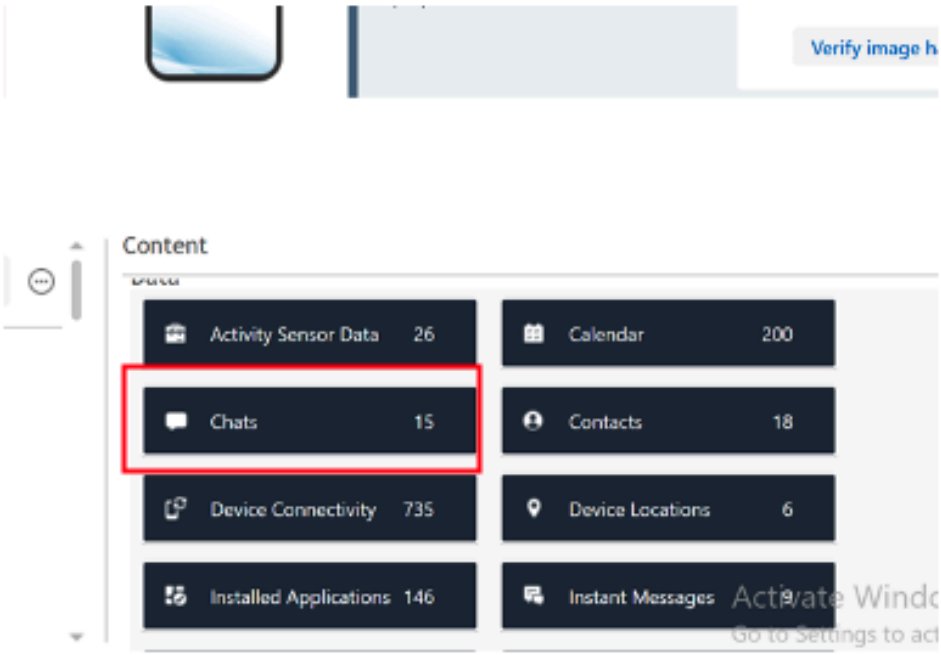
3C


File
View
Tools
Report
Help
Open UFDR file...
Ctrl+O
Recent
Add external file
Close tabs
Close current tab
Ctrl+F4
Close
Ctrl+W
Save project session
Load project session
Exit
Welcome
Logical
11/10/2023 10:11:36 AM
Extraction end date/time

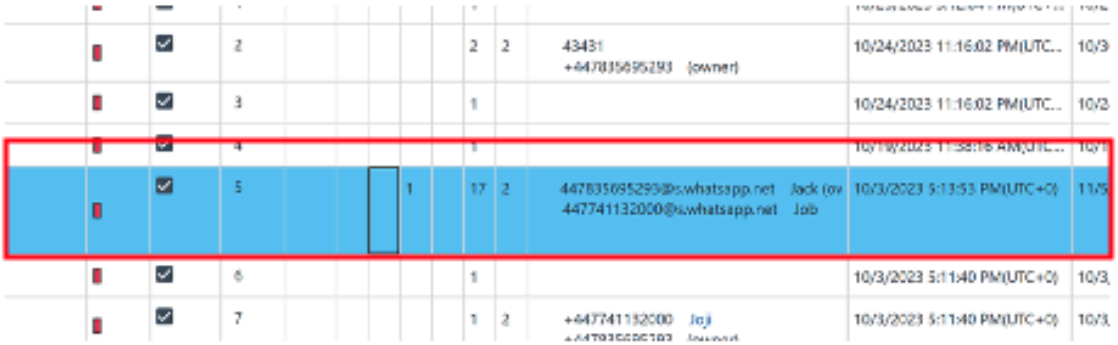
3D


EvidenceCollection_202...
Welcome
Extraction Summary (2)
All Content
Advanced Logical
Logical
Extraction Summary
Extractions: 2
Advanced Logical
Apple iPhone 6s (A1688)
Advanced Logical
11/10/2023 10:11:26 AM
11/10/2023 10:13:22 AM
Image Hashes
Hash data is available for this extraction.
Verify image hash
Logical
Apple iPhone 6s (A1688)
Logical [iTunes Backup]
11/10/2023 10:14:52 AM
11/10/2023 10:15:44 AM
Image Hashes
Hash data is available for this extraction.
Verify image hash
Case Information
Examiner name
Luke Dawson
Device Info
Generate preliminary device report
Advanced Logical
Content
Data
Activity Sensor Data 26
Calendar 220
Chats 15
Contacts 58
Device Connectivity 720
Device Locations 6
Installed Applications 146
Instant Messages
Activate Windows
Go to Settings to activate Windows.

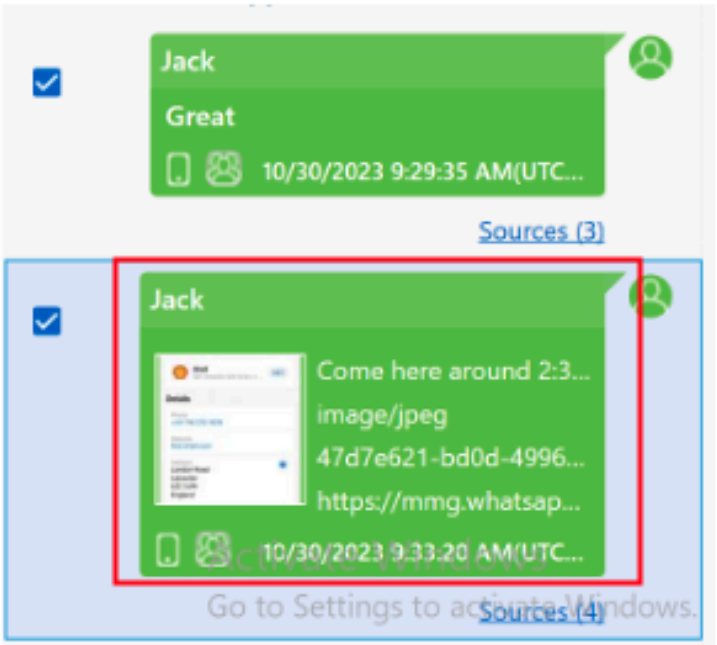
3E


Verify image h
Content
Activity Sensor Data 26
Calendar 200
Chats 15
Contacts 18
Device Connectivity 735
Device Locations 6
Installed Applications 146
Instant Messages 9

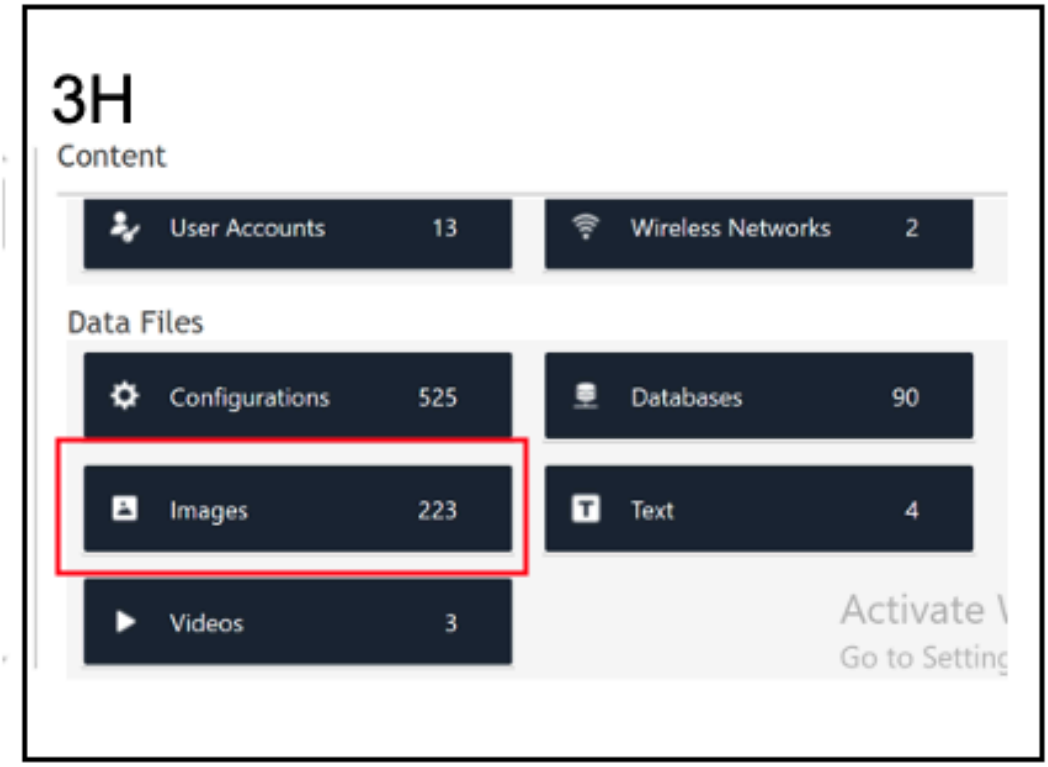
3F


2
2 2
43431
+447835695293 (owner)
10/24/2023 11:16:02 PM(UTC...
3
1
10/24/2023 11:16:02 PM(UTC...
5
1
17 2
447835695293@s.whatsapp.net Jack (ov
447741132000@s.whatsapp.net Job
10/3/2023 5:13:53 PM(UTC+0)
6
1
10/3/2023 5:11:40 PM(UTC+0)
7
1 2
+447741132000 Joj
10/3/2023 5:11:40 PM(UTC+0)

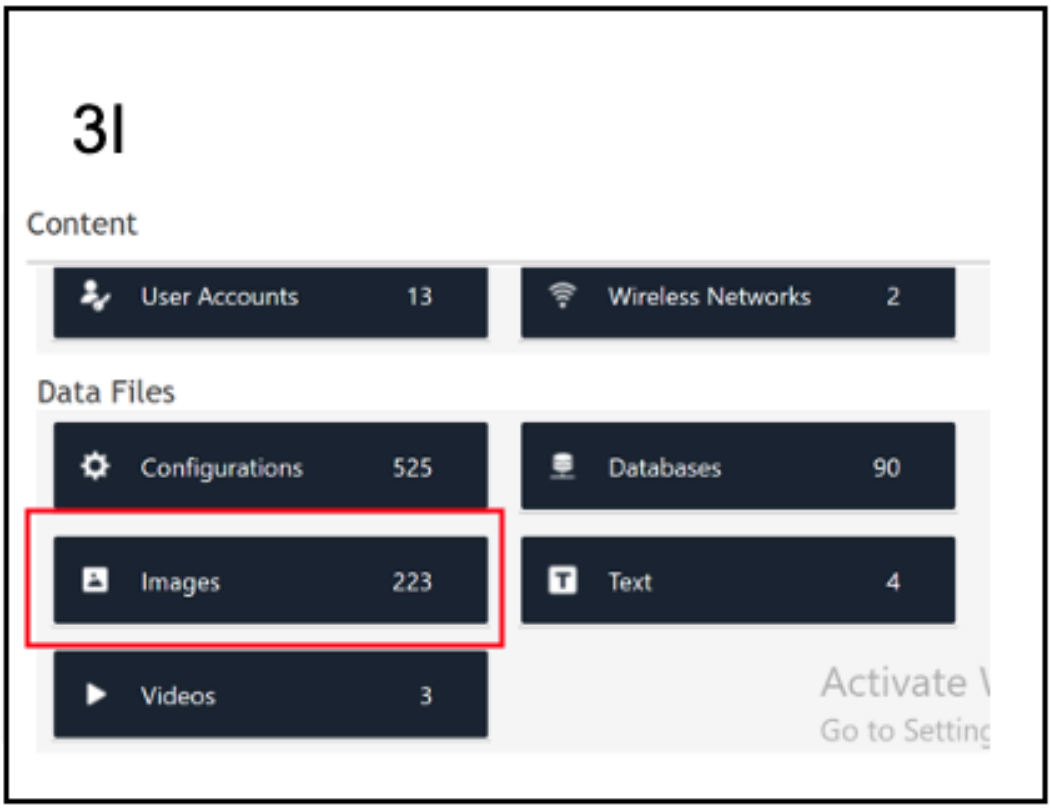
3G


Jack
Great
10/30/2023 9:29:35 AM(UTC...
Sources (3)
Jack
Come here around 2:3...
image/jpeg
47d7e621-bd0d-4996...
https://mmg.whatsap...
10/30/2023 9:33:20 AM(UTC...
Sources (4)

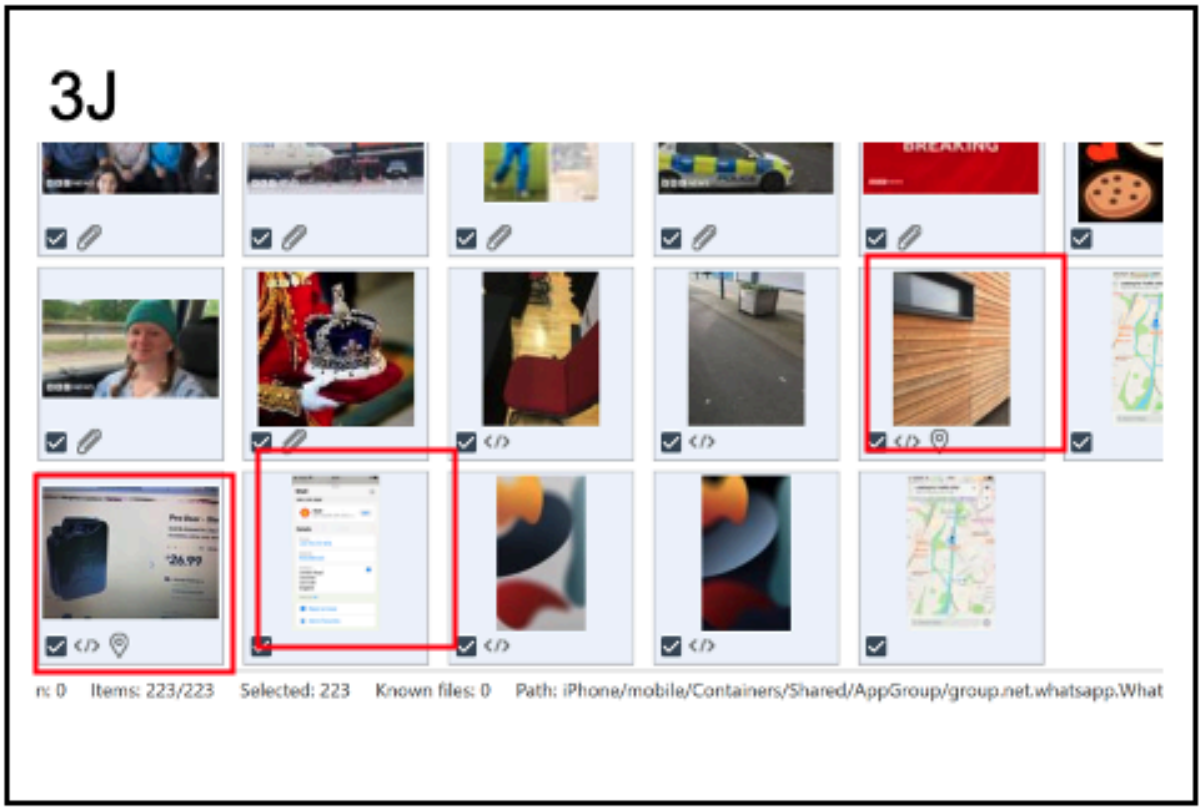
3H


Content
User Accounts 13
Wireless Networks 2
Data Files
Configurations 525
Databases 90
Images 223
Text 4
Videos 3

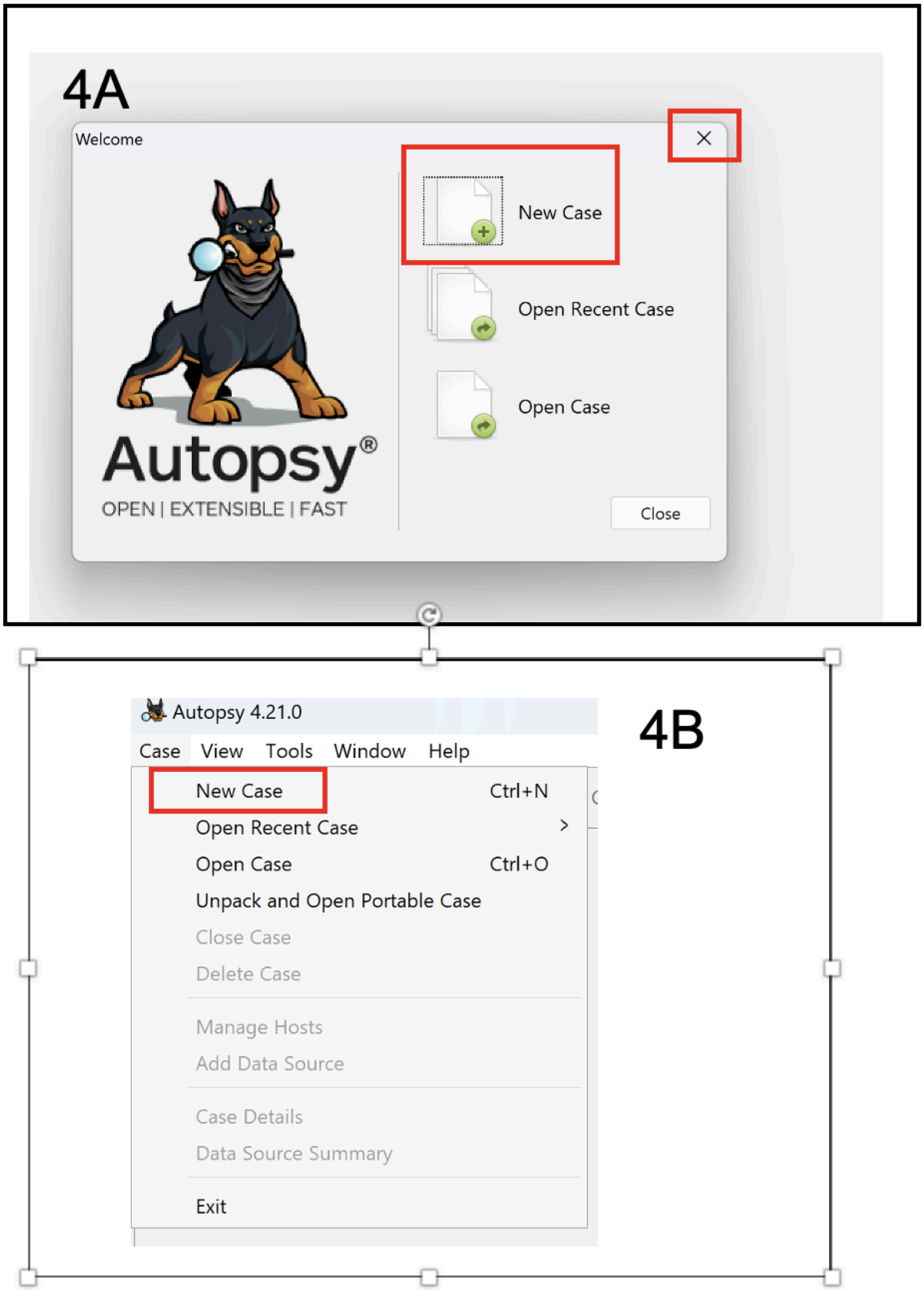
3I


Content
User Accounts 13
Wireless Networks 2
Data Files
Configurations 525
Databases 90
Images 223
Text 4
Videos 3
Activate
Go to Setting

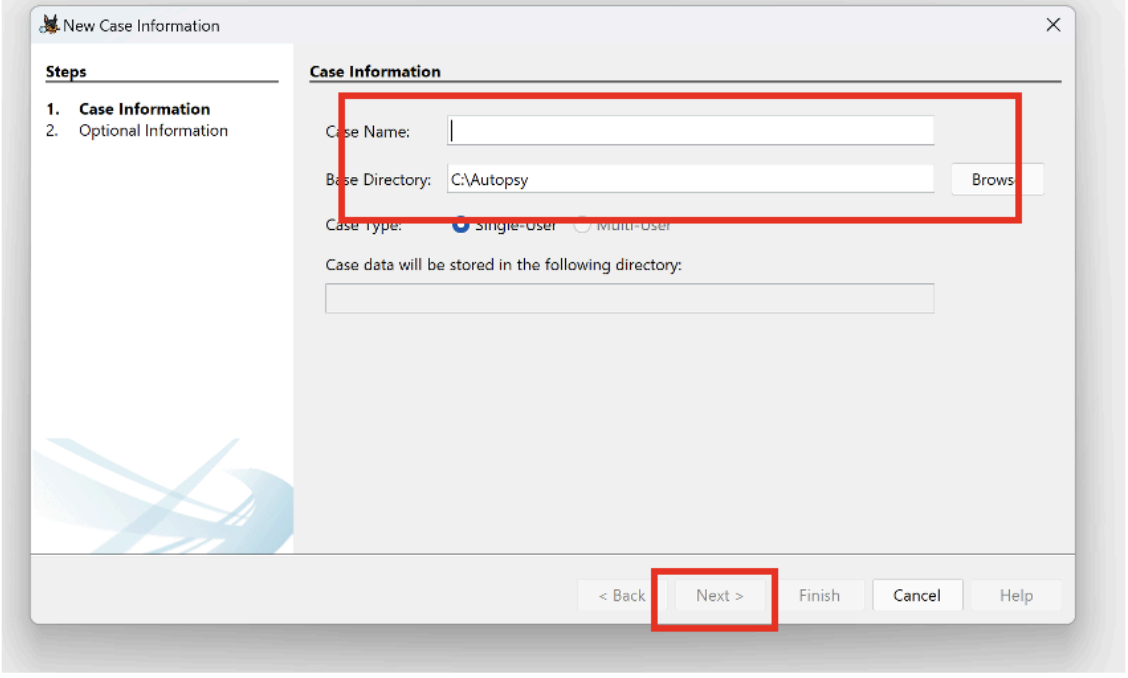
3J


n: 0 Items: 223/223 Selected: 223 Known files: 0 Path: iPhone/mobile/Containers/Shared/AppGroup/group.net.whatsapp.What

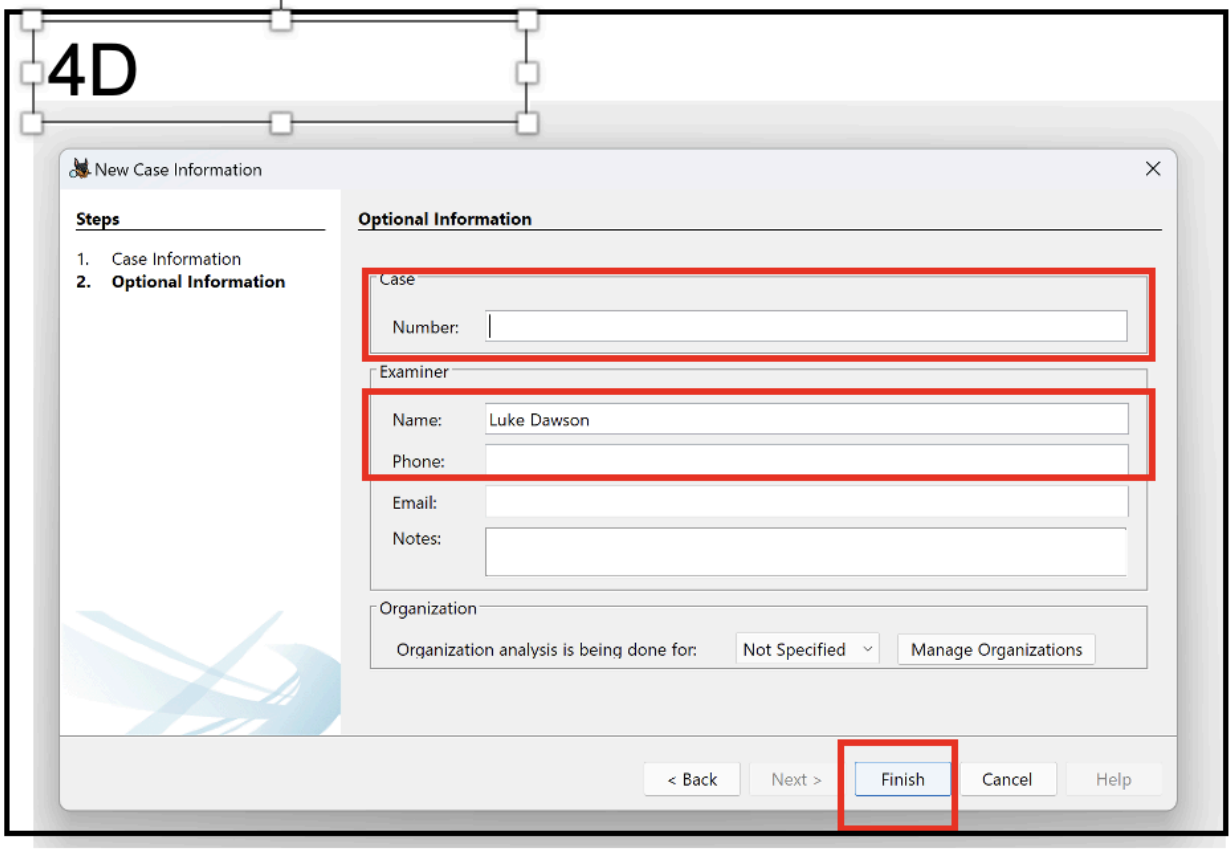
4: Analysis - SSD & USB Drive



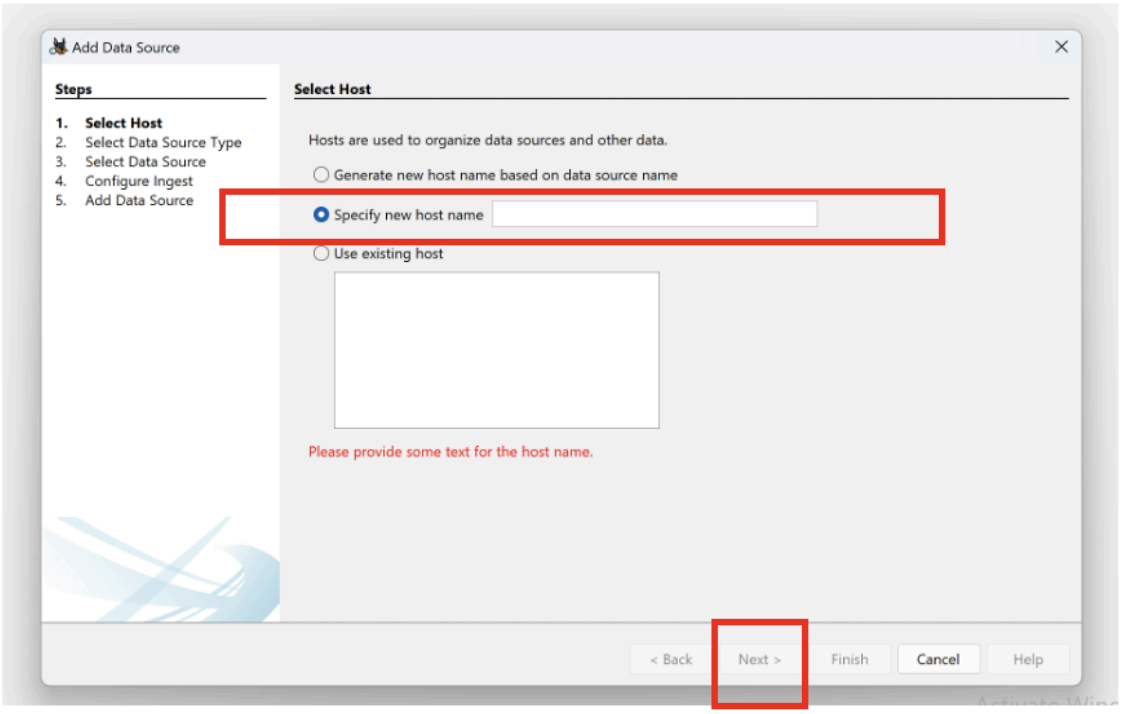
4C

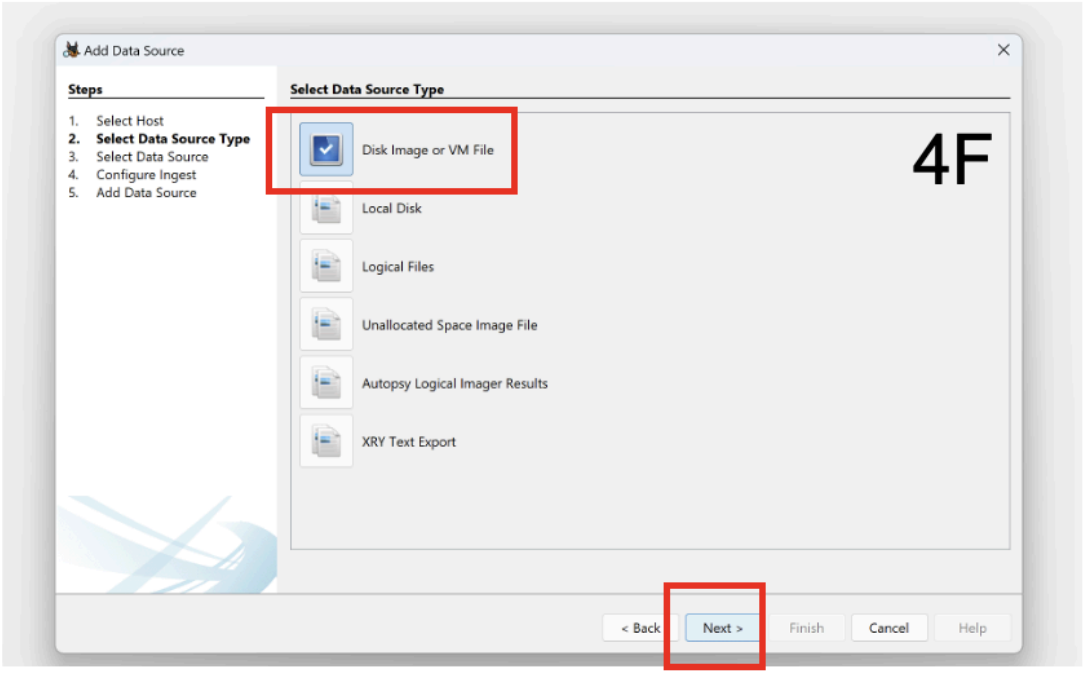

New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name:
Base Directory:
C:\Autopsy
Brows
Case Type:
Single-User
Multi-User
Case data will be stored in the following directory:
< Back
Next >
Finish
Cancel
Help

4D

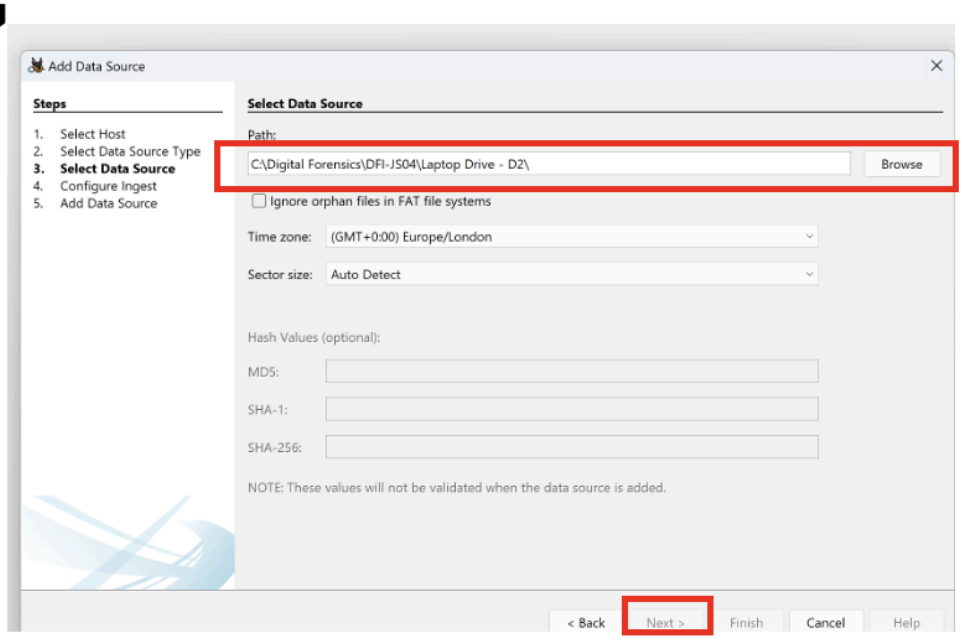

New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number:
Examiner
Name:
Luke Dawson
Phone:
Email:
Notes:
Organization
Organization analysis is being done for:
Not Specified
Manage Organizations
< Back
Next >
Finish
Cancel
Help

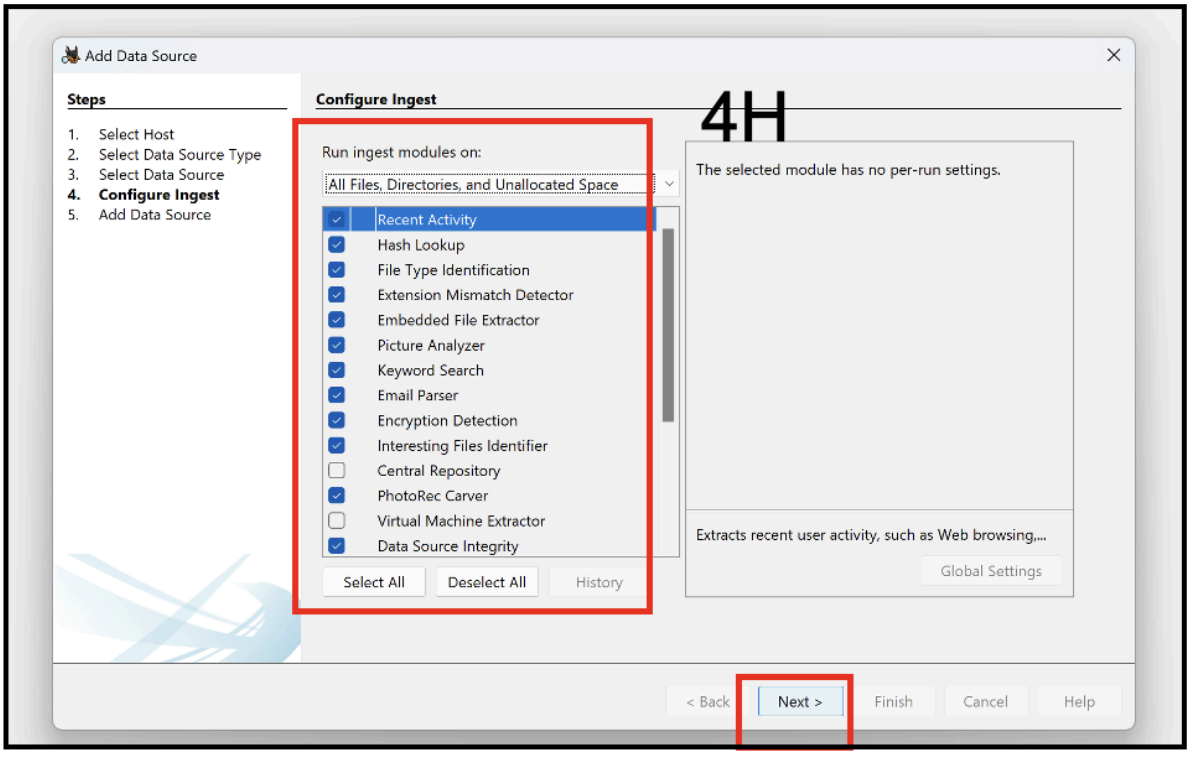
4E


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
Please provide some text for the host name.
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
4F
< Back
Next >
Finish
Cancel
Help

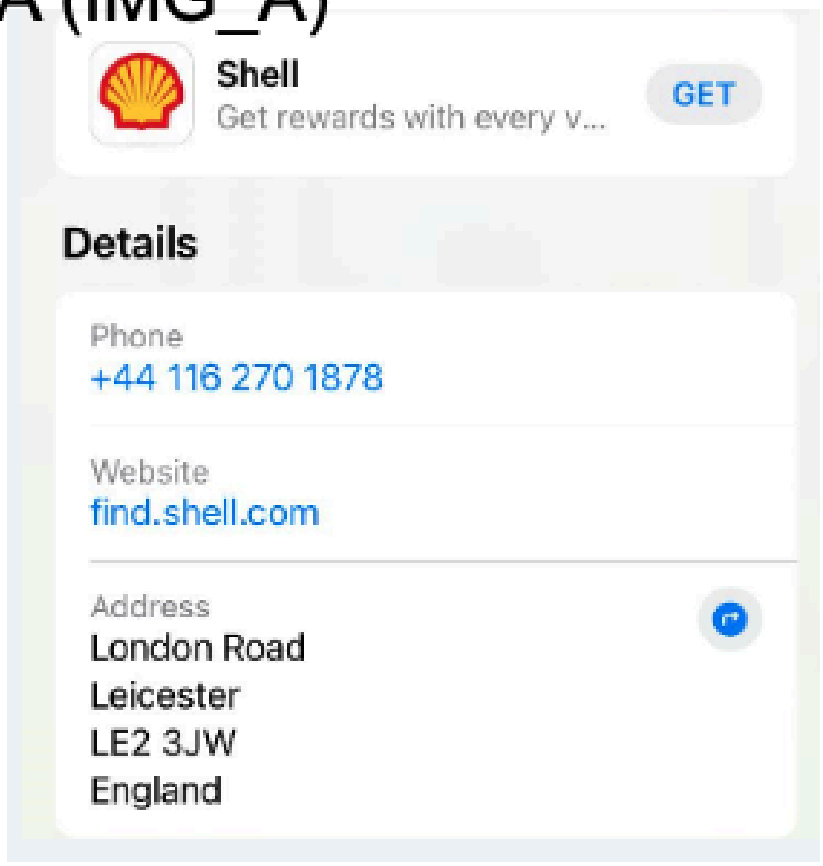
4G


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
C:\Digital Forensics\DFI-JS04\Laptop Drive - D2\
Browse
Ignore orphan files in FAT file systems
Time zone: (GMT+0:00) Europe/London
Sector size: Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
4H
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing,...
Global Settings
< Back
Next >
Finish
Cancel
Help

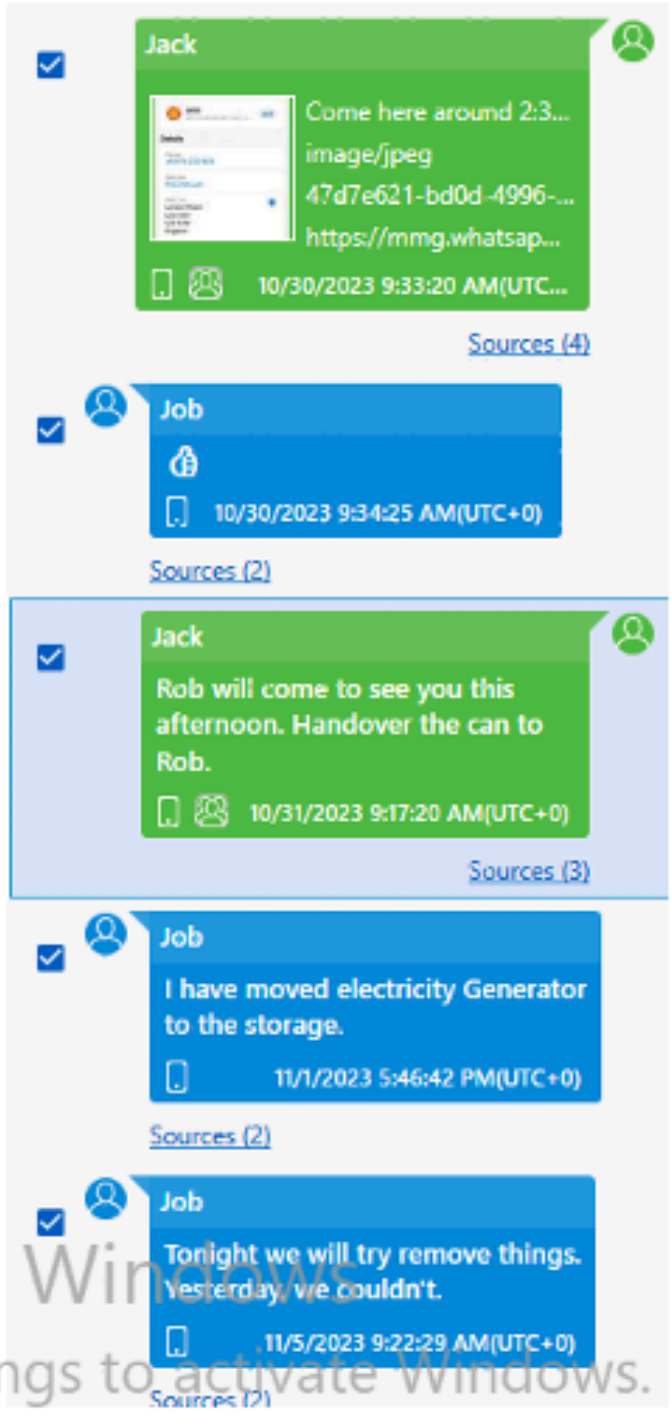
5: Evidence - Mobile Phone & SIM Card

5A (IMG_A)



- Image from the text messages and phone gallery from Jack Shroffs Phone
- IMG_A shows image of Shell Petrol Station location, phone number and website

5B (Text_A – Text_E)



- Screen shot of the text message chain between Mr. Shroff and an associate titled "Job"
- Screenshot shows the text communications regarding a pick-up of a Fuel Can at a Shell Garage

[No

5C (IMG_0006)

Save

Name:	IMG_0006.JPG
Type:	Images
Size (bytes):	7187838
Path:	iPhone/mobile/Media/DCIM/100APPLE/IMG_0006.JPG
Created:	10/23/2023 8:50:16 AM(UTC+0)
Accessed:	10/23/2023 8:50:17 AM(UTC+0)
Modified:	10/23/2023 8:50:17 AM(UTC+0)
Changed:	
Deleted:	10/31/2023 12:50:24 PM(UTC+0)
Extraction:	Advanced Logical
MD5:	5433020d421ca650c82da3e01e58cc7c
Source file:	IMG_0006.JPG

Metadata

Camera Make:	Apple
Camera Model:	iPhone 6s
Capture Time:	23/10/2023 09:50:17
Pixel resolution:	4032x3024
Resolution:	72x72 (Unit: Inch)
Orientation:	Horizontal (normal)
Lat/Lon:	52.597261 / -1.283167

Map

Position:
Address:
Map Address:

- Screenshot of the image found on Mr Shroffs phone.
- Image shows a picture of a website that sells a Jerry Can that is later referred to in text messages sent by Mr Shroff

5D (IMG_0003)

Save

Name:	IMG_0003.JPG
Type:	Images
Size (bytes):	2988809
Path:	iPhone/mobile/Media/DCIM/100APPLE/IMG_0003.JPG
Created:	10/10/2023 11:57:59 AM(UTC+0)
Accessed:	10/10/2023 11:57:59 AM(UTC+0)
Modified:	10/10/2023 11:57:59 AM(UTC+0)
Changed:	
Deleted:	
Extraction:	Advanced Logical
MD5:	011e9d935c85e218cc880f9100366800
Source file:	IMG_0003.JPG

Metadata

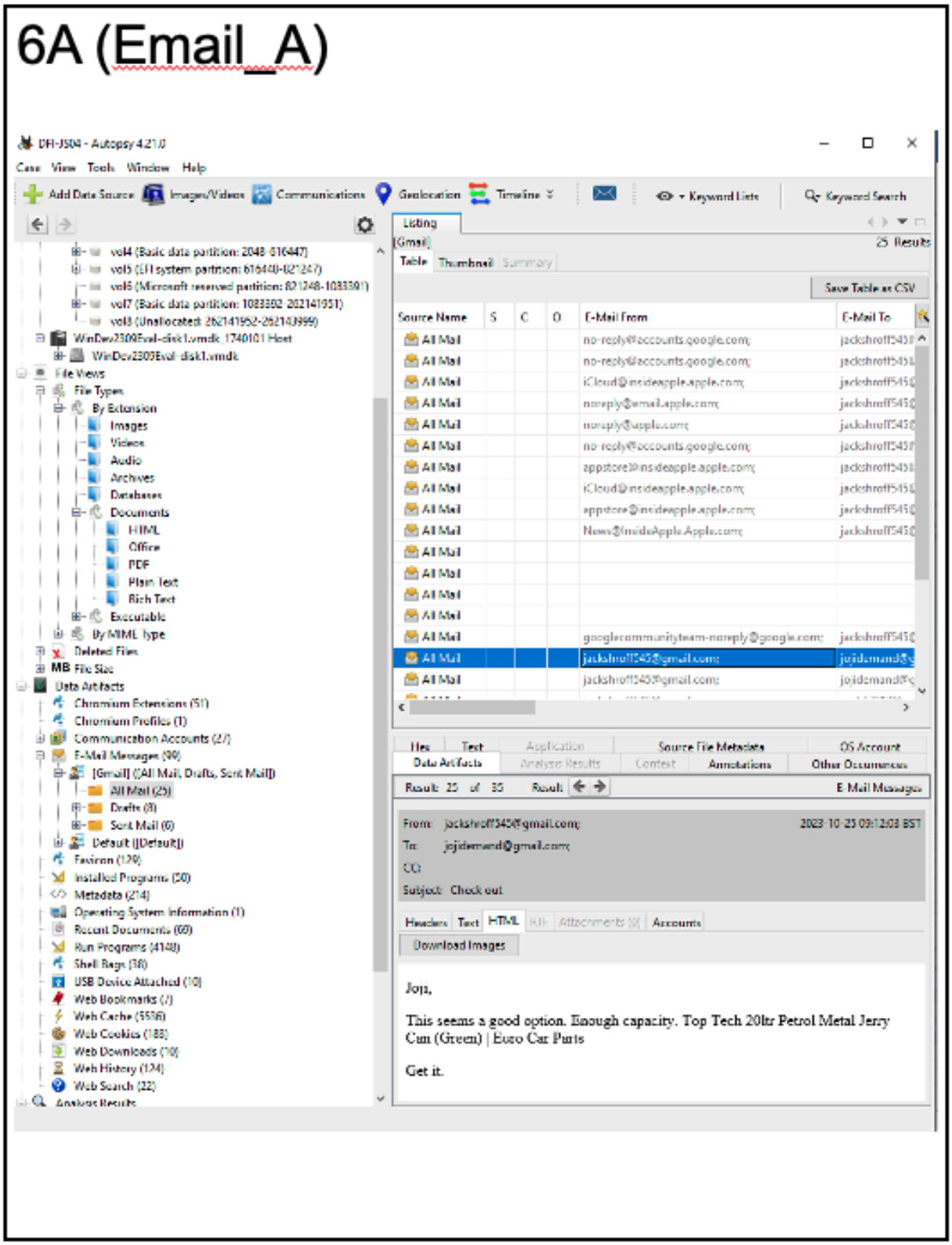
Camera Make:	Apple
Camera Model:	iPhone 6s
Capture Time:	10/10/2023 12:57:59
Pixel resolution:	4032x3024
Resolution:	72x72 (Unit: Inch)
Orientation:	Rotate 90 CW
Lat/Lon:	52.631916 / -1.143789

- Screenshot of the image found on Mr Shroffs phone.
- Image shows a picture of a what can be inferred to as the Storage Container in question within this investigation

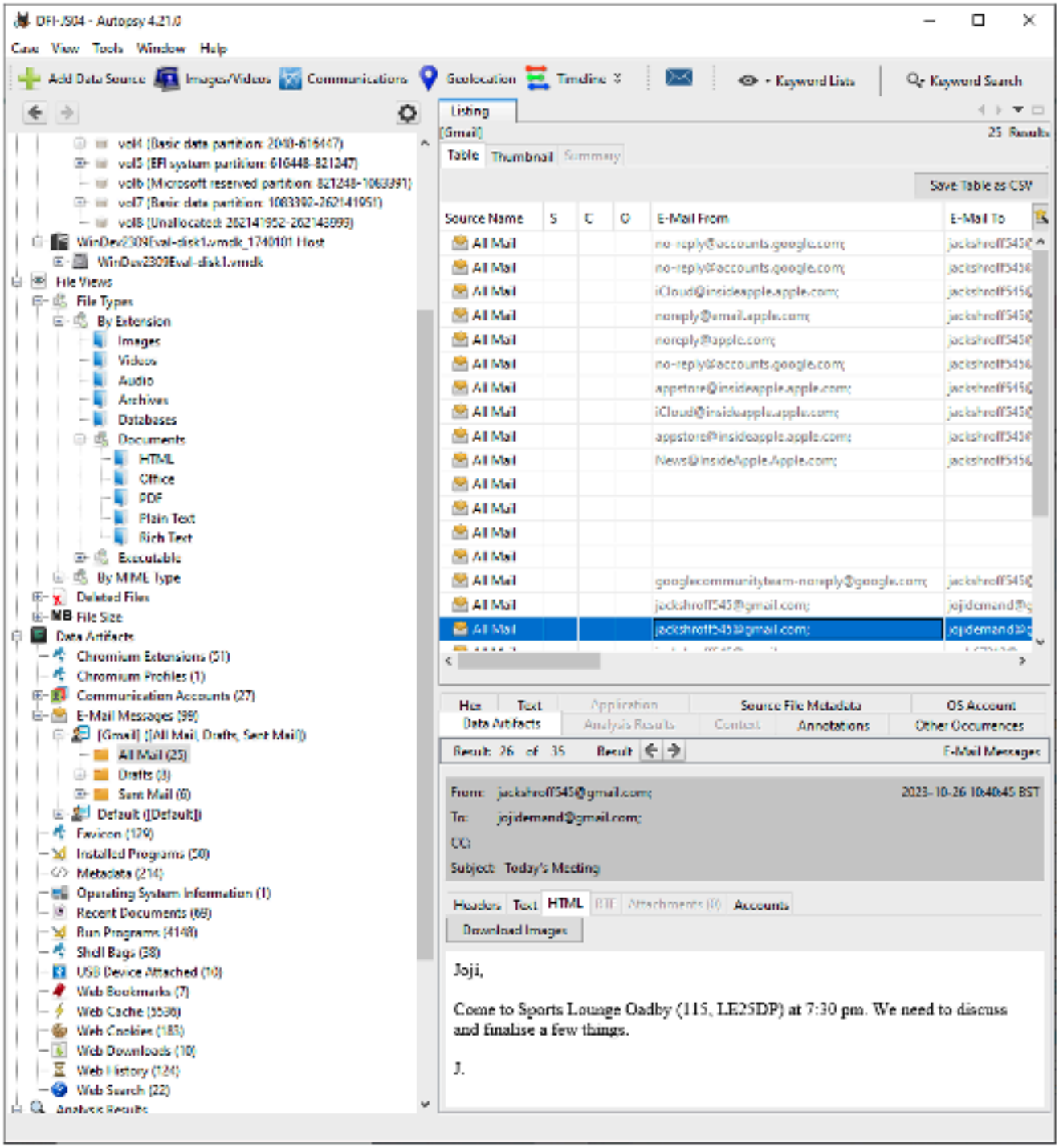
[No

6: Evidence - SSD & USB Drive

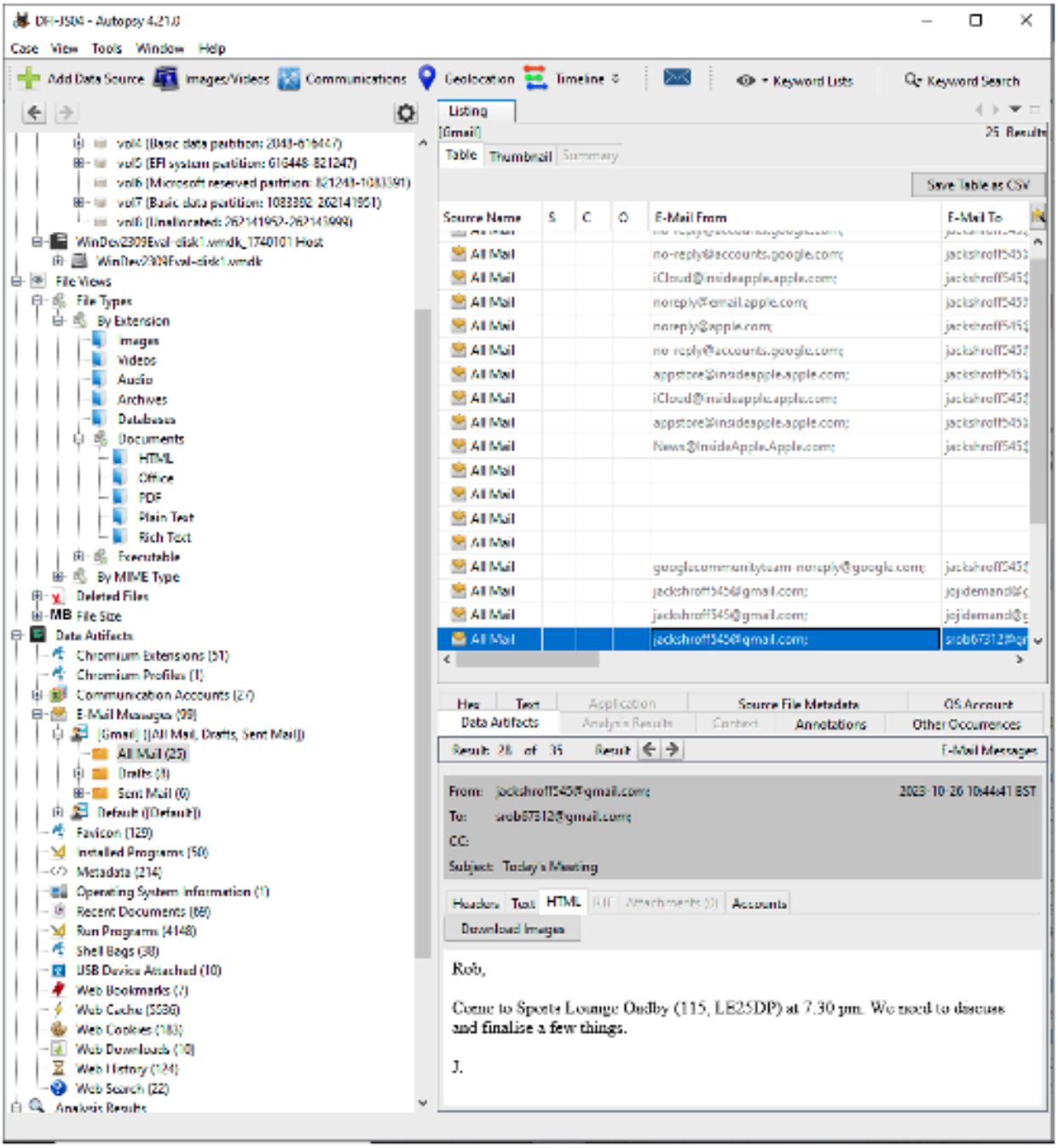
6A (Email_A)



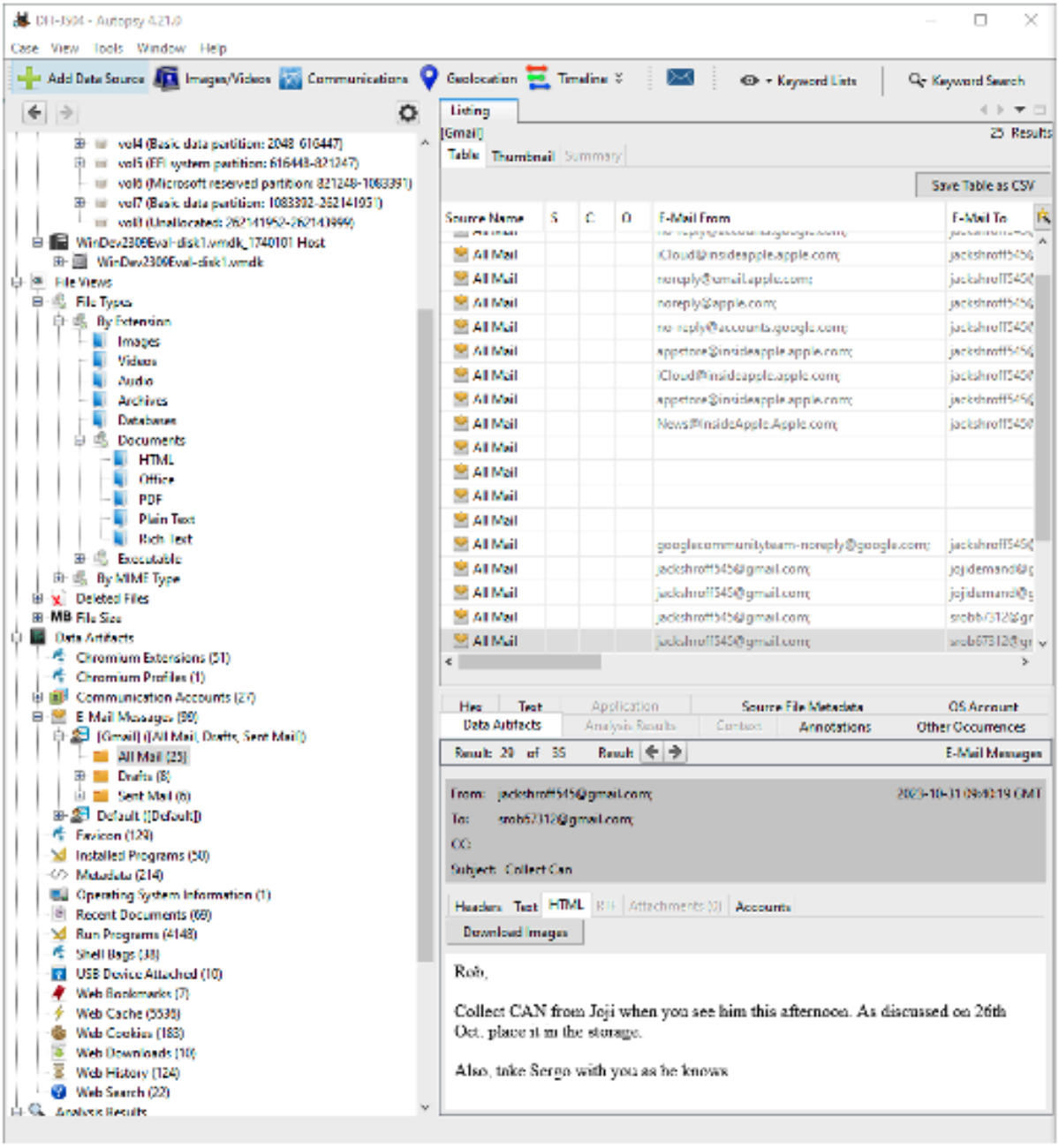
6B (Email_B)


DFI-504 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Listing
[Gmail]
25 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
E-Mail From
E-Mail To
All Mail
no-reply@accounts.google.com
jackshroff5456@gmail.com
no-reply@accounts.google.com
jackshroff5456@gmail.com
iCloud@insideapple.apple.com
jackshroff5456@gmail.com
noreply@email.apple.com
jackshroff5456@gmail.com
noreply@apple.com
jackshroff5456@gmail.com
no-reply@accounts.google.com
jackshroff5456@gmail.com
appstore@insideapple.apple.com
jackshroff5456@gmail.com
iCloud@insideapple.apple.com
jackshroff5456@gmail.com
appstore@insideapple.apple.com
jackshroff5456@gmail.com
News@InsideApple.Apple.com
jackshroff5456@gmail.com
googlecommunityteam-noreply@google.com
jackshroff5456@gmail.com
jackshroff545@gmail.com
jojidemand@gmail.com
jackshroff545@gmail.com
jojidemand@gmail.com
Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 26 of 35
Result
E-Mail Messages
From: jackshroff545@gmail.com
2023-10-26 10:40:45 BST
To: jojidemand@gmail.com
CC:
Subject: Today's Meeting
Headers
Text
HTML
RTF
Attachments (0)
Accounts
Download Images
Joji,
Come to Sports Lounge Oadby (115, LE25DP) at 7:30 pm. We need to discuss and finalise a few things.
J.
Data Sources
File Views
File Types
By Extension
Images
Videos
Audio
Archives
Databases
Documents
HTML
Office
PDF
Plain Text
Rich Text
Executable
By MIME Type
Deleted Files
File Size
Data Artifacts
Chromium Extensions (51)
Chromium Profiles (1)
Communication Accounts (27)
E-Mail Messages (99)
[Gmail] ([All Mail, Drafts, Sent Mail])
All Mail (23)
Drafts (3)
Sent Mail (6)
Default ([Default])
Favicon (179)
Installed Programs (30)
Metadata (214)
Operating System Information (1)
Recent Documents (69)
Run Programs (4149)
Shell Bags (38)
USB Device Attached (10)
Web Bookmarks (7)
Web Cache (3536)
Web Cookies (185)
Web Downloads (10)
Web History (124)
Web Search (22)
Analysis Results

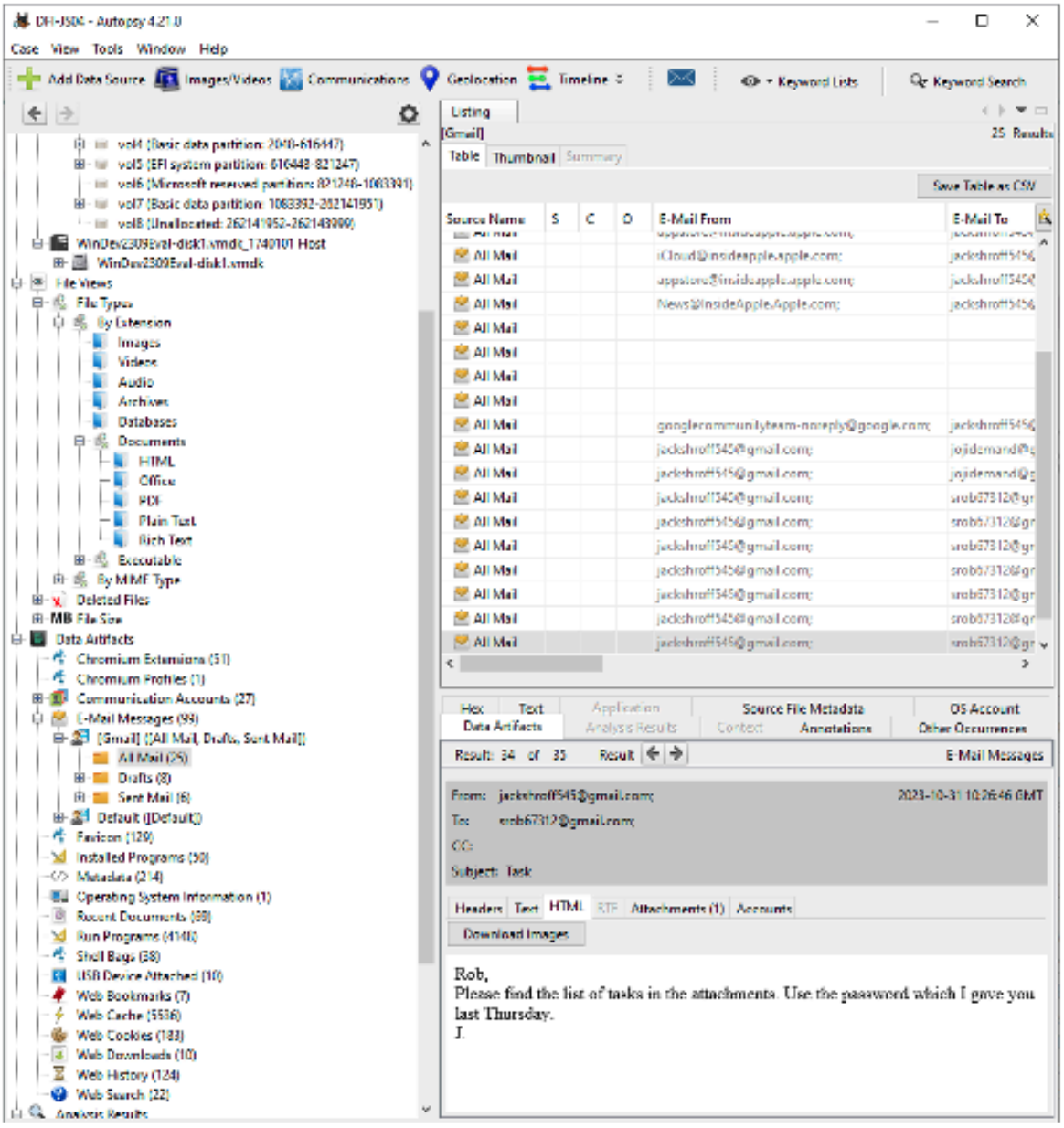
6C (Email_C)


DFI-ISAI - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Listing
[Gmail]
25 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
E-Mail From
E-Mail To
All Mail
no-reply@accounts.google.com;
iCloud@insideapple.apple.com;
noreply@email.apple.com;
noreply@apple.com;
appstore@insideapple.apple.com;
News@InsideApple.Apple.com;
googlecommunityteam-noreply@google.com;
jackshroff5454@gmail.com;
File Views
File Types
By Extension
Images
Videos
Audio
Archives
Databases
Documents
HTML
Office
PDF
Plain Text
Rich Text
Executable
By MIME Type
Deleted Files
File Size
Data Artifacts
Chromium Extensions (51)
Chromium Profiles (1)
Communication Accounts (27)
E-Mail Messages (39)
[Gmail] [All Mail, Drafts, Sent Mail]
All Mail (25)
Drafts (3)
Sent Mail (6)
Default ([Default])
Favicon (120)
Installed Programs (50)
Metadata (214)
Operating System Information (1)
Recent Documents (68)
Run Programs (4148)
Shell Bags (38)
USB Device Attached (10)
Web Bookmarks (7)
Web Cache (5080)
Web Cookies (183)
Web Downloads (10)
Web History (124)
Web Search (22)
Analysis Results
Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 25 of 25
Result
E-Mail Messages
From: jackshroff5454@gmail.com;
2023-10-26 10:44:41 BST
To: srob67512@gmail.com;
CC:
Subject: Today's Meeting
Headers
Text
HTML
RTF
Attachments (0)
Accounts
Download Images
Rob,
Come to Sports Lounge Oadby (115, LE25DP) at 7.30 pm. We need to discuss and finalise a few things.
J.

6D (Email_D)

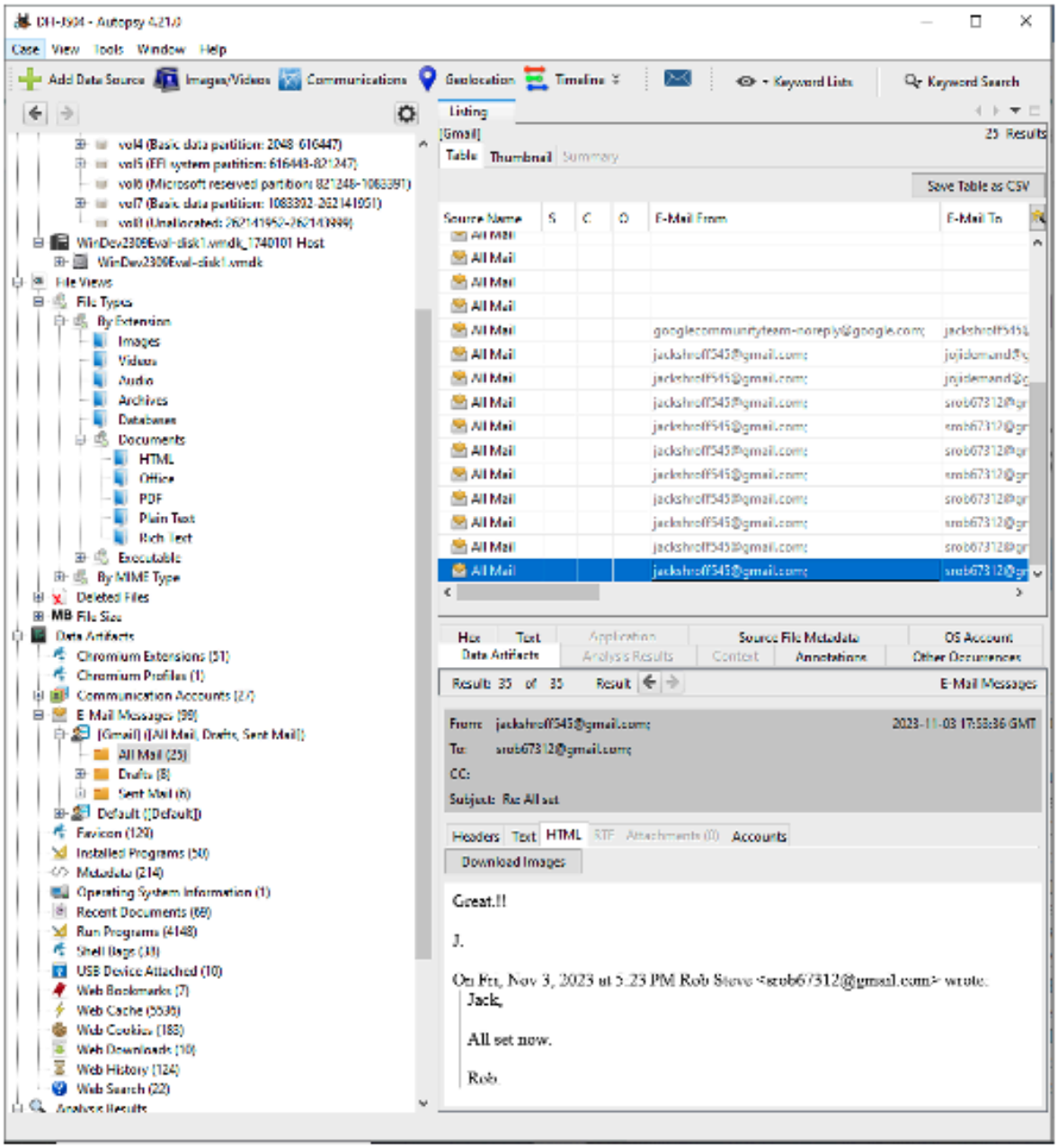

Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Listing
[Gmail]
25 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
E-Mail From
E-Mail To
All Mail
Cloud@insideapple.apple.com
noreply@email.apple.com
noreply@apple.com
no-reply@accounts.google.com
appstore@insideapple.apple.com
iCloud@insideapple.apple.com
News@InsideApple.Apple.com
googlecommunityteam-noreply@google.com
jackshroff5456@gmail.com
snobb67312@gmail.com
Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 20 of 35
Result:
E-Mail Messages
From: jackshroff5456@gmail.com
To: snobb67312@gmail.com
CC:
Subject: Collect Can
Headers
Text
HTML
RTF
Attachments (0)
Accounts
Download Images
Rob,
Collect CAN from Joji when you see him this afternoon. As discussed on 26th Oct, place it in the storage.
Also, take Sergo with you as he knows
Case
View
Tools
Window
Help
File Views
File Types
By Extension
Images
Videos
Audio
Archives
Databases
Documents
HTML
Office
PDF
Plain Text
Rich Text
Executable
By MIME Type
Deleted Files
MB File Size
Data Artifacts
Chromium Extensions (21)
Chromium Profiles (1)
Communication Accounts (27)
E-Mail Messages (99)
[Gmail] ([All Mail, Drafts, Sent Mail])
All Mail (25)
Drafts (8)
Sent Mail (6)
Default ([Default])
Favicon (129)
Installed Programs (30)
Metadata (214)
Operating System Information (1)
Recent Documents (69)
Run Programs (4148)
Shell Bags (38)
USB Device Attached (10)
Web Bookmarks (7)
Web Cache (3538)
Web Cookies (183)
Web Downloads (10)
Web History (124)
Web Search (22)

6E (Email_E)

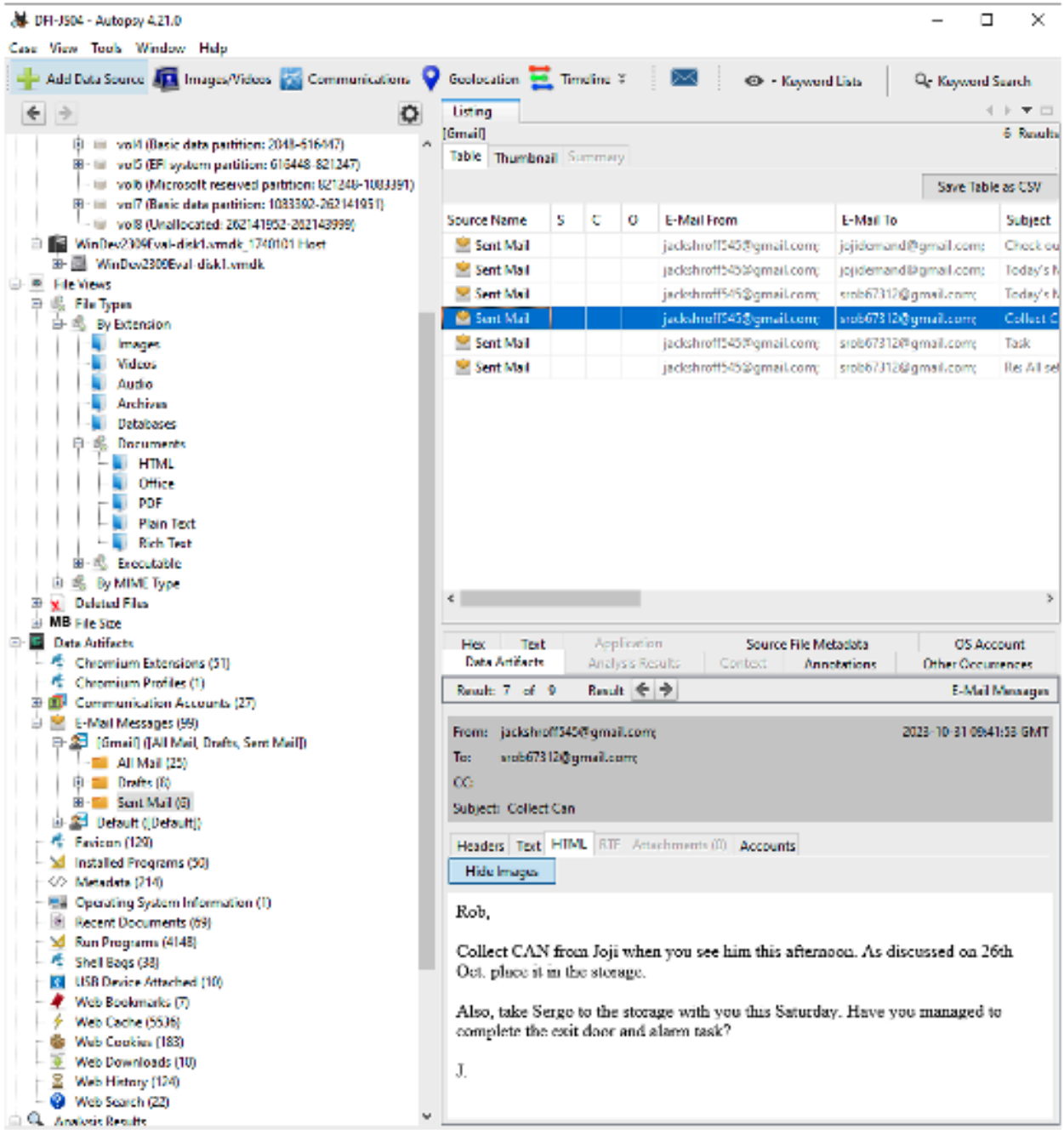

DH-J50 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Listing
[Gmail]
25 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
E-Mail From
E-Mail To
All Mail
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 34 of 35
Result
E-Mail Messages
From: jackshroff545@gmail.com
2023-10-31 10:26:46 GMT
To: srob67312@gmail.com
CC:
Subject: Task
Headers
Text
HTML
RTF
Attachments (1)
Accounts
Download Images
Rob,
Please find the list of tasks in the attachments. Use the password which I gave you last Thursday.
J.

[No Title]

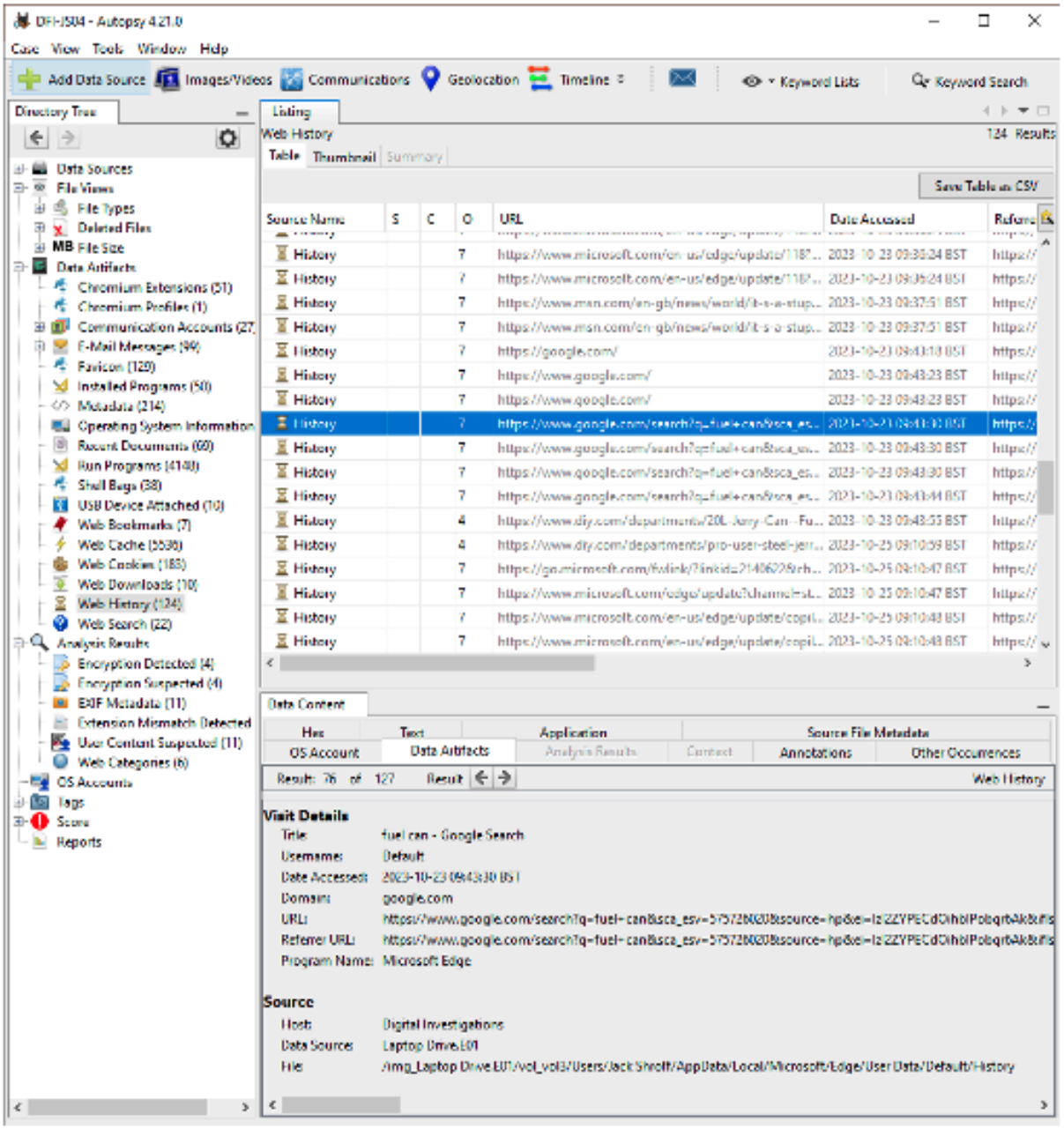
or (Email_F)



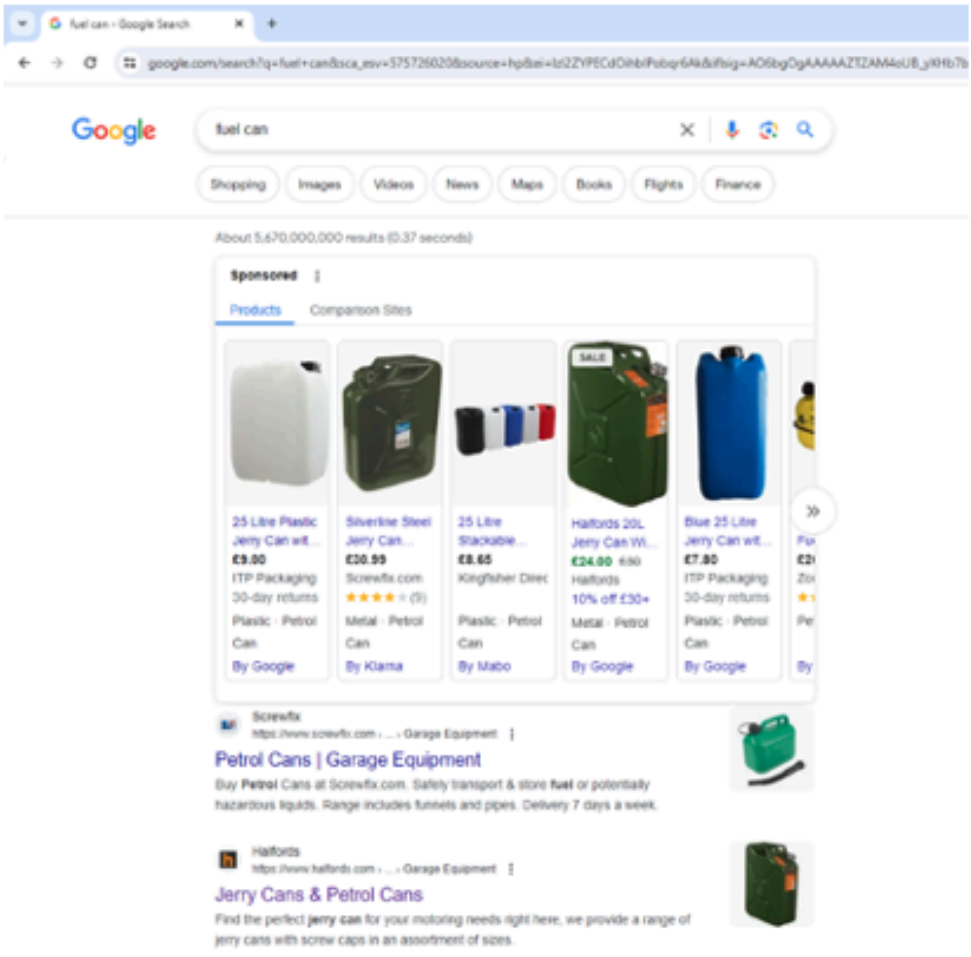
6G (Email_G)


DFI-J504 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Listing
[Gmail]
6 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
E-Mail From
E-Mail To
Subject
Sent Mail
jackshroff5405@gmail.com;
jojidemand@gmail.com;
Check ou
Sent Mail
jackshroff5405@gmail.com;
jojidemand@gmail.com;
Today's h
Sent Mail
jackshroff5405@gmail.com;
srob673126@gmail.com;
Today's h
Sent Mail
jackshroff5405@gmail.com;
srob673126@gmail.com;
Collect C
Sent Mail
jackshroff5405@gmail.com;
srob673126@gmail.com;
Task
Sent Mail
jackshroff5405@gmail.com;
srob673126@gmail.com;
Re: All set
File Views
File Types
By Extension
Images
Videos
Audio
Archives
Databases
Documents
HTML
Office
PDF
Plain Text
Rich Text
Executable
By MIME Type
Deleted Files
MB File Size
Data Artifacts
Chromium Extensions (31)
Chromium Profiles (1)
Communication Accounts (27)
E-Mail Messages (99)
[Gmail] ([All Mail, Drafts, Sent Mail])
All Mail (25)
Drafts (6)
Sent Mail (8)
Default (,Default])
Favicon (120)
Installed Programs (30)
Metadata (214)
Operating System Information (1)
Recent Documents (69)
Run Programs (4148)
Shell Bags (38)
USB Device Attached (10)
Web Bookmarks (7)
Web Cache (5536)
Web Cookies (183)
Web Downloads (10)
Web History (124)
Web Search (22)
Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 7 of 9
Result
E-Mail Messages
From: jackshroff5405@gmail.com;
2023-10-31 09:41:58 GMT
To: srob673126@gmail.com;
CC:
Subject: Collect Can
Headers
Text
HTML
RTF
Attachments (0)
Accounts
Hide Images
Rob,
Collect CAN from Joji when you see him this afternoon. As discussed on 26th Oct, place it in the storage.
Also, take Sergo to the storage with you this Saturday. Have you managed to complete the exit door and alarm task?
J.

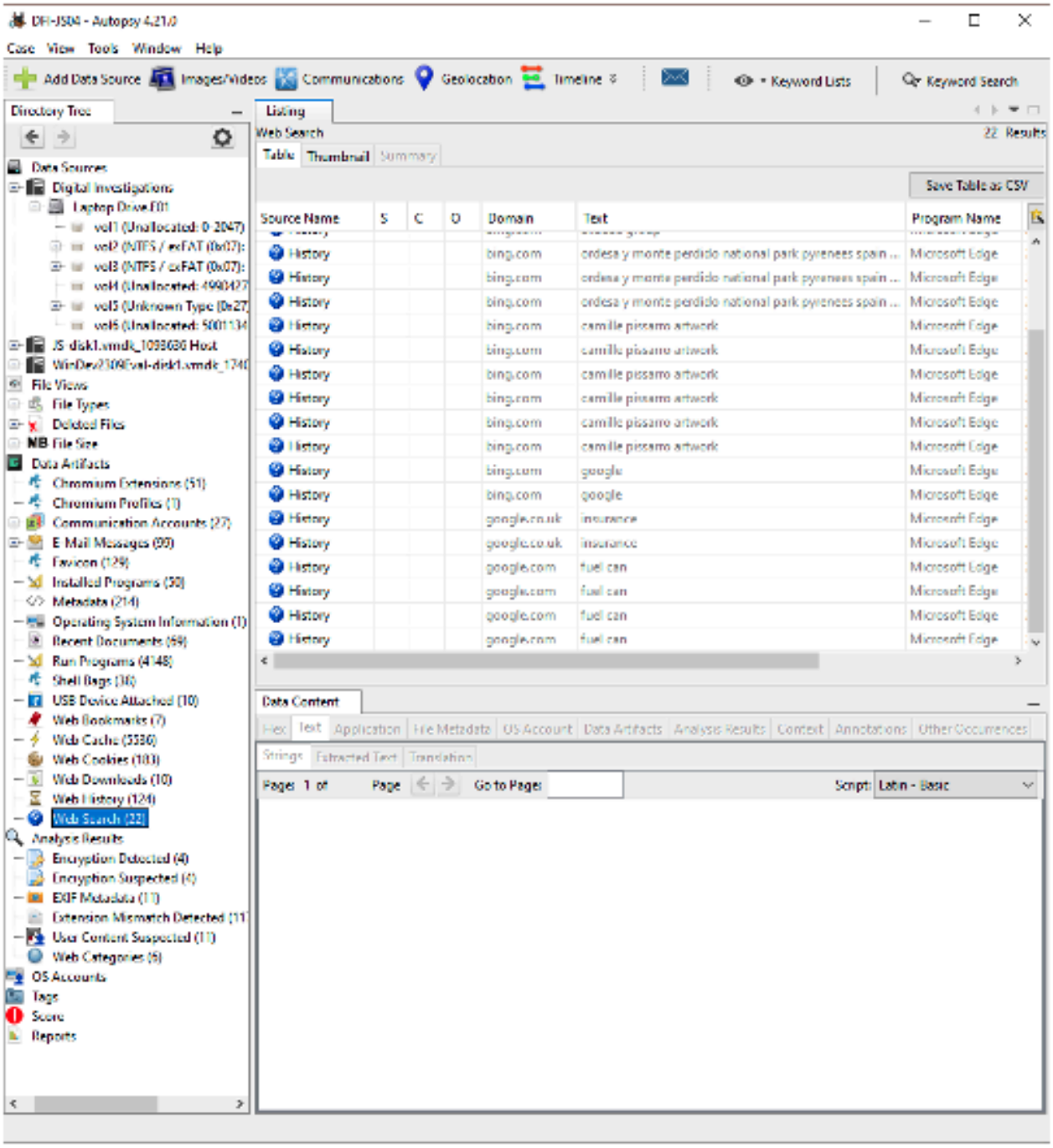
6H (BH_A)


DFI-504 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Directory Tree
Listing
Web History
124 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
URL
Date Accessed
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Chromium Extensions (51)
Chromium Profiles (1)
Communication Accounts (27)
E-Mail Messages (99)
Favicon (120)
Installed Programs (50)
Metadata (214)
Operating System Information
Recent Documents (69)
Run Programs (4148)
Shell Bags (38)
USB Device Attached (10)
Web Bookmarks (7)
Web Cache (5530)
Web Cookies (183)
Web Downloads (10)
Web History (124)
Web Search (22)
Analysis Results
Encryption Detected (4)
Encryption Suspected (4)
EXIF Metadata (11)
Extension Mismatch Detected
User Content Suspected (11)
Web Categories (6)
OS Accounts
Tags
Score
Reports
Data Content
Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 76 of 127
Result
Web History
Visit Details
Title: fuel can - Google Search
Username: Default
Date Accessed: 2023-10-23 09:43:30 BST
Domain: google.com
URL:
Referrer URL:
Program Name: Microsoft Edge
Source
Host: Digital Investigations
Data Source: Laptop Drive.E01
File: /img_Laptop Drive.E01/vol_vol3/Users/Jack Shroff/AppData/Local/Microsoft/Edge/User Data/Default/History

6H (BH_A)

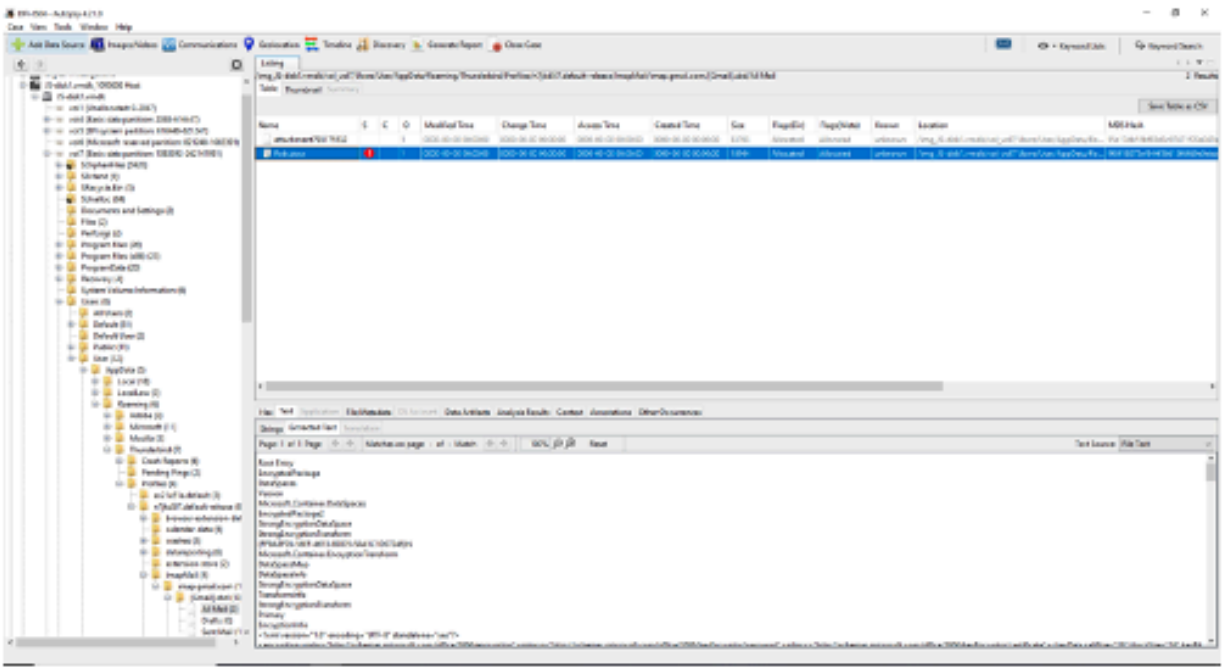

fuel can - Google Search
Google
fuel can
Shopping
Images
Videos
News
Maps
Books
Flights
Finance
About 5,670,000,000 results (0.37 seconds)
Sponsored
Products
Comparison Sites
25 Litre Plastic Jerry Can wit...
£9.00
ITP Packaging
30-day returns
Plastic · Petrol Can
By Google
Silverline Steel Jerry Can...
£30.99
Screwfix.com
Metal · Petrol Can
By Klarna
25 Litre Stackable...
£8.65
Kingfisher Direc
Plastic · Petrol Can
By Mabo
SALE
Halfords 20L Jerry Can Wi...
£24.00 £30
Halfords
10% off £30+
Metal · Petrol Can
By Google
Blue 25 Litre Jerry Can wit...
£7.80
ITP Packaging
30-day returns
Plastic · Petrol Can
By Google
Screwfix
Petrol Cans | Garage Equipment
Buy Petrol Cans at Screwfix.com. Safely transport & store fuel or potentially hazardous liquids. Range includes funnels and pipes. Delivery 7 days a week.
Halfords
Jerry Cans & Petrol Cans
Find the perfect jerry can for your motoring needs right here, we provide a range of jerry cans with screw caps in an assortment of sizes.

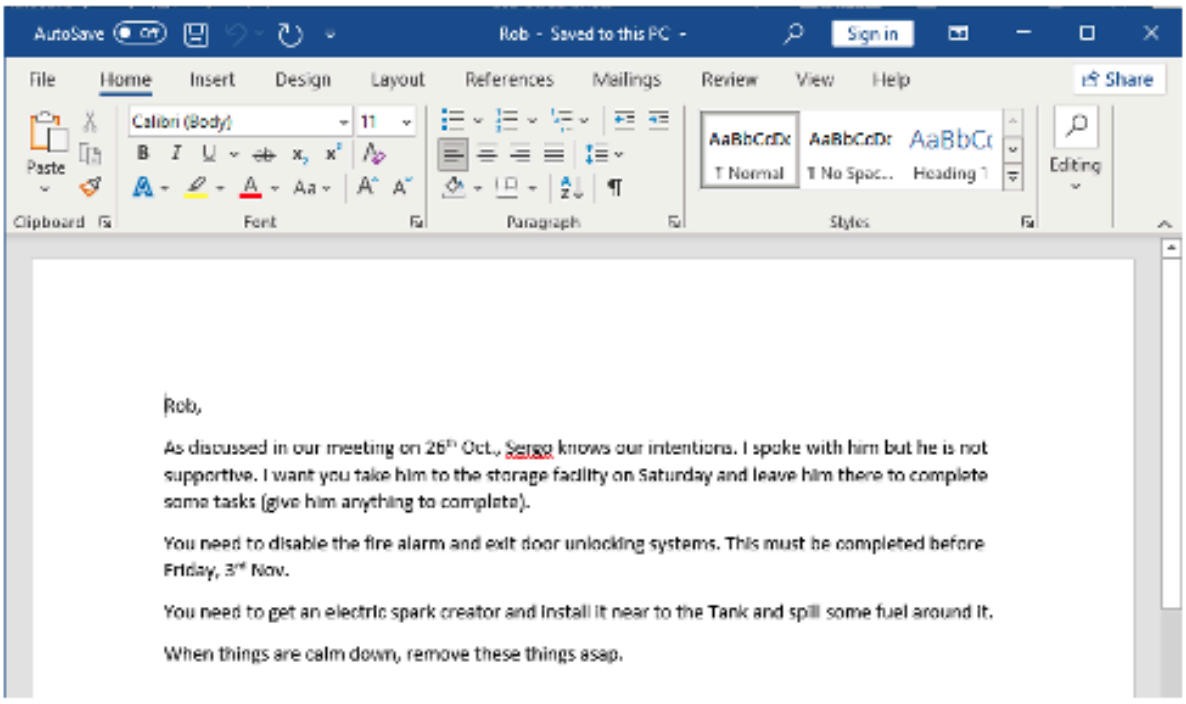
6I (BH_B)


DFI-JSN - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Directory Tree
Listing
Web Search
22 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
Domain
Text
Program Name
History
bing.com
ordesa y monte perdido national park pyrenees spain ...
Microsoft Edge
camille pissarro artwork
google
insurance
fuel can
Data Content
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Strings
Extracted Text
Translation
Page: 1 of
Page
Go to Page:
Script: Latin - Basic
Data Sources
Digital Investigations
Laptop Drive.E01
File Views
File Types
Deleted Files
File Size
Data Artifacts
Chromium Extensions (51)
Chromium Profiles (1)
Communication Accounts (27)
E-Mail Messages (90)
Favicon (129)
Installed Programs (30)
Metadata (214)
Operating System Information (1)
Recent Documents (69)
Run Programs (4148)
Shell Bags (36)
USB Device Attached (10)
Web Bookmarks (7)
Web Cache (3336)
Web Cookies (183)
Web Downloads (10)
Web History (124)
Web Search (22)
Analysis Results
Encryption Detected (4)
Encryption Suspected (4)
EXIF Metadata (11)
User Content Suspected (11)
Web Categories (5)
OS Accounts
Tags
Score
Reports

6J (EF_A)

6K (EF_B)




AutoSave
Rob - Saved to this PC
Sign in
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Help
Share
Calibri (Body)
11
Paste
Clipboard
Font
Paragraph
Styles
Editing
Normal
No Spac...
Heading 1
Rob,
As discussed in our meeting on 26th Oct., Sergo knows our intentions. I spoke with him but he is not supportive. I want you take him to the storage facility on Saturday and leave him there to complete some tasks (give him anything to complete).
You need to disable the fire alarm and exit door unlocking systems. This must be completed before Friday, 3rd Nov.
You need to get an electric spark creator and install it near to the Tank and spill some fuel around it.
When things are calm down, remove these things asap.