

# DIGITAL FORENSICS ANALYSIS

Rohan Chavan (2212517)  
UNIVERSITY OF WALES TRINITY SIANT DAVID

## Contents

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| Task 1 .....                                                                       | 2  |
| Introduction .....                                                                 | 2  |
| Current State of the Field [1].....                                                | 2  |
| Intersection of Digital Forensics and Cybersecurity .....                          | 2  |
| Emerging Trends .....                                                              | 3  |
| Key Challenges [9] [10] [11] .....                                                 | 4  |
| National and International Job Market [11] .....                                   | 5  |
| Conclusion.....                                                                    | 5  |
| Task 2 .....                                                                       | 6  |
| Current State of Digital Forensic Tools: Features and Capabilities .....           | 6  |
| Introduction to the Comparison of Digital Forensic Tools [20] [21] [22] [23] ..... | 7  |
| Conclusion of Digital Forensic Tools Comparison .....                              | 8  |
| Task 3 .....                                                                       | 8  |
| Part 1.....                                                                        | 8  |
| Scenario- co-operate crime.....                                                    | 8  |
| Part 2.....                                                                        | 15 |
| Scenario Summary:.....                                                             | 17 |
| Extracted Evidence from attacker's machine as show below.....                      | 18 |
| Conclusion.....                                                                    | 19 |
| Presentation on Task 3: .....                                                      | 20 |
| Task 4 .....                                                                       | 22 |
| Investigation Team.....                                                            | 24 |
| Team Discussions: Strategy and Collaboration.....                                  | 24 |
| Risk assessment phone One.....                                                     | 25 |
| Risk assessment phone Two.....                                                     | 25 |
| Initial Device One Assessment: .....                                               | 25 |
| Identification of Challenges and Strategies:.....                                  | 26 |
| Initial Device Two Assessment: .....                                               | 28 |
| Analysis and Examination of Data of Phone 2 .....                                  | 29 |
| Photo Analysis: .....                                                              | 29 |
| File System Exploration: .....                                                     | 32 |
| Call Log Analysis: .....                                                           | 32 |
| Audio File Analysis: .....                                                         | 32 |
| Final Assessment of Investigation.....                                             | 33 |
| Team Members Ratings.....                                                          | 34 |

## Task 1

### Introduction

In the rapidly evolving landscape of technology, the fields of digital forensics and cybersecurity have become increasingly interconnected. This intersection is shaping new trends, presenting unique challenges, and influencing the global job market. In this detailed exploration, we'll delve into the current state of these fields, their converging paths, emerging trends, key challenges, and the implications for the national and international job markets.

### Current State of the Field [1]

In today's technology-driven era, the role of digital forensics has become increasingly crucial. This branch of forensic science is dedicated to the meticulous process of recovering, examining, and preserving digital evidence, all while adhering to strict legal protocols. The global forensics market is on an upward trajectory, with projections indicating a growth to approximately \$27,705 million by 2028, according to a report by Vantage Market Research. This surge is largely attributed to the relentless progression in technological innovation and the pervasive integration of digital technologies across various sectors.

Originally referred to as 'Computer Forensics', the field has evolved into 'Digital Forensics', reflecting its expansion beyond computers to encompass a wide array of digital devices interconnected by the Internet of Things (IoT). This evolution started gaining momentum in the 1980s, marked by significant milestones such as the FBI's inauguration of its computer forensics program and the development of the first honeypot trap by Cliff Stoll.

Digital forensics today is fundamental in the analysis of digital crime scenes, extending its reach to any device capable of storing digital data. It plays a dual role, serving both law enforcement agencies in criminal and civil matters and corporate incident response teams in tackling cyber threats like data breaches. In the corporate realm, digital forensic investigations are typically initiated in response to specific incidents such as network anomalies, suspected espionage, cyberattacks, or for compliance with industry standards.

The field has diversified into various specialized domains, including but not limited to electronic discovery, network and computer forensics, and analysis of databases, disks, cloud systems, and malware. Each specialization caters to different facets of digital investigations, reflecting the complexity and breadth of today's digital landscape.

The methodology employed in digital forensics is methodical and structured, varying slightly depending on whether the focus is law enforcement, corporate auditing, or incident response. In summary, the significance and complexity of digital forensics continue to grow in parallel with the advancement of technology, cementing its place as an indispensable component in the realm of modern forensic science and cybersecurity.

### Intersection of Digital Forensics and Cybersecurity

Digital forensics, a crucial subset of forensic science, is the technical art of uncovering, preserving, and interpreting data from digital devices. It plays a pivotal role in the legal system, often forming the

backbone of evidence in criminal proceedings. The intersection of digital forensics and cybersecurity is fundamental to contemporary organizations, serving multiple purposes from legal compliance to effective incident response in the event of a cybercrime. [2]

Professionals in this arena are expected to possess a diverse skill set that spans digital technology, legal knowledge, and forensic proficiency. This combination is critical because digital forensics extends beyond mere cybersecurity. It encompasses the retrieval of digital data from an array of devices, such as smartphones, street cameras, and even automobiles, which can be instrumental in solving crimes.

This interdisciplinary field includes several branches: [2]

- Mobile device forensics focuses on recovering evidence from portable devices.
- Computer forensics ensures the integrity and analysis of data from computer systems.
- Database forensics examines alterations and access to database systems.
- Network forensics analyzes network traffic to detect and gather evidence of cyber intrusions.
- Forensic data analysis scrutinizes structured data within databases, often in financial crime cases.

The convergence of digital forensics and cybersecurity not only aids in legal proceedings but also enhances an organization's cybersecurity measures. It informs the development of robust systems that can detect weaknesses and mitigate future cyber threats. Legal and ethical considerations are paramount, with digital investigations involving personal data that must be handled within the boundaries of privacy laws and constitutional protections against unreasonable searches or self-incrimination. [3]

To remain effective, digital forensics experts must navigate the intricacies of laws such as the Wiretap Act and the Stored Wire and Electronic Communication Act. Their work ensures continuous improvement in cybersecurity protocols and provides cost-effective solutions by pre-empting potential breaches, thereby safeguarding the digital assets of organizations and upholding the integrity of the legal process. [3]

The intersection of digital forensics and cybersecurity is a critical area, as the skills and tools of each field are increasingly overlapping. Cybersecurity measures are essential for preventing attacks, but when breaches occur, digital forensics plays a crucial role in understanding the attack and preventing future incidents. [2]

This convergence has led to a holistic approach to digital threats, where organizations not only focus on prevention but also on the post-breach analysis. Digital forensics experts are now often part of cybersecurity teams, contributing their expertise in tracing the source of breaches and gathering evidence for legal proceedings.

### Emerging Trends

The digital world evolves at breakneck speed, and the tools and techniques of digital forensics must keep pace. In this ever-shifting landscape, several key trends are poised to reshape the field, demanding attention from investigators and cyber warriors alike.

1. AI-powered Investigations: Artificial intelligence (AI) is no longer science fiction. Machine learning algorithms are being trained to analyse vast quantities of digital data, identifying patterns and

anomalies beyond human capabilities. This can expedite investigations, uncover hidden connections, and predict future attack vectors. Tools like deep learning and natural language processing are already assisting in image and video analysis, malware detection, and automated incident response. [4]

2. Cloud Forensics: As data migrates to the cloud, so too must forensic investigations. New challenges arise in this decentralized environment, with data distributed across multiple servers and potentially subject to different jurisdictions. Cloud forensics tools are rapidly developing to address these challenges, enabling investigators to collect and analyse evidence from cloud storage providers like Google Drive and Amazon S3, while respecting legal and privacy considerations. [5]

3. Blockchain: Unveiling the Tamper-proof Trail: Blockchain, the technology behind cryptocurrencies, offers an immutable record of transactions. This tamper-proof ledger can be utilized in digital forensics to track data provenance, verify the integrity of digital evidence, and identify instances of data manipulation. While still in its infancy, blockchain applications have the potential to revolutionize evidence handling and chain of custody protocols. [6]

4. Internet of Things (IoT) Investigations: The proliferation of connected devices presents a new frontier for digital forensics. The sheer volume and diversity of data generated by smart devices, wearables, and sensors pose both challenges and opportunities. New methodologies are emerging to analyse sensor data, reconstruct activity timelines, and extract evidence from these ubiquitous devices. [7]

5. Social Media Forensics: Social media platforms have become vital battlegrounds for disinformation, cyberbullying, and criminal activity. Forensic techniques are adapting to analyse social media posts, track online communities, and identify digital personas used in malicious campaigns. Understanding online behaviour and social media networks is crucial for investigators navigating this complex digital landscape. [8]

Several emerging trends are shaping the future of digital forensics and cybersecurity. One significant trend is the increasing reliance on cloud-based services, which introduces new vulnerabilities and complexities in data protection. The Internet of Things (IoT) is another area where the proliferation of connected devices has expanded the attack surface for cyber threats. [8]

Artificial intelligence and machine learning are being increasingly utilized for predictive analytics in cybersecurity, enhancing the ability to anticipate and mitigate potential threats. In digital forensics, these technologies are improving the efficiency of data analysis in investigations.

### Key Challenges [9] [10] [11]

Challenges in the field of digital forensics are multifaceted and constantly evolving, primarily due to the rapid pace of technological innovation and the increasing sophistication of cybercriminals. One of the most significant hurdles is the sheer volume and variety of data. With the proliferation of devices capable of storing digital information, from Internet of Things (IoT) gadgets to cloud storage solutions, forensic experts must sift through an overwhelming amount of data, which can be both time-consuming and technically demanding.

Another key challenge is encryption. Advanced encryption techniques have become commonplace, offering robust protection for data security. While encryption is vital for privacy, it presents a significant obstacle for digital forensic investigators, who must find legally permissible ways to decrypt information without altering it, which sometimes can be an impossible task.

Additionally, the dynamic nature of digital data presents a problem. Unlike physical evidence, digital data can be altered, deleted, or corrupted with just a few clicks. Ensuring the integrity of this data for use in legal proceedings requires rigorous chain-of-custody protocols and forensic soundness, which can be difficult to maintain in complex IT environments.

The legal landscape itself poses a challenge. Laws and regulations often struggle to keep pace with technological advancements, leading to legal grey areas that can complicate investigations. Privacy laws, differing international legislations, and jurisdictional boundaries further complicate the process of acquiring and using digital evidence.

Furthermore, the shortage of trained professionals in digital forensics exacerbates these challenges. The field requires a high level of expertise and ongoing education to stay abreast of the latest technologies and forensic methodologies, but there is a global shortfall of individuals with the necessary skills.

Finally, the rise of anti-forensic techniques, where individuals use tools or methods to obfuscate their digital footprints intentionally, makes the task of digital forensic experts even more demanding. These challenges collectively contribute to a complex and demanding environment for digital forensics professionals, requiring constant learning, adaptability, and resourcefulness.

### National and International Job Market [11]

The digital forensics market in the UK is experiencing significant growth, driven by the increasing need for cybersecurity and data analysis in various sectors. As of 2023, the market is expanding steadily, with projections indicating a substantial rise in demand and market value over the next few years. The global market value of digital forensics, estimated at USD 2453.06 million in 2022, is anticipated to reach USD 5211.15 million by 2028, growing at a CAGR of 13.38% during the forecast period.

This growth is attributed to the rising incidence of cyber-crime and the need for effective digital evidence management in criminal and civil court cases. The UK market is particularly responsive to these trends due to its advanced technological infrastructure and the presence of key market players like Magnet Forensics, Guidance Software Inc., and Cellebrite. The market encompasses various segments, including computer forensics, mobile device forensics, and network forensics, catering to diverse applications across sectors like government, healthcare, and finance.

The increasing sophistication of cyber-attacks and the need for secure information handling in the digital age are key drivers for the market. The UK's focus on enhancing its digital forensics capabilities is evident in the growing investment in this sector, reflecting its commitment to combating cyber threats and ensuring digital security.

### Conclusion

The dynamic intersection of digital forensics and cybersecurity is an area of continuous growth and evolution. As technology advances, new challenges and trends emerge, shaping the job market and requiring ongoing development of skills and strategies. The future of these interconnected fields is promising, with significant opportunities for professionals and critical implications for the security of digital infrastructures globally. Addressing the challenges and embracing the emerging trends will be key to advancing in these vital sectors.

## Task 2

### Current State of Digital Forensic Tools: Features and Capabilities

Digital forensics, a vital field within the realm of cybersecurity and criminal investigation, has evolved rapidly over the past few years. The current state of digital forensic tools reflects a dynamic interplay between technological advancements and the growing sophistication of digital crimes. This overview provides insights into the general features, capabilities, and trends in digital forensic tools as of 2023.

**1. Advanced Data Acquisition [13]:** Modern digital forensic tools have significantly improved in acquiring data from a myriad of digital sources. This includes not only traditional computer systems but also mobile devices, cloud storage, IoT devices, and even social media platforms. The ability to acquire data in a forensically sound manner, ensuring that it remains unaltered during the process, is paramount.

**2. Enhanced Data Analysis Capabilities [14]:** The core of digital forensics lies in the analysis of collected data. Contemporary tools are equipped with sophisticated algorithms to analyse massive volumes of data. They can recover deleted files, decrypt encrypted data, and analyse artifacts from various operating systems. Tools now also include advanced functionalities like timeline analysis, keyword searches, and data carving.

**3. Increasing Emphasis on Mobile and Cloud Forensics [15]:** With the proliferation of smartphones and cloud computing, digital forensic tools have adapted to handle data from these platforms. Mobile forensics involves extracting data from mobile devices, including call logs, messages, and app data. Cloud forensics poses unique challenges due to its distributed nature, necessitating tools that can efficiently access and analyse data stored remotely.

**4. Integration of Artificial Intelligence and Machine Learning [16]:** AI and machine learning have been game-changers, enabling tools to handle larger datasets more efficiently and identify patterns or crucial pieces of evidence that might elude human investigators. These technologies aid in predictive analysis, anomaly detection, and even in automating certain aspects of the investigative process.

**5. User Interface and Experience [17]:** There is a growing emphasis on making forensic tools more user-friendly. Simplified interfaces, comprehensive dashboards, and guided workflows are becoming common, making these tools accessible to a broader range of professionals, including those with limited technical expertise.

**7. Legal and Ethical Compliance [18]:** Digital forensic tools are designed to meet legal standards for evidence gathering. This includes maintaining the integrity of data, ensuring chain of custody, and providing detailed audit trails. Ethical considerations are also paramount, especially regarding privacy concerns and data handling.

**8. Challenges and Adaptability [19]:** Despite advancements, digital forensic tools must continually overcome challenges such as encryption, evolving data formats, and increasing data volumes. The adaptability of these tools to emerging technologies and novel cyber threats is crucial for their effectiveness.

### Conclusion

The current landscape of digital forensic tools is characterized by a blend of sophistication, adaptability, and user-centric design. As digital devices and platforms evolve, so do the tools and

techniques in digital forensics, continually shaping the capabilities and methodologies of investigators in this ever-changing field.

### Introduction to the Comparison of Digital Forensic Tools [20] [21] [22] [23]

In the realm of digital forensics, the choice of tools plays a pivotal role in the success of investigations. This comparison aims to provide a clear perspective on the differences and similarities between widely used open-source and commercial digital forensic tools. The table below compares Autopsy and FTK Imager, representing open-source tools, against Cellebrite and EnCase from the commercial spectrum. The comparison focuses on various critical aspects such as cost, primary use, data imaging, file system support, user interface, data analysis capabilities, legal acceptance, user support, customization, and ideal use cases. This structured overview assists in understanding how each tool aligns with specific forensic needs and scenarios, thereby guiding professionals in selecting the most appropriate tool for their investigative requirements.

| Feature/Criteria           | Autopsy (Open-Source)                                      | FTK Imager (Open-Source)                                 | Cellebrite (Commercial)                                              | EnCase (Commercial)                                                |
|----------------------------|------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------|
| <b>Cost</b>                | Free                                                       | Free                                                     | Paid (Subscription/Purchase)                                         | Paid (Subscription/Purchase)                                       |
| <b>Primary Use</b>         | Comprehensive digital investigations, file system analysis | Data imaging and preview, basic forensic analysis        | Specialized in mobile device forensics, cloud data retrieval         | Broad spectrum digital investigations, court-validated methodology |
| <b>Data Imaging</b>        | Supported                                                  | Advanced Imaging Capabilities                            | Advanced Imaging, specialized for mobile devices                     | Advanced Imaging, supports a variety of digital media              |
| <b>File System Support</b> | Broad Support                                              | Broad Support                                            | Focused on mobile systems, also supports common file systems         | Extensive support for numerous file systems                        |
| <b>User Interface</b>      | User-friendly, GUI-based                                   | Simplified interface with preview capability             | Intuitive, streamlined for mobile forensics                          | Professional, comprehensive forensic interface                     |
| <b>Data Analysis</b>       | In-depth analysis with plug-in integration                 | Basic analysis with preview                              | Deep mobile data analysis, cloud data analysis                       | Comprehensive data recovery and analysis                           |
| <b>Legal Acceptance</b>    | Widely accepted in academic and some legal scenarios       | Suitable for preliminary investigations and academic use | Widely accepted in legal proceedings, especially for mobile evidence | Extensively accepted in legal and law enforcement contexts         |
| <b>User Support</b>        | Community-driven, online forums                            | Community support, limited official guidance             | Professional support and training                                    | Professional support, training, and documentation                  |
| <b>Customization</b>       | High, open to community-driven enhancements                | Limited customization                                    | Limited, focus on specialized, proprietary features                  | Limited, focus on proprietary features and standards               |

|                       |                                                               |                                       |                                                           |                                                          |
|-----------------------|---------------------------------------------------------------|---------------------------------------|-----------------------------------------------------------|----------------------------------------------------------|
| <b>Ideal Use Case</b> | Suitable for educational purposes, small-scale investigations | Preliminary data imaging and analysis | High-stakes, complex mobile investigations, corporate use | Large-scale, complex investigations, law enforcement use |
|-----------------------|---------------------------------------------------------------|---------------------------------------|-----------------------------------------------------------|----------------------------------------------------------|

### Conclusion of Digital Forensic Tools Comparison

The comparison between Autopsy and FTK Imager (open-source) and Cellebrite and EnCase (commercial) highlights significant variations in digital forensic tools, catering to different investigative needs and environments. Open-source tools, characterized by their accessibility and customization, are ideal for educational purposes and smaller-scale investigations. In contrast, commercial tools offer advanced features, professional support, and are often preferred in high-stakes, legally sensitive investigations, especially in corporate and law enforcement contexts. This delineation underscores the importance of choosing the right tool based on specific case requirements, budget constraints, and the desired level of support and sophistication. As digital forensic technology continues to evolve, staying updated with the latest capabilities of these tools remains essential for effective and efficient digital investigations.

## Task 3

### Part 1

#### Scenario- co-operate crime.

An online dating company called Red Hot Passion has received veiled threats that confidential information such as (Payment information, Names, Address, Job positions, Photographs) stored in database documentation as well other communications via text messages emails, videos could be leaked by unknown source.

This information is more so sensitive due to the nature of website that provides a platform for married members to engage in infidelity. This is an invasion on the user's privacy who trusted that website would confidentially retain their information. A lot of the users of the website are work in high positions of importance such as at working fortune 500 companies and working in high-end managerial positions who could be under pressure of firing if this information was leaked as well as effecting their security of their marriages.

It is believed that serval employee/employees of administration staff could have potentially had access to this sensitive information that have left the company within a recent period. These employees could have potentially been disgruntled and could have had reasons to want to take revenge against the company due to previous payment disputes.

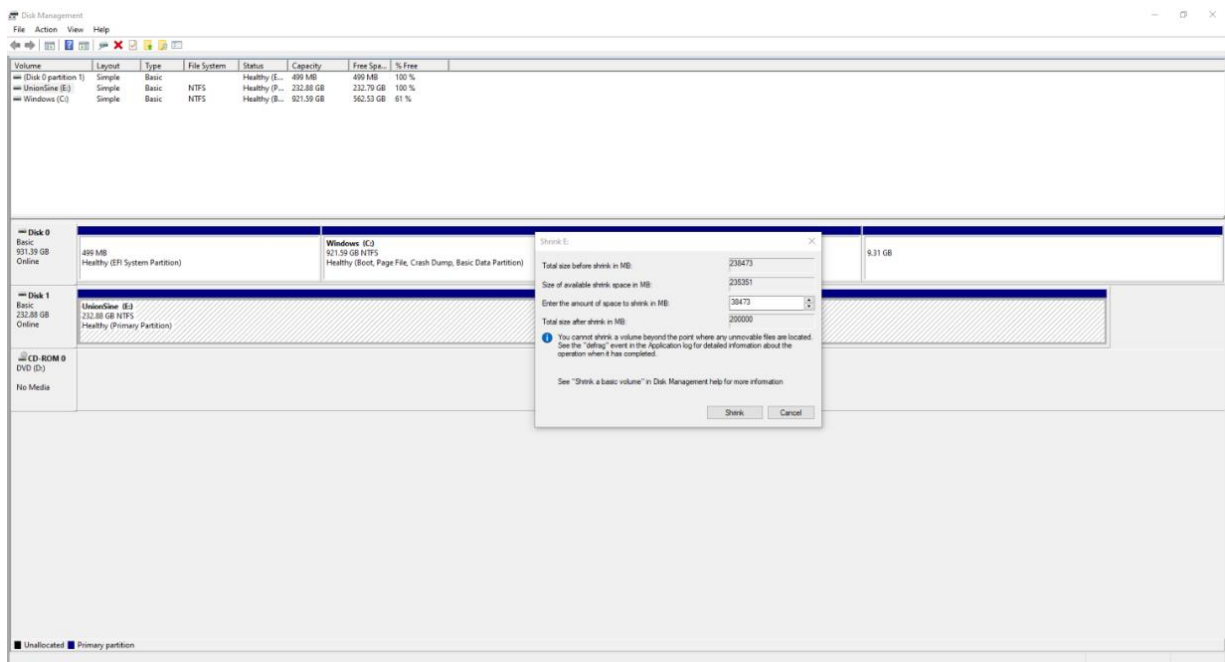
We ask that during your investigation you provide data integrity to ensure that the culprits can be made liable for breach of the companies' data policies and potential cyber terrorism against the company. The integrity of the data is important as this information may need to be used in a trial in the future.

| <u>Group Members</u>               | <u>Designated tasks</u>                                                                                                                                                                             |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rohan Chavan                       | researched ways to hide data, created data and hid within partition. Worked on acquiring data on both phone and hard drive, led a lot of the practical <u>in regards to</u> the collection of data. |
| Thomas Ellis Bennett – Team leader | Guided the team - Collected batch files and added them onto hard drives, helped hide data                                                                                                           |
| Connor Wilson                      | Report writing, helped create partitions and hide data.                                                                                                                                             |
| John Hughes                        | Report writing, helped hide data.                                                                                                                                                                   |
| Lara Costa                         | Report writing, note taking,                                                                                                                                                                        |
| Dawid Trochim – vice team leader   | Took over team guidance when Ellis was not in. Collected data, researched ways to hide data, created data and hid within partition. Led the practical when it came to hiding the data.              |

### Passwords

| <u>Part</u>                          | <u>Password</u>              |
|--------------------------------------|------------------------------|
| 3. <u>veracrypt</u> password         | nitheesh123hseehtin          |
| 7. <u>Bitlocker</u> Drive encryption | <u>youarewastingyourtime</u> |

Accessing and Formatting the HDD: The hard disk drive (HDD), originally formatted in exFAT, was used with a SOAC lab computer. To facilitate the partitioning of its 256GB capacity, it was reformatted to the NTFS file system.



## Collected data- include timestamps- size of data

| File types     | Details                  | size      | Time stamps | Location of data                                          |
|----------------|--------------------------|-----------|-------------|-----------------------------------------------------------|
| Jpg file       | Barclay's bank statement | 432 kb    | 9/1/2020    | Partition I – 37.5 g<br>- Embedded within the MP4 video - |
| Txt file       | bank details             | 706 bytes | 15/1/2020   | Partition I-                                              |
| Mp4 video file | meeting video            | 3.74 mb   | 20/2/2020   | Partition I                                               |
| Sql database   | customer data            | 362 kb    | 1/5/2020    | Partition I                                               |
| Png            | email conversation       | 35 kb     | 7/5/2020    | Partition I                                               |

sample-data.sql

```

1 SET IDENTITY_INSERT Customer ON
2 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(1,'Maria','Anders','Berlin','Germany','030-0074321')
3 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(2,'Ana','Trujillo','México D.F.','Mexico','(5) 555-4729')
4 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(3,'Antonio','Moreno','México D.F.','Mexico','(5) 555-3932')
5 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(4,'Thomas','Hardy','London','UK','(171) 555-7788')
6 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(5,'Christina','Berglund','Luleå','Sweden','0921-12 34 65')
7 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(6,'Hanna','Moos','Mannheim','Germany','0621-08460')
8 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(7,'Frédérique','Citeaux','Strasbourg','France','88.60.15.31')
9 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(8,'Martín','Sommer','Madrid','Spain','(91) 555 22 82')
10 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(9,'Laurence','Lebihan','Marseille','France','91.24.45.40')
11 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(10,'Elizabeth','Lincoln','Tsawassen','Canada','(604) 555-4729')
12 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(11,'Victoria','Ashworth','London','UK','(171) 555-1212')
13 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(12,'Patricio','Simpson','Buenos Aires','Argentina','(1) 135-5555')
14 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(13,'Francisco','Chang','México D.F.','Mexico','(5) 555-3392')
15 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(14,'Yang','Wang','Bern','Switzerland','0452-076545')
16 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(15,'Pedro','Afonso','Sao Paulo','Brazil','(11) 555-7647')
17 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(16,'Elizabeth','Brown','London','UK','(171) 555-2282')
18 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(17,'Sven','Ottlieb','Aachen','Germany','0241-039123')
19 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(18,'Janine','Labrunne','Nantes','France','40.67.88.88')
20 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(19,'Ann','Devon','London','UK','(171) 555-0297')
21 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(20,'Roland','Mendel','Graz','Austria','7675-3425')
22 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(21,'Aria','Cruz','Sao Paulo','Brazil','(11) 555-9857')
23 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(22,'Diego','Roel','Madrid','Spain','(91) 555 94 44')
24 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(23,'Martine','Rancé','Lille','France','20.16.10.16')
25 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(24,'Maria','Larsson','Bräcke','Sweden','0695-34 67 21')
26 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(25,'Peter','Franken','München','Germany','089-0877310')
27 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(26,'Carine','Schmitt','Nantes','France','40.32.21.21')
28 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(27,'Paolo','Accorti','Torino','Italy','011-4988260')
29 INSERT INTO [Customer] ([Id],[FirstName],[LastName],[City],[Country],[Phone])VALUES(28,'Lino','Rodriguez','Lisboa','Portugal','(1) 354-2534')

```

Figure 1 sql Data

| A1 | First Name |           |        |     |            |           |           |             |           |        |                |   |   |   |  |  |
|----|------------|-----------|--------|-----|------------|-----------|-----------|-------------|-----------|--------|----------------|---|---|---|--|--|
|    | A          | B         | C      | D   | E          | F         | G         | H           | I         | J      | K              | L | M | N |  |  |
| 1  | First Name | Last Name | Gender | Age | Email      | Phone     | Education | Occupatio   | Experienc | Salary | Marital Status |   |   |   |  |  |
| 2  | Julian     | Perry     | Male   | 24  | j.perry@r  | 904-1346- | Doctoral  | Actor       | 11        | 74541  | Single         |   |   |   |  |  |
| 3  | Anna       | Spencer   | Female | 18  | a.spencer@ | 991-9321- | Primary   | Singer      | 6         | 185046 | Single         |   |   |   |  |  |
| 4  | Paige      | Chapman   | Female | 19  | p.chapmai  | 210-1185- | Doctoral  | Interprete  | 0         | 140255 | Married        |   |   |   |  |  |
| 5  | Mike       | Clark     | Male   | 18  | m.clark@r  | 882-1972- | Upper sec | Journalist  | 1         | 36225  | Single         |   |   |   |  |  |
| 6  | Steven     | Crawford  | Male   | 26  | s.crawford | 064-0058- | Master    | Medic       | 12        | 164627 | Married        |   |   |   |  |  |
| 7  | Alford     | Payne     | Male   | 30  | a.payne@   | 141-4025- | Doctoral  | Mathemat    | 13        | 185664 | Married        |   |   |   |  |  |
| 8  | Steven     | Cameron   | Male   | 24  | s.cameron  | 726-5409- | Primary   | Carpenter   | 2         | 166508 | Married        |   |   |   |  |  |
| 9  | Roland     | Jones     | Male   | 30  | r.jones@r  | 444-1110- | Lower sec | Social Wor  | 13        | 100688 | Single         |   |   |   |  |  |
| 10 | Aiden      | Barrett   | Male   | 26  | a.barrett@ | 804-8609- | Doctoral  | Engineer    | 10        | 118130 | Married        |   |   |   |  |  |
| 11 | Blake      | Murphy    | Male   | 25  | b.murphy@  | 304-2961- | Primary   | Interprete  | 2         | 38178  | Single         |   |   |   |  |  |
| 12 | Edwin      | Alexander | Male   | 22  | e.alexand  | 054-0614- | Primary   | Composer    | 10        | 185024 | Single         |   |   |   |  |  |
| 13 | Alexander  | Ryan      | Male   | 18  | a.ryan@r   | 562-5095- | Lower sec | Mechanic    | 6         | 109107 | Married        |   |   |   |  |  |
| 14 | Sydney     | Myers     | Female | 26  | s.myers@r  | 088-6209- | Primary   | Manager     | 5         | 184887 | Single         |   |   |   |  |  |
| 15 | Adrianna   | Perry     | Female | 19  | a.perry@r  | 699-1793- | Bachelor  | Carpenter   | 4         | 108099 | Single         |   |   |   |  |  |
| 16 | Clark      | Douglas   | Male   | 21  | c.douglas@ | 374-6085- | Bachelor  | Geologist   | 2         | 138814 | Single         |   |   |   |  |  |
| 17 | Freddie    | Warren    | Male   | 23  | f.warren@  | 757-7789- | Upper sec | Interior De | 1         | 91611  | Married        |   |   |   |  |  |
| 18 | Ada        | Clark     | Female | 27  | a.clark@r  | 224-5309- | Doctoral  | Auditor     | 8         | 93996  | Married        |   |   |   |  |  |
| 19 | Ellia      | Brown     | Female | 23  | e.brown@   | 404-7542- | Bachelor  | Journalist  | 10        | 101923 | Married        |   |   |   |  |  |
| 20 | George     | Cameron   | Male   | 26  | g.cameron  | 747-6685- | Bachelor  | Botanist    | 10        | 36998  | Single         |   |   |   |  |  |
| 21 | George     | Perkins   | Male   | 24  | g.perkins@ | 133-3505- | Doctoral  | Physicist   | 4         | 140457 | Married        |   |   |   |  |  |

Figure 2 Fake data

sample-model.sql

```
1  if exists (select 1|
2  |   from sys.sysreferences r join sys.sysobjects o on (o.id = r.constid and o.type = 'F')
3  |   where r.fkeyid = object_id('\"Order\"') and o.name = 'FK_ORDER_REFERENCE_CUSTOMER')
4  alter table \"Order\"
5  | drop constraint FK_ORDER_REFERENCE_CUSTOMER
6  go
7
8  if exists (select 1
9  |   from sys.sysreferences r join sys.sysobjects o on (o.id = r.constid and o.type = 'F')
10 |   where r.fkeyid = object_id('OrderItem') and o.name = 'FK_ORDERITE_REFERENCE_ORDER')
11 alter table OrderItem
12 | drop constraint FK_ORDERITE_REFERENCE_ORDER
13 go
14
15 if exists (select 1
16 |   from sys.sysreferences r join sys.sysobjects o on (o.id = r.constid and o.type = 'F')
17 |   where r.fkeyid = object_id('OrderItem') and o.name = 'FK_ORDERITE_REFERENCE_PRODUCT')
18 alter table OrderItem
19 | drop constraint FK_ORDERITE_REFERENCE_PRODUCT
20 go
21
```

*Figure 3 Sql Data*

Nitheesh Corporation.txt

```
1  Card Issuer
2  Card Number
3  4634794354869731
4  Full Name
5  Damon Haley
6  CVV
7  327
8  Pin
9  5749
10 Expiration Date
11 12/2027
12
13
14 Card Number
15 348266720430642
16 Full Name
17 Bayley Messner
18 CVV
19 309
```

Partitioning and Data Addition: Six partitions were established on the drive, and one of them was configured as "hidden". A mock spreadsheet, including customer and payment information, was

stored in one of these partitions.

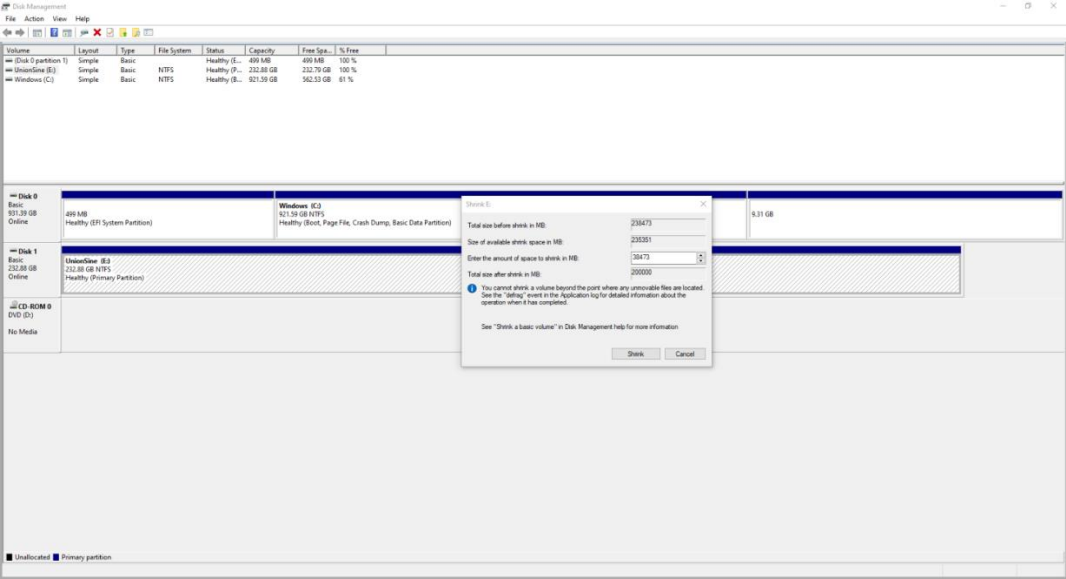


Figure 4 Creating volumes

Password Protection and MD5 Hashing: A unique passphrase was used to secure the partition containing the spreadsheet, and for enhanced security, this passphrase was encrypted using MD5 hashing.

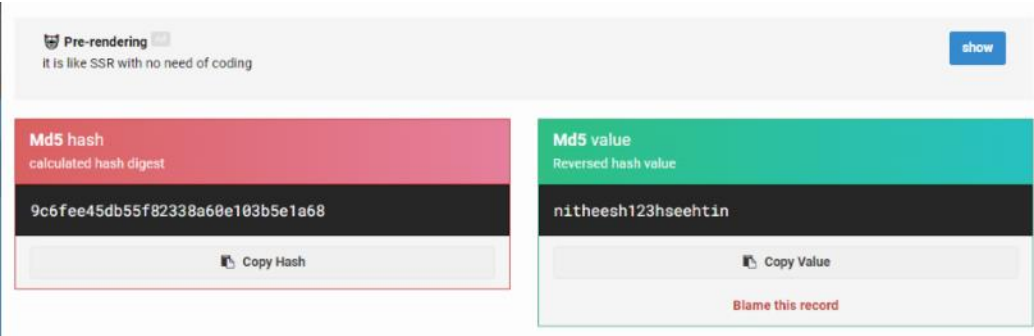
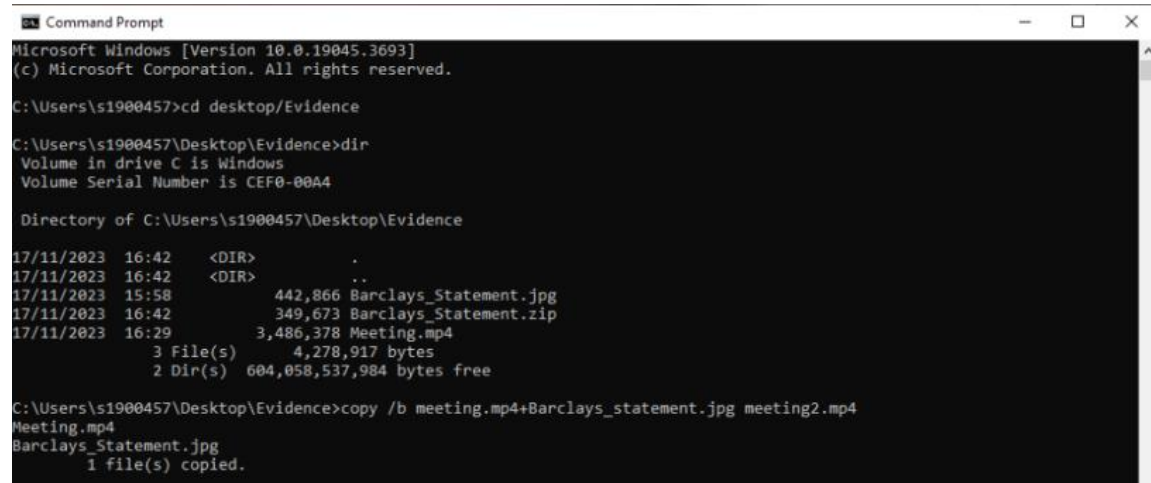


Figure 5 Hashing

Steganography Implementation: To add complexity, steganography techniques were employed. JPEG images containing bank statements were concealed inside MP4 video files using a simple command

line approach on a Windows system.



```
Microsoft Windows [Version 10.0.19045.3693]
(c) Microsoft Corporation. All rights reserved.

C:\Users\s1900457>cd desktop/Evidence

C:\Users\s1900457\Desktop\Evidence>dir
Volume in drive C is Windows
Volume Serial Number is CEF0-00A4

Directory of C:\Users\s1900457\Desktop\Evidence

17/11/2023  16:42    <DIR>          .
17/11/2023  16:42    <DIR>          ..
17/11/2023  15:58             442,866 Barclays_Statement.jpg
17/11/2023  16:42             349,673 Barclays_Statement.zip
17/11/2023  16:29             3,486,378 Meeting.mp4
               3 File(s)              4,278,917 bytes
               2 Dir(s)              604,058,537,984 bytes free

C:\Users\s1900457\Desktop\Evidence>copy /b meeting.mp4+Barclays_statement.jpg meeting2.mp4
Meeting.mp4
Barclays_Statement.jpg
               1 file(s) copied.
```

Figure 6 Steganography

Data Encryption with VeraCrypt: The gathered data was subsequently secured with VeraCrypt encryption, guaranteeing its safety and necessitating decryption expertise for access.

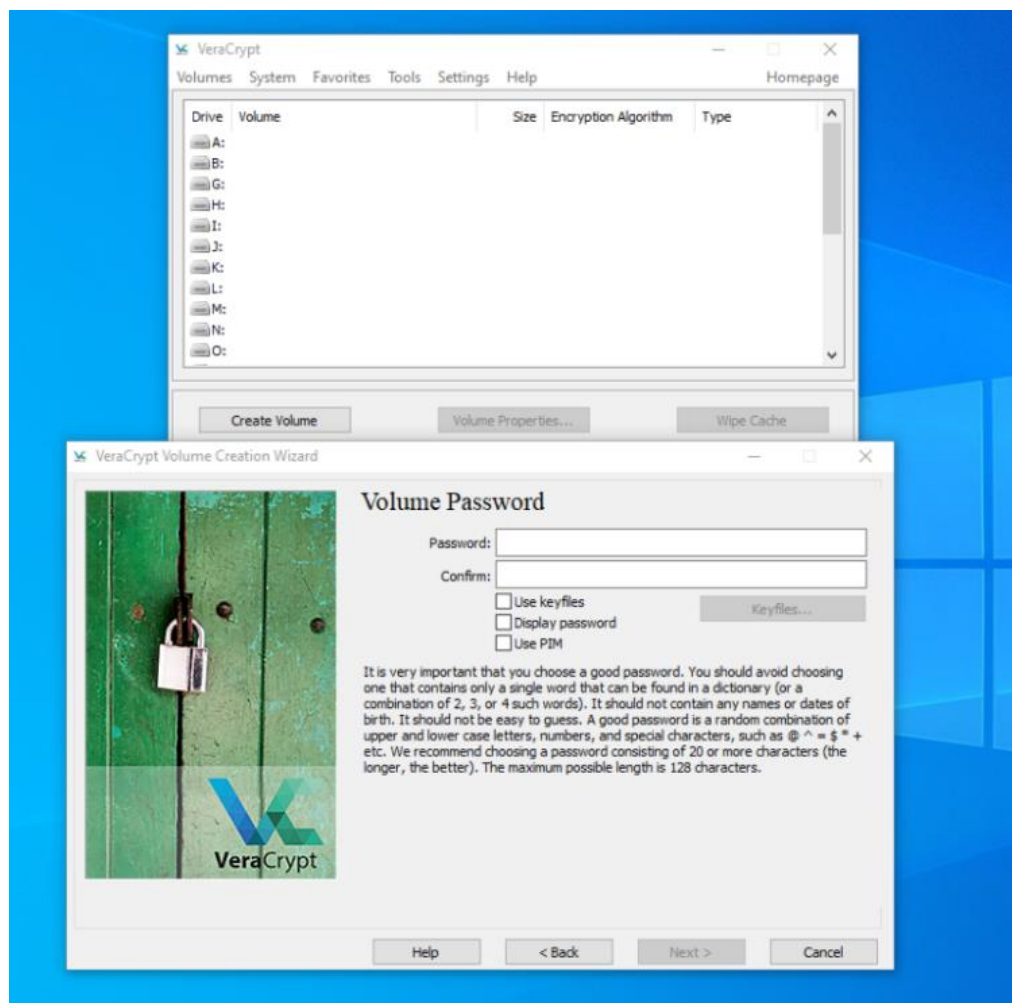


Figure 7 Encrypting the volume

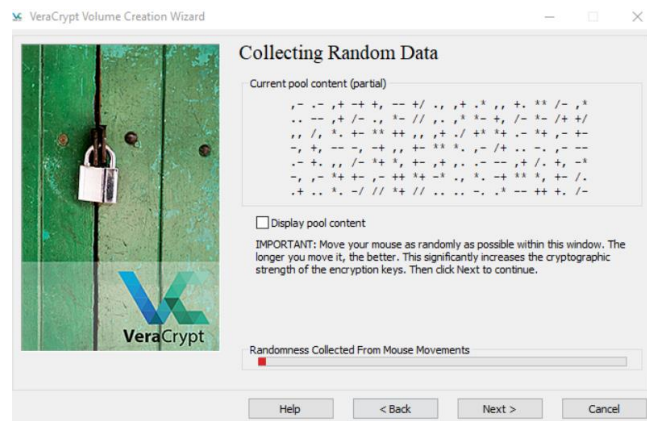


Figure 8 Encrypting the volume

### Batch File Conversion and Testing:

Collected batch files were transformed into executable programs and tested on a Windows Virtual Machine for safety verification prior to being incorporated into the HDD.

| <u>Batch files- mock malware</u>          | <u>What it does</u>                                    | <u>Size</u> | <u>File type</u>           | <u>Method of resolve</u>                                      | <u>Location</u> | <u>Folder</u>          |
|-------------------------------------------|--------------------------------------------------------|-------------|----------------------------|---------------------------------------------------------------|-----------------|------------------------|
| <u>PleaseDon'tOpenMe</u>                  | Inverts mouse clicks                                   | 1kb         | <u>.bat</u><br><u>.exe</u> | Change in settings                                            | Partition E.    | Why are you still here |
| <u>HintsForThePassword</u>                | Gives 50 different hints for the password              | 4kb         | <u>.bat</u><br><u>.exe</u> | No repercussions, the person can just keep clicking cancel.   | Partition E.    | Why are you still here |
| <u>ThisIsVirusDoNotOpenNoPasswordHere</u> | Multiple text messages                                 | 1kb         | <u>.bat</u><br><u>.exe</u> | No repercussions, the person can just keep clicking cancel.   | Partition E     | Why are you still here |
| <u>whywouldressthis</u>                   | Creates multiple tabs which causes the system to crash |             | <u>.bat</u><br><u>.exe</u> | After the system crashes it will load up back to normal after | Partition E     | Why are you still here |

**Disclaimer- Please do not open any of these files in an uncontrolled environment unless you are ready for the results.**

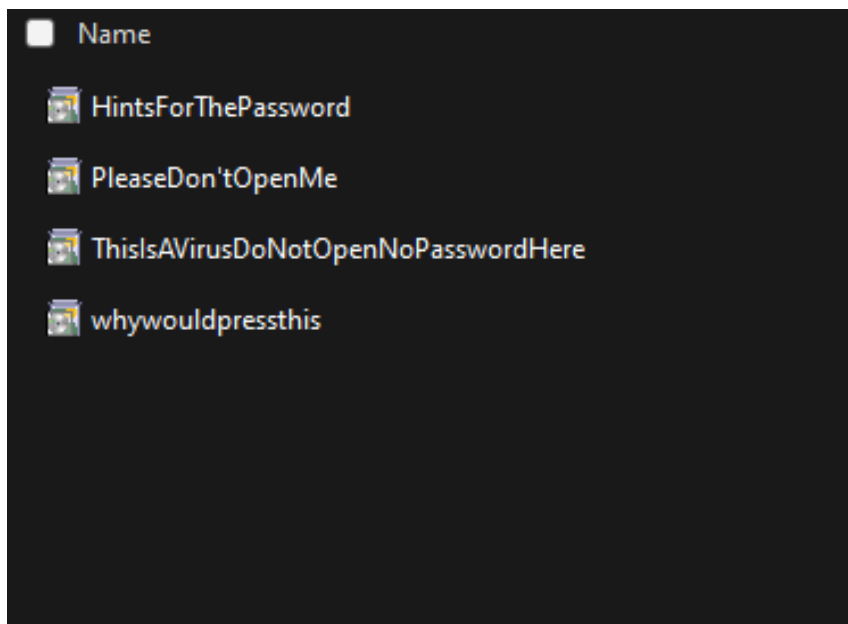


Figure 9 Batfiles

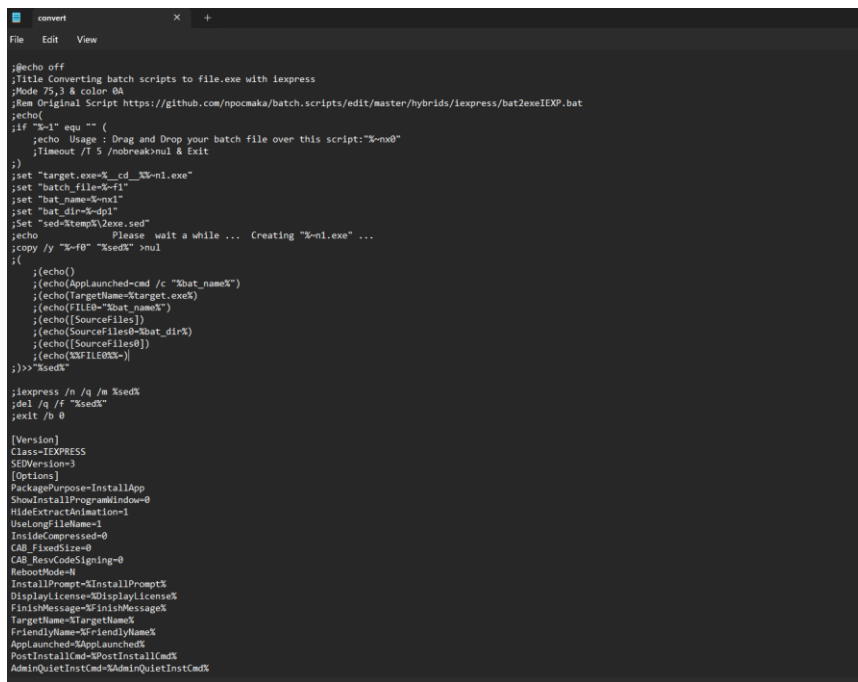


Figure 10 Python Script

Finalization for Handover: Following extensive preparation and testing, the HDD was considered prepared and subsequently handed over to Team B for their analysis.

## Part 2

HDD individual tasks:

Lara costa: Leads the documentation and chain of custody for the HDD, ensuring legal protocols are followed.

John H: Manages the risk assessment for the HDD, detailing hardware risks and

data integrity checks.

Ellis Bennet: Takes charge of the technical aspect of HDD imaging and analysis using FTK Imager and Autopsy Software.

Dawid Trachim : Oversees the decryption process, handling encrypted files and leading the effort to access hidden data.

Connor Wilson: Conducts a detailed examination of file structures and data corruption issues, communicating with other teams for additional context.

Rohan Chavan: Focuses on the analysis of extracted data, decoding hidden messages and encrypted files.

## Risk assessment

### HDD Preparation

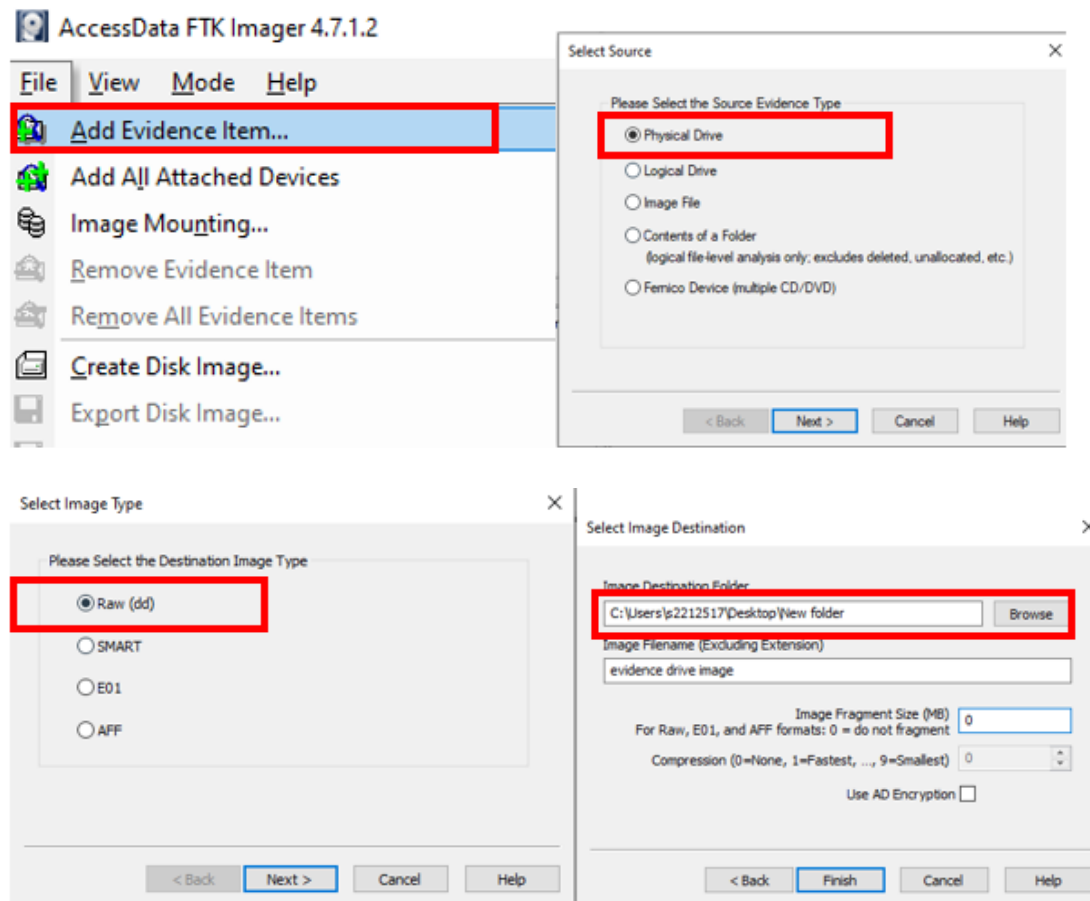
|                                    |                                                                                                                                                                                                                                      |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Chain of Custody</b>            | From point of receipt of HDD to handover to team B, a chain of custody was maintained to prove proper handling, transfer and storage was met                                                                                         |
| <b>Hardware Risks</b>              | Condition of HDD was assessed upon receiving the device, to ensure it was functional, compatible and fit for purpose                                                                                                                 |
| <b>Data Privacy and Compliance</b> | To Ensure that any data used complies with privacy laws and regulations, we ensured that no personally identifiable information was present on the disk. We also ensured that financial data was fictional and not in breach of laws |
| <b>Data Integrity</b>              | To assess risk related to data loss or corruption, we tested its accessibility and ensured the data was retrievable. All data on drive was also backed up                                                                            |
| <b>Ethical Integrity</b>           | Ethical standards were always adhered to, ensuring data and device were appropriate and acceptable                                                                                                                                   |
| <b>Incident Response Plan</b>      | Incident response plan consisting of backing up data, ensuring device functionality                                                                                                                                                  |

### HDD Analysis

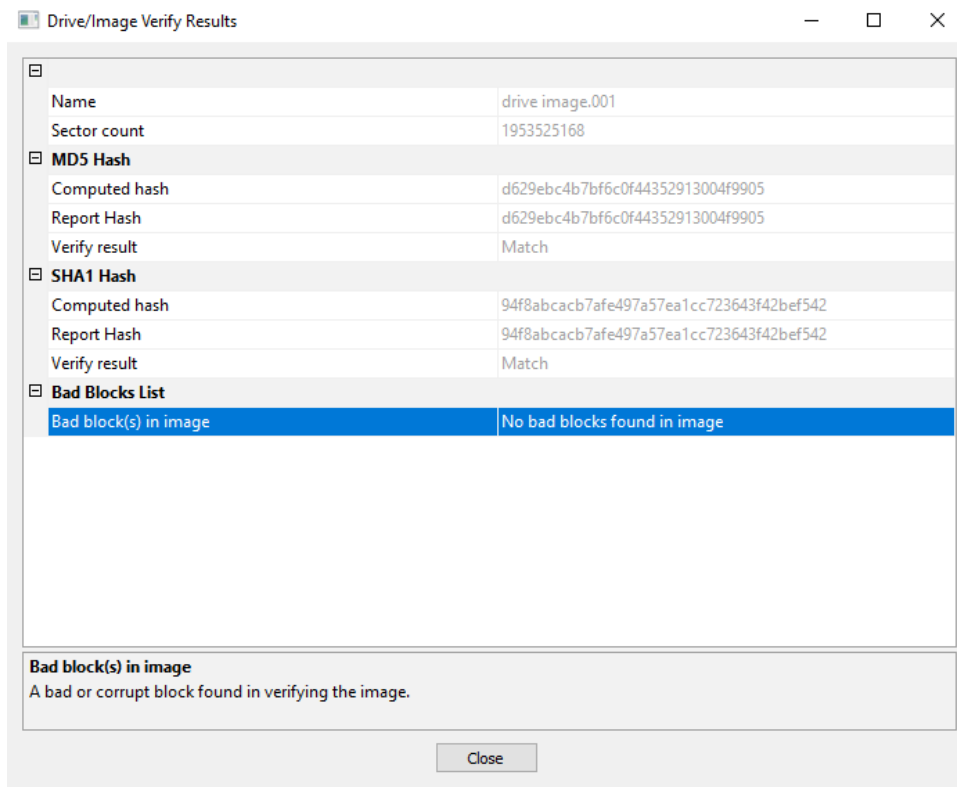
|                               |                                                                                                                                                |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data Integrity</b>         | Use write-blocking tools to prevent data corruption. Use hash values to confirm data integrity                                                 |
| <b>Hardware Damage</b>        | Use safe storage in Faraday case. Adopt correct handling procedures                                                                            |
| <b>Software Risks</b>         | Access data in isolated environment using VM's                                                                                                 |
| <b>Confidentiality Breach</b> | Avoid accessing unnecessary data                                                                                                               |
| <b>Legal Compliance</b>       | Legal requirements are complied with by receiving permission to access data                                                                    |
| <b>Chain of Custody</b>       | From point of receipt from Team C, chain of custody was maintained to prove proper handling, transfer and storage, as well as non-repudiation. |
| <b>Technical Competence</b>   | Ensure all team members understand their roles and responsibilities                                                                            |
| <b>Technical Challenges</b>   | Analyse the file system and format. Be prepared for encrypted data                                                                             |
| <b>Incident Response</b>      | Store disk image backups to prevent data loss. Analyse file types to identify relevant data, avoiding sensitive and unnecessary information    |

### Scenario Summary:

A hacker gains control of a victim's home Wi-Fi network to spy on their online behaviour for personal gain. Initially, the hacker deceives the victim with a phishing email, eventually accessing and misusing their credit card information for financial fraud. The victim, unaware of wireless security risks, becomes an easy target for these hacking activities.

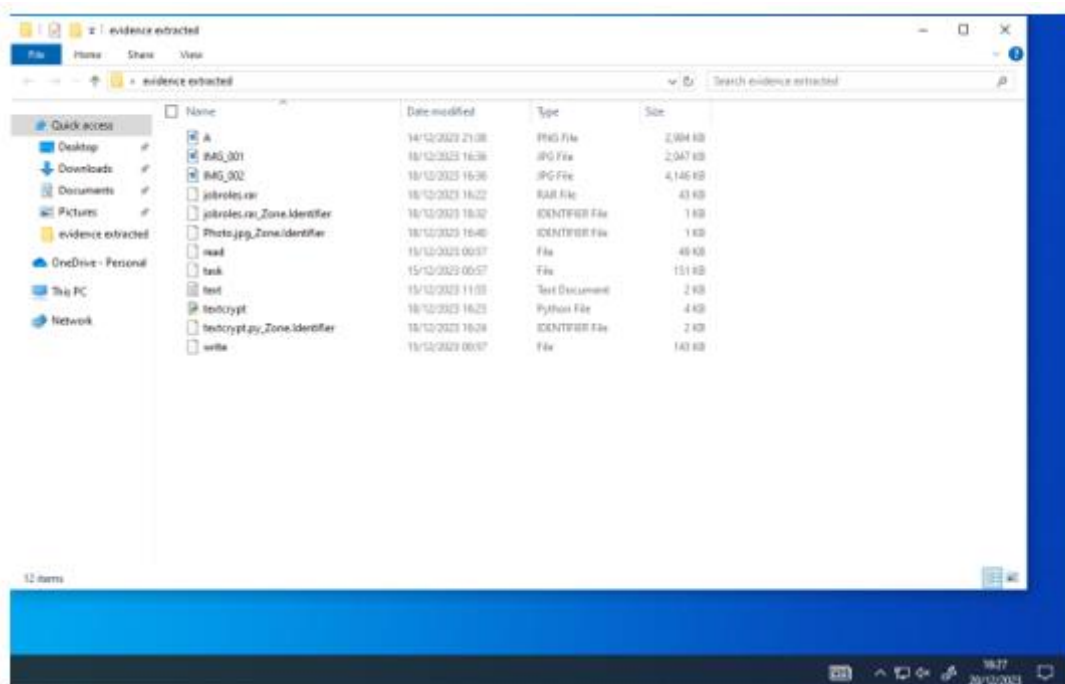


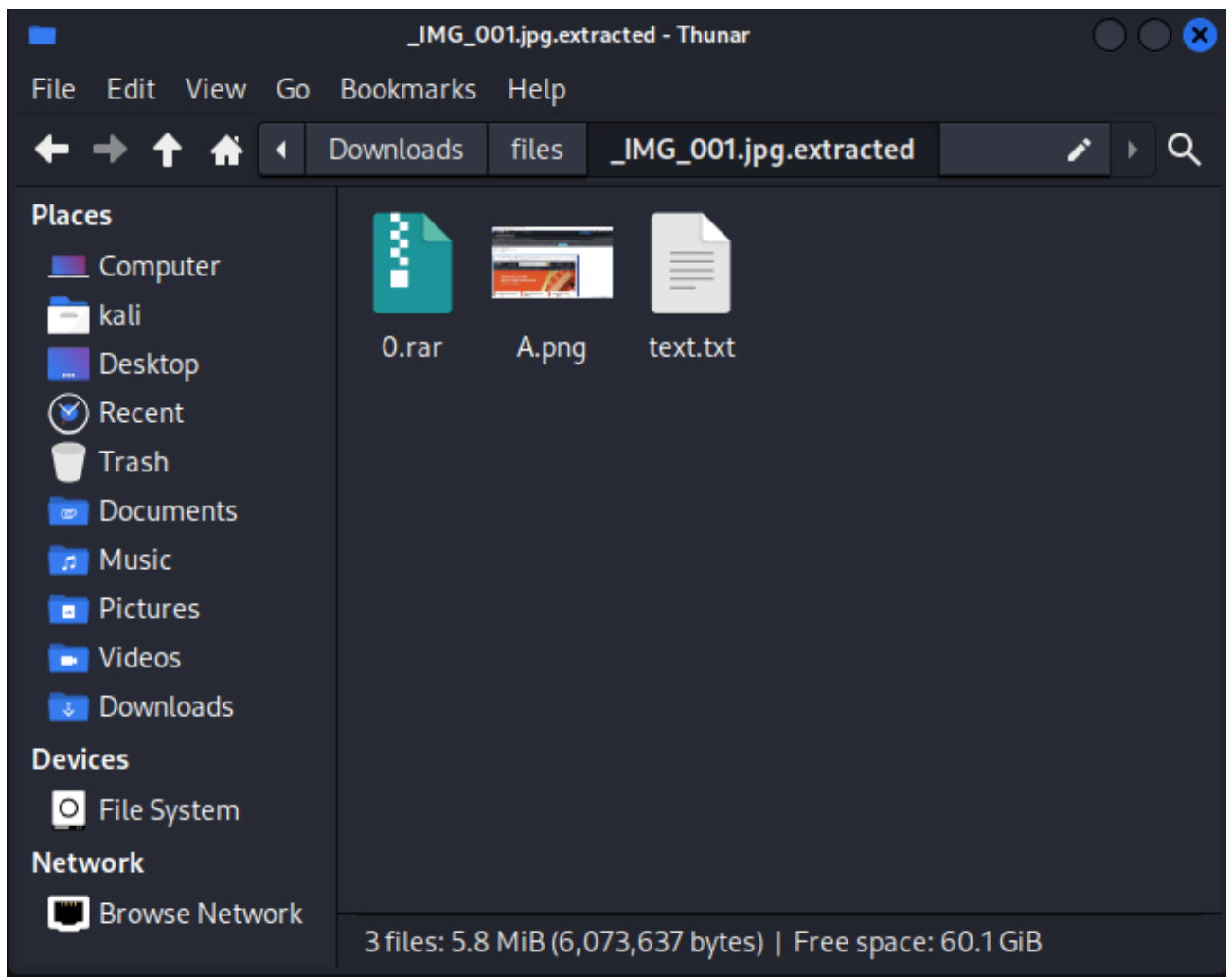
Upon receiving the hard drive we took a physical image of the hard drive using FTK imager in Raw DD format as shows in above figures.



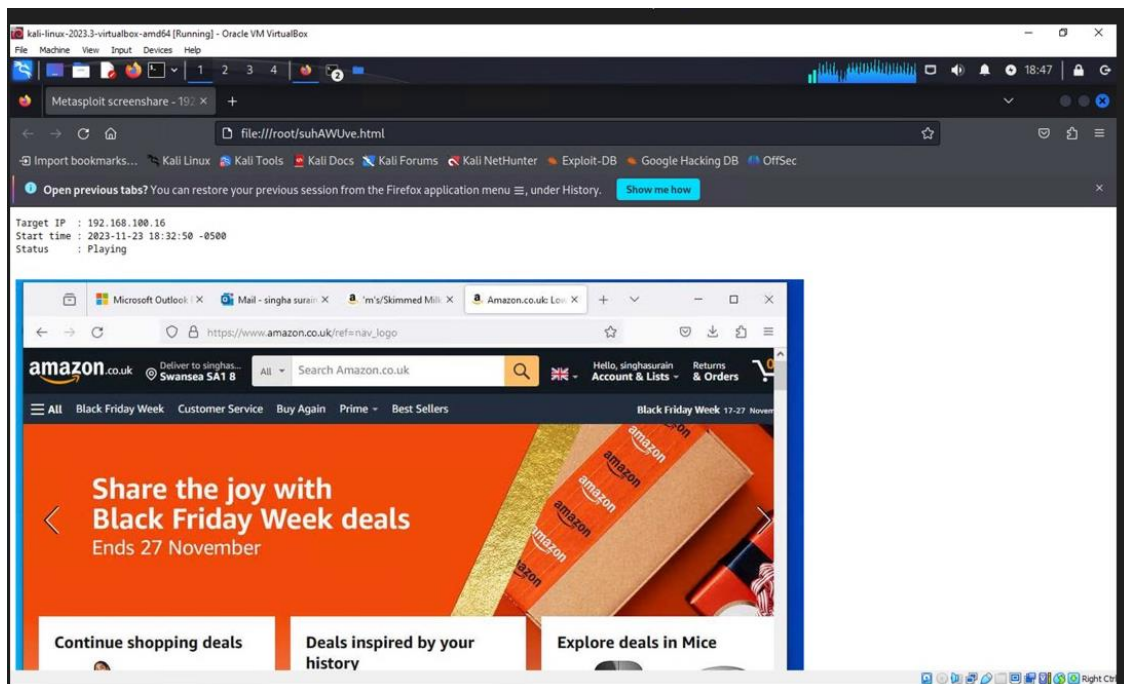
Disk image integrity check was done as shown in above figure.

Extracted Evidence from attacker's machine as show below.





## Conclusion



Above figure indicates that attacker had a successful remote access to victim's device

Presentation on Task 3:

[https://uowtsd-](https://uowtsd-my.sharepoint.com/:v/g/personal/2003893_student_uowtsd_ac_uk/ETi_mT4TeYBKu12o7I3kvSkBL300I5UPVJqKwdfQi5Brzg?e=jIYtMD)

[my.sharepoint.com/:v/g/personal/2003893\\_student\\_uowtsd\\_ac\\_uk/ETi\\_mT4TeYBKu12o7I3kvSkBL300I5UPVJqKwdfQi5Brzg?e=jIYtMD](https://uowtsd-my.sharepoint.com/:v/g/personal/2003893_student_uowtsd_ac_uk/ETi_mT4TeYBKu12o7I3kvSkBL300I5UPVJqKwdfQi5Brzg?e=jIYtMD)

**UWTSO Police Department**  
**EVIDENCE CHAIN OF CUSTODY TRACKING FORM**

Case Number: 01

Offense: Cyber-attacks (phishing email, reverse shell payload)

Submitting Officer: (Name/ID#) Digital forensics group A / 01

Victim: N/A

Suspect: N/A

Date/Time Seized: 6/11/2023

Location of Seizure: University IQ building

| Description of Evidence |          |                                                                    |
|-------------------------|----------|--------------------------------------------------------------------|
| Item #                  | Quantity | Description of Item (Model, Serial #, Condition, Marks, Scratches) |
| 01                      | 01       | 1 TB- External Hard Drive                                          |

| Chain of Custody |            |                                               |                                                                           |                                                                                                              |
|------------------|------------|-----------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Item #           | Date/Time  | Released by (Signature & ID#)                 | Received by (Signature & ID#)                                             | Comments/Location                                                                                            |
| 01               | 6/11/2023  | Digital forensic investigation team B         | Digital forensic investigation team A – Ellis, Rohan, John, Dawid, Connor | Exchange of hard drives                                                                                      |
| 01               | 13/11/2023 | Digital forensic investigation team A- Connor | Digital forensic investigation team A – Ellis, Rohan, John, Dawid, Connor | First official session of the investigation- FTK image was collected – evidence item was                     |
| 01               | 14/11/2023 | Digital forensic investigation team A- Connor | Digital forensic investigation team A – Ellis, Rohan, John, Dawid, Connor | Majority of data found was corrupted. One encrypted file needed to be decrypted using a python and pip code. |

|    |            |                                               |                                                                           |                                              |
|----|------------|-----------------------------------------------|---------------------------------------------------------------------------|----------------------------------------------|
| 01 | 16/11/2023 | Digital forensic investigation team A- Connor | Digital forensic investigation team A – Ellis, Rohan, John, Dawid, Connor | pieces of data were uncovered                |
| 01 | 17/11/2023 | Digital forensic investigation team A- Connor | Digital forensic investigation team A – Ellis, Rohan, John, Dawid, Connor | decryption of data was attempted             |
| 01 | 20/11/2023 | Digital forensic investigation team A- Connor | Digital forensic investigation team A – Ellis, Rohan, John, Dawid, Connor | decryption of data was attempted – continued |
| 01 | 22/11/2023 | Digital forensic investigation team A- Connor | Digital forensic investigation team A – Ellis, Rohan, John, Dawid, Connor | Found data was recorded                      |
| 01 | 23/11/2023 | Digital forensic investigation team A- Connor | Digital forensic investigation team A – Ellis, Rohan, John, Dawid, Connor | Investigation continued                      |
| 01 | 27/11/2023 | Digital forensic investigation team A- Connor | Digital forensic investigation team A – Ellis, Rohan, John, Dawid, Connor | A table was drawn of found data              |
| 01 | 28/11/2023 | Digital forensic investigation team A- Connor | Digital forensic investigation team A – Ellis, Rohan, John, Dawid, Connor | Work was finalized                           |

| Final Disposal Authority                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <b>Authorization for Disposal</b><br>Item(s) #: 01 external hard drive on this document pertaining to (suspect): N/A<br>Is/are no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)<br><input checked="" type="checkbox"/> Return to Owner <input type="checkbox"/> Auction/Destroy/Divert<br>Name & ID# of Authorizing Officer: Digital forensic investigation group A Date: 10/01/2024                                         |  |
| <b>Release to Lawful Owner</b><br>Item(s) #: 01 on this document was/were released by Evidence Custodian digital forensic investigation team A<br>Name Lara Costa<br>Address: University of Wales Trinity Saint David Kings Road, Swansea, West Glamorgan, SA1 8EW<br>Under penalty of law, I certify that I am the lawful owner of the above item(s).<br><br>Copy of Government-Issued photo identification is attached. <input type="checkbox"/> Yes <input type="checkbox"/> No |  |
| This Evidence Chain-of-Custody form is to be retained as a permanent record by the UWTSD Police Department.                                                                                                                                                                                                                                                                                                                                                                        |  |

## Task 4

### UWTSD Police

#### Digital Forensics Department

## EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: 02 Offense: Selling Intellectual Property of Company to Competitors and uninformed national and International Trips

Submitting Officer: (Name/ID#) Team A

Victim: Confidential Suspect: Undisclosed

Date/Time Seized: Device1: 27/11/2023 & Device2: 11/12/2023.

Location of Seizure: 205 IQ Swansea

| Description of Evidence |          |                                                                             |
|-------------------------|----------|-----------------------------------------------------------------------------|
| Item #                  | Quantity | Description of Item (Model, Serial #, Condition, Marks, Scratches)          |
| 1                       | 1        | Huawei POT-LX1 P Smart, usual wear and tear, no major scratches, or damages |
| 2                       | 1        | Ulefone Note 14, usual wear and tear, no major scratches, or damages        |

| Chain of Custody |            |                    |                    |                                                                                                                                                                                                                                                                                                                                        |
|------------------|------------|--------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item #           | Date/Time  | Released by (Name) | Received by (Name) | Comments/Location                                                                                                                                                                                                                                                                                                                      |
| 1                | 27/11/2023 | Niteesh            | John               | Phone was collected.<br>205, UWTSD, IQ Swansea                                                                                                                                                                                                                                                                                         |
| 1                | 01/12/2023 | John               | Connnor            | phone was kept in Connor's accommodation.<br>205, UWTSD, IQ Swansea                                                                                                                                                                                                                                                                    |
| 1                | 04/12/2023 | Connor             | Ellis              | Today we attempted to guess the password.<br>The phone was transported to the university and was brought to room 205<br>205, UWTSD, IQ Swansea                                                                                                                                                                                         |
| 1                | 04/12/2023 | Ellis              | Nitheesh           | Phone was given to Niteesh to check the passcode.<br>205, UWTSD, IQ Swansea                                                                                                                                                                                                                                                            |
| 1                | 04/12/2023 | Nitheesh           | Rohan              | The phone was connected to the Cellebrite kit and reset. When the phone was reset, it remained in a bootloop and was unable to be unlocked.<br>However the software said the phone is not supported. The device was also subjected to an attempted eRecovery to no success, the device remained in bootloop.<br>205, UWTSD, IQ Swansea |

|   |            |       |         |                                                                                                                                                                                                                                                                  |
|---|------------|-------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | 04/12/2023 | Rohan | Ellis   | The device was reset due to the malfunction and no data was able to be recovered. There was also no sim card available so there would haven't not been much data to recover. All data that was able to be recovered was all bloatware.<br>205, UWTSD, IQ Swansea |
| 1 | 08/12/2023 | Ellis | Niteesh | The phone was handed back as we were not able to recover the relevant data due to limitation of the device.<br>205, UWTSD, IQ Swansea                                                                                                                            |

## EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM

(Continued)

| Chain of Custody |            |                                      |                                            |                                                                                                                                   |
|------------------|------------|--------------------------------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Item #           | Date/Time  | Released by (Name)                   | Received by (Name)                         | Comments/Location                                                                                                                 |
| 2                | 11/12/2023 | Team B                               | John and Connor                            | An extraction process was started and accomplished.<br>205, UWTSD, IQ Swansea                                                     |
| 2                | 15/12/2023 | John and Connor                      | Rohan, Connor, Ellis, Lara                 | Data was uncovered using Cellebrite. This showed prove of travel to India, Dubai, Poland and UK London.<br>205, UWTSD, IQ Swansea |
| 2                | 20/12/2023 | Rohan, Connor, Ellis, Lara           | Rohan, Connor, Ellis, John, Lara and Dawid | Images, Videos and Audios were retrieved and analyzed.<br>205, UWTSD, IQ Swansea                                                  |
| 2                | 21/12/2023 | Rohan, Connor, Ellis, Lara and Dawid | Team B                                     | Mobile was handed to team B for their investigation.<br>205, UWTSD, IQ Swansea                                                    |

| Final Disposal Authority                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Authorization for Disposal</b></p> <p>Item(1) #: <u>Huawei POT-LX1 P Smart</u> on this document pertaining to (suspect): <u>N/A</u><br/> is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)</p> <p> <input checked="" type="checkbox"/> Return to Owner (Nitheesh)      <input checked="" type="checkbox"/> Auction/Destroy/Divert </p> <p>Name &amp; ID# of Authorizing Officer: <u>INVESTIGATION Team A</u> Signature: <u>Team A</u> Date: <u>08/12/2023</u></p> |

### Authorization for Disposal

Item(2) #: Ulefone Note 14 on this document pertaining to (suspect):N/A  
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☒ Return to Owner (Team B)      ☒ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: INVESTIGATION Team A Signature: Team A Date: 21/12/2023

**This Evidence Chain-of-Custody form is to be retained as a permanent record by the UWTSD Police Department.**

### Investigation Team

|                    |               |
|--------------------|---------------|
| <b>Team leader</b> | Ellis Thomas  |
| <b>Member</b>      | Lara Costa    |
| <b>Member</b>      | John Hughes   |
| <b>Member</b>      | Dawid Trochim |
| <b>Member</b>      | Connor Wilson |
| <b>Member</b>      | Rohan Chavan  |

### Team Discussions: Strategy and Collaboration

The team convened to strategize the investigation of the Technical Officer's mobile phone, ensuring clarity in roles and adherence to legal protocols.

**Dawid Trachim:** Took initial responsibility, meticulously documenting the phone's chain of custody – a crucial step for maintaining the investigation's integrity.

**Lara Costa:** Conducted a thorough examination of the phone's hardware, checking for any anomalies or tampering signs.

**John Hughes:** Scrutinized the installed applications for irregularities, seeking indicators of unauthorized information transfer.

**Ellis Bennett:** Utilizing tools like Cellebrite, focused on extracting hidden or deleted data, potentially crucial for the investigation.

**Connor Wilson:** Meticulously combed through call logs, texts, and contacts, searching for suspicious communications,

**Rohan Chavan:** analysed geolocation data from photos and other digital traces to reconstruct the TO's movements.

Each team member's unique expertise was pivotal, forming a cohesive unit that enhanced the investigation's effectiveness. This collaborative approach was essential in piecing together the mobile phone's digital story, vital for uncovering the truth behind the TO's activities.

## Risk assessment phone One

| <u>scenario</u>                                                                                   | <u>Risk</u> | <u>Mitigation methods used</u>                                                                                                                                                            | <u>Severity of risk</u> | <u>Did it occur?</u> | <u>Did the mitigation methods work</u> |
|---------------------------------------------------------------------------------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|----------------------|----------------------------------------|
| May be unable to get into the phone due to password lock                                          | 10          | Guessing password                                                                                                                                                                         | 5                       | yes                  | Yes                                    |
| Phone was in a state of <u>bootloop</u> after being connected to <u>celebrite</u> and being reset | 10          | For this case there are two possible routes, <u>One</u> is make use of <u>Hisuite</u> tool software to get device out of boot loop.<br><br>The other is to make use of <u>eRecovery</u> . | 10                      | yes                  | No                                     |
| No Sim Card was found                                                                             | 10          | (No possible mitigation methods)                                                                                                                                                          | 1                       | Yes                  | -                                      |
| Tampering and alterations                                                                         | 7           | By using the Cellebrite kit, little to no tampering of the original evidence item is needed.                                                                                              | 7                       | No                   | Yes                                    |

## Risk assessment phone Two

| <u>scenario</u>                                                                                                                                                                                                         | <u>Risk</u> | <u>Mitigation methods used</u>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <u>Severity of risk</u> | <u>Did it occur?</u> | <u>Did the mitigation methods work</u> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|----------------------|----------------------------------------|
| We suspect that there are potentially <u>whatsapp</u> and email conversations present on the phone, but to access <u>them</u><br><br>second scenario- directly view on phone which may compromise data <u>integrity</u> | 10          | One scenario is that we could take an image of the phone and analyse it. This would be done using autopsy, which will show emails, however, may not be possible to uncover WhatsApp messages. For this we would have to route the phone which would result in possible corruption of the phone. <u>Logical</u> extraction, did not extract all needed data.<br><br>second scenario is that we would directly view on phone and uncover the data this way, which may compromise data integrity. It is legal to have a manual extraction in some cases. | 10                      | -                    | Scenario one was chosen.               |

## Initial Device One Assessment:

The initial examination of the Ulefone Note 14, conducted on 04/12/2023, revealed crucial aspects about its physical and software state. The phone was found powered off, without a SIM card, and displayed signs of regular usage with no significant physical damage. Upon powering up, it was discovered that the device, running on Android OS, was secured with a 6-digit passcode. Our team successfully deduced the passcode as 122024. However, an attempt to create a mobile image using the Cellebrite tool led to the phone entering a bootloop state, posing a significant challenge in the data extraction process.



## Extraction Report - Google Android Generic

### Summary

|                                      |                                                                |
|--------------------------------------|----------------------------------------------------------------|
| Cellebrite Physical Analyzer version | 7.60.1.9                                                       |
| Report creation time                 | 08/12/2023 17:52:17 +00:00                                     |
| Time zone settings (UTC)             | Original UTC value                                             |
| Examiner name                        | John Hughes                                                    |
| Location                             | SOAC Lab                                                       |
| Case number                          | 001                                                            |
| Case name                            | Huawei Factory Reset                                           |
| Evidence number                      | 1                                                              |
| Department                           | Forensics                                                      |
| Organization                         | Team A                                                         |
| Investigator                         | N/A                                                            |
| Crime type                           | N/A                                                            |
| Notes                                | Phone was stuck in endless loop. Factory reset and taken image |

### Source Extraction

|                                      |                                      |
|--------------------------------------|--------------------------------------|
| <b>File System</b>                   |                                      |
| Extraction start date/time           | 08/12/2023 17:30:26                  |
| Extraction end date/time             | 08/12/2023 17:35:52                  |
| Unit identifier                      | 2001539118                           |
| UFED version                         | 7.62.0.173                           |
| Internal version                     | 7.62.0.173                           |
| Selected manufacturer                | HUAWEI                               |
| Selected device name                 | POT-LX1                              |
| Machine name                         | SC-IQ205-29                          |
| Extraction type                      | File System [ Android ADB ]          |
| Extraction ID                        | 93E8A9A4-81CA-4D2E-BCE2-3AA7E170B25E |
| Extraction (UFD) file data integrity | Intact                               |

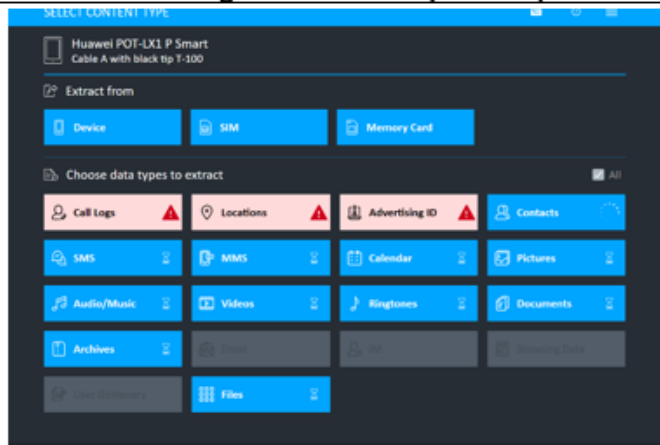
### Device Information

| Name                      | Value                                |
|---------------------------|--------------------------------------|
| <b>File System</b>        |                                      |
| Chipset                   | kirin710                             |
| Model                     | POT-LX1                              |
| OS                        | Android 10                           |
| OS Version                | Android 10                           |
| SecurityPatchLevel        | 2020-08-01                           |
| Vendor                    | HUAWEI                               |
| Bluetooth device name     | HUAWEI P smart 2019                  |
| Android ID                | 4e2147b661afad7a                     |
| Bluetooth device address  | BC:2E:F6:B3:27:5E                    |
| Mock locations allowed    | False                                |
| Location Services Enabled | True                                 |
| Advertising ID #1         | b5868257-6cae-4d08-a559-ada62e380d11 |
| <b>Tethering</b>          |                                      |
| Hotspot AP Name           | HUAWEI P smart 2019                  |
| Hotspot password required | 66cbba150422                         |

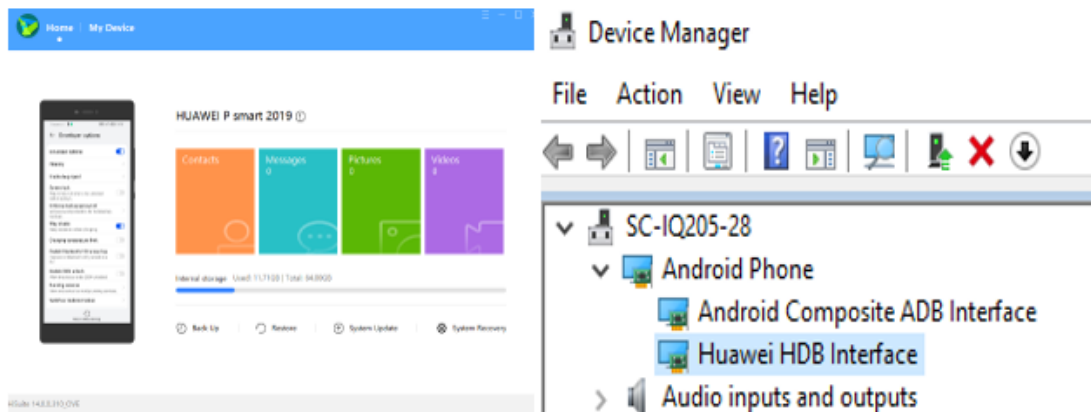
## Identification of Challenges and Strategies:

The primary obstacle encountered was the device's bootloop issue during the Cellebrite extraction attempt. To halt the bootloop, a factory reset was necessary, which unfortunately resulted in data loss. This outcome presented a considerable setback, as the phone was no longer recognized in disk management systems, rendering it undetectable by various data recovery software. Our team explored multiple recovery options, but the inability of the device to connect post-reset posed a significant barrier. This incident underscores the delicate nature of digital forensics, where data extraction attempts can sometimes lead to unforeseen complications, necessitating careful risk assessment and contingency planning in future investigative strategies.

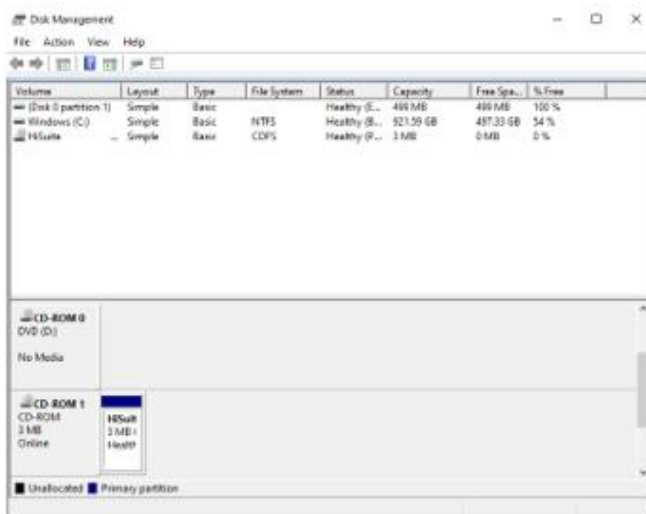
### Documentation of investigation of Mobile phone 1 (Huawei POT-LX1 P Smart):



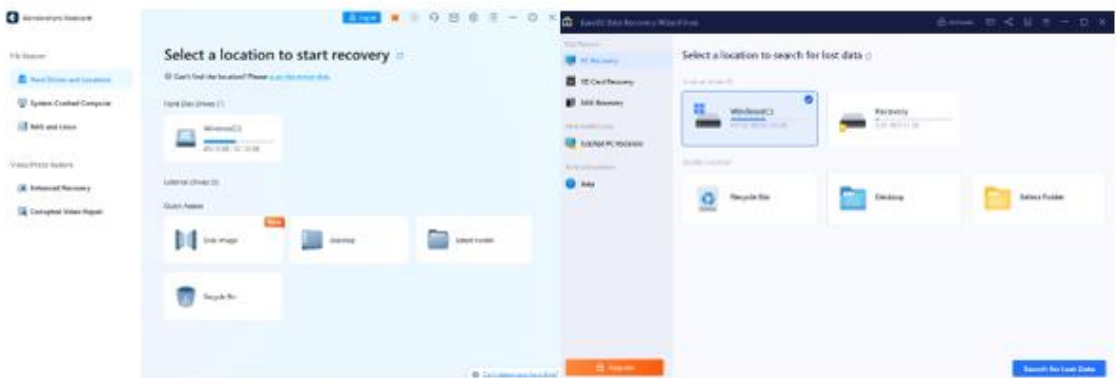
(before phone was factory reset, the process of obtaining data was failing)



(Detection on Huawei software and device manager)



(Device not detected on disk management)



(Device not detected in both EaseUS or Wondershare)

### Initial Device Two Assessment:

During the preliminary examination of the Ulefone Note 14 on 14/12/2023, it was noted that the device operated on an Android OS and was secured by a 4-digit passcode (1224). The physical inspection of the device revealed no apparent damage. For extracting data, forensic tools such as Cellebrite and Autopsy were utilized in the assessment. Screen has a few scratches. Besides that, it is as new. The phone comes in a purple colour.

| Phone Examination Preview Report Properties                                           |                                                               |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Selected Manufacturer:                                                                | Detected Model                                                |
| Selected Model:                                                                       | Note 14                                                       |
| Detected Manufacturer:                                                                | Ulefone                                                       |
| Detected Model:                                                                       | Note 14                                                       |
| Revision:                                                                             | 12 SP1A.210812.016 1679135682                                 |
| IMEI:                                                                                 | 355617730545771                                               |
| MSISDN:                                                                               | 918778244595                                                  |
| Advertising ID:                                                                       | 0a24f44d-5908-42bd-a7cb-f7e37ea3aad5                          |
| Extraction start date/time:                                                           | 14/12/2023 18:09:37 (GMT)                                     |
| Extraction end date/time:                                                             | 14/12/2023 18:15:39 (GMT)                                     |
| Phone Date/Time:                                                                      | 14/12/2023 18:11:14 (GMT)                                     |
| Connection Type:                                                                      | USB Cable                                                     |
| UFED Version:                                                                         | Product Version: 7.62.0.173 , Internal Build: 7.62.0.173 UFED |
| UFED S/N:                                                                             | 2001539118                                                    |
| License for educational purposes                                                      |                                                               |
| Note: This device is using client in order to communicate with UFED                   |                                                               |
| For complete analysis and advanced reporting, open in UFED Physical/Logical Analyzer. |                                                               |

Figure 11 Examination Report

## Analysis and Examination of Data of Phone 2

In the comprehensive analysis of the mobile device, utilizing Cellebrite, several critical pieces of evidence were uncovered, substantiating the initial suspicions regarding unauthorized travels and activities.

| Phone Examination Preview Report Properties                                           |                                                               |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Selected Manufacturer:                                                                | Detected Model                                                |
| Detected Model:                                                                       | Note 14                                                       |
| Detected Manufacturer:                                                                | Ulefone                                                       |
| Detected Model:                                                                       | Note 14                                                       |
| Revision:                                                                             | 12 SP1A.210812.016 1679135682                                 |
| IMEI:                                                                                 | 355617730545771                                               |
| MSISDN:                                                                               | 918778244595                                                  |
| Advertising ID:                                                                       | 0a24f44d-5908-42bd-a7cb-f7e37ea3aad5                          |
| Phone Date/Time:                                                                      | 14/12/2023 18:11:14 (GMT)                                     |
| Connection Type:                                                                      | USB Cable                                                     |
| UFED Version:                                                                         | Product Version: 7.62.0.173 , Internal Build: 7.62.0.173 UFED |
| UFED S/N:                                                                             | 2001539118                                                    |
| License for educational purposes                                                      |                                                               |
| Note: This device is using client in order to communicate with UFED                   |                                                               |
| For complete analysis and advanced reporting, open in UFED Physical/Logical Analyzer. |                                                               |

| Location |                                                                                                                                                                                              |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| #        | Name                                                                                                                                                                                         |
| 1        | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 2        | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 3        | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 4        | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 5        | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 6        | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 7        | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 8        | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 9        | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 10       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 11       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 12       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 13       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 14       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 15       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 16       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 17       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 18       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 19       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 20       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 21       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 22       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 23       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 24       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 25       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 26       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |
| 27       | C:\Users\j21517\Desktop\mobile\20\image\UFED\20\Detected\%20Model\%20Note\%2014\%202023_12_14\%200001\AdvancedLogical\%2001\Detected\%20Model_Note\%2014\logical\Report_LocationSection.html |

Figure 12 Data found on mobile

## Photo Analysis:

The retrieval of multiple photographs from the device was pivotal. According to the Cellebrite report, these images, complete with timestamps and geolocation data, indicated that the device owner had undertaken several trips, both domestically and internationally. This was evident from the documented images showing the use of various transportation modes, including trains and airports. Specific images of a Visa card and a screenshot displaying weather and Wi-Fi information, the latter commonly used in train services, further corroborated the travel evidence. These photos provided concrete proof of travel to destinations like India, Dubai, Poland, and London, UK.

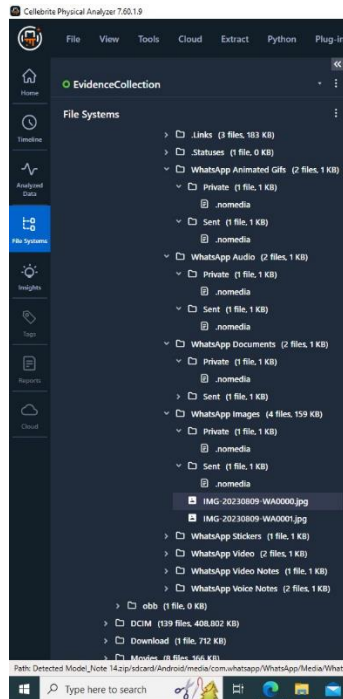


Figure 13 Data in mobile

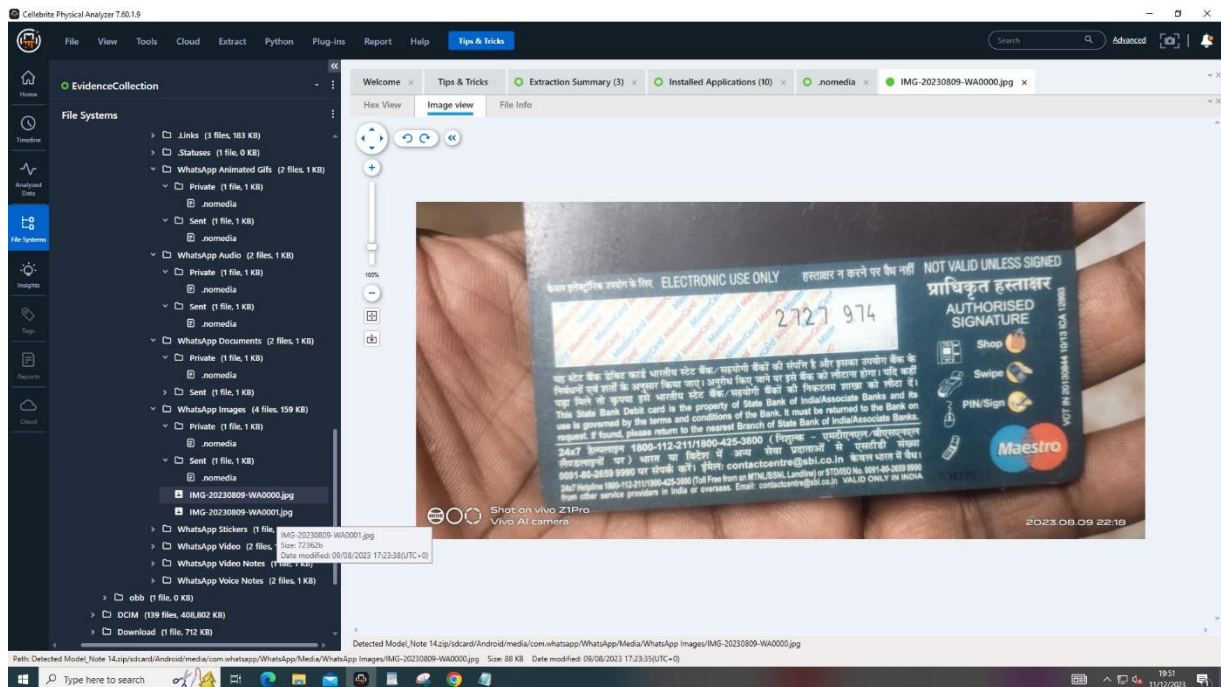


Figure 14 cvv of a Debit/credit card

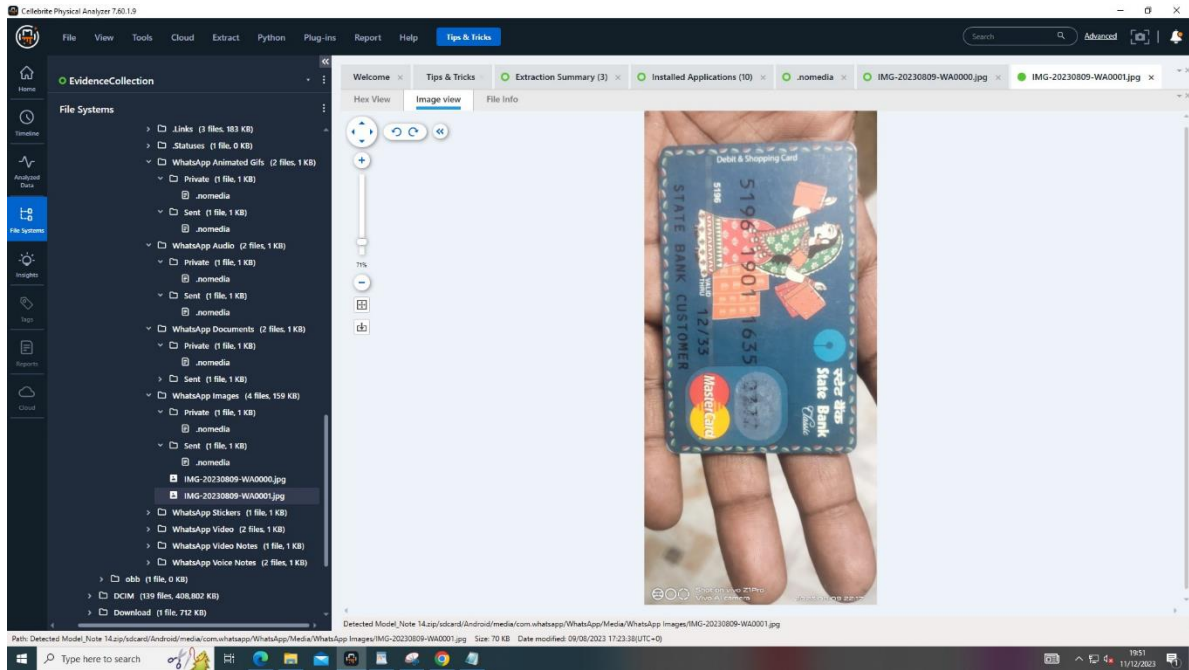


Figure 15 Card details

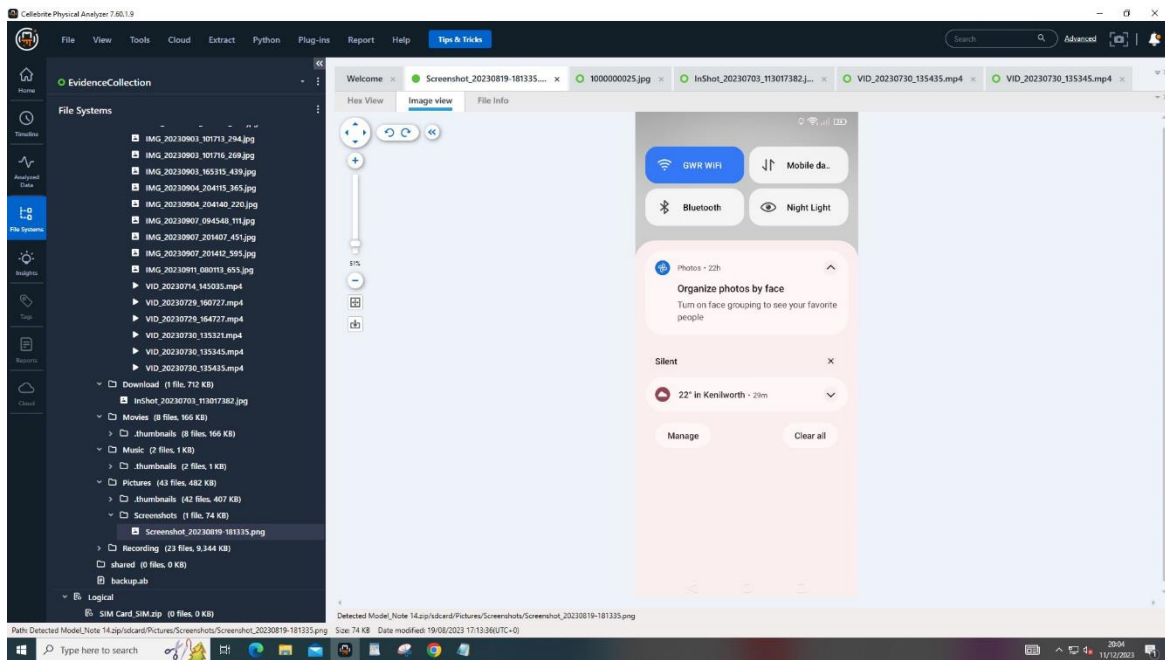


Figure 16 wifi connection screenshot

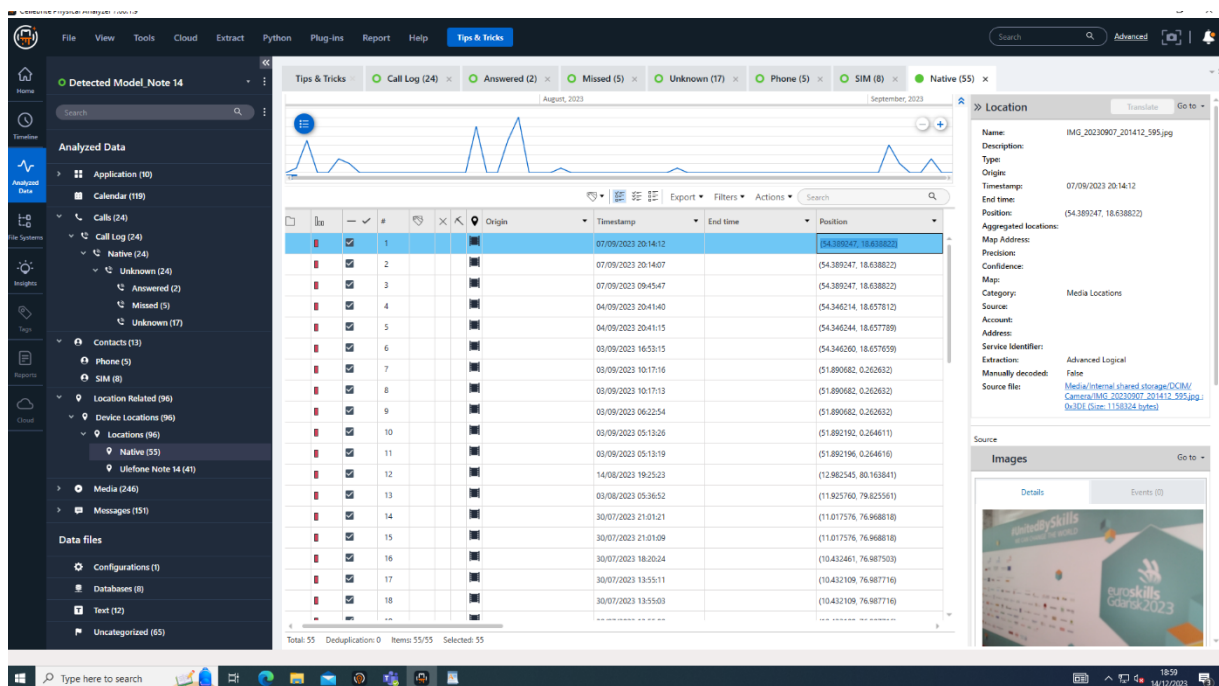


Figure 17 Images found on mobile with locations and date

## File System Exploration:

Investigating the main file system for logical backups led to the discovery of a WhatsApp folder structure in the SD card media folder. However, the files were encrypted due to WhatsApp's security protocols. Despite this, two significant images were found in a separate folder, enhancing the evidence pool.

## Call Log Analysis:

The examination of call logs revealed connections with phone numbers associated with an Indian service provider. This finding suggests that an Indian SIM card was utilized on the mobile device, further indicating international communications and possible connections in India.

## Audio File Analysis:

The analysis of various audio files provided substantial insights into the movements and activities of the individual. The audio recordings included announcements and conversations that revealed travel to Chennai, Abu Dhabi, and London, and the use of different transportation methods like trains, coaches, and flights. Notably, specific recordings captured announcements on a London tube, with mentions of Bond Street and Paddington station, and a train journey towards Swansea. These audio files enriched the investigation by offering chronological and locational evidence of the individual's travels.

## Audio Analysis

| Audio file name | Description                                                   |
|-----------------|---------------------------------------------------------------|
| 202230709210610 | it mentions that person has taken a flight to Chennai (India) |
| 20230717181657  | person in train location unknown                              |
| 20230814202312  | flight to Abu Dabi announcement                               |
| 20230814215741  | emirates flight to London                                     |
| 20230815100753  | taken a coach, location unknown                               |
| 20230818155949  | taken <del>gwr</del> location unknown                         |
| 20230903102023  | on flight announcement, location unknown                      |
| 20230911103719  | on London tube, bond street                                   |
| 20230911103753  | on London tube, next Paddington station                       |
| 20230911105232  | train to Swansea                                              |
| 20230911105253  | train to Swansea                                              |

This meticulous examination of data from the mobile device, facilitated by advanced forensic tools, has unveiled significant evidence pointing to extensive and potentially unauthorized travel activities of the individual under investigation. The integration of photo, call log, and audio analyses paints a comprehensive picture of the device owner's movements and actions, vital for the ongoing investigation.

## Final Assessment of Investigation

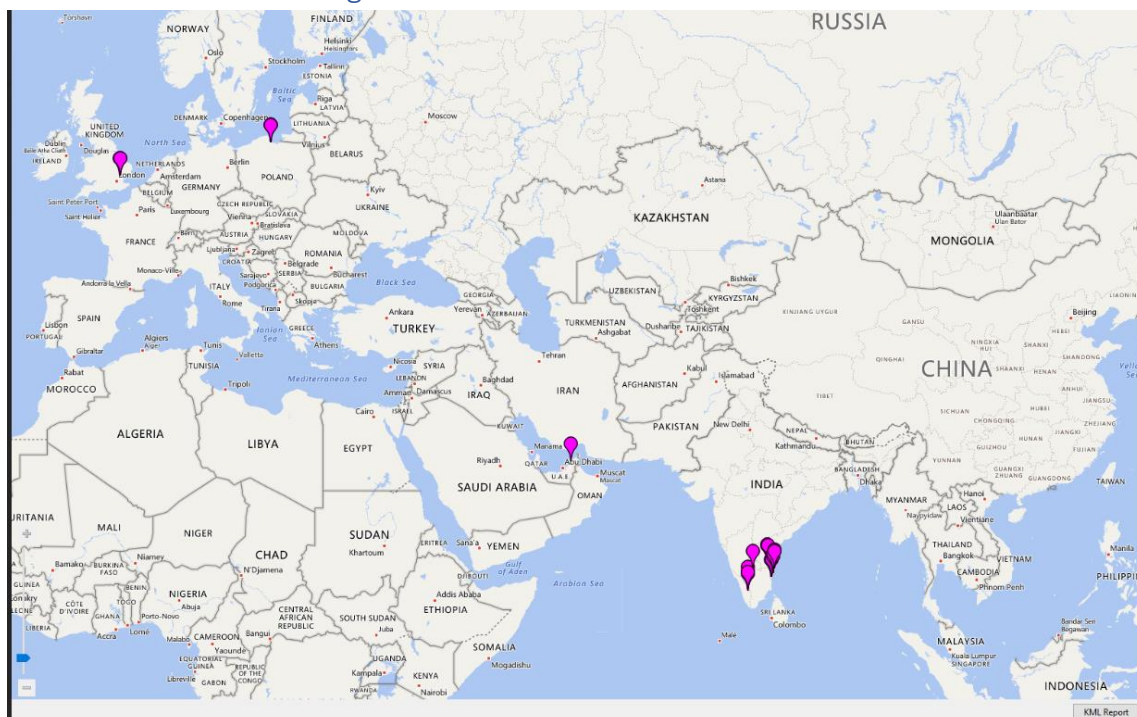


Figure 18 Locations of TO's Travel

The comprehensive analysis of the mobile device yielded substantial evidence of extensive travel, both domestic and international, as indicated by recovered photos, call logs, and audio files. However, despite the detailed examination using advanced forensic tools like Cellebrite, there was no definitive evidence found that linked these travels to the sharing of research data with competitors.

The absence of direct proof in the device's data regarding the unauthorized dissemination of sensitive project information leaves this aspect of the investigation inconclusive. While the travel activities of the individual were extensively documented, the primary concern of intellectual property leakage remains unverified through this forensic examination.

### Team Members Ratings

|               |    |    |
|---------------|----|----|
| Ellis Bennet  | 10 | 10 |
| Lara Costa    | 10 | 10 |
| Rohan Chavan  | 10 | 10 |
| John Hughes   | 10 | 10 |
| Connor Wilson | 10 | 10 |

### References

- [1] "www.spiceworks.com," www.spiceworks.com, [Online]. Available: <https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-digital-forensics/>. [Accessed 12 12 2023].
- [2] "onlinedegrees.nku.edu," onlinedegrees.nku.edu, [Online]. Available: <https://onlinedegrees.nku.edu/programs/business/master-legal-studies-digital-law-and-technology/digital-forensics-and-law/>. [Accessed 12 12 2023].
- [3] "www.forensicsinsider.com," www.forensicsinsider.com, [Online]. Available: <https://www.forensicsinsider.com/digital-forensics/digital-forensics-and-cybersecurity/>. [Accessed 12 12 2023].
- [4] "subrosacyber.com," subrosacyber, [Online]. Available: <https://subrosacyber.com/blog/artificial-intelligence-digital-forensics>. [Accessed 12 12 2023].
- [5] "www.appdirect.com," www.appdirect.com, [Online]. Available: <https://www.appdirect.com/blog/cloud-forensics-and-the-digital-crime-scene#:~:text=What%20Is%20Cloud%20Forensics%20and,and%20can%20better%20preserve%20evidence..> [Accessed 13 12 2023].
- [6] I. M. S. A. D. J. H. J. P. S. P. B. K. F. S. A. Anders Flaglien, Digital Forensics, 23 May 2017.
- [7] "International Journal of Digital Crime and Forensics (IJDCF)," 2022.
- [8] "medium.com," [Online]. Available: <https://medium.com/@lsc cybersecurity/the-role-of-cyber-forensics-in-digital-investigations-uncovering-the-truth-b9c31eb5bd07>. [Accessed 14 12 2023].
- [9] "nvlpubs.nist.gov," nvlpubs.nist.gov, [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf>. [Accessed 15 12 2023].
- [10] "cs.uwaterloo.ca," cs.uwaterloo.ca, [Online]. Available: <https://cs.uwaterloo.ca/~brecht/courses/854-IoT-2016/readings/surveys/Internet-of-Things->

New-security-and-privacy-challenges\_2010\_Computer-Law-Security-Review.pdf. [Accessed 15 12 2023].

- [11] "www.igi-global.com," www.igi-global.com, [Online]. Available: <https://www.igi-global.com/gateway/article/250211#pnfRecommendationForm>. [Accessed 15 12 2023].
- [12] "www.linkedin.com," www.linkedin.com, [Online]. Available: <https://www.linkedin.com/pulse/digital-forensics-market-demand-2023-2030-upcoming/>. [Accessed 17 12 2023].
- [13] "www.eccouncil.org," www.eccouncil.org, [Online]. Available: <https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/data-acquisition-digital-forensics/>. [Accessed 19 12 2023].
- [14] "www.forensicfocus.com," www.forensicfocus.com, [Online]. Available: <https://www.forensicfocus.com/articles/the-enhanced-digital-investigation-process-model/>. [Accessed 19 12 2023].
- [15] "Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications," *International Conference on Computational Intelligence and Data Science (ICCIDS 2019)*, vol. 167, pp. 907-917, 2020.
- [16] "A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning," *Forensic Science International: Digital Investigation*, 2023.
- [17] "Rethinking People Analytics With Inverse Transparency by Design.," *ACM on Human-Computer Interaction.*, pp. 1-29, 2023.
- [18] O. P. C. A. Maria Ioanna Maratsi, "Ethical and Legal Aspects of Digital Forensics Algorithms: The Case of Digital Evidence Acquisition," *15th International Conference on Theory and Practice of Electronic*, pp. 32-340, 2022.
- [19] "securityscorecard.com," [Online]. Available: <https://securityscorecard.com/blog/future-of-digital-forensics/>. [Accessed 19 12 2023].
- [20] "https://www.autopsy.com/," www.autopsy, [Online]. Available: <https://www.autopsy.com/>. [Accessed 20 12 2023].
- [21] "www.exterro.com," exterro, [Online]. Available: <https://www.exterro.com/ftk-imager>. [Accessed 20 12 2023].
- [22] "celebrite.com," celebrite, [Online]. Available: <https://celebrite.com/en/home/>. [Accessed 20 12 2023].
- [23] D. Ayers, "A second generation computer forensic analysis system," *Digital Investigation*, vol. 6, pp. s34-s42, 2009.
- [24] D. illis, B. A. Becker, T. O'Sullivan and M. and Scanlon, "Current Challenges and F ent Challenges and Future Resear e Research Areas for Digital eas for Digital," in *Annual ADFSL Conference on Digital Forensics, Security and Law*, 2016.

