

Digital forensics

by Kyle Aldridge

Submission date: 07-May-2026 01:39PM (UTC+0100)

Submission ID: 282609467

File name: 56770_Kyle_Aldridge_Digital_forensics_737277_1627818020.docx (412.6K)

Word count: 5781

Character count: 34754

SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE SCENARIO

Kyle Aldridge

Student University of Wales Trinity St David, Swansea, Wales

2404215@student.uwtsd.ac.uk

Abstract- This report evaluates several digital forensic tools, including Exterro FTK, FTK Imager, Cellebrite UFED, and Autopsy. It compares their features, strengths, and limitations while examining their role within the CHFI forensic process. The report highlights the importance of using appropriate forensic tools to ensure investigations are conducted in a forensically sound and legally admissible manner.

I. Introduction

Computer/Digital forensics is the utilisation of science to aid the identification, collection, inspection, and analysis of all electronic data in a manner that preserves their integrity, reliability, and repeatability through approved techniques and maintains the chain of custody of the evidence [1].

Digital Forensics is a major component of modern policing/investigations. This is due to the ever-growing involvement in crime, utilising technology and social media. It is estimated that around 90% of crime has a digital element, which results in a large workload for Digital Forensics units (DFU) [2]. In England and Wales, approximately 25,000 devices were awaiting analysis by a DFU in August 2022, underscoring the vital role of digital forensics [3].

When DFUs investigate devices for evidence, they must use the right tool for the right task. This is because there is no single best tool which is universal for all situations [3]. This is because technology evolves rapidly and changes constantly; therefore, each tool has its strengths, and one tool will outperform another on certain devices or in certain situations as technology evolves.

Therefore, this report will critically evaluate four different tools. It will consist of two imaging tools, which are Cellebrite UFED and Exterro FTK Imager and two All-in-One Forensic suites, which are Exterro FTK and Autopsy. By analysing these tools, we can gain insight into Commercial vs open-source products and how one tool may be better suited to certain scenarios than others.

II. Overview of forensic tools

There are many different categories of forensic tools. Each of them aims to support investigators in acquiring, preserving, and analysing evidence[3]. These tools are therefore essential for ensuring that evidence is collected in a forensically sound manner, suitable for presentation in legal proceedings[4].

Imaging tools – These tools create exact forensic copies (bit-by-bit images) of storage devices [4], [5]. This includes capturing all data, such as deleted files and unallocated space, without altering the original evidence[5]. This process is critical for maintaining evidence integrity[4]. Examples include FTK Imager and EnCase.

Analysis tools – These tools are used to examine forensic images and extract meaningful information and evidence[3]. They can then be scrutinised by investigators to examine file systems, recover deleted files, and identify relevant artefacts such as documents, emails, or registry edits[4], [5]. Examples include Autopsy or Magnet AXIOM.

Mobile forensics – These tools specialise in extracting data from Mobile devices and can aid in analysing the data[6]. They can recover various types of data such as messages, call logs, application data and deleted content by utilising various acquisition methods[4], [6]. Examples include Cellebrite UFED or FTK Imager Pro.

Memory/RAM analysis tools – These tools capture and examine volatile data stored in a system's RAM[7]. This type of data is lost when a system is shut down or loses power, so live acquisition is critical[7]. This is because it can reveal live processes, encryption keys, and active network connections[7]. An example is Magnet RAM capture.

Network forensics – These tools monitor and analyse network traffic, helping identify security breaches and detect suspicious activity[3], [8]. They can be utilised to identify data exfiltration, unauthorised access, or communication between systems[8]. Examples include Wireshark or TCPdump.

Cloud and social media analysis – These tools are used to acquire and analyse data stored in cloud services and social media platforms[9]. They can extract information such as account activity, stored files, and communication logs, often utilising Application Programming Interfaces (API) or browsing artefacts[9]. Examples include Magnet AXIOM Cyber, Cellebrite UFED or X1 Social Discovery.

Browser forensics/dump tools – These tools focus on extracting and analysing browsing data, history, cookies, passwords, and cached files[10]. This information can be used to establish user activity and access to online services[10]. Examples include DumoZilla or NetAnalysis.

The selection of forensic tools depends on the nature and circumstances of the investigation, the types of devices involved, and the form of evidence required to be presented[3], [4]. In practice, investigators often use a combination of these tools, multiple in some categories, to ensure comprehensive evidence collection and analysis[11].

III. Tools for analysis

1. Imaging tools

1.1 Cellebrite UFED

Cellebrite UFED is a commercial Mobile forensics suite designed for the acquisition and analysis of data from mobile devices[12]. Its primary purpose is to enable lawful access to various mobile devices for analysis, allowing investigators to extract data while maintaining the chain of custody (CoC) and ensuring forensically soundness[13].

One of Cellebrite's key strengths is its ability to support a wide range of modern Android and iOS devices, including those which are encrypted or protected[4]. UFED supports various extraction methods and device platforms and, therefore, is compatible with FFS, EXT4/F2FS, and APFS/HFS+[4]. Enabling it to handle a diverse range of mobile data[13]. The types of evidence that can be extracted include call logs, SMS messages, files, hidden or deleted files/data, emails, browsing data, and more[13].

In terms of reporting capabilities, Cellebrite UFED can generate a detailed forensically sound report in PDF, HTML, and its own UFDR format[4]. These reports include extracted evidence, metadata, hash values, and investigator annotations such as case details and screenshots[13]. It may also contain a timeline analysis depending on the file format, making it easier to reconstruct user activity[4], [13]. The reports are generally clear, well-structured, and suitable for presentation in legal proceedings[14].

However, despite its strengths, it is a specialist, high-cost commercial tool that will limit the number of smaller organisations that can afford it[12], [15]. Additionally, effectiveness is not guaranteed on modern devices due to their security features and the variety of device models, particularly on newer or heavily encrypted devices. This is also true for heavily damaged phones[4].

1.2 Exterro FTK imager

Exterro FTK Imager is a commercial imaging tool, but it is free to use unless you wish to image iOS devices, in which case it will cost £374.00 for the Pro package[16]. It is designed for the acquisition and basic analysis of data from hard drives and devices[17]. It is primarily designed for creating forensic images of storage devices, allowing investigators to capture data in a forensically sound manner while maintaining the chain of custody (CoC)[17].

Its main function is to enable data acquisition and preview of data from various sources, including hard drives, external storage devices and volatile memory[17]. It also enables advanced file decryption for services like BitLocker or FileVault under the Pro package[16]. FTK Imager also supports multiple file systems, including NTFS, EXT2/3/4, FAT32, and

APFS, enabling it to handle a diverse range of data, storage mediums, and file formats[17]. The types of evidence that can be imaged include Physical and logical drives, file-level data, Volatile memory capture, deleted files / slack space, mobile artefacts, and encrypted data preview[16], [17].

FTK Imager's reporting capabilities focus on providing technical, detailed text reports containing case information, image verification data, Hash codes, and evidence integrity logging[17], [18]. This ensures that the evidence gathered is forensically sound and can be presented in court, while also maintaining the CoC[3]. It is more basic than other reports, but that is because its main purpose is imaging rather than an all-in-one suite[17], [18]. Once the device is imaged, it can be moved into an analysis tool.

However, despite its strengths and low cost, FTK Imager lacks many advanced analysis features, automation, and integrated reporting tools found in more comprehensive forensic platforms. Additionally, its functionality is concentrated on acquisition rather than the in-depth analysis[17]. This results in its use alongside other forensic tools as part of a forensic investigation workflow[11].

2. All-in-One Forensic Suites

2.1 Exterro FTK

Exterro FTK is a commercial, all-in-one forensic suite widely used in law enforcement[19]. It's designed as a comprehensive suite of forensic investigation tools[20]. It can therefore be utilised for data acquisition via FTK Imager, processing and indexing of evidence, and in-depth analysis with reports suitable for legal proceedings[21].

Its key features include a powerful AI-assisted indexing engine for fast search of large datasets; advanced file filtering and keyword search; and built-in password and encryption-cracking tools for various types of data/images[20], [21]. It also has strong email, registry and timeline analysis tools[20], [21]. Due to its extensive features, it also supports a wide variety of file systems/formats, including NTFS, APFS/HFS+, FAT, EXT2/3/4, E01, DD, RAW, UFDR, ZIP, 7Z, and many more[20]. This allows it to handle diverse types of evidence, including disk images, documents, emails, browser artefacts, encrypted, password-protected and deleted files[19].

FTK can generate detailed reports in multiple formats, including PDF, HTML, and CSV[20]. These reports include important details such as the case details, evidence summaries, file metadata and hash values, keyword hits and a timeline of evidence[21]. This is then also presented in a suitable format for the courts[18].

Exterro FTK is overall a very powerful tool due to its impressive search and indexing features, its ability to handle large volumes of data efficiently, and its strong reporting tools[20]. It is also a well-recognised industry-standard tool[18]. However, it requires an expensive licence, which prevents small companies from utilising the suite[19]. Staff also need training on how to use it effectively due to the complexity of its advanced features, along with capable hardware, as it can be resource-intensive[3], [19].

2.2 Autopsy

Autopsy is an open-source, all-in-one digital forensic suite built on The Sleuth Kit (TSK), making it a powerful and free-to-use forensic tool[22]. It is designed for forensic analysis of disk images and is used for file

system analysis, recovery of deleted data and for investigation of user activity[23].

Some of Autopsy's key features include file system browsing, keyword searching, timeline analysis, file recovery, web artefact analysis, and email analysis[19]. It also provides strong support for 3rd-party plug-ins/modules[19], [22]. Autopsy supports a wide range of file systems, including NTFS, FAT/FAT32, EXT2/3/4, and HFS+[20]. It can also utilise images in various formats, including DD, RAW, E01, and VMDK[22]. This, therefore, allows it to thoroughly analyse deleted files, documents/media files, browser artefacts, email data, and file metadata[22].

Autopsy can generate reports in HTML and Excel formats[23]. This may include timeline data, browser history, files with associated hash values, and extracted artefacts[23]. This is also in a suitable format for legal proceedings[22].

Autopsy overall is a very good suite with lots of flexibility and features, available at no cost, and has an active community that supports the future of the software[19]. It is also friendly for learners who may wish to start learning about digital forensics[19], [20]. It also has a unique plugin support feature, enabling more features to be added easily[19]. However, when compared to commercial tools, it may be less powerful and may struggle with larger datasets[22]. It also offers fewer automation features and a simpler report than other tools[22].

IV. Comparative table

Tool	Type	Cost	Key Features	File Systems / Formats	Types of Evidence Handled	Reporting Capabilities
Exterro FTK	Commercial all-in-one forensic suite	Paid licence	Advanced indexing and search, keyword filtering, password cracking, email and registry analysis, timeline analysis	NTFS, FAT/exFAT, EXT2/3/4, APFS/HFS+; E01, RAW (DD), ZIP, UFDR	Disk images, emails, documents, deleted files, registry data, browser artefacts, encrypted files	PDF, HTML, CSV reports; includes metadata, hash values, timelines, keyword hits; suitable for court
FTK Imager	Free forensic imaging tool	Free	Disk imaging, data preview, RAM capture, hash verification (MD5/SHA), supports forensic acquisition	NTFS, FAT32, EXT2/3/4, APFS; E01, RAW (DD)	Physical and logical drives, file-level data, deleted files, slack space, memory (RAM)	Basic technical logs; includes hash values, acquisition details, verification; limited reporting features
Cellebrite UFED	Commercial mobile forensic suite	Paid licence	Mobile data extraction, supports Android/iOS, logical/file system/physical extraction, handles encrypted devices	Supports mobile OS (Android/iOS); various device file structures	Call logs, SMS, app data, emails, browser data, deleted/hidden data	PDF, HTML, UFDR reports; includes metadata, timelines, hash values, annotations; court-suitable
Autopsy	Open-source forensic suite	Free	File system analysis, keyword search, timeline analysis, file recovery, plugin support, web/email artefact analysis	NTFS, FAT/FAT32, EXT2/3/4, HFS+; E01, RAW (DD), VMDK	Disk images, deleted files, documents, media, browser artefacts, email data, metadata	HTML, Excel reports; includes artefacts, timeline data, hash values; less detailed than commercial tools

Table 1 - Shows a Comparative table of 4 different forensic tools

The comparison shown in table1 highlights clear differences between commercial and open-source forensic tools. Exterro FTK provides the greatest level of functionality, as it is the most comprehensive, offering advanced indexing, analysis, and reporting features suitable for large-scale

investigations[23]. It does, however, come with a high license cost and high resource requirements[24]. In contrast, Autopsy offers a free alternative with a strong core of forensic capabilities, but it is less powerful, and its reporting capabilities are more limited[23].

FTK Imager serves a specialised role, focusing on the acquisition and preservation of evidence rather than a full analysis suite[17]. This makes it an essential supporting tool in a forensic workflow[17]. Cellebrite UFED is similar to FTK Imager, as it is a specialised mobile forensics tool that offers capabilities general forensic tools cannot, such as extracting and imaging data from modern smartphones[4].

Overall, the choice of tool or tools relies on the type and requirements of an investigation[3]. This is because the method for extracting the evidence depends on the source and the investigator's available resources[3], [22]. In practice, investigators often use a combination of tools to ensure comprehensive collection and analysis of evidence[5].

V. Critical evaluation

Exterro FTK is a highly effective analysis tool due to its ability to scale to the demands of an investigation, particularly when handling large datasets that require processing terabytes of data [25]. Its powerful indexing and keyword search capabilities significantly reduce investigation time while maintaining high accuracy and reliability[23]. This, therefore, enables investigators to process and investigate more cases in the same period of time while also aiding understanding of complex cases[20].

However, the tool requires a carefully thought-out configuration to avoid overlooking any evidence or producing excessive, irrelevant data[20], [21], [23]. As a result, there is a steep learning curve, and even some experienced users may still encounter challenges when utilising its more advanced features[23]. This may, in turn, affect the quality and relevance of the

results produced during an investigation[22], [23].

Therefore, because of its complexity and high-performance hardware requirements for large datasets, it is best suited to professional environments where large datasets or a high number of cases need to be processed and analysed efficiently[23].

Autopsy is well-suited to smaller investigations and educational institutions, as it is free to use and offers many features found in larger, licensed software platforms[19]. It also includes plugin support, which enables third parties to easily extend or modify its functionality[19]. This is aided by the software being open source, which allows the code to be validated and a large community to help improve it over time[19], [23].

Despite this, some plugins may be inconsistent in quality and affect reliability if not properly validated due to poor code[23]. Autopsy also has limited enterprise support due to its open-source nature[23]. Furthermore, the software struggles with large datasets, which can cause issues in larger investigations, as it may run too slowly or become unstable[19]. This can reduce efficiency and increase the time required to analyse and interpret evidence.

Overall, Autopsy is a very useful tool for small teams of investigators or for learning about digital forensics, but a different tool may be better suited to larger organisations with many cases or large datasets[22].

FTK Imager is a lightweight, easy-to-use tool that is extremely reliable for forensic acquisition[17]. This is because it is widely trusted for forensically soundness and repeatability, and its evidence integrity through hashing meets the required standard while being free to use[11], [17].

However, it lacks advanced analytical capabilities and relies heavily on other tools; as a result, it cannot conduct a full investigation independently[16], [17]. Further to this, it may struggle to complete an image on a failing or heavily damaged disk due to bad sectors[17]. This results in multiple tools being required to perform a full investigation.

In general, FTK Imager is a useful and reliable tool that can image most disks for free; however, it must be used in conjunction with other tools to investigate a case and in certain situations where it may not perform reliably, such as with older or damaged storage devices[17].

Cellebrite is an industry leader in mobile forensics with its UFED tool[14]. This is because it may be able to bypass device locks and, in some cases, access encrypted devices[12]. The company also continually researches new methods to gain access to new devices and Operating Systems (OS) versions, making it a vital tool in a forensic toolkit[4], [13].

However, its success rate varies by device model and OS version, as manufacturers continue to develop and deploy security updates to prevent unauthorised access[4]. It also requires expensive licensing, which may limit accessibility for smaller digital forensics units[15]. Furthermore, it requires specialist training to utilise its advanced features, and some features may be restricted or require additional authorisation from Cellebrite[4], [12].

Overall, Cellebrite's UFED is an extremely powerful and core component of a digital forensics toolkit, enabling forensic analysis of mobile devices. However, its high cost, training requirements, and variable success rates mean it is best suited to well-resourced organisations. Tools used in CHFI Process

The Computer Hacking Forensics Investigator (CHFI) process has five distinct stages to ensure digital evidence is handled correctly, in a forensically sound and efficient manner[26].

Identification stage – This is the initial stage where tools/equipment are used to identify and prioritise sources of digital evidence, such as computers, mobile devices, storage media and SIM cards[27]. Tools such as Exterro FTK and Autopsy can be utilised to preview data and determine its relevance to an investigation[23].

Collection/Acquisition stage – Tools such as FTK Imager or EnCase are used to create forensic images of each storage device[16], [18]. This ensures that a bit-by-bit copy of the data is captured, preserving all potential evidence without altering the original[26]. For mobile devices, tools such as Cellebrite UFED or Magnet AXIOM/Acquire can be used to extract data from smartphones and tablets[12], [28].

Preservation stage – This stage focuses on by verifying integrity using hashing[27]. The tools used could be FTK Imager or Cellebrite UFED, as they both support hashing (e.g., MD5, SHA-1) to verify that the data has not been altered and to maintain the CoC[4], [12], [17].

Examination/Analysis stage – Tools such as Exterro FTK and Autopsy are used to analyse the acquired data from various sources[20], [23]. These tools allow investigators to recover deleted files, examine file systems, and user activity and can aid in the identification of relevant evidence[26].

Reporting / Presentation stage – Tools such as Exterro FTK, Autopsy, and Cellebrite UFED can generate forensic reports in various formats such as PDF and HTML[23]. These will contain any evidence, timelines, metadata and case information which can be presented in legal proceedings[23].

Using the appropriate tools at each stage ensures that evidence is whole and remains accurate, reliable and admissible in court[26].

VI. Conclusion

The evaluation of the four forensic tools demonstrated that each tool has its own strengths and weaknesses, meaning there is no single solution that can address all aspects of a forensic investigation. As a result, a combination of tools is required to support a comprehensive and forensically sound investigation while adhering to industry standards and legal requirements[3], [26]. This is because each tool provides capabilities that others may not, particularly where some tools are designed for specialised tasks such as data acquisition or mobile forensics.

Commercial tools such as Exterro FTK and Cellebrite UFED offer advanced functionality, strong reporting capabilities, and support for complex investigations, but they require significant financial investment and specialist training. In

contrast, open-source tools such as Autopsy provide a low-cost alternative with strong core features, although they may have limitations in performance, scalability, and reporting.

Specialised tools such as FTK Imager and Cellebrite UFED further highlight the need to select the appropriate tool for each stage of an investigation, as different stages require different capabilities, including acquisition and mobile data extraction.

Overall, digital forensic investigations rely on the effective combination of tools to ensure that evidence is collected, preserved, analysed, and presented in a forensically sound and legally admissible manner.

Task 2

Table of Contents

Task 2	9
Introduction.....	10
Forensic methodology	10
Investigation plan	10
Evidence acquisition	10
Detecting anti-forensics	11
File recovery	11
Cloud evidence.....	11
Tool justification/Analysis	12
Investigation Steps.....	12
Findings	13
Evaluation	13
Conclusion.....	14
Appendix	15
Hash Log	15
Sample Report.....	15
Invoice	15
References.....	16
 Figure 1 - screenshot of the hash values of the Browsing evidence	15
Figure 2 - screenshot of the hash values of the Windows evidence	15
 Table 1 - Shows a Comparative table of 4 different forensic tools	5

Introduction

This investigation aims to identify and analyse digital evidence from a corporate laptop related to a suspected cyber incident involving potential company sabotage of trade secrets. The objective is to identify relevant artefacts, recover potentially deleted data, and determine user activity, utilising appropriate tools and techniques to ensure forensic integrity throughout the investigation.

Forensic methodology

The methodology behind the investigation will be based on the ACPO and CHFI Forensic process. These ensure that digital evidence is handled in a structured, forensic and legally admissible manner. The investigation will follow key stages, including identification of potential evidence sources, acquisition, preservation, analysis and reporting.

Initially, potential sources of digital evidence will be identified, including where and how data may have been stored, accessed, or transferred. A forensically sound image of the relevant storage media will then be acquired using appropriate tools which have been tested for forensically sound acquisition. This ensures that the integrity of the original evidence is maintained. This includes using hashing algorithms to verify that no changes occurred during acquisition.

The acquired image will then be analysed to identify relevant evidence, which will be documented and presented in a standardised and formal report suitable for use in legal proceedings. Throughout all stages of the investigation, the Chain of Custody (CoC) will be maintained, ensuring that evidence is comprehensively documented and can be verified and repeated if required.

Investigation plan

Evidence acquisition

For data acquisition, an appropriate tool is FTK Imager, as it can perform a Bit-By-Bit copy and provide SHA-1 and MD5 hash values. This ensures that the image taken is both forensically sound, can be verified, and captures all data on the disk, including unallocated space and slack space. This provides the best possible opportunity to gather residual data, including deleted files, for later analysis while preserving the integrity of the original evidence.

Detecting anti-forensics

If the drive is encrypted using BitLocker, specialist tools such as Cellebrite Inspector or Exterro FTK may be used, where appropriate, to assist in identifying or accessing encryption artefacts. Once access has been obtained, the data can be analysed using Exterro FTK. FTK can then be used to identify deleted files and attempt recovery of residual data from the disk.

Evidence of anti-forensic activity, such as the use of wiping tools, may still be identified even if the original data has been removed. This can be achieved by analysing system artefacts, including registry entries, log files, and application traces. For example, registry paths within HKEY_CURRENT_USER\Software may indicate the installation or execution of wiping software. In addition, system logs and file system artefacts may provide evidence of file deletion activity or the use of secure wiping tools.

Furthermore, FTK can be used to analyse areas such as unallocated space, slack space, and the recycle bin to identify remnants of deleted files. If files have been hidden or intentionally obscured, further analysis techniques and tools may be required to detect them.

This approach ensures that, even when data has been intentionally removed or concealed, traces of anti-forensic activity can still be identified and used as evidence within an investigation.

File recovery

The disk image may be analysed using file carving techniques to recover deleted data, particularly where file system metadata is missing. This approach uses file signatures, such as headers and footers, to reconstruct files, increasing the likelihood of recovering usable evidence.

Cloud evidence

Browser artefacts may provide evidence of cloud storage usage, including file uploads, downloads, and access to online services. These artefacts can be analysed using tools such as Exterro FTK to identify user interaction with platforms such as Google Drive.

For example, URLs stored within browser history may contain identifiable patterns (such as references to document IDs or paths ending in “/edit” or “/view”), which can indicate that files were accessed, modified, or shared. Additionally, search queries (e.g. those related to cloud services such as drive.google.com) may provide insight into user activity, including attempts to locate or upload files.

These artefacts can help reconstruct user behaviour and may provide evidence of data exfiltration or unauthorised access to cloud-based storage. Even if the original files are no longer present on the local device, these traces can still demonstrate interaction with external storage services.

Tool justification/Analysis

For overall analysis of the image, Exterro FTK will be utilised due to its strong indexing, keyword searching, and file recovery capabilities. This allows efficient processing of large datasets and identification of relevant evidence.

Cellebrite Inspector may be used, where required, to assist with encrypted data access, enabling the disk to be analysed effectively once moved into FTK. The findings will then be documented in a structured report suitable for use in legal proceedings.

Investigation Steps

Initially, an image of the laptop's hard disk was acquired using FTK Imager, with a read-only cable to ensure no data was written to the disk. This image was then duplicated to create three copies: the original evidence, a master copy, and a working copy. This ensured that the evidence could be thoroughly analysed while preserving the integrity of the original data. Each copy, including the original evidence, was verified using MD5 and SHA-1 hashing, which matched across all copies to confirm authenticity.

Subsequently, the evidence was loaded into Exterro FTK. Cyfusion Mobile Manufacturing Company (CMMC) provided the BitLocker recovery key, enabling FTK to decrypt the drive for analysis. FTK then indexed the image to prepare it for efficient searching and analysis and performed file carving to detect deleted file artefacts.

Keyword searches were conducted, including terms such as "drive.google", file extensions such as ".ma" and ".mb", and references to wiping tools such as "Eraser". Additional patterns, such as hexadecimal values and repeated data sequences, were also analysed to identify potential evidence of file wiping or obfuscation.

Following this, browser artefacts were analysed, including URLs and cookies, to identify evidence of cloud storage usage and any relevant user activity.

Finally, all recovered files were analysed to identify Autodesk Maya project files that had been deleted or lost. All findings and search criteria were documented within the investigation report and recorded as part of the Chain of Custody (CoC) where required. This structured process ensured that all analysis was conducted in a forensically sound and repeatable manner in line with ACPO and CHFI principles.

Findings

When analysing the file artefacts, it was identified that large files had been uploaded to Google Drive over a 3-month period. Some of the files had generic or unclear names but were identified as Autodesk Maya file types, suggesting that attempts may have been made to obscure the true nature of the files.

A large number of files had also been deleted; however, only a small number were considered suspicious. Regarding deleted emails, only the subject lines were recoverable, which lacked significant evidential value. Analysis of browser artefacts identified regular access to websites such as Google Drive and other work-related platforms, indicating consistent interaction with cloud storage services.

Timeline analysis suggested that the activity began around 17/10/2025 and continued until approximately one week before Rich handed in his notice. Additionally, the third-party deletion tool "Eraser" was downloaded approximately three weeks before his departure and appeared to have been used regularly during that period. This may indicate attempts to securely remove files or reduce the likelihood of data recovery prior to leaving the organisation.

Overall, the findings suggest that cloud storage services were used to transfer or access Autodesk Maya project files and that efforts may have been made to conceal or remove evidence through file deletion and the use of anti-forensic tools.

Evaluation

During analysis, Exterro FTK was unable to correctly process some files containing partial or corrupted evidence. In addition, the system crashed several times while generating reports, requiring the reporting process to be repeated and significantly increasing the investigation time. This appeared to be caused by limited system hardware resources, which struggled to efficiently process the volume of data being analysed.

Despite these issues, FTK remained relatively easy to use and navigate, enabling efficient searching, indexing, and analysis of the majority of the evidence. Its interface and investigative features enabled a more in-depth analysis and improved the overall efficiency of the investigation.

However, the instability observed during analysis underscores the importance of suitable hardware and system configuration when conducting large-scale forensic investigations, as performance limitations can affect both efficiency and reliability.

Conclusion

At the start of the investigation, the laptop was successfully imaged, and the hash values matched, as shown in Figure 1, confirming that a forensically sound image had been created. The subsequent investigation identified the use of cloud storage services to upload large files over a period of time. In addition, Autodesk Maya project files were successfully recovered, enabling CMMC to continue with the patent process for the recovered designs. Evidence also suggested attempts to conceal files through the use of generic file names and the use of a dedicated file deletion tool to permanently remove data.

Exterro's FTK enabled detailed analysis of the majority of the evidence and generated comprehensive reports of the findings. Hash values remained consistent throughout the investigation, ensuring that evidence integrity and the Chain of Custody (CoC) were maintained. This supported a thorough and legally defensible investigation conducted in accordance with ACPO and CHFI principles and guidelines.

Some limitations were identified during the investigation, including system instability caused by underpowered hardware, which resulted in FTK crashing during analysis. In addition, not all deleted files could be recovered from the disk image.

Overall, the investigation was successful, as key evidence and the deleted Autodesk Maya files were recovered. The findings may support further legal action relating to breach of trade secrets and potential corporate espionage.

Hash Log

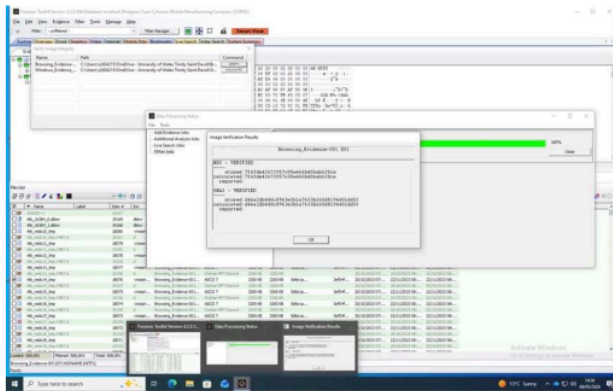


Figure 1 - screenshot of the hash values of the Browsing evidence

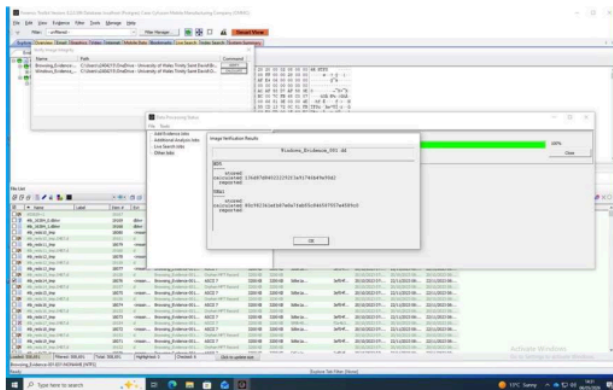


Figure 2 - screenshot of the hash values of the Windows evidence

Sample Report

Please see the additional files for the sample report.

Invoice

Please see the additional files for the invoice.

References

- [1] College of policing, "Forensics | College of Policing." Accessed: Apr. 24, 2026. [Online]. Available: <https://www.college.police.uk/app/investigation/forensics>
- [2] "NATIONAL POLICING DIGITAL STRATEGY".
- [3] "ACPO Good Practice Guide for Digital Evidence".
- [4] Cellebrite, "Cellebrite Certified Operator Level: Intermediate Participant Guide," 2023.
- [5] E. Commission, "Book 5-Digital Investigation Techniques and Tools."
- [6] A. Almuqren, H. Alsuwaelim, M. M. Hafizur Rahman, and A. A. Ibrahim, "A Systematic Literature Review on Digital Forensic Investigation on Android Devices," *Procedia Comput. Sci.*, vol. 235, pp. 1332–1352, Jan. 2024, doi: 10.1016/J.PROCS.2024.04.126.
- [7] M. Parekh and S. Jani, "MEMORY FORENSIC: ACQUISITION AND ANALYSIS OF MEMORY AND ITS TOOLS COMPARISON," *International Journal of Engineering Technologies and Management Research*, vol. 5, no. 2, pp. 90–95, Apr. 2020, doi: 10.29121/ijetmr.v5.i2.2018.618.
- [8] E. Commission, "Book 6-Network Forensics." [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso->
- [9] "Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges | Enhanced Reader."
- [10] A. Yadav, A. Kumar, K. Baranwal, and R. Kumar, "Special Issue) Forensic Analysis of Web Browser Artifacts using Open-Source Tools," *Indian Journal of Forensic Medicine and Pathology*, vol. 18, no. 2, pp. 301–311, doi: 10.21088/ijfmp.0974.3383.18225.32.
- [11] P. Joseph and P. Viswanathan, "A comprehensive survey and analysis on multi-domain digital forensic tools, techniques and issues," *Cogent Eng.*, vol. 13, no. 1, 2026, doi: 10.1080/23311916.2026.2652147/ASSET/FD669423-6AAC-4D92-B9D8-F195EE2802D2/ASSETS/GRAPHIC/OAEN_A_2652147_F0004_C.JPG.
- [12] Cellebrite, "Cellebrite UFED | Mobile Device Extraction Tool for iOS." Accessed: May 01, 2026. [Online]. Available: <https://cellebrite.com/en/products/ufed/>
- [13] M. Albreiki, A. Wani, F. Alazemi, F. Iqbal, and N. Seghid, "Forensic Examination of iOS Platform Artifacts: A Comparative Multi-Tool Study Using Publicly Available Data", doi: 10.1109/NTMS65597.2025.11077003.
- [14] "Preparing Testimony about Cellebrite UFED in a Daubert or Frye Hearing", Accessed: May 01, 2026. [Online]. Available: <http://www.guidancesoftware.com/resources/Pages/doclib/Docu->
- [15] "UFED Ultimate License - 1 year." Accessed: May 01, 2026. [Online]. Available: <https://www.detective-store.com/ufed-ultimate-license-1-year-461.html>
- [16] "FTK Imager Pro | Encryption Detection & iOS Collections – Exterro." Accessed: May 01, 2026. [Online]. Available: <https://store.exterro.com/products/ftk-imager-pro>
- [17] M. C. E. Lim *et al.*, "Analysis of Forensic Disk Imaging Tools for Data Acquisition and Preservation," *Journal of Informatics and Web Engineering*, vol. 4, no. 2, pp. 158–181, Jun. 2025, doi: 10.33093/jiwe.2025.4.2.11.
- [18] I. Ismail and K. A. Zainol Ariffin, "The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance," *PLoS One*, vol. 20, no. 9 September, Sep. 2025, doi: 10.1371/JOURNAL.PONE.0331683.
- [19] E. Herrera, "Open-Source Forensics Tools are great tools for critical used Open-Source Forensics Tools are great tools for critical used machines machines", Accessed: May 01, 2026. [Online]. Available: <https://scholarworks.sfasu.edu/etds>

- [20] M. Farnan, J. Pratt, A. David, and M. Shakiba, "Digital Forensic Tools: Comparison of Autopsy TSK and Forensic Explorer," in *2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS)*, IEEE, Jun. 2024, pp. 1–5. doi: 10.1109/ICITEICS61368.2024.10625076.
- [21] "FTK CENTRAL PROCESSING OPTIONS GUIDE", Accessed: May 01, 2026. [Online]. Available: www.exterro.com
- [22] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions," *IEEE Access*, vol. 10, pp. 11065–11089, 2022, doi: 10.1109/ACCESS.2022.3142508.
- [23] V. Agboola, J. Osamor, and F. Olajide, "Evaluating the Efficiency of FTK, Autopsy, and Mobile Forensic Tools: A Comparative Study in Criminal Investigations," 2024, doi: 10.20533/ijicr.2042.4655.2024.0156.
- [24] "FTK Physical License – Exterro." Accessed: May 01, 2026. [Online]. Available: https://store.exterro.com/products/ftk?_su_rec=kCYCDhrDirHF_cL4qZaZHaqSNW4VXoFgCnynXz8AZinnP89mXJbywInWvyTljri82kuwZlwrAUierv2QAzbMm2rL33zeaw_QaO0HikWwd24J9V8FD5VQORfnNrJ0jCn gxB9JrQkLgDKGm4MvEcYYasA1-l6VW_LsHeWr9iNLfNTThejSeU116rfGNrSSclu8vSKnsJPYm4qFOgpbwXJ-vH-mSp45YcPI1n1CngGU8UUYlewFQZ4ePmVpumeaJsWiF6CplFo8kxz0o_PN0&_su_rec_id=9fce1f40-3fbd-4574-823d-e08d2e045fc5-1777658112
- [25] "West Midlands Police Force | Node4 Client Story." Accessed: May 01, 2026. [Online]. Available: <https://node4.co.uk/case-study/west-midlands-police-force/>
- [26] J. T. . MILLS, *CHFI COMPUTER HACKING FORENSIC INVESTIGATOR THE ULTIMATE STUDY GUIDE TO ACE THE EXAM*. JAKE T MILLS, 2023.
- [27] "Computer Hacking Forensic Investigator (CHFI)", Accessed: May 07, 2026. [Online]. Available: [https://elhacker.info/manuales/Análisis%20forense/\(ebook.-.PDF\)\[informatica\]\[forense\].FBI-.Computer.Hacking.Forensic.Investigator\(Chfi\).pdf](https://elhacker.info/manuales/Análisis%20forense/(ebook.-.PDF)[informatica][forense].FBI-.Computer.Hacking.Forensic.Investigator(Chfi).pdf)
- [28] M. Siamukulule, "A Deep Dive into Magnet AXIOM's Workflow: Exploring the Roles of AXIOM Process and AXIOM Examine in Digital Evidence Acquisition and Analysis", Accessed: May 07, 2026. [Online]. Available: www.ijfmr.com

FINAL GRADE

GENERAL COMMENTS

92/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

GRADING FORM: L5 CF (ACCD5000)

KYLE ALDRIDGE**92****ENGAGEMENT WITH LITERATURE SKI**

Your work must include articles published by peer reviewed journals, conference proceedings, books, and related website (e.g. IEEE, ACM, Science direct). Information from website such as how, wiki, forums, etc. will not be accepted. (20 marks)



The report demonstrates excellent engagement with forensic literature, forensic methodologies, and digital forensic technologies. Appropriate references are included regarding FTK, FTK Imager, Cellebrite UFED, Autopsy, forensic standards, and CHFI methodology. The comparative discussion demonstrates independent research and awareness of both commercial and open-source forensic environments.

18**KNOWLEDGE AND UNDERSTANDING SK**

On chosen topic, your work must demonstrate understanding of concepts and underlying principles. You should explain and analyse the tools you have chosen from the research in a meaningful way. The IEEE

report format must be used for the research aspect (task 1) but not mandatory for the case study (task 2). (10 marks)



The submission demonstrates excellent understanding of forensic acquisition, forensic analysis, mobile forensics, volatile memory analysis, evidence preservation, and reporting procedures.

Technical explanations are generally accurate and demonstrate strong understanding of forensic workflows and evidential integrity.

9

COGNITIVE AND INTELLECTUAL SKI

Your work must demonstrate critical analysis and evaluation of the investigation and reporting documentation. Your work must also justify Computer Forensics Investigation procedures. The labs you do in class should help you to complete the processes or forensic methods Barry would have used. (45 marks)



The report demonstrates excellent analytical reasoning and logical investigative structure throughout both tasks. Appropriate evaluative comparison is demonstrated regarding the operational suitability and limitations of forensic tools across different investigative contexts. The report demonstrates investigative planning and operational awareness.

36

PRACTICAL SKILLS

Marks will be awarded based on the sample professional forensics report generated by a forensics tool. AccessData FTK tool is recommended as this tool is on the computers in room IQ 205 or any other of your choice will be accepted. Use sample evidence file(s) from

the shared folder. Less than 40% will be awarded for Internet downloaded report. (15 marks)



The submission demonstrates Excellent practical understanding of forensic imaging, mobile acquisition, evidence preservation, and forensic reporting procedures. Appropriate forensic workflows are identified throughout the investigation discussion and demonstrate reasonable practical realism. Evidence of relevant screenshot within the report. Additional files submitted for sample report and invoice.

20

TRANSFERABLE SKILLS FOR LIFE A

The report should be presented in an academic way (IEEE/ACM format) and therefore must include an abstract, an introduction, a conclusion and a list of references. The report must be submitted via Turnitin as well. (10 marks)



The report is generally well structured and professionally organised with effective use of headings, comparative tables, and technical explanations.
overall professional presentation.

9