

Synthesize a solution to a potential real-life scenario

Agogu  Floriane

Abstract

Computer forensic investigations depend on specialised tools. Each tool is adapted to specific scenarios and types of evidence. This report examines three forensic tools. It analyses their strengths, limitations, and optimal use-cases.

Keywords – Forensics, tools, evidence, investigation

I. INTRODUCTION

Computer forensics is an important aspect of cybersecurity. It focuses on the recovery and analysis of computer-based material to be presented as digital evidence for legal purposes. Although the basics in computer forensics remain constant, methods and especially tools change continuously. Choosing the right tool depends on the specifics of each investigation. This report explores and evaluate different forensic tools. It categorises and analyses their features, benefits and drawbacks. It shows the most suitable tools for specific scenarios.

II. ENCASE

Digital forensics professionals rely on tools like EnCase Forensic to meet the challenges of cybercrime and data breaches. EnCase Forensic was developed by Guidance Software – now OpenText. This tool can collect and processing digital evidence in a forensic manner. It is used by law enforcement, government agencies and private investigators.

A. Capabilities

EnCase Forensics provides investigators with a flexible set of modules for various forensic tasks. Firstly, EnCase Forensic excels in the acquisition of digital evidence. It uses bit-by-bit imaging technique to create exact copies of hard disks, removable media, and other storage devices. So that, obtained evidence is not modified and is acceptable to the courts. According to Widup [1], the tool strictly offers data integrity using cryptographic hash functions like MD5, SHA-1, and SHA-256. It guarantees data has not been altered during capture to presentation.

This tools also enables file carving and recovery. Indeed, thanks to file signature analysis, EnCase can recover deleted, fragmented or hidden files regardless of the file system structure. Furthermore, an indexing engine allows investigators to perform searches for specific keyword, including regular expressions and proximity searches. EnCase also facilitates the reconstruction of user and system activity over a defined period of time. It enables log and artefact analysis. Investigators can analyse system logs and application artefacts to discover user behaviour, installed software and evidence of tampering. It can also extract and examines emails from different email clients. It has an option of bookmarking to mark items of interest during an analysis.

EnCase support various operating systems like Windows, Linux, macOS, and multiple file systems. This compatibility

allows investigators to work across different platforms. Now, recent versions support the acquisition of mobile devices.

Moreover, EnCase is capable of analysing RAM dumps, to detect, for example, malware, or running processes.

B. Application to Stenography

EnCase is very useful for detailed analysis of data hidden using steganography and encryption techniques.

A case study [2] shows how EnCase was used to detect hidden information in PowerPoint files using steganography techniques. EnCase revealed for example hidden messages in images and text areas thanks to its Transcript view. They use techniques such as the LSB (Least Significant Bit) method or manipulating text colour, to decipher invisible text (text with the same background colour). The Transcript view makes it much easier to detect for example overlapping images, fake hyperlinks, hidden texts by extracting metadata and textual content invisible to the normal user.

C. Limitations

Although EnCase is very effective for data acquisition and analysis, it does have a few limitations. One limitation is the cost and resource intensity of EnCase. It requires a financial investment, which makes EnCase less accessible to small organisations than free tools. It also requires high system performance, in particular a large memory for large datasets.

With EnScript, professionals can create custom workflows to automate repetitive tasks, for example. However, these advanced features also pose challenges. It can require advanced scripting skills, particularly when using EnScript for advanced forensic analysis.

D. Key points

EnCase Forensic is an important tool in digital investigations. It offers a suite of robust tools capable of handling complex investigative scenarios, from data recovery and chronological analysis to advanced detection of steganography. Although its cost and complexity of use can present challenges, its comprehensive capabilities make it indispensable in investigations, where data integrity, court admissibility and detailed reporting are essential.

III. FTK IMAGER

FTK Imager (Forensic ToolKit) is an imaging tool developed by AccessData. It has become one of the most used tools for forensic imaging and acquiring evidence. It is used by forensic scientists to create exact bit-by-bit copies (images) of drives and different digital storage devices. It ensures that digital evidence can be acquired and analysed without making any modifications on the original data [4], which is the key to admissibility in court.

A. Functional overview

FTK Imager is designed as an acquisition tool, enabling forensic examiners to create both physical and logical images of storage devices. According to *Mastering FTK Imager* [5], the tool supports a big variety of image formats, like E01 (EnCase Evidence File), AFF (Advanced Forensic Format), or RAW (Raw bitstream copy). Each format has its advantages. For example, the E01 format can store metadata (hash values, timestamps). The tool is also valued for its ability to preview files and directories prior to imaging, allowing forensic examiners to sort systems efficiently. This feature is very useful for triage during operations, as investigators can determine whether potential evidence is present before performing resource-intensive imaging processes. In addition, FTK Imager allows live capture of volatile data such as system memory (RAM). It also allows forensic images to be exported for analysis with other tools like FTK Toolkit or Autopsy.

One advantage of this tool is that it is lightweight and can be run from a USB stick without installation [4]. Moreover, Casey notes that FTK Imager's graphical user interface (GUI) is intuitive, making it accessible to both experienced forensic analysts and those new to the field. As well as its accessibility, FTK Imager offers high efficiency and good execution speed. Indeed, experimentally, FTK Imager has demonstrated impressive performance, creating a forensic image of a 1GB device in around 1 minute [6]. It also has good compatibility with common file systems, supporting NTFS, FAT12/16/32 and others, making it versatile in many OS environments.

An important feature of FTK Imager is its ability to present data in different views, which helps forensic analysts interpret digital content more efficiently depending on their goals. These include: Hex view, Text view and natural view. Hex view displays raw data in hexadecimal format, allowing precise byte-level examination. This view is essential when analysing binary files, headers, or looking for signatures and anomalies. The text view shows the ASCII (and optionally Unicode) representation of data, which is helpful for quickly identifying readable strings or commands embedded in files. Finally, the natural view attempts to render the content as it would normally appear to a user like plain text or simple file content, improving readability and contextual understanding for certain file types. The table below outlines the main use of each FTK Imager view (*Table 1*).

Table 1 - Use of each FTL Imager view

Views	Purpose	Use case
Hex	Displays raw hexadecimal and ASCII values	Deep inspection of file headers, metadata...
Text	Shows the ASCII representation of data	Searching for readable text in logs or memory
natural	Plain text or simple file content	Reviewing documents or simple file content

B. Application in investigations

FTK Imager is frequently used in different investigations. In particular, it is used in criminal investigations: seizing and imaging of suspect computers for analysis in cases of fraud, child exploitation or intellectual property theft. It is also used in corporate investigations for internal investigations related to policy violations. FTK Imager is also suitable for incident response operations requiring volatile memory capture.

In *Mastering FTK Imager* [5], case studies demonstrate its application in operations in the field, where speed and reliability are essential. The portability of the tool and its ability to sort through previews are big advantages when dealing with large-scale incidents or multiple devices.

C. Limitations

Although FTK Imager excels in the acquisition phase, it is not an all-in-one forensic suite. Firstly, its analysis capabilities are limited. In fact, unlike full forensic platforms (e.g. EnCase), FTK Imager does not have in-depth analysis tools such as keyword searching, data sculpting or correlation functions [4]. Its role is to acquire and store data, leaving analysis to other platforms. It also lacks a reporting engine. FTK Imager does not include an integrated report generator, forcing investigators to document results externally [5]. Finally, it also has no automation or scripting support. FTK Imager does not have scripting capabilities to automate repetitive tasks.

D. Summary

Both sources emphasise the importance of the chain of custody and documentation throughout the imaging process [4][5]. FTK Imager complies with legal and procedural requirements for handling digital evidence by providing detailed logs, hash verifications and the ability to export acquisition reports manually.

FTK Imager is an indispensable tool in the digital evidence acquisition phase. Although it does not offer extensive analysis functions, its reliability, portability and speed make it a preferred choice among practitioners.

IV. PALADIN

Paladin is a complete suite of Linux-based investigative tools. This tool is designed to help investigators conduct examinations and data acquisitions in a manner consistent with forensic science requirements. Developed by SUMURI LLC, Paladin is a versatile CD distribution offering a wide range of open source and proprietary investigative tools suitable for disc imaging, data carving, memory acquisition and triage.

A. Features and capabilities

Paladin is mainly used for hard disk imaging, live acquisition and digital triage. It includes well-known tools such as dc3dd and dd for bit-by-bit imaging, and Guymager for graphical front-ends. The acquired images are then subjected to hash verification (e.g., MD5, SHA-1, SHA-256) to ensure data integrity. It also includes Foremost for secure data wiping and data carving. Furthermore, it

includes The Sleuth Kit and Autopsy for timeline and file system analysis. Paladin is fully compatible with the main forensic image formats. It supports formats such as E01, Ex01, RAW (dd), SMART, AFF, VHD, and VMDK.

According to *The Art of Memory Forensics* [9], Paladin can facilitate the collection of volatile memory when deployed on compatible systems. It allows investigators to capture evidence related to active processes, malware and other threats residing in memory. The versatility of Paladin allows investigators to acquire data without altering the source, thus preserving the integrity of the digital evidence. Indeed, the creation of verified images is fundamental to the reliability of forensic expertise [10].

The main advantage of Paladin is that it is open source and is compatible with different platforms. Moreover, Paladin does not require any installation. The tool combines different forensic utilities. It reduces the dependence on multiple platforms. It also allows memory acquisition to be taken over. Indeed, although Paladin is not primarily a memory analysis tool like Volatility, its integration with tools such as LiME allows it to capture memory if necessary. Its graphic interface is sufficiently accessible for experienced investigators but also for beginners.

B. Case of study

In a comparative study entitled “An Analysis of Smartphones Using Open Source Tools versus the Leading Commercial Tool”, Marcie Bachler evaluated the effectiveness of Paladin in the field of digital smartphone investigation. The study highlighted that, although Paladin provides a wide range of digital investigation utilities, its success in recognising and imaging different smartphone models was mixed. For example, some phones were recognised as mountable drives suitable for imaging, while others were only detected as internal storage devices, limiting the possibility of performing full forensic imaging. This case illustrates the importance of checking tool-device compatibility during investigations, and demonstrates the practical value of Paladin in certain acquisition scenarios despite its limitations with mobile devices [11].

C. Limitations

In terms of limitations, Paladin, like many Linux-based live distributions, may have hardware compatibility issues, especially with newer devices or proprietary drivers. In addition, post-processing is limited. Indeed, Paladin focuses mainly on acquisition and initial triage, so analysts may still need additional tools (e.g., Autopsy on Windows/Linux) for more in-depth analysis and expert reporting. Furthermore, in-depth memory analysis is limited.

D. Summary

Paladin is a flexible solution for digital forensics professionals who focus on disk imaging, data triage and live system acquisitions. It represents the open source philosophy of transparency and accessibility [10], while providing a basis for memory forensics tasks [9]. For organisations or individuals looking for a cost-effective forensics toolkit without sacrificing functionality, Paladin remains a valuable asset.

V. AUTOPSY

Autopsy is a digital forensics platform that provides investigators with a great interface to conduct analyses of computer systems. Originally developed by Brian Carrier, Autopsy is built on top of The Sleuth Kit and is widely recognized in forensic communities for its robustness and modularity.

A. Features and capabilities

Autopsy is a solution for disk analysis, file recovery, timeline generation, keyword searching, hash filtering, and web artifact analysis. As highlighted by Carrier in *File System Forensic Analysis* [12], Autopsy leverages the Sleuth Kit’s powerful back-end utilities, enabling detailed file system examinations, including NTFS, FAT, Ext, and HFS+ volumes.

The tool offers a wide range of analysis capabilities. In fact, it enables timeline analysis by reconstructing user activities through metadata examination. It facilitates the detection of incriminating evidence via keyword search and pattern matching. Autopsy also supports hash analysis, it verifies files against known good or bad hash sets using algorithms such as MD5, SHA-1, and SHA-256. Moreover, it assists in web artifacts recovery by extracting browsing history, cache, cookies, and downloads from popular web browsers. It provides email analysis by parsing common formats like PST and MBOX. Finally, its module-based extensibility permits the integration of external plug-ins, including modules dedicated to EXIF metadata extraction, photo analysis, and even Bitcoin wallet identification.

According to *Digital Forensics with Open Source Tools* [14], Autopsy is compatible with evidence files in formats such as E01, AFF, and RAW (dd). Its intuitive graphical user interface is particularly praised for lowering the entry barrier for novice forensic analysts while remaining sufficiently powerful for experienced professionals.

Furthermore, Cowen in *Computer Forensics: A Beginner’s Guide* [13] emphasizes that Autopsy ensures forensic soundness by maintaining read-only access to evidence during analysis and produces detailed audit logs, supporting the admissibility of findings in court proceedings.

B. Case of study

In *Digital Forensics with Open Source Tools* [14], the authors discuss a case study involving the use of Autopsy for investigating insider threats in a corporate environment. In this study, investigators were able to identify unauthorized data exfiltration activities by analysing recovered deleted files, browser histories, and user login events. Autopsy’s timeline feature allowed the reconstruction of the suspect’s activities across multiple workstations. It culminates in conclusive evidence that withstood legal scrutiny. This case emphasized Autopsy’s role in providing comprehensive analysis with minimal risk of evidence contamination.

C. Limitations

Despite lots of strengths, Autopsy still has limitations. As Carrier notes [12], while Autopsy provides an efficient interface, the underlying analysis relies heavily on The Sleuth Kit's command-line tools, which may require manual troubleshooting for complex file system anomalies. Additionally, Cowen [13] points out that Autopsy's performance can degrade we deal with extremely large datasets, especially if hardware resources are limited.

Another limitation is the dependency on module availability. Although Autopsy's modular architecture is an advantage, the quality and maintenance of third-party plug-ins can vary, potentially affecting reliability in critical investigations.

D. Summary

Autopsy represents a great, open-source digital forensic solution that bridges the gap between accessibility and advanced forensic capabilities. It empowers investigators to perform thorough disk analysis, timeline reconstruction, and artifact recovery with minimal risk to evidence integrity. Despite some performance and plug-in ecosystem limitations, Autopsy remains a perfect open-source digital forensics tools [12][13][14].

VI. COMPARAISON

EnCase, FTK Imager, Paladin, and Autopsy each play different roles in digital forensic investigations.

A. Evidence Acquisition

All four tools are effective for forensic imaging. FTK Imager and Paladin are particularly perfect for a quick field acquisition. In fact, they are lightweight and can be operated from a portable media. EnCase provides robust and court-admissible acquisition procedures, it uses bit-by-bit imaging and cryptographic hash verification. Autopsy, on the other hand, is not primarily designed for evidence acquisition but excels in the analysis of already acquired images, relying on external tools such as The Sleuth Kit for forensic imaging processes.

B. Data Analysis

For this category, EnCase is the best in terms of data analysis capabilities. It has some artifact reconstruction, email extraction, and steganography detection. Autopsy also offers powerful analysis capabilities, including timeline creation, web artifact recovery, and keyword searches. Paladin offers more basic analysis functions with tools like The Sleuth Kit and Autopsy. FTK Imager is limited to previewing and exporting data and has no built-in analytical functions.

C. Ease of Use

FTK Imager is very intuitive, it makes it perfect for some quick tasks and beginners. Paladin offers a great environment, combining a graphical interface with good command-line utilities. Autopsy, with its modular and accessible design, set a balance between usability and analytical depth. EnCase, while powerful, requires an important expertise, particularly for EnScript.

D. Cost and Accessibility

Paladin and Autopsy are open source and free to use. FTK Imager is free for acquisition purposes but limited when it comes to advanced analysis. EnCase is a commercial tool and can be expensive for individuals.

E. Compatibility

EnCase and Paladin support a large range of file systems and platforms. FTK Imager is compatible with common formats like NTFS, etc., but has fewer advanced features for uncommon systems or mobile devices. Autopsy supports multiple file systems and evidence types, although its mobile device capabilities are limited compared to EnCase.

The following table, Table 2 summaries the key features, strengths, and limitations of EnCase, FTK Imager, and Paladin.

Table 2 - Comparative Analysis of FTK Imager, EnCase, Paladin and Autopsy

Criteria	EnCase Forensic	FTK Imager
Evidence Acquisition	Highly reliable	Fast, portable, reliable
Data Analysis	Advanced	Limited to preview
Ease of Use	Complex, requires training	Very user-friendly
Cost	High	Free
Supported Formats	E01, L01, RAW, AFF, others	E01, AFF, RAW
RAM Acquisition	Yes	Yes
OS Compatibility	Windows, Linux, macOS	Mostly Windows
Main Limitations	Expensive, resource-intensive	No deep analysis, no reporting, no scripting

Table 3 - Comparative Analysis of EnCase, FTK Imager, Paladin, and Autopsy (continued)

Criteria	Paladin	Autopsy
Evidence Acquisition	Reliable	Relies on external acquisition (e.g., Sleuth Kit)
Data Analysis	Basic (via Sleuth Kit, Autopsy)	Advanced (timeline, web artifacts, hash analysis)
Ease of Use	Moderate, GUI but Linux-based	User friendly GUI
Cost	Free and open-source	Free and open-source
Supported Formats	E01, Ex01, RAW, SMART, AFF, VHD, VMDK	E01, AFF, RAW, VHD (through modules)
RAM Acquisition	Yes (with integrated tools)	No (focused on post-mortem disk analysis)
OS Compatibility	Linux-based, multi-platform	Windows, Linux
Main Limitations	Hardware issues, shallow memory analysis	No acquisition feature, depends on back-end tools

VII. CONCLUSION

The task 1 has examined and compared several essential forensic tools: EnCase, FTK Imager, Paladin, and Autopsy. Each tool presents different strengths and limitations. This makes them more or less suitable depending on the specific investigative scenario.

Ultimately, there is no single perfect tool for all forensic investigations. The choice of the most appropriate tool depends on factors such as the nature of the evidence, the goals of the investigation, available expertise, and resource constraints. Forensic investigators must be able to select, combine, and apply these tools appropriately. By understanding the strengths and weaknesses of each tool, investigators can synthesize effective solutions tailored to real-life forensic challenges.

REFERENCES

- [1] S. Widup, *Computer Forensics and Digital Investigation with EnCase Forensic v7*. McGraw-Hill Education, 2014. ISBN: 978-0-07-180791-3.
- [2] H. Kim, N. Bruce, S. Park, and H. Lee, "EnCase Forensic Technology for Decrypting Stenography Algorithm Applied in the PowerPoint File," *Dongseo University Research Paper*, Korea. [Online]. Available: <https://ieeexplore.ieee.org/document/7423534>
- [3] M. Salman et al., "A Study of Forensic Tools Data Recovery Performance," *The Hashemite University Research Paper*, Jordan. [Online]. Available: <https://ieeexplore.ieee.org/document/10590383>
- [4] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed., Academic Press, 2011.
- [5] Anonymous, *Mastering FTK Imager: 50 Expert Questions for Digital Forensic Professionals*, Independent Publishing, 2024.
- [6] M. Mohite, J. Deshmukh, and P. Gulve, "Qualitative and Quantitative Analysis of Cloud Based Digital Forensic Tool," *IEEE Xplore*, 2020. [Online]. Available: <https://ieeexplore.ieee.org/document/7727074>
- [7] Chapter 7, *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, Elsevier, 2020.
- [8] Q. R. McCluskey, M. M. Chowdhury, S. Latif, and K. Kambhampaty, "Computer Forensics: Complementing Cyber Security," *International Journal of Computer Science and Security*, vol. X, no. Y, pp. 507–512, 2020.
- [9] M. Hale Ligh, A. Case, J. Levy, and A. Walters, *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Wiley, 2014.
- [10] C. Altheide and H. Carvey, *Digital Forensics with Open Source Tools*. Syngress, 2011.
- [11] M. Bachler, *An Analysis of Smartphones Using Open Source Tools versus the Leading Commercial Tool*, Huntington, WV, USA: Marshall University Forensic Science Center, Aug. 2015. [Online]. Available: https://www.marshall.edu/forensics/files/BACHLER_MARCIE_Research-Paper_Aug-5.pdf
- [12] B. Carrier, *File System Forensic Analysis*, Addison-Wesley, 2005.
- [13] D. Cowen, *Computer Forensics: A Beginner's Guide*, McGraw-Hill, 2013.
- [14] C. Altheide and H. Carvey, *Digital Forensics with Open Source Tools*, Elsevier, 2011.

Task 2

Case study: Sabotage

Professional Forensics report
CMMC (Cyfusion Mobile Manufacturing Company)

1. Introduction

This forensic report documents the investigation conducted by Troy Simpson, CHFI and CEH certified forensic expert. It concerns the deliberate sabotage of confidential design files on the company computer used by Mr. Rich Daley at Cyfusion Mobile Manufacturing Company (CMMC), London.

2. Investigation process

The investigation process followed a standard digital forensics methodology, there is the identification, collection, and examination phases.

A. Identification phase

The first step was to establish the identity of the devices, suspect, and potential witnesses involved. When arrived at the CMMC premises, investigators confirmed that the primary suspect was Rich Daley, a former employee who had recently resigned under suspicious circumstances. His assigned workstation was located and identified as the primary piece of digital evidence.

The suspect's computer was found powered on. Immediate actions were required. In fact, the volatile data, like open files, network connections, could be lost if the machine was powered off, we needed to preserve these data.

First of all, investigators took photos from different angles, they captured the machine, from the front and the back, and the whole workstation. These images are used for the visual record of the state of the system prior to examination and can be valuable for the legal part. We ensured that the integrity of the evidence was collected. Then, we used FTK Imager to acquire the system's RAM.

After that the identity of the suspect device and the risk to volatile data had been addressed, the next step is to secure and collect digital evidence to ensure it remains intact for examination.

B. Collection phase – practical task

A basic inspection of active network sessions was conducted. This revealed recent outbound connections. So, a more in-depth examination is required.

The next step after that is to disconnect the workstation of Rich from all the network connections with the company, like Ethernet cables or Wi-Fi adapters, to avoid any updates for example. The device was properly shut down. The investigator also recorded all details for the identification of the device like the serial number and the device name.

To simulate a real forensic scenario, an environment was created using a sample Windows evidence disk image. I used OSFMount to mount the forensic image, the drive appeared as a USB device on the system. On the mounted drive, Maya files were downloaded from the internet and put in a document. These files were then deleted to simulate sabotage.

After this, I used FTK Imager to create a forensic copy of the disk in EnCase E01 format. This is to ensure that no analysis was conducted directly on the original disk image, to avoid damaging it. Then the file was opened with FTK Toolkit. This screenshot below shows the processing status of the loaded forensic image – Sabotage.E01.

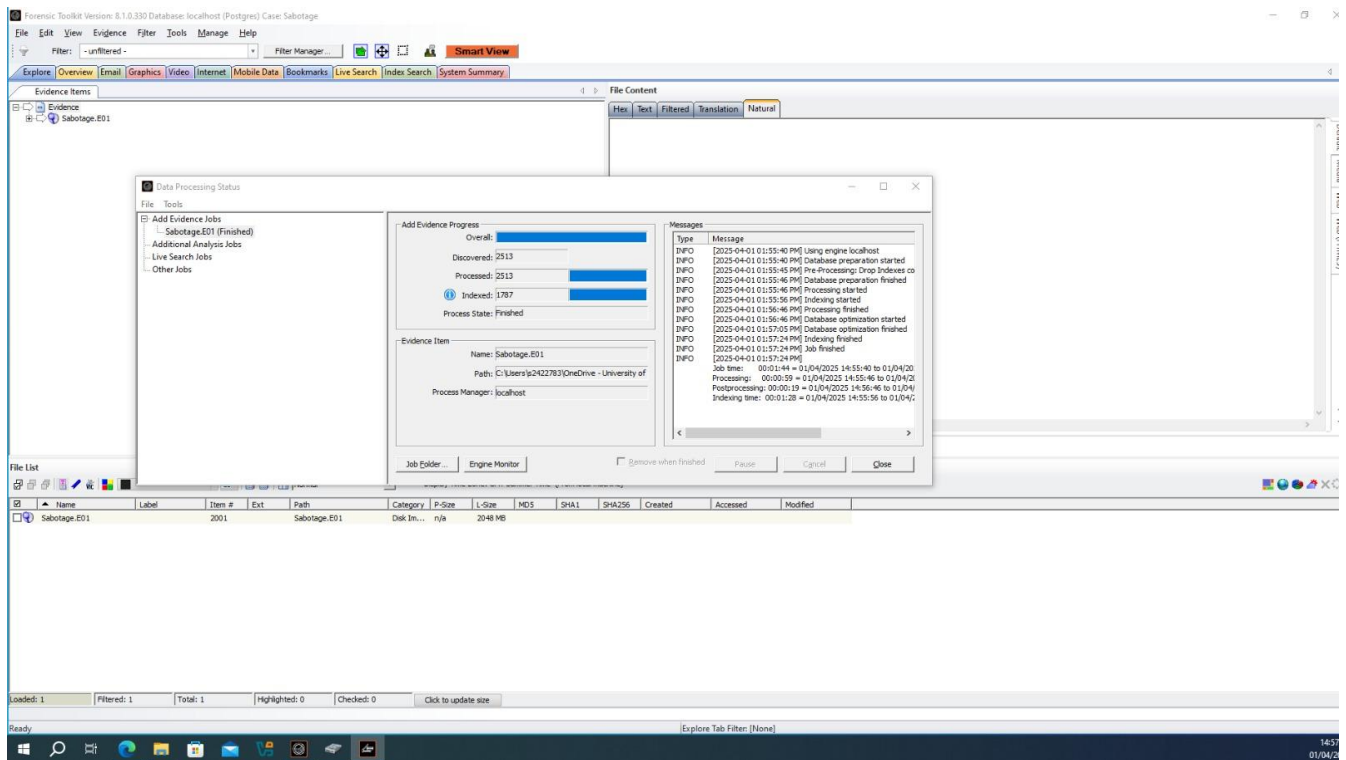


Figure 1 - Evidence Processing Status in FTK Toolkit

With the successful forensic acquisition and all the collected data preserved, investigators moved on to an examination of the memory and disk images to uncover evidence of sabotage.

C. Examination phase

During the examination phase, the forensic analysis focused on the memory capture and forensic image obtained from the suspect's workstation.

First, the investigators found that the outbound connections were directed to a remote server located in Singapore. It was associated with the hosting provider Contabo. Contabo is used for anonymized file exchanges. So this is very suspect. Furthermore, a WHOIS lookup, which identifies the owner and location of an IP address, confirmed that the server is not part of the infrastructure of CMMC.

Moreover, during the memory analysis, a browser was open with multiple tabs. Two of them were some file-sharing platforms named SendSpace and WeTransfer, with completed upload files. This had been accessed just hours before. These findings raise suspicions of possible data exfiltration. Additionally, an active SFTP client process was detected, showing recent access to a hidden folder named ".archive_temp" on the user's desktop. This folder contained several files with non-descriptive or misleading names.

This justified the imaging of the hard drive and deeper forensic analysis.

I used FTK Toolkit to do a keyword search and find the deleted files. One particular file named "minion" was identified in the evidence screen. After inspection, this file contained the actual GUI design files for the Samsung Galaxy Z Flip 6. Metadata analysis showed file deletions occurred shortly before Rich's resignation. This confirms that the data had not been lost but deliberately deleted. The

suspect lied about that the designs were lost, when in fact he deliberately deleted and hid them. The screenshot shows the list of recovered deleted files from the mounted forensic image.

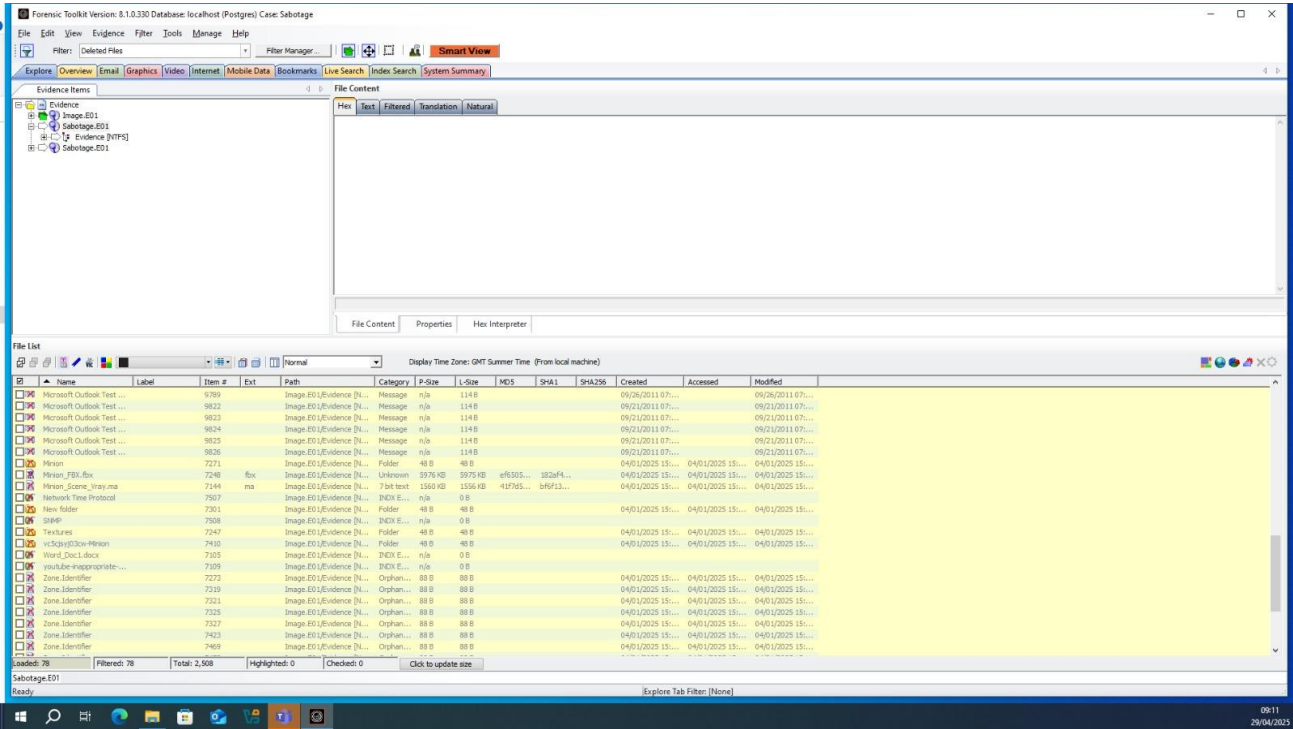


Figure 2 – Recovered Deleted Files in FTK Toolkit

Then, an investigator found new evidence. During the file check, there was a mismatch in file hash values for one of the image files located inside the “*.archive_temp*” folder. So, a steganographic analysis was employed in this case. Steganography is a technique used by cybercriminals to hide data inside digital files or streams. There were hidden contents.

All recovered evidence, the deleted Autodesk Maya files and the extracted steganographic content, was compiled, hashed, and documented. Some screenshots were taken to validate the recovery process.

With all the findings, it seems to provide important proof that Rich Daley had attempted to steal the project of CMMC.

After the recovery and analysis of the evidence, the final part of the investigation is to assemble the findings, preserve the recovered data and prepare all the documentation for legal and organisational use.

3. Post-Investigation part

After the completion of the forensic acquisition and live memory capture, investigators conducted a full post-investigation.

Firstly, the forensic images and memory were analysed using FTK Toolkit. There has been a recovery of the deleted files and an identification of any artefacts indicating external data transfers. We have therefore recovered the deleted Autodesk Maya files. These files have been renamed but on inspection they are indeed the GUI designs for the Samsung Galaxy Z Flip 6 project.

An automated forensic report was generated with FTK Toolkit. It documents all the procedures, files recovered, and analysis performed.

In addition, to prevent future incident like this, some recommendations were told to the company. Some examples are the implementation of a full disk encryption and regular backups, a restricted access to important projects or monitoring outbound traffic for anomalies indicating potential data exfiltration.

The forensic investigation concluded with a meeting where the findings were presented. The next step is now to take legal action against Mr. Rich Daley.

4. Conclusion

The forensic investigation conducted by Troy Simpson Consulting Ltd. successfully identified and documented the deliberate sabotage theft committed by Mr. Rich Daley at CMMC.

Through a structured process with the identification, collection, and examination of digital evidence, the investigative team was able to recover deleted design files, trace suspicious network activity, and uncover steganographic methods used to conceal sensitive data.

Thanks to the use as FTK Imager and FTK Toolkit, the evidence clearly demonstrates that the deletion of the Samsung Galaxy Z Flip 6 GUI designs was intentional. Rich Daley not only attempted to delete all traces of his actions but also used external services and hidden folders.