

COMPUTER FORENSIC ASSIGNMENT

Ewenn Daligaud

Student University of Wales Trinity St David, Swansea, Wales & ISEP Paris, France

2422774@student.uwtsd.ac.uk

TASK 1

ABSTRACT

This coursework is divided into two different parts, the first one is a research part. We are going to choose three different computer forensics tools we will be working on, preferably the most frequently used ones, then we will analyze them and use a table to categorize them. In the second task, a case study, in which a professional has deleted files from his computer, is given to us. First, we need to use the knowledge acquired from the research part and the Computer Forensics module to document the forensics methodology is to be used to investigate and restore the deleted files on the computer. Then, we need to provide the company concerned with a professional forensics report based on the actions taken to restore the data. Finally, we have to provide an invoice for the professional service taken to restore the files and the written professional forensics report.

INTRODUCTION

With the modern age of digitalization, computer forensics has become an important discipline in cybersecurity and criminal investigation that include systematic detection, extraction and analysis of digital evidence from computer devices. Due to the dynamic nature of technology, forensics investigators must continuously update their techniques and tools. Where the principles of digital forensics remain the same, the tools rapidly evolve to support emerging data types, storage formats, and new cyber threats. From commercial tools that offer end-to-end solutions, to open-source tools that offer freedom, openness and low cost, no tool can fulfill all forensic requirements. Thus, investigators choose tools according to specific circumstances and evidence types. This research categorizes and compares multiple popular computer forensic tools by their functionality, uses, and features.

FTK IMAGER

FTK Imager, developed by AccessData, is a widely recognized tool within the digital forensics community. It is identified by multiple sources as an essential forensics analysis tool due to its stability and versatility. Forensic image acquisition is the

most frequent use of FTK Imager, required to preserve the integrity of digital evidence. FTK Imager, according to the book “Real Digital Forensics” by Keith J. Jones, is characterized by its capability to create forensic images in various formats like EO1, RAW and AFF [1]. It is very interesting for data integrity purposes. It also makes full use of FTK Imager in providing features of advanced analysis before the image is made, allowing examiners to explore file systems, find deleted data, and examine files that are hidden or protected by the system. It also highlights the requirements of FTK Imager for acquiring volatile evidence, such as RAM files, particularly in real-time forensic examination [1].

The book “Computer Forensics with FTK” by Fernando Carbone comes at it from the same angle, focusing on working directions and covering very comprehensive analysis of interface and utilization of FTK Imager. It presents the tool as user-friendly, not only by mentioning easy installation and set-up, but also a portable lite and free version for in-field uses. [2]. It describes how FTK Imager allows forensic examiners to examine evidence in different modes, such as Hex, Text, and Natural views. Carbone emphasizes again its capacity to mount forensic images in RAW, EO1, AFF and AD1 formats to allow the investigators to see the images as virtual drives, so it facilitates the easy evaluation of evidence without any fear of manipulating the data [2].

The research article “FTK Image For Forensic Data Processing In Forensic Tools” is an explanation of the usability and effectiveness of FTK Imager in computer forensics. In this research article, the authors state the capability of the software to perform physical imaging from USB drives and other media to describe the entire process from device detection to selection of appropriate drive, image mode and check of hash values to verify the good integrity of the data. The document gives special attention to the benefits of using FTK Imager according to the national Institute of Justice (NIJ) forensics standard, in order to organize and properly document a computer forensic analysis in the scientific way through multiple pre-defined steps of preparation, acquisition, examination, analysis and reporting [3].

The most notable similarity among all these scientific documents is the remarkable file compatibility of FTK Imager such as FAT, NTFS, EXT, HFS, ISO, UDF. Other than that, the versatility of FTK Imager to accommodate other image file formats contributes to the compatibility with other computer forensic tools such as EnCase. Another advantage of FTK Imager is that it also has an encryption detection module for Windows Encrypted File System, very useful to have when a case involving encrypted data is being handled. FTK Imager detects files that are encrypted in good time, alerting the forensic investigator of possible evidence that can be used in the investigation [2]. The primary characteristic highlighted here is the necessity of using hardware-based write blockers while using FTK Imager so that there is no unintended alterations of the original evidence.

In conclusion, FTK Imager has a superior role in computer forensic analysis because of its simplicity of usage, very strong and useful features and integrity of its forensic results. Its main strength lies in its ability to have powerful forensic image features and integrity check, making it a very important tool for any forensic investigation. FTK Imager is remarkable by the fact that it has the perfect balance between technical capabilities and daily practicality. Its usage in a forensic investigation is indispensable.

EnCase

EnCase, developed by Guidance Software, is a very common forensic tool used by many forensic investigators. It is designed to capture, examine, and report digital evidence in forensic investigations. EnCase plays a vital role in digital investigations within law enforcement as well as within businesses due to its robust functionality of handling evidence, full reporting, and support for legal admissibility [4][5][6].

EnCase allows investigators to purchase, preserve, and examine digital proof on various devices. It allows to capture full disk images in proprietary formats (EO1, Ex01), with data integrity through hash verification (MD5, SHA1). The application offers modules for keyword searching, folder management, timeline construction and email analysis. Its design includes a number of panes to browse and dynamically categorize evidence [4].

In addition, EnCase utilizes EnScript as its own scripting language to support automation of processes. It makes it particularly good at dealing with large-scale investigations or where repetitive processes are necessary. The software also supports varied evidence sources like smartphone, network shares, encrypted volumes, and virtual environments [4].

EnCase has long been a widely accepted tool in court. It has been very useful in many cases when attempting to recover deleted information, particularly on EXT2/3 file systems, compared to other tools like FTK (40% recovery rate against 20% using FTK) [6].

EnCase has some features for forensic imaging, evidence authenticity check, image mounting. It also allows to create detailed reports in HTML among other formats. This feature ensures that each step taken by the investigator during the entire investigation process can be verified and is reproducible and is done in a manner that follows the rules [4].

EnCase has some limits, it is a first generation forensic tool and it suffers from architectural vulnerabilities and processing speed. Every time a case is opened, EnCase analyzes the data/evidences, even if it has already been analyzed the last time. This problem makes the software very slow, especially when working on huge cases with a very large amount of data being treated. It also does not have the advanced distributed processing features, which is now very important to have for today's large scale investigation cases [5].

In terms of interface design, which is very important to talk about as it can be a big part of the evaluation of a tool, some users find the layout very confusing, but the experts and more experienced users find it very flexible and efficient. In addition, EnCase only supports MD5 hashing by default and fails to signal files with bad signatures (partially recovered or damaged files) as good as FTK [4][6].

EnCase is both advantageous and disadvantageous as it has a timeline view, enhanced Linux file system management and a powerful scripting interface through EnScript. FTK has better support for hash functions, better interface for beginners and less experienced users, and better features for identifying files with bad signatures. FTK stores analyzed evidence in a database, thus being faster once analyzed, while EnCase re-analyzes every time the case is opened, making it slower. FTK also supports more image types [5][6].

EnCase remains a much used and one of the main tools when speaking about forensic investigations, particularly in legal and professional cases where data integrity, report generation and automating investigation are imperative. It has many advantages like full evidence handling, scripting capabilities and large support for digital media. However, it needs improvement in performance, and user accessibility. It may not be the best tool to use to manage large scale investigations but can be useful for other smaller cases [4][5][6].

Autopsy

Among other existing tools that we already talked about like FTK or EnCase, Autopsy is a main open-source digital forensic tool created to simplify the process of a forensic investigation. This review explores Autopsy's multiple functionalities, features and practical applications based on reliable sources.

Autopsy is what can be called a GUI (stands for Graphical User Interface) over The Sleuth Kit (TSK), a command line forensic tool that is basically a CLI (Command-Line Interface). TSK performs the forensic task, but autopsy is very important to enhance the usability of the tool by offering a very easy to use interface to the investigator. The interface provides keyword searching, data examination, viewing deleted file, and generating structured reports [7]. Autopsy provides support for many operating systems including Windows, Linux, and macOS, it accepts various file formats like disk images (EO1, etc.), virtual machines and local disks [8].

Autopsy has many features that are implemented by something called "ingest modules" that automatically extracts the important information that a forensic investigator should be the most interested to have when analyzing an evidence. Some of these modules offer file type identification, analysis of recent activity and file filtering [8]. A strong feature of Autopsy is keyword searching, examiners can find exact matches to locate the key pieces of evidence. For example, a keyword list can include IP addresses, credit card information, email addresses to identify fraud, forced login attempts, or hidden messages [9]. The matching data can be transformed into a comprehensive report to be presented in a court of law.

Autopsy also offers the capability to generate timelines of events, allowing investigators to rebuild the chronological sequence of events on a system. The timeline module integrates file creation and modification dates, providing a good overview of the system activity. The reporting module can export reports in multiple formats like HTML and Excel. Investigators can still create customized reports by selecting what type of information they want the report to present in particular cases [9].

Autopsy usefulness has been experimented in mock case studies. A great example was the identification of a brute-force authentication attack through the keyword search module. The examiners discovered patterns such as login attempts from Apache server log (file that records everything that is happening on a website/server using Apache web server). The results were highlighted and then the evidence was transformed into something called *Forensic Lucid format* which is a clear and

structured way to present an evidence that is to be used [9].

The benefits of Autopsy, next to its competitors, are its many features. Also, it is open-source. It provides an extensive range of features and tools within it at a professional level without the expense of commercial offerings. Moreover, it supports many types of data and file systems, that makes it useful in a wide range of investigation cases [8].

However, there are also some limitations. For example, while keyword search is a powerful feature, it doesn't automatically understand the order of events in time unless you add yourself that information. Reports also limit character display in preview fields, which may omit useful information [9]. Finally, while autopsy is very good at identifying known attack patterns, it may require other tools to for detailed malware or memory analysis, which is a task that is often left to other tools.

Autopsy is a robust, flexible, and one of the main forensic tools that continues to be used in the world of digital forensic investigations. Its GUI, automation capabilities and strong features make it a great choice for both beginners and experienced investigators. Despite some disadvantages listed above, its support for external modules and its ability the generate structured and clear reports in multiple format make it more usable in professional setups [7][8][9].

Criteria	FTK Imager	EnCase	Autopsy
1. Evidence Acquisition & Integrity	Supports multiple image formats, strong integrity verification via MD5, SHA1, SHA256; detects encrypted files (EFS); requires hardware write blockers for safety.	Captures full disk images (E01, Ex01); verifies integrity using MD5 and SHA1; less effective in identifying bad signatures; evidence handling follows court standards.	Acquires various image types; performs hash checks; keyword match module identifies attack patterns; may lack depth for memory or malware analysis and does not infer event chronology automatically.
2. User Interface & Usability	User-friendly interface; supports multiple viewing modes (Hex, Text, Natural); portable and easy setup; widely recommended for beginners.	Interface seen as complex/confusing for some; flexible for advanced users; layout allows dynamic categorization of evidence.	Very intuitive and accessible GUI over Sleuth Kit; good for beginners and experienced users; supports OS variety and offers modular design with ingest modules.
3. Automation & Analysis	Allows preview before imaging and analysis of deleted/hidden files; no scripting/automation system; strong for structured manual investigations.	Uses EnScript scripting for powerful automation; ideal for repetitive tasks and large-scale investigations; includes modules like timeline, folder management, email analysis.	Uses ingest modules to extract key data automatically (file types, activity); good keyword searching; supports timeline creation; lacks full automation and advanced memory/malware analysis.
4. Performance & Scalability	Efficient and fast due to use of stored analysis database; compatible with many formats and tools like EnCase.	Slower performance: re-analyzes data with every case opening; lacks distributed processing; not optimal for large-scale investigations.	Efficient for moderate cases; performance depends on system and data volume; well-suited for varied investigative scenarios, but may require complementary tools for advanced tasks.
5. Cost & Licensing	Free to use (including portable lite version); excellent balance between technical capability and accessibility.	Commercial tool; often used in professional and legal environments; well-accepted in court but may be expensive and complex for some users.	Free and open-source; highly capable alternative to commercial tools; offers many professional-grade features without cost, making it suitable for academic and budget-limited investigations.

References :

- [1] Keith J. Jones, *Real Digital Forensics: Computer Security and Incident Response*, Addison-Wesley Professional, 2005.
- [2] Fernando Carbone, *Computer Forensics with FTK*, Packt Publishing, 2012.
- [3] S. H. Dange, P. M. Ghodekar, and N. R. Chopde, *FTK Image for Forensic Data Processing in Forensic Tools*, International Journal of Innovative Research in Computer and Communication Engineering, 2022.
- [4] Suzanne Widup, *Computer Forensics and Digital Investigation with EnCase Forensic v7*, 2014.
- [5] Daniel Ayers, *A Second Generation Computer Forensic Analysis System*, 2009.
- [6] Narayan P. Bhosale, *Evidence Recovery using EnCase and FTK in Forensic Computing Investigation*, International Journal of Scientific Research in Computer Science and Engineering, 2021.
- [7] Autopsy User Documentation, <https://sleuthkit.org/autopsy/docs/user-docs/4.0/>.
- [8] Ashok Kumar Mohan & Paul Selwin, *Digital Forensic Investigation Using Sleuth Kit Autopsy*, Conference Paper, 2016.
- [9] Ahmed Almutairi et al., *Evaluation of Autopsy and Volatility for Cybercrime Investigation*, International Journal of Digital Crime and Forensics, 2020.

TASK 2

Contents

1 - Introduction	7
2 - First decisions to take	7
3 - Imaging and data Acquisition	7
4 – Hardware configuration	8
5 – File system analysis and deleted file recovery	8
6 – User activity	9
7 – Reporting of evidence	9
8 - Conclusion	9

1 - Introduction

The following work is a forensic process utilized to investigate suspected data sabotage by an employee, Rich Daley, in Cyfusion Mobile Manufacturing Company (CMMC), London, UK. The attack involves unauthorized deletion and potential exfiltration of intellectual property design files created using Autodesk Maya for Samsung Galaxy Z Flip 6. The designs have high commercial value and are intended to be sold to mobile phone producers.

The objective of this investigation was to confirm whether or not sabotage occurred, restore and identify potentially erased data or hidden files and provide admissible digital evidence for potential use in a court of law.

2 - First decisions to take

Upon notification by the executive management team of CMMC, the first response was the isolation of the computer system involved in order to prevent potential manipulation of data. As an initial measure to secure the integrity of digital evidence, the workstation must be physically disconnected from wired and wireless networks to avoid any possible remote interference or data alteration. To provide sufficient documentation, multiple photos of the computer, peripherals, and the complete setup must be taken. Such photos are a record of the initial state of the system when it was found by the investigation team. Moreover, notes were taken, such as the serial number of the device, its name, and any other possible details that could be used to identify the machine.

The investigation has to follow a legal guideline to support the admissibility of evidence. That is why permission for the forensic analysis was requested from the CMMC management team.

3 - Imaging and data Acquisition

The integrity of the digital evidence is based on capturing data without altering its state. A forensic copy of the storage was taken with FTK Imager, a widely trusted software in digital forensics.

To ensure the integrity and admissibility of the digital evidence collected from Rich's workstation, a forensic acquisition procedure was strictly followed. The source drive was connected through a hardware write-blocker to prevent any unintentional or intentional modification while imaging the drive. This step is crucial to keep the data in its initial state and to make sure that the evidence will not be falsified when conducting the investigation. Once the drive was blocked, an identical copy was created with FTK Imager, which produced a forensic image in the EO1 format, a professional digital investigative standard to keep data and maintain compression. MD5 and SHA-256 cryptographic hash values were calculated and recorded before and after acquisition to ensure integrity and authenticity of the image. These values act as digital proof of authenticity, ensuring that nothing was modified or at least altered during the copying process. Finally, the forensic image was duplicated and saved on an encrypted external

safe storage device, kept in a secure location with restricted access to protect the data from unauthorized use or consultation. It also prevent it from being lost.

Each imaging process was recorded in a chain of custody log, which will be used in the court if needed. Hash values and timestamps were also recorded and checked using different tools.

4 – Hardware configuration

Rich's machine was running on Windows 10 Pro with the tools Autodesk Maya installed. The system had :

- 2TB NVMe SSD
- 64GB of RAM
- NVIDIA RTX 5000 (GPU for professional use)
- Intel Xeon w3-2525 (CPU for professional use)

There was no external backup device. This lack is both positive and negative : while file recovery was imperative since there was no backup, there was less chance that data had been overwritten by any programs.

5 – File system analysis and deleted file recovery

Using FTK Toolkit and Autopsy, two well-trusted forensic tools, Rich's workstation forensic image was deeply analysed to try to find files that may have been deleted by Rich. Autopsy and FTK Toolkit provided robust features for analysing the NTFS file system and retrieving data that would otherwise go unnoticed. Deleted file recovery was the first significant step. NTFS doesn't immediately delete files when deleted, instead, it marks the space as free but maintains references to the deleted data in the Master File Table (MFT). This allowed to recover some files with the .ma and .mb file types – two of the native file types of Autodesk Maya – whose deletion dates were the day of Rich's resignation. Other than traditional recovery, data carving techniques were also used to recover incomplete files. The methods involve pattern matching and identification of header/footer to recreate files that may not have retained complete metadata. Keyword searching was also used. The key words such as "Samsung", "galaxy", "Flip6", "Autodesk", "maya", and "confidential" were selected in relation with the actual scope of the project conducted by Rich. The search in this case generated matches in files as well as in emails, incriminating Rich even more in this case of missing files. Additionally, an extensive search of the Windows recycle bin was made. This revealed that a certain amount of design files had been deleted just days before Rich left the company, providing a strong indication of intentional sabotage. These recovered data and their metadata formed the basis of the digital evidence used to confirm malicious intents.

6 – User activity

To authenticate file deletion and determine whether any data exfiltration has occurred, user activity logs were examined:

- Windows event logs: login sessions, file access, and external device connection to the machine were inspected.
- The user activity on folders and files opened most recently was inspected, some of which matched recovered design filenames
- Browser history and emails : evidence from every messaging/emailing app (Microsoft outlook, gmail,etc.) and every browser (Microsoft Edge, Google Chrome, Mozilla, Firefox...) were deeply inspected and revealed that Rich had recently been in contact with an external domain (360tech.co.uk) before giving his resignation.
- FTK Registry Viewer was used to identify USB devices that had been recently plugged in the machine. It reported that one external device has been plugged two days before Rich resigned. Moreover, it was the same time stamp of the file deletions.

All these information former a timeline of very suspicious activity that happened just before Rich resigned and it is letting us know that something is wrong.

7 – Reporting of evidence

All recovered data were put in a secure case repository. The evidence was:

- Transferred on a secured forensic archive system that was dedicated and encrypted.
- Indexed with metadata including hash values and timestamps.
- Included in the professional report of evidence location, recovery process, and relevance generated by FTK.

It was then completed by a timeline that shows significant events such as file deletions, USB pugging, login/logout precise dates, etc.

8 - Conclusion

This forensic investigation confirms that several files from the Autodesk Maya app related to the Samsung Galaxy Flip 6 project were intentionally deleted from Rich's computer. Metadata, file paths, user activity logs, and external communication logs together constitute a case of sabotage. The retrieved data has been authenticated and can be used in a court of law if a trial has to occur.

Some recommendations for the future are to force regular backups (for example every week) to prevent these kind of things to happen again. But also to deploy some systems of data loss prevention. One important thing that could have avoid this sabotage is to limit high-risk users to have external communication within the company.