

Computer Forensics - Assignment

Nour AL MUTWALY
UWTSD
Swansea, Wales

Digital Forensics is crucial in today's criminal investigations, as it enables the retrieval, analysis and presentation of digital evidence from a wide range of devices, such as computers, mobile phones, and network system. Due to the increasing complexity of cybercrimes, forensics analysts must rely on trustworthy tools.

I- MOST USED TOOLS BY FORENSICS ANALYSIS

In the first part of our project, we will examine the four most used tools by computer forensics professionals. To do this, we will first present and analyze each of them. Then, we will categorize them in a table to more understand the uniqueness of each tools.

A. Analyze of each tools

1) Tool n°1: EnCase

EnCase is a digital forensics and investigation software designed to assist investigators in collecting, preserving and analyzing electronic evidence. It can gather evidence from a wide range of digital devices, including computers, mobile phone and other storage media. It helps with investigation in various digital areas, such as cybercrime, intellectual property theft, and data breaches.

The main feature of EnCase's tool is its capability to acquire and preserve digital evidence while maintaining forensic integrity. In other words, it ensures that the collected evidence remains admissible in court and can withstand challenges from opposing counsel. This means that the evidence collected with EnCase is strong enough to withstand challenges from opposing counsel, which is crucial in criminal investigations. All evidence collected by this tool is securely stored in EnCase evidence file formats.

Additionally, it can uncover more evidence and conduct in-depth investigative research. Therefore, investigators can efficiently triage digital evidence quickly both in the field and the lab, to determine priority, collect and decrypt data from a wide range of devices. Additionally, it has the advantage of identifying relevant evidence, including deleted items. Also, it can close investigations faster and increase investigative capacity.

Nowadays, professionals prefer to use this tool because of its compatibility with various operating systems. In fact, initially, EnCase was limited to 32-bit Windows system. But now, it can support both 32-bit and 64-bit Windows. It can also be compatible with Linux and Unix operating systems.

Moreover, it is very useful for corporate security and cybersecurity experts, as it can be used to perform investigation remotely. It means that digital forensic experts can examine evidence from another machine without needing physical access.

However, there are some features that EnCase needs to improve. In fact, like other tools, EnCase tool needs to have high processing speeds to efficiently handle urgent evidence processing that might be required in court of appeal. This is mainly because processing volumes of the evidential data tend to take time, as forensics analysis must give large amount of time in processing any evidential data, even when the evidence presentation is urgently required.

Another lack of feature that EnCase have is the keyword weighting. When investigators search for specific keywords within files, EnCase does not rank the results by importance of relevance. This feature is very crucial for investigators otherwise they must manually sift through all search results without an automatic ranking system.(4)

2) Tool n°2: Autopsy

Autopsy is a tool that is widely used in digital forensics. Its main feature is that it is accessible and customizable, as it is a powerful open-source platform and free software designed for the analysis and investigation of digital evidence. It provides features that are just as extensive as those found in many commercial programs.

Like EnCase, it conducts in-depth examinations of digital devices and file systems. Thanks to this tool, investigators can understand what happened on a computer by analyzing data. It can therefore recover deleted files, conduct keyword searches, and extract system and file metadata. It can analyze various types of data such as documents, images, browser histories, and even system logs.

Additionally, due to its user-friendly interface and comprehensive documentation, Autopsy is suitable for all users. It is well-known among the professionals due to its reliability. It is also suitable for companies on a tight budget, as it is a cost-effective solution with good functionalities. However, the inconvenient is that it presents some challenges for newcomers who are unfamiliar with its interface.

However, Autopsy has some issues, especially with extremely fragmented data. When a file is split into several pieces scattered across a hard drive, it becomes more difficult to reconstruct, and this is a limitation of Autopsy. Moreover, it relies on external plugins for certain features, which can sometimes make the platform unstable, causing bugs or crashes.

There are some features that need to be improved for Autopsy. In fact, this tool needs to enhance its image analysis functionality to efficiently analyze large numbers of images stored on a device's hard drive. (1)(3)(4)

3) Tool n°3: X-Ways

X-Ways is a forensic tool for data extraction, analysis and recovery. It is one of the leading forensic tools on the market for conducting thorough forensic examination. It's a powerful disk analysis tool due to its ability to capturing free space, slack space, and text. Therefore, it can generate a comprehensive table of drive contents, including all existing and deleted files, and more.

It is also fully portable and can be run directly from a USB stick on any Windows system without requiring installation. However, if desired, it is very easy to download and install thanks to its small executable file size.

It also serves as a low-level disk imaging and cloning tool, capable of creating true mirrors. It can also handle drives and files of unlimited size.

One of the advantages of this tool is that it is very efficient to use and runs very fast. However, this requires a knowledgeable analyst, as the analyst performing the cloning must understand the differences between logical and physical media, as well as the implications of writing pattern to suspected bad sectors. Therefore, an inexperienced analyst who wants to use this tool might encounter some difficulties.

Due to its reliability and its trustworthiness, this tool has become one of the most important investigative tool for forensic examiners.

Nowadays, cybercrimes are becoming increasingly sophisticated and complex. Therefore, some features of X-Ways need to be improved and updated. For instance, the compatibility of its operating system should be enhanced to support both Android and iOS environments. Additionally, the developers should consider hosting the application online to eliminate the need for downloading and installing the executable file before use. This would make the application more accessible and secure for digital forensics analysts. (4)

4) Tool n°3: Cellebrite

Cellebrite is a mobile forensic tool that is widely use to investigate crimes ranging from cyber-attacks to terrorism. It provides advanced data extraction techniques that are essential for mobile device analysis.

The main disadvantage of this tool is that it is very expensive, but it offers some features that are very important, such as efficient system resource utilization, high data recovery accuracy and fast processing speeds.

This tool is well- known for its rapid data extraction and high accuracy levels.

It is a crucial tool for deciphering smartphones and tablets that have been taken during investigations. The fact that this tool can collect and analyze mobile data such as call logs, text messages and app data, makes it even more unique in the eyes of forensics analysts. (1)



Fig. 1. Procedure for gathering data.

B. Comparison for the tools

Criteria	EnCase	Autopsy	X-Ways	Cellebrite
Tool type	Closed-source, Commercial	Open source	Commercial, Closed-source	Commercial, Closed-source
Most appropriate for	Deep forensic analysis, large-scale investigations	File carving, recovering deleted files, open source adaptability	Data extraction and analysis, Disk imaging and cloning	Mobile device forensics, extraction of data from smartphones and tablets
Effectiveness	Ease of use, Scalability	Exels in carving and data recovery	Capturing free space, Generate a comprehensive table of drive contents	Efficient for extracting data from mobile devices

Cost	Very Expensive	Free	Expensive	Expensive
Customizability	Moderate supports, EnScripts and plugins	Highly customizable with plugins and scripts	High, support-s scripting, templates and configuration	Limited customizability, focused on mobile forensics
Support and Documentation	Very good, robust support and certification options	Robust community support, but reliant on the open-source community	Good, detailed manuals, limited direct support	Extensive support with training resources and updates
Speed	Fast, optimized for large-scale investigations	Moderate, speed can vary based on plugin efficiency	Fast, highly optimized engine with minimal resource usage	Quick for obtaining data from mobile devices

The investigation began by creating a new case within the FTK Toolkit, which is a fundamental procedure that ensures the forensic process remains structured, secure and properly documented. It offers a user-friendly interface for managing forensic cases, which enable investigators to enter critical case-specific information such as the case name, examiner's name and a case description. The information entered in these fields will be useful for report generation at a later step. This step is essential, as it ensures that all artifacts and metadata are properly linked to the corresponding case.

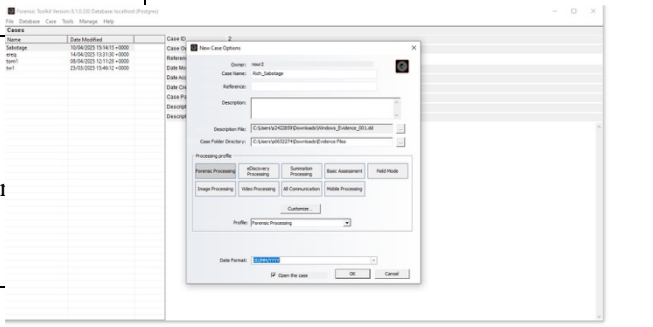


Fig. 2. Creation of a new Case

The next step was the creation of a disk image of Rich's computer. This step is crucial in digital forensics because it allows the examiner to work on a bit-for-bit copy of the original data while also leaving the actual source unaltered. So, this preserves the chain of custody and preserves the forensic integrity of the evidence.

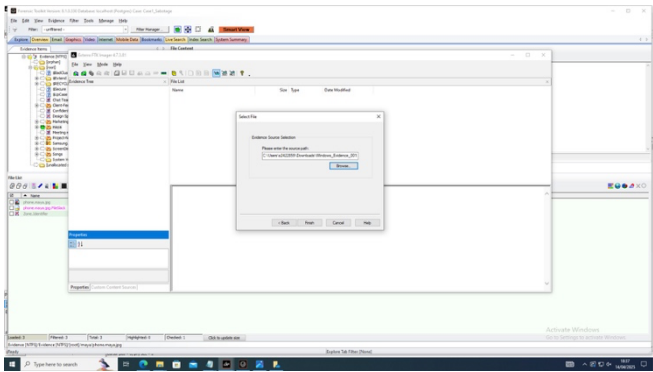


Fig. 3. Creation of the Disk Image

II. CASE STUDY: SABOTAGE

In this part, we will solve a case study that will allow us to understand how to investigate and restore deleted files from a computer. We will provide a professional forensics report based on the actions taken to restore the data. An invoice will also be included for the professional services used to restore the files and produce the written professional forensic report.

A. Case Study: Sabotage

1) Summary of Situation

Our case is about the disappearance of vital design files from the company, assigned computer of Mr. Rich Daley, a former GUI designer at Cyfusion Mobile Manufacturing Company, in London.

He was in charge to develop a confidential graphical user interface for the upcoming Samsung Galaxy Z Flip 6, using Autodesk Maya.

Soon after Mr. Daley resigned from the company, engineers were shocked to notice that there were plenty of important files that has been deleted. Only Mr. Daley had access to the data.

So our mission is to carry out a forensic investigation to provide evidence of Rich's sabotage, and retrieve the data.

2) Forensic Methodology for Data Recovery

Then, I used OSF Mount to mount the disk Image. I enabled write access on the mounted image to allow for modification of the disk contents.

Once mounted, I customized the crime scene by adding Maya files. I also included documents such as design's specification of the Samsung Galaxy.

Then, I deleted the files manually, which means that all the data was lost. That simulate intentional file removal. Manual deletion refers to the process where files are either sent to the Recycle Bin or directly removed from the files system's

directory structure, while the actual data remains in unlocated space until it is eventually space until it is eventually overwritten.

Our crime scene was successfully simulated. So, following this, I returned to the FTK Toolkit to initiate the forensic recovery process. I then used FTK Toolkit to identify these deleted files, which I referred to as “fichier maya”. FTK Toolkit began automatically indexing the disk image, thoroughly examining both allocated and unlocated space to detect digital artifacts, recover deleted files, and extract critical metadata essential for a thorough forensic examination. The photo below shows how FTK Toolkit proceeded in restoring the data.

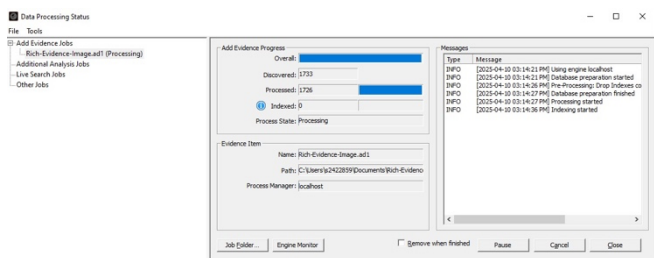


Fig. 4. Data Processing Status

After selecting all the required data and customizing the report format, FTK Toolkit generates the final forensic report. In fact, this report functions as the official report of the investigation and is appropriate for submission in legal, academic, or corporate contexts.

Thanks to the File Status filters, I was able to isolate files marked as deleted. In fact, I searched for file extension related to Maya. These recovered files were referred to as “fichier Maya”, which represented the critical pieces of evidence in this investigation.

FTK Toolkit not only identified the deleted files but also reconstructed their contents where possible. Furthermore, it extracted key metadata such as the original file path, file size, creation timestamp, last access time, and last modification date.

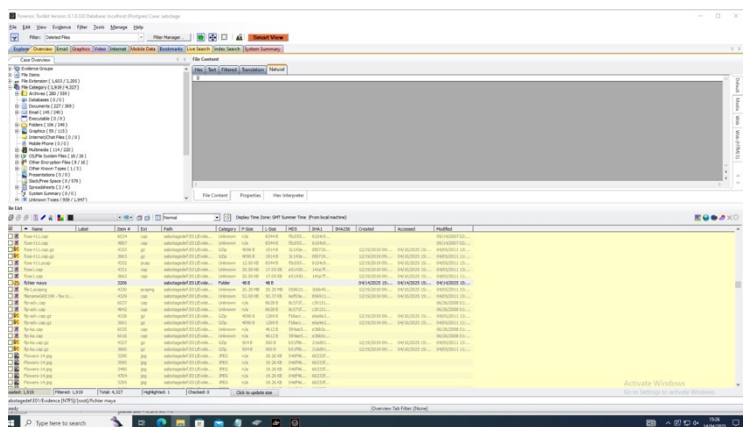


Fig5. Restore deleted files

In addition to the forensic report, I also prepared an invoice for professional services rendered. This invoice outlines the scope of the investigation, including the tools employed, the time spent, and a detailed breakdown of services such as disk imaging, data recovery and forensic analysis.

Conclusion

This study case showcases how digital analysts go about to retrieving deleted files using TFK Toolkit. Thanks to this project, we have gained a deep understanding of the role of an investigator. We were able to simulate a realistic crime scene, recover data, generate a detailed forensic report , and produce a professional invoice.

REFERENCES

- [1] <https://infonomics-society.org/wp-content/uploads/Evaluating-the-Efficiency-of-FTK-Autopsy-and-Mobile-Forensic-Tools.pdf>. Rieder, *Engines of Order: A Mechanology of Algorithmic Techniques*. Amsterdam, Netherlands: Amsterdam Univ. Press, 2020.
- [2] <https://www.sciencedirect.com/science/article/pii/S2666281723001981>
- [3] <https://www.autopsy.com>
- [4] <https://iopscience.iop.org/article/10.1088/1757-899X/834/1/012034/pdf>
- [5] https://www.engineering.iastate.edu/~guan/course/backup-0982/CprE-592-YG-Fall-2002/paper/atstake_opensource_forensics.pdf
- [6] <https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools>
- [7] <https://www.sciencedirect.com/science/article/pii/S2665917423001964>

