

Computer Forensics

Rim Al Mutwaly

University of Wales Trinity Saint David

The first part of this report presents research on digital forensics tools about their many characteristics such as these features and more, including a comparative table. However, the main objective of this report is to present the results of a digital forensics investigation conducted for Cyfusion Mobile Manufacturing Company (CMMC) caused by a suspected internal sabotage. The company's former employee, Rich Daley, is accused to have deleted confidential design file for a new smartphone interface before leaving his job. To do so, professional forensic techniques were used to simulate, examine, and resolve this case.

I. REASERCH

A. FTK Imager

FTK Imager is a crucial tool in digital forensics that is used to obtain a comprehensive forensics image for investigations by allowing forensics investigators to create images of hard drives, partitions, and logical drives. During this process, the software captures bit-for-bit copy of the data, ensuring a complete representation of the original storage media. It can analyse several file systems including FAT, NTFS, EXT2 and EXT3 which enable examination of wide range of digital artefacts such as documents, videos, emails and system files. FTK Imager features powerful file filtering and search functionality, it also can extract metadata associated with files, providing valuable information about file information, modification timestamps or user details.

Thanks to FTK Imager's ability to create forensics images of storage media, it enables the identification of key evidence and supports investigation processes. Moreover, its interface is user-friendly which make it accessible for forensic professionals and those who are completely new to this field. Its combability with different operating systems ensures smooth integration into existing forensic workflows. FTK Imager has an advanced analysis capability that helps investigators to examine files, extract metadata and perform keyword research efficiently that leads to the discovery of crucial evidence.

On top of that, it has a live RAM acquisition functionality that is used to capture volatile memory data which reveals valuable information, that can be crucial in understanding system activity and identifying potential threats, such as running process, open network connections and encryption key. Thus, FTK Imager is a vital tool in digital forensics that provides the investigators with the

necessary tools to find vital evidence and support the forensic investigation process.

B. Wireshark

Wireshark is a free and open-source network protocol analyser, originally known as Ethereal. It is wildly used by cybersecurity professionals, system administrators, and digital forensics investigators to capture, view and analyse network traffic in real time or from previously saved capture files. In the field of computer forensics, Wireshark plays an important role in network traffic analysis, helping investigators trace malicious activities, detect data exfiltration, identify unauthorized communications or uncover evidence of cyberattacks within a network.

It supports deep inspection of hundreds of network protocols, with updates and new features added regularly. Wireshark enables both live capture and offline analysis, making it suitable for a wide range of forensics scenarios. It can collect packets from many different type of network interfaces (Ethernet, Wi-Fi, loopback, etc.), providing deep visibility into how data flows across a network.

This tool captures entire streams of traffic, often comprising tens of thousands of packets, and allows users to filter, slice, and analyse this data with precision. With powerful display and capture filters, investigators can narrow down the traffic to only what is relevant, whether they are looking for suspicious IP addresses, specific protocols (such as DNS or HTTP), or signs of intrusion.

Wireshark also allows users to follow TCP streams to reconstruct full conversations, export packets for legal evidence or further analysis, color-codes traffic for easier interpretation of errors or anomalies, detect misconfigurations or malicious payloads and it allows integration with tools like Tshark and other forensic utilities for scripting and automation. On top of that, it runs on multiple platforms (including Windows, Linux, macOS, and more), and it is supported by a large community of developers and cybersecurity experts. However, it is important to note that Wireshark is a passive analysis tool that

doesn't prevent or stops attacks. Also, encrypted traffic limits the visibility unless encryption keys are available, or SSL decryption is configured. In summary, Wireshark is a key tool for looking at network traffic and helps investigators spot and understand suspicious activity on a network.

C. Blacklight

BlackLight is an integrated digital forensic tool developed by BlackBag Technologies (now part of Exterro). It is mainly designed to analyse data from Apple devices, including Mac computers, iPhones and iPads. The tool is widely used by law enforcement, digital forensic investigators, and cybersecurity professional. However, Blacklight works best on MacOSX systems, especially versions newer than Mavericks, but it can also run on Windows (32 bit and 64 bit) even if the tool is known to be less stable on Windows and more reliable on macOS, making it a better choice for investigators who works with Apple devices.

BlackLight offers many useful features for forensic investigations, it allows users to view files and folders from hard drives but also from SSD's and disk images. Thanks to this tool, users can recover data from unallocated space, where deleted files can still exist and can interprets system data such as Emails, web history (Safari, Chrome, etc...), messages (iMessage, SMS) but also calendar entries, maps and notes. BlackLight is especially good at reading and analysing Apple's HFS and HFS+ file systems by automatically finding and extracting key forensic data like user profiles, operating systems details, installed apps and device usage information. One unique feature, is that BlackLight uses the macOS keychain to interpret encrypted filesystem like EFS, making it easier to access protected data which is something many other tools cannot do easily.

The fact that it is built to analyse Apple devices, make it perfect when investigating a Mac computer involved in a cybercrime or data breach, an iPhone or iPad containing potential evidence and a disk image created from Apple system. If we are looking for where to find exactly a forensic artifact on macOS, BlackLight helps by locating and organizing that data automatically. Despite all these useful features, Blacklight can only support FAT, HFS and HFS+ file systems but not NTFS or EXT4. Also, it is less effective, on Windows or Linux systems and it is not an open-source, and its cost (around \$2,600) can be a barrier for smaller teams or students.

Comparative tools table:

Criteria	FTK Imager	Wireshark	BlackLight
Type of tool	Free tool made by a company	Open-source software	Paid tool made for Mac forensics
Best use	Making copies of hard drive and checking files safely	Watching and analyzing live network traffic	Checking Mac user activity and system info
Ease of use	Simple and lightweight, easy for beginners to use	Easy, but needs some knowledge about networks	Simple interface, works best for Mac users
Speed and Power	Fast and good at making exact copies	Very fast, works in real-time	Works well on Mac, sometimes slow on Windows
Scalability	Suitable for small to medium forensic tasks	Scalable for small to large network environments	Best for small-scale MacOS analysis, not ideal for complex or large datasets
Data type compatibility	Disk images, file systems, memory dumps	Network packets (PCAP, live traffic)	File systems, SSDs, memory snapshots, mobile and Apple data

II. CASE STUDY : SABOTAGE

As part of the investigation into the sabotage case involving Rich Daley at Cyfusion Mobile Manufacturing Company (CMMC), the goal was to recover deleted Maya design file from the computer used by Rich Daley. The company believes that Rich deleted the design before leaving, as part of the sabotage. To investigate this case, I followed standard forensics methods used by professional in the field to recover the deleted design file. The investigation required industry-standard forensic tools, a careful preparation of the crime scene, and precise documentation on each step to ensure that I am following a forensic procedure. In this section, I will describe in detail the different forensic tools that I will have to use, the forensic procedure followed including the creation of a forensic image, simulation and creation of the crime scene, recovery of deleted data and generation of a report.

The first and most critical step in any digital forensic investigation was to create forensic image of Rich Daley's disk using FTK Imager, which is a very important step because we never work directly on the original evidence since the image helps to preserve the integrity of the original data and allows us to investigate without deleting original evidence. FTK Imager is a reliable and widely used tool for creating exact, bit-by-bit copy of storage devices. This process ensures that the entire content of the drive is captured, including hidden and deleted files from the suspect's drive, slack space, and system metadata.

To create the forensic image, I had to select the source disk, configuring the output format which is E0 format in this case because it is most of the time accepted in the forensic community, and allow FTK Imager to read and copy every sector of the disk. Then, the forensic image was saved in a secure and read only format to avoid any accidental modification. In top of that, hash values were (MD5 and SHA1) were generated during imaging to conform the integrity of the image. This step is also very important because it ensure the investigation will not interfere with the original data and that all analysis is performed on copies derived from this image which serves to maintain proper chain of custody but also, most importantly, to ensure that the results are admissible in court.

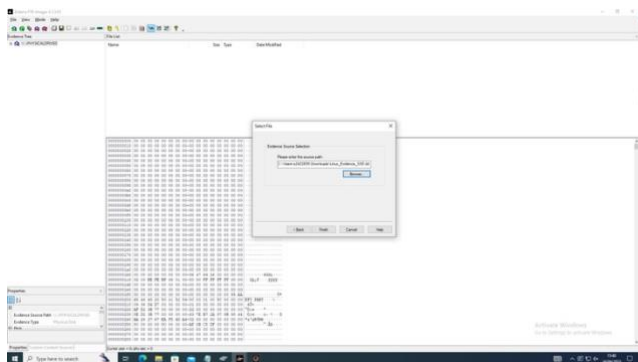


Figure 1: Creation of a disk image

To simulate the sabotage described in the scenario, I had to mount the copy of the forensic image using OSFMount with write access enabled, which allowed me to customize the disk files to build a realistic crime scene. I searched for an Autodesk maya file which I introduced to the mounted volume and then deleted this file manually through the file system, just as Rich Daley might have done. This step allowed me not only to build a realistic case study for file recovery but also to test the efficiency of forensic tool in a simulated real world case study condition.

The next step was to recover the deleted maya file from the original forensic image. To do so, I returned to the original forensic image and loaded it into FTK Toolkit, which is a professional tool that allows investigators to examine, index, and look for deleted files and to recover important data but also to view both deleted and active files. It is designed to load forensic images and navigate the entire file structure,

including allocated and unallocated space. The software can identify deleted files that are still present in the system's unallocated space and extract them, along with their metadata.

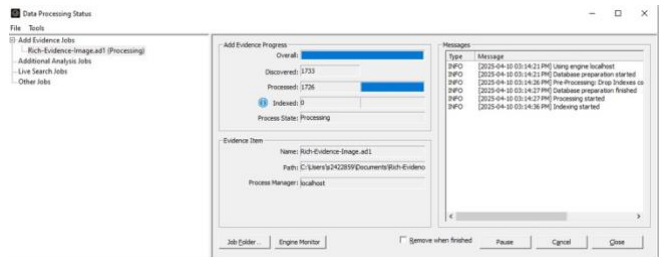


Figure 2: FTK Imager

Thanks to FTK's filter and search tools, I succed to find the file by filtering the content of the disk image display by looking for keyword searches and timeline analysis to find the file named "maya" that I was looking for.

When I finally recovered the deleted file, FTK Toolkit provided with metadata about the file, such as its original path, file name and extension, reation date with time, last modified time, last accessed date and deletion status. These informatins were crucial to confirm the file's authenticity which support the scenario of intentional data destruction by Rich Daley.

FTK Toolkit showed me multiple deleted files, I selected the deleted file that I was looking for and used the recovery function to extract it and verified its integrity.

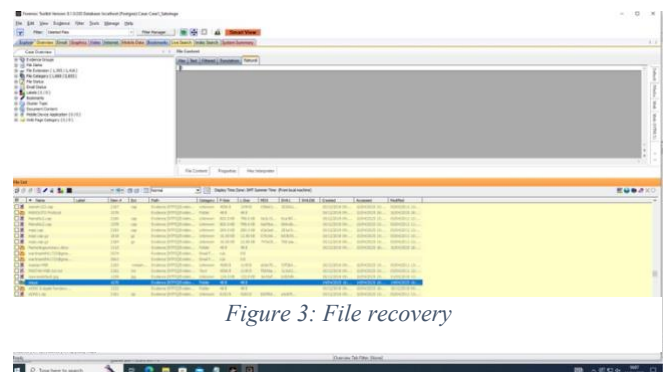


Figure 3: File recovery

After recovering the deleted file and simulating the sabotage scenario, I used FTK Toolkit's Report Build to create a professional forensics report that included summary of the evidence files recovered, some file detail (such as the size, path, hash value and timestamps), some case metadata (case name, analyst, date), screenshots and references tables. This FTK forensic report was exported to PDF format, it follows a typical structure required in legal or corporate investigations. This report serves multiple purposes such as the fact that it provides transparency into the methode used, supports the evidence presented and helps communicate the findings to CMMC managment or legal teams. The report is provided in a separate attachment.

I also provided a professional invoice to summarize the work completed during the case. It outlines the time spent on each task (including imaging, mounting, simulation, analysis, reporting and documentation) and the associated cost, simulating a real-world forensic billing process. Each task is listed with the number of hours worked but also with fixed hourly rate, resulting in a total cost. Creating an invoice helped me to understand how forensic services are priced and presented in a business context. This invoice is also provided as a separate attachment.

Thanks to all different forensic tools, the investigation has achieved its main objective: recovering and analyzing a deleted Autodesk Maya file believed to have been removed by Rich Daley. We succeeded to simulate the sabotage scenario, to recover the deleted file, and extract valuable metadata that confirms its origin and deletion timeline. All steps were done following standard forensic procedures to ensure that the evidence remained reliable and accessible. This case shows how digital forensics can play an important role in resolving incidents, protect data and support legal action.

REFERENCES

- <https://infonomics-society.org/wp-content/uploads/Evaluating-the-Efficiency-of-FTK-Autopsy-and-Mobile-Forensic-Tools.pdf>
- <https://iopscience.iop.org/article/10.1088/1757-899X/834/1/012034/pdf>
- https://www.sciencedirect.com/science/article/pii/S2666281722000129?ref=pdf_download&fr=RR-2&rr=938e954b0e563d75
- <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>
- <https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools>