

Computer Forensics Assessment

Task 1 - Research:

In Computer Forensics the Concept never changes, the Method is partially change but the Tools always change. Some tools are commercial while some are open source. There is no one size fits all tool. Various tools are used based on the type of case and the kind of evidence to be gathered.

You are required to conduct research on a minimum of three computer forensic tools, analyse them and use a table to categorise them. There is no limit to the number of tools you can research but it is recommended that you analyse and categorise the most frequent use tools by Computer Forensics professionals.

The concept of computer forensics is to “extract data from electronic devices to investigate and establish facts in criminal or civil courts of law”: It’s an axiom that never changes. The method may partially change but is divided mainly by this process: collecting – analyzing and presenting. Different tools may be used for the same method in this domain. Computer forensics is basically the science of identifying, preserving and presenting digital evidence. We will analyze and explain some of them since they are useful for professionals.

To have good documentation of the chain of custody, to produce sufficient proof for an investigation, the main concept is to collect data. We’ll mainly talk about Encase, Forensics Tool Kit (FTK) and Sherlock: Encase copies bit by bit forensically justifiable data, Forensics Tool Kit is similarly collecting and analyzing numerical proofs such as deleted files to reconstructs event, where Sherlock collects public data thanks to an Open-source Intelligence. Digital forensics process mainly follows those 3 main stages: Collection (Capturing data from devices and keeping it as less damaged as possible), Analysis (Investigating the data and find evidence), and Presentation (Documenting and findings for legal usages). All those processes lead to or create a numerical footprint, which is a key step in the investigation of a suspect or its victims. Let’s talk about the different tools we can use.

EnCase is a non-open-source commercial tool developed by Guidance Software. It is widely recognized in the law enforcement and corporate sectors and mainly used in criminal investigations and corporate internal investigations (like an employee misconduct, for example.). Its main strengths are the fact that it captures every bit on a disk thanks bit by bit to reconstruction from hardware (bit-level imaging) and allows deep recovery of deleted, or even corrupted files. It’s usable and admissible in court since it has a strong credibility for legal cases, supports various systems such as NTFS or FAT, making the presentation and flexibility viable. However, its main weaknesses are the fact that it has a high cost and may require high level skills to be used efficiently. It also integrates well with enterprise environments and can automate case documentation, which is very important in large-scale investigations.

Forensics Tool Kit, or FTK from its initials, is another commercial tool for computer forensics developed by AccessData. Similarly, to Encase, it allows reconstruction of broken and damaged

files. It is mostly used in civil litigations like recovering emails or contracts, and for analyzing quickly large datasets. And it has its own strengths: it has a better search performance with a very fast indexing of data, has a built-in data carving that allows the reconstruction of files, has a more user-friendly and understandable graphic interface, and supports email analysis and password cracking modules. However, it also has its own weaknesses such as requiring powerful hardware and may be overwhelming for beginners. That's what we will use during the second task. During internal audits for short audits or when facing data breaches that require timely action. It helps memory analysis and makes it suitable for volatile data investigations.

Sherlock is an open-source intelligence tool coded in Python downloadable on GitHub and focuses on gathering public information across multiple platforms. With that, we can easily build digital footprint of a suspect and its reconnaissance. It's good because it's free and lightweight, it does not use much performance and can scan hundreds of websites to find usernames quickly. It's also easy to install and customize. However, it has a lot of limitations since it only depends on public data and can only do profiling and footprinting since it does not have hard-drive forensic analysis. So only for online profiling. To give other open-source intelligences like Sherlock, you have tools such as The Sleuth Kit, Autopsy or Digital Forensics Framework. Sherlock is often used in the early phases of an investigation to quickly verify aliases or user profiles across platforms. But there's also Autopsy, for example, acts as a graphical interface for The Sleuth Kit, making it very efficient in court-friendly documentation.

We can see that each forensic tool has its specific advantages and disadvantages depending on the context. EnCase remains the gold standard for judicial investigations because of its credibility and depth of analysis. FTK is a powerful alternative when speed and user-friendliness are prioritized (particularly for civil litigation or internal reviews as it was said). And Sherlock is increasingly valuable for reconnaissance and initial profiling. Basically, Computer Forensics Investigations demands a variety of specialized tools. Professionals often combine multiple tools to balance accuracy for cost, ease and use. And the open-source tools complement heavier commercial solutions by expanding the investigation scope without increasing costs. By understanding the strengths and weaknesses of all different solutions, investigators can select the most appropriate tool sets to achieve what they need. In conclusion, a successful digital forensics investigation does not rely on a single tool, but on a toolkit of different elements adapted to the case. As threats and dangers evolve, the tools and methods of Computer Forensics should evolve, making it important to always learn about it and to be flexible, since it's essential in this field.

Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet Hardcover – 2011

“EnCase Forensics Overview”, OpenText: <https://www.opentext.com/products/forensic>

“FTK Overview”, Exterro: <https://azuremarketplace.microsoft.com/en-us/marketplace/apps/accessdata-group.ext-azftk-1.svr?tab=overview>

“Sherlock OSINT Tool”, GitHub: <https://github.com/sherlock-project/sherlock>

NIST, *“Guide to Integrating Forensics Techniques into Incident Response”, August 2006:*
<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf>

Task 2 – Case study: Sabotage

Rich Daley works in Cyfusion Mobile Manufacturing Company (CMMC) in London, UK. The company designs mobile phone interfaces and GUI for popular vendors. CMMC has become a market leader in its segment within a very short span of time. Rich was involved in the design of the latest Samsung Galaxy Z flip 6 phones. He managed to design a GUI interface for the phone which will rivalled soon to released Apple’s iPhone 17 Flip that was leaked. The company used Autodesk Maya to design the work. He was proud of his design and had secretly planned to offer the design to CMMC’s competitors. He contacted CMMC’s competitor 360tech and struck a deal for selling them the design. A week later, Rich resigned and left CMMC.

CMMC’s engineers were shocked to notice many of the mobile phone designs in the Rich’s computer were missing. Millions of pounds were spent on research and development of these designs, especially the new Samsung Galaxy Z flip 6 phone design. Rich had sabotaged the designs before he left the company. Rich’s system was never backed up due to high confidential nature of the work. Only Rich had access to these designs.

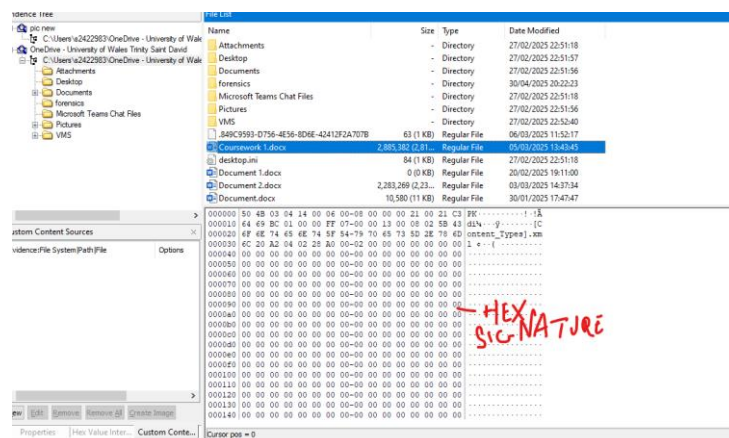
The CEO of CMMC Ms Ker Walters was very disturbed. CMMC planned to patent the designs, so that they can license the technology to mobile telephone manufacturers around the world. The company stands to lose millions of pounds if the designs are leaked out.

Ms Ker Walters has read success stories of computer forensics investigation around the world. She hired Troy Simpson, a CHFI and CEH certified professional, to investigate and provide evidence of Rich’s sabotage, and retrieve the data.

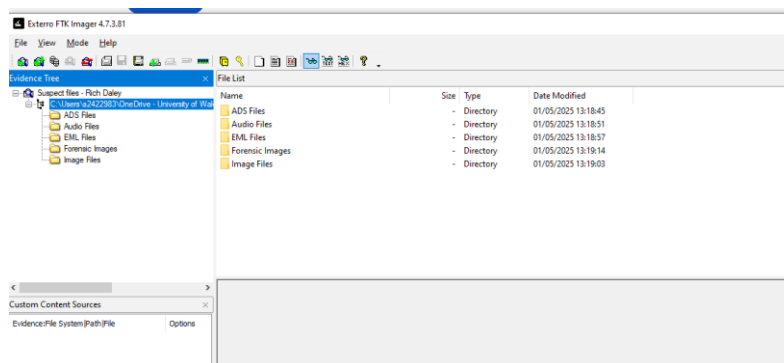
The objective of our report is, in context of digital investigations, to identify, preserve and analyze electronic evidence of what could have been in the case study of sabotage. Whether in criminal cases, in company cases, or in academic investigations, the ability to retrieve digital data in a verifiable and reliable way is crucial for future analysis and case investigation conclusion in juridic situations. We will try to demonstrate the practical application of forensic analysis through FTK Imager, which is, as said in the first part, recognized in digital forensics. The project involved imaging a physical or logical storage drive (that can be source of evidence) and

One of the key goals here was to explore the ability to explore corrupted or lost data from an unallocated disk space, where suspects can attempt to delete or hide digital evidence. In this process, I met both technical challenges but also learning opportunities. Especially because of the large volume of files and fragmented and unreadable datas. But with this I gain experience and learn the importance of careful planning and tool mastery, and of course patience for investigation in forensics. I'll explain the challenges, steps and tools used and explain them during the process and the results I've got. While not all expectations led to conclusive recoveries, the experience reflects the realities of what forensics work can be. Where precision, persistence and attention to digital footprint are keys and makes difference between success and failure.

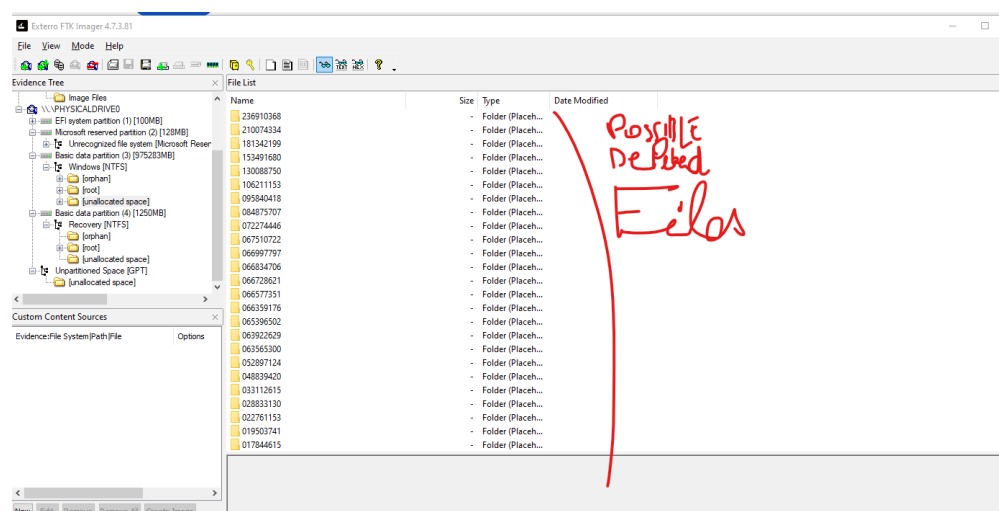
Then, to test the tool we just put some files as adding evidence item for testing. In my case, I added some pictures and written files on FTK and received a hex signature of some of them.



In my situation, I created a folder called “Suspect files – Rich Daley” with files made from Forensics labs classes. On that case, it permits to create a pseudo evidence preparation to simulate what a suspect disk could look like and analyze. I deleted all animal related images for example to find them later inside FTK, let’s take a look:



What we do next is to add evidence to its own folder for the investigation. To do that, we can try to look up the previously. I tried to add the physical drive and eventually find unallocated files and restore them by putting them in the evidence folder. In that case, in Basic Data Partition folder I went to the unallocated space to find some possible deleted folder. Those files need to be recovered but lacks information after their deletion. We’ll try to recover those by exporting them again and reconstruct them to build more credible evidence and data finding to build Rich Daley’s folder. Those files are mostly described as numbers and hexadecimal signatures. To determine if we are checking a previous image, we need to look at some part of the file information. For example, PNG and PDF have specific signatures such as 89 50 4E 47 0D 0A 1A 0A and 25 50 44 46. We imagine that the phone models will be the animals pictures that I’ve deleted and threw from the bin.



I first collected data in a forensically sound manner by acquiring a digital image of the storage device and creating my own file called “Suspect Files – Rich Daley”, made with fragments of elements found in “Evidence” inside on the Forensics Tools lab that we did before doing the



The image destination cannot be on the disk being imaged.

OK

Add Overflow Location

[illegible]

In a professional investigation, stricter protocols would be followed. In this project, although performed under limited conditions, the process served as a realistic introduction to forensic acquisition methodology where preservation always comes before investigation.

Once the disk image had been successfully acquired using FTK Imager and saved in AD1 format, I proceeded to the analysis phase within FTK Toolkit. The primary goal of this step was to identify traces of deleted content and examine digital artefacts that could be considered evidence in a real forensic investigation. Opening the ad1 file from the physical drive revealed a large and complex file system. As this was a school computer with multiple partitions and users, the system included thousands of files that were not useful to my activity. In what I had the “Unallocated Space” was where I theorized as where I can find my file, since that’s where deleted data typically resides. FTK automatically categorized files based on their location, or file system artefacts.

But the unallocated space also contained thousands of unnamed files, often represented by sequences of numbers and without readable file extensions. These are what seems to be parts or fragments of deleted data not fully overwritten, but it might have contained media files or partial documents. However, without precise knowledge of their original names or extensions, the process of finding a specific deleted file was complicated since it means I would have checked all the thousand file precisely one by one. I tried to replicate a real case scenario by intentionally deleting all animal-related image files from the desktop of the Windows system from the Forensics tool Evidence folder. Despite this, it was difficult to clearly identify all this specific kind of image file among the overwhelming number of fragments present in Unallocated space. This highlighted one of the biggest challenges in forensic recovery: deleted data can be overwritten, fragmented or unreadable, making it difficult to reconstruct fully.

FTK does offer features to sort and categorize files by type, preview file headers, and search using known hash values or file signatures. I attempted some of these, but due to the volume of data, system restrictions, and lack of distinctive identifiers, I had difficulties to solve all the hided files, but in real situation with more experience could have been easier for me to recover them, even if I was on the right path. However, I was able to explore how FTK tracks deleted content using artefacts like “MFT” entries, timestamps, and metadata. While FTK Toolkit and FTK Imager provided a strong introduction to the forensic investigation process, I quickly became aware of their limitations — particularly when working on a shared and heavily-used system. The overwhelming volume of residual files, many of which had no clear identifiers, made the recovery of a specific deleted item difficult and time-consuming.

While this task was educational, it reflected how messy forensic work can be and gave me insight into how even small details like user accounts, partitions, and logical structure can affect data recovery.

Several improvements could have been made by incorporating different forensic tools or combining FTK with another software. For example, Autopsy offers a much more user-friendly interface for timeline analysis, keyword searching, and deleted file recovery. It also provides file

carving, which is the process of reconstructing deleted files based on known file signatures, even when metadata is missing. This would have made it easier to locate image files I deleted during testing, especially by filtering for PNG extensions in my case. Another potential tool is Recuva, which is less sophisticated than FTK but very effective at scanning specific folders and recovering recently deleted files in a simpler desktop interface.

Finally, employing a Windows (or Linux in the continuity of the module) virtual machine with a clean environment and deleting files intentionally before imaging would have provided a more controlled and pedagogically efficient case. It would isolate the files of interest, reduce irrelevant data, and make the process more focused. Beyond technical skills, this task also put into practice my understanding of lessons I saw in class like data integrity, chain of custody, and evidence admissibility. These are foundational in computer forensics and must guide every step, from acquisition to reporting. I didn't have success in data recovery, but I was able to document my process which is essential in forensic work.

In conclusion, this project challenged me to engage with tools and methods I was not used to. In a professional context, I learn that it's more preparation, that there is importance in the nuances of digital artefacts, and some learnings about role of forensic software in missions such as solving cases like this one.

Brian Carrier, File System Forensic Analysis. Addison-Wesley – 2005

Bill Nelson, Guide to Computer Forensics and Investigations. Cengage Learning – 2018 (for the recommended 6th edition)

Guide to Integrating Forensics Techniques into Incident Response:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

AccessData / Exterro FTK Imager User Guide: <https://accessdata.com/product-download/ftk-imager-version-4-2>

Palmer G, A Road Map for Digital Forensic Research (In Proceedings of the Digital Forensic Research Workshop (DFRWS)) - 2001

Slenth Kit / Autopsy - <https://www.slenthkit.org/autopsy/>

DFIR Training Resources (Digital Forensic and Incident Response - <https://www.dfir.training/>

Digital Forensic Wiki - <https://forensics.wiki>