

THE COPARISON OF THE COMPUTER FORENSIC TOOLS

Yueliang HAN

Student University of Wales Trinity St David, Swansea, Wales
2422998@student.uwtsd.ac.uk

Abstract:

With the acceleration of the digitalization process, the means of cybercrime are becoming increasingly intelligent and hidden, making it difficult for traditional investigative methods to meet the challenges of technologized crime. Computer forensics technology as the core means of revealing the truth of digital crime, the choice of tools is directly related to the effectiveness of evidence and investigation efficiency. This paper focuses on four mainstream forensic tools, Autopsy, FTK, Volatility and EnCase, and systematically compares them from the dimensions of functional coverage, judicial recognition, and technological threshold to provide practical references for the selection of tools in different scenarios.

Keywords:

Computer forensic, EnCase, FTK, Autopsy, Volatility.

I. Introduction:

In the current era of highly developed informationization and intelligence, digital technology has been fully integrated into all aspects of human society. Whether it is the operation of enterprises, government governance, or personal work and life, almost all key behaviors and data rely on computer systems for processing and storage. The wave of technology continues to drive social productivity and efficiency to a new level, and the convenience and changes brought about by digitization can be said to be unprecedented.

However, technology itself has neutrality, it can be used for positive innovation, but also may be used by lawless elements as a means of crime. Especially in cyberspace, with the continuous upgrading of attack methods, computer crime has gradually shown a trend of “intelligence, concealment, automation”. Hacking, ransomware, data theft, digital forgery and other behaviors are endless, these new types of crimes not only cause huge economic losses to enterprises, but also a serious threat to national security and social trust.

Traditional means of investigation and law enforcement due to the lack of complex digital environment of the depth of analysis capabilities, often difficult to effectively identify, trace and extract electronic evidence. Therefore, “computer forensics” technology came into being, and rapidly developed into an important and indispensable means of support for network security and judicial investigation. It covers the extraction, analysis, verification and presentation of data in electronic devices, and the core purpose is to restore the truth of the incident under the premise of legal compliance, and to provide a judicially recognized chain of evidence.

In practical application, the choice of computer forensics tools directly affects the efficiency of the investigation, the completeness of the evidence and the legal admissibility of the Summary. Different tools vary in terms of functional scope, applicable scenarios, learning threshold, processing performance and so on. Some tools are good at disk analysis, some focus on memory forensics, and some place more emphasis on graphical operation or automated processing flow. For investigators, understanding the core capabilities, advantages and disadvantages, and limitations of the use of these tools will help them make reasonable choices in different case contexts and enhance the professionalism and accuracy of forensic work.

I have selected four representative computer forensic tools - Autopsy, FTK, Volatility and EnCase - and compared them through literature research, functional comparison, and from various perspectives, such as technology, direction of application, difficulty of use, and legal acceptance, in the hope that those who need them can get a better understanding of their core capabilities and limitations. We hope to provide reference for those who need it.

II. FTK:

What is FTK:

Forensic Toolkit (FTK) is a commercially available computer forensics software developed by AccessData and currently taken over by Exterro for maintenance and continuous optimization. It is widely used in scenarios such as law enforcement agencies, corporate security departments, forensic analysis labs, etc. Its main function is to perform in-depth forensic analysis of storage devices, including file recovery, email extraction, registry analysis, keyword searching, file carving, etc. FTK has been regarded by the industry as one of the most comprehensive and reliable commercial forensic solutions.

Features:

One of the most important features of FTK is that it is accompanied by another important tool -- FTK Imager, a powerful disk image acquisition tool that makes a complete copy of the hard disk contents and generates a legally valid forensic image. These image files can be saved in a variety of formats and a hash value is generated to verify data integrity, thus ensuring that the image has not been tampered with. The software also has the ability to analyze the registry, scan for file fragments in the loose space of the disk, check emails, check for deleted files, search and filter files, categorize images, documents, audio, video and other files.

Advantages of FTK:

FTK's functions are very comprehensive, and the analysis speed is very fast, it can quickly analyze the imported content and produce corresponding tables for people to access, and different kinds of files will be quickly categorized and organized. Unlike other computer forensic tools on the market, FTK can crack passwords and can be used to decrypt files. [2] In addition, another major advantage of the tool is that even if the computer crashes during use, the information will not be lost [2], The full version of FTK provides the ability to mount the acquired image as a physical drive or logical volume, which allows analysts to view the contents of the image as if accessing a real disk, with a user-friendly interface. [1] Moreover, FTK can automatically generate a report on a single Case, which is very convenient and fast. At the same time, FTK is widely recognized by the court as a legal computer forensics tool due to its output format and report structure in line with the requirements of most legal procedures, which also reflects his professionalism and reliability. FTK uses a graphical user interface (GUI) design that allows the user to complete most operations by means of clicks and menu selections, lowering the learning threshold.

Disadvantages of FTK:

However, FTK is too expensive and may be unaffordable for students, individual researchers, small and medium-sized organizations. There are also organizations with limited budgets for

whom open source tools such as Autopsy or Volatility are more attractive.

FTK is affected by the performance of the hardware, which requires more computing power. If the host computer is not powerful enough, it will slow down the progress of forensics.

Moreover, many advanced features of FTK need to be expanded by themselves, which requires a strong knowledge background and is not very friendly to beginners.

Summary:

FTK is an extremely powerful commercial computer forensics tool widely used in judicial and corporate investigations. It is stable and efficient, although the cost is not low, but for digital investigations in demanding environments, it is irreplaceable in terms of accuracy, completeness, and legal recognition.

III. Autopsy:

What is Autopsy:

Autopsy is a full-featured open source digital forensics platform developed by Sleuth Kit Labs. It is presented in a graphical user interface (GUI) that simplifies the otherwise complex command line operations and improves usability and user experience. Its underlying reliance on the core engine is the well-known file system forensics engine The Sleuth Kit (TSK)[3]. As a powerful alternative to commercial forensic tools, Autopsy is a fast, thorough, and efficient solution for hard disk investigations, and is constantly evolving to meet the different needs of the times.

Features:

Autopsy offers highly modular digital forensics features that cover a wide range of categories from disk analysis to user activity reconstruction, including timeline analysis, file recovery, registry parsing, browser history tracking, email viewing, keyword searching, hash value verification, and even image recognition and video extraction. In addition, Autopsy can collect and organize evidence to generate a preliminary report.

Benefits of Autopsy:

The technical foundation behind Autopsy is The Sleuth Kit (TSK), which is a suite of file system forensic tools created by Brian Carrier. It is portable, extensible, and open- source.[1] Carrier developed it to overcome the limitations of The Coroner's Toolkit, providing cross-platform support and improved usability.[3] This is both a reflection of Autopsy's expertise and one of the reasons why Autopsy is so widely used.

Autopsy is an open source digital forensics tool with a user-friendly interface, which means it is more suitable for beginners and small businesses. At the same time, Autopsy has taken the initiative to provide systematic learning materials and training courses on their web page, so that beginners won't be confused, and it's easy for newbies to get started quickly.[5]

Moreover, Autopsy allows users to freely extend the program with plug-ins, so that they can add modules according to their needs. This also encourages more communication between beginners and experienced people. It is maintained by the Sleuth Kit Foundation and users around the

world, and was updated again in January this year to attract newcomers and bring a better and more active community environment.

Disadvantages of Autopsy:

Autopsy does not support in-memory forensics, which means that it cannot handle data generated temporarily by the computer, and cannot recognize active processes on the system, such as reverse shells, hidden processes, or some suspicious services. This also makes it impossible for Autopsy to restore unsaved user activity.

Autopsy's performance is adequate for everyday use, but when it comes to large amounts of data, it is not comparable to commercial computer forensic tools (such as FTK or EnCase), and the response time is significantly slower, especially when dealing with terabyte images or complex file system analysis, where its processing power is relatively limited.

Autopsy generates reports in a relatively basic format that is not as complete as EnCase or FTK, and is therefore less legally binding.

Summary:

Autopsy is a cost-effective computer forensic tool (after all, it's technically free) that is stable, efficient and feature-rich. The tutorials on the official web page and the active community make it easy for beginners to get started.

Despite its limitations in memory analysis and large-scale case processing, its overall capabilities can be improved by combining it with other tools. The technical engine behind it, The Sleuth Kit, has been widely used in academic research and real-world cases, making Autopsy reliable and an ideal platform for learning and practicing forensic skills.

IV. EnCase:

What is EnCase:

EnCase is a commercial digital forensics tool developed by OpenText, formerly owned by Guidance Software and used by law enforcement agencies worldwide. It is known as one of the "most court-approved" forensic tools, and its output report format, operational procedures, and chain-of-evidence records are all in line with international judicial standards, making it one of the tools of choice for corporate security audits, government investigations, and legal compliance checks.

Features:

EnCase's operation is based on project workflow, and users can complete forensic tasks step by step: from data collection, identification of suspicious activities, metadata extraction to automatic generation of audit logs and investigation reports, which greatly guarantees the rigor and repeatability of investigations. It allows users to create drive images without changing the contents of the drive and calculate hash values for subsequent verification. It can locate hidden drives or partitions within a drive, as well as hidden files or media that cannot be found by some other programs [2]

Benefits of EnCase:

Encase has been used by law enforcement agencies worldwide. There are recognized by legal agencies around the world, with very strong professionalism and reliability. A case in point is that of the terrorists who bombed the Indian Parliament on December 13, 2001. Investigators in India used Encase software to find evidence that the laptop of a terrorist suspect, Mohammed Afzal.[2] EnCase is very comprehensive, with integrated disk analysis, email recovery, registry parsing and other modules, supporting a full range of forensics from traditional hard drives to smartphones, and even remote data acquisition for forensic analysis. Moreover, in large-scale investigations, EnCase supports users to modify the script rules by themselves, which can significantly improve the efficiency of work. So it is very suitable for large-scale enterprises. And EnCase also uses a graphical interface structure, looks clear and practical.

Disadvantages of EnCase:

EnCase's license cost is very high and is only suitable for large enterprises with very large budgets. It is difficult for SMEs or individual users to afford its high license cost.

Moreover, EnCase's hardware requirements are not easy, usually requiring a mainframe computer capable of handling terabyte-sized files. If the processor or memory performance is insufficient, the analysis process may lag or be interrupted.

Despite its user-friendly interface, EnCase's full-featured modules, scripting mechanisms, and advanced configurations require a long professional training cycle, making it very unfriendly to beginners.

Summary:

EnCase provides a professional, systematic, and compliant full-process solution for the world, so it is irreplaceable in judicial compliance and complex case handling. Its rigorous evidence management processes, automated scripts and cross-platform support provide investigators with an efficient and reliable full-link solution. Despite the high cost and steep learning curve, its professional value in government, finance and other high-security demand scenarios is untouchable.

V. Volatility:

What is Volatility:

Volatility is an open source memory forensics tool originally released in 2007 and developed, maintained and updated with the support of the Volatility Foundation.[4] Written in Python, Volatility is commonly used to detect malicious code, analyze active processes, and discover hidden driver and network connection information.

Features:

Volatility's core mechanism is a plug-in architecture that allows users to invoke different modules from the command line to perform multi-dimensional analysis of a memory dump. Volatility is used to obtain “volatile” data such as active processes, kernel modules, network connections, dynamically loaded malicious code, and so on. Volatility also supports exporting analysis results

to standard text or CSV format for further organization, archiving and reporting.

Benefits of Volatility:

The biggest advantage of Volatility is its focus on memory mirroring. Compared to traditional hard disk forensics, Volatility is able to capture runtime information such as active processes, memory injections, remote sessions, etc., which are difficult to find with traditional tools.

As an open source project, Volatility is free for users to download and use, making it suitable for teaching and research environments. And it has a huge plug-in library, which is updated by the community for a long time and covers almost all key dimensions related to memory.[5] The official website and community provide detailed user guides, plug-in documentation, usage examples and practical demonstrations, making it easy to get started and advanced learning.[4] Volatility supports multiple operating systems (e.g. Windows, Linux, macOS) and multiple memory dump formats. This cross-platform compatibility greatly enhances the flexibility and adaptability of Volatility in real-world investigations.

Disadvantages of Volatility:

Volatility does not have a graphical user interface (GUI), and all operations require parameters and paths to be entered on the command line, which requires high requirements for memory structure, plug-in usage, command parameters, etc., and a large learning cost for beginners.

Volatility's output results are primitive, often requiring users to understand the Windows/Linux kernel mechanism and memory distribution to make reasonable judgments, and often need to be combined with FTK, Autopsy and other disk tools to cross-validate.

Summary:

Volatility is an indispensable memory analysis tool in the field of digital forensics. With its focus, open source and professionalism, Volatility has been widely adopted in security research, malware analysis, combat attack and defense, emergency response and other scenarios. Despite its learning difficulty and lack of visualization, Volatility has unique advantages in revealing runtime attack behavior and countering advanced threats.

VI. Conclusion:

In the field of digital forensics, different tools show different advantages and applicability according to their design goals, usage scenarios and authorization methods. Open source tools such as Autopsy and Volatility are characterized by low cost, active community and flexibility; Autopsy has a complete graphical interface, is suitable for teaching and small to medium-sized cases, and is particularly good at file system analysis and timeline reconstruction. Volatility, on the other hand, focuses on memory forensics, and although it operates on the command line and has a steeper learning curve, it has irreplaceable value in malicious code analysis, APT detection and emergency response.

Comparatively speaking, commercial tools such as FTK and EnCase are more focused on “court admissibility” and “full integration”; FTK has the advantage of high-speed indexing, email analysis, and password cracking integration, which is suitable for law enforcement scenarios that need to analyze massive amounts of data quickly; and EnCase is the industry's most popular tool. EnCase

is the industry-recognized standard tool for justice, with its evidence management process, EnScript, and reporting structure widely adopted by legal agencies. Despite their high cost and resource consumption, their level of professionalism and stability are important to enterprises and government agencies.

In summary, no single tool can handle all types of forensic tasks. We should choose the most appropriate combination of tools based on the goals of the investigation. The use of a reasonable combination of these tools can help build a more comprehensive, controllable and legally supportive digital forensics system.

Reference:

- [1] R. Boddington, *Practical Digital Forensics*, Packt Publishing, 2016.
- [2] M.-H. Maras, *Computer Forensics: Cybercriminals, Laws, and Evidence*, 2nd ed. Burlington, MA: Jones & Bartlett Learning, 2012.
- [3] The Sleuth Kit, *Autopsy - Digital Forensics*. [Online]. Available: <https://www.autopsy.com/>. Accessed: May. 1, 2025.
- [4] The Volatility Foundation, *The Volatility Framework: Memory Forensics*. [Online]. Available: <https://volatilityfoundation.org/the-volatility-framework/>. Accessed: Apr. 29, 2025.
- [5] C. Altheide and H. Carvey, *Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on Target Systems*, 1st ed. Burlington, MA: Syngress, 2011.

THE INVESTIGATION REPORT OF THE LOST
DESIGN FILES FROM CYFUSION MOBILE
MANUFACTURING COMPANY(CMMC)

Investigator:

Troy Simpson

Tool Platform:

FTK Forensic Toolkit

Date:

02.05.2025

Background:

CMMC (Cyfusion Mobile Manufacturing Company) is a company that provides interface and GUI design for mobile device manufacturers. Rich Daley, the company's core designer, suddenly deleted all the GUI design files for the Samsung Galaxy Z Flip 6, a project he had been involved in developing, before resigning. As the project represented a significant investment and future commercial licensing value for the company, and Rich was the only possible file holder, the incident posed a serious threat to the company.

Our Target:

Most volumes contain a large amount of potentially interesting data beyond of the viewable, allocated files on a mounted file system. This includes several categories of "deleted data." :

Deleted files, which its recovery only need to recording the relevant file name and metadata structures and then extracting the data units.

Orphaned files, which are similar to deleted files but can't find the direct link between the file name and the recovered data,

Unallocated files, which can only recovered by carving the data units that have not yet been reused from the unallocated space of the volume.

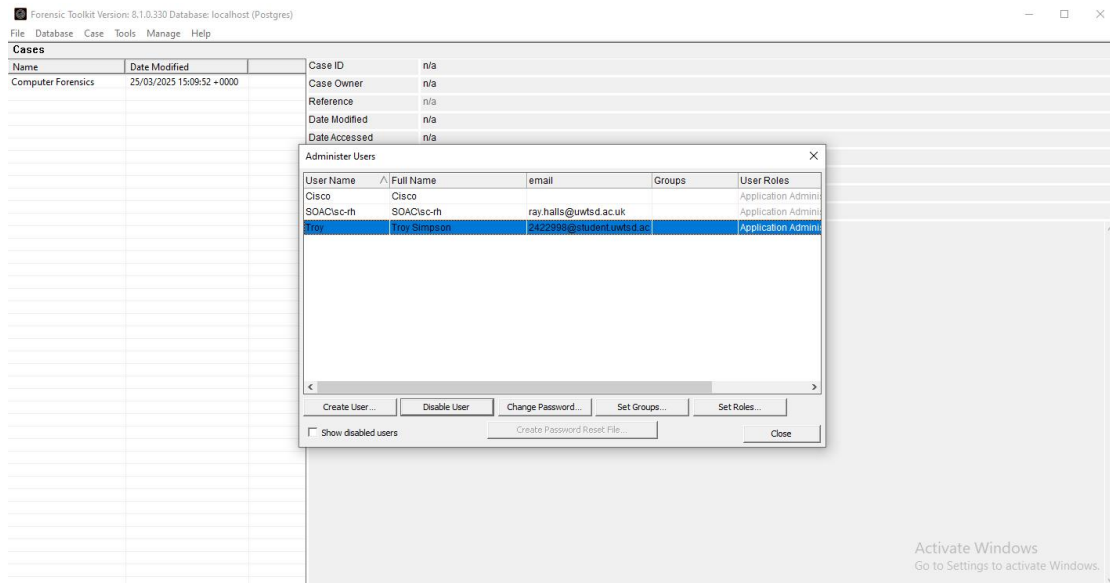
and Overwritten files, which is impossible to fully recover, but partial recovery may depend on the extent of overwriting.

Therefore, we need to figure out what kind of files are the lost designs of Samsung Galaxy Z flip 6 phone in the Rich's computer and try to recover them by FTK tools.

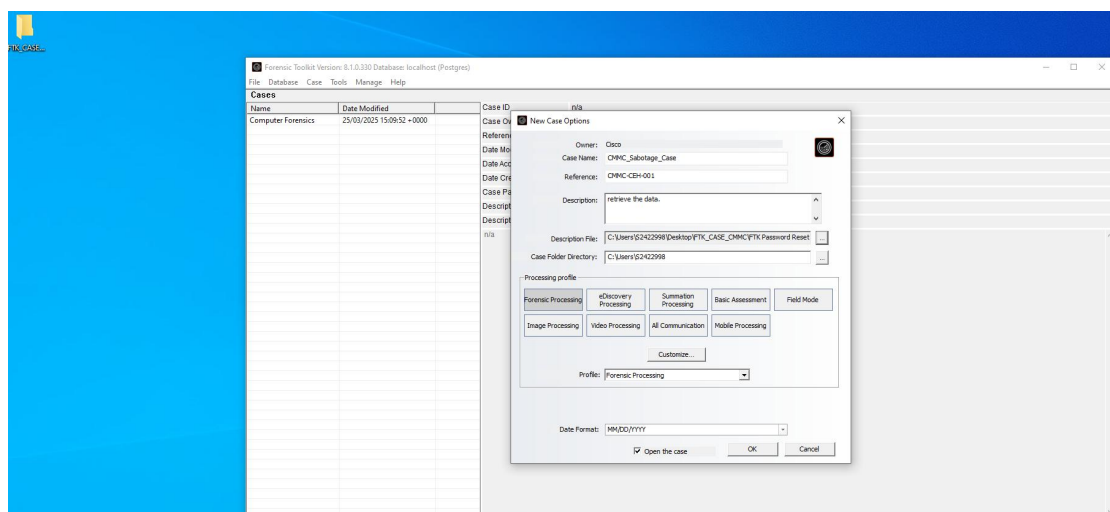
Also, we need to use FTK tools to investigate there was a possibility of a data breach, and generate a report that is recognised by the court.

My working procedures:

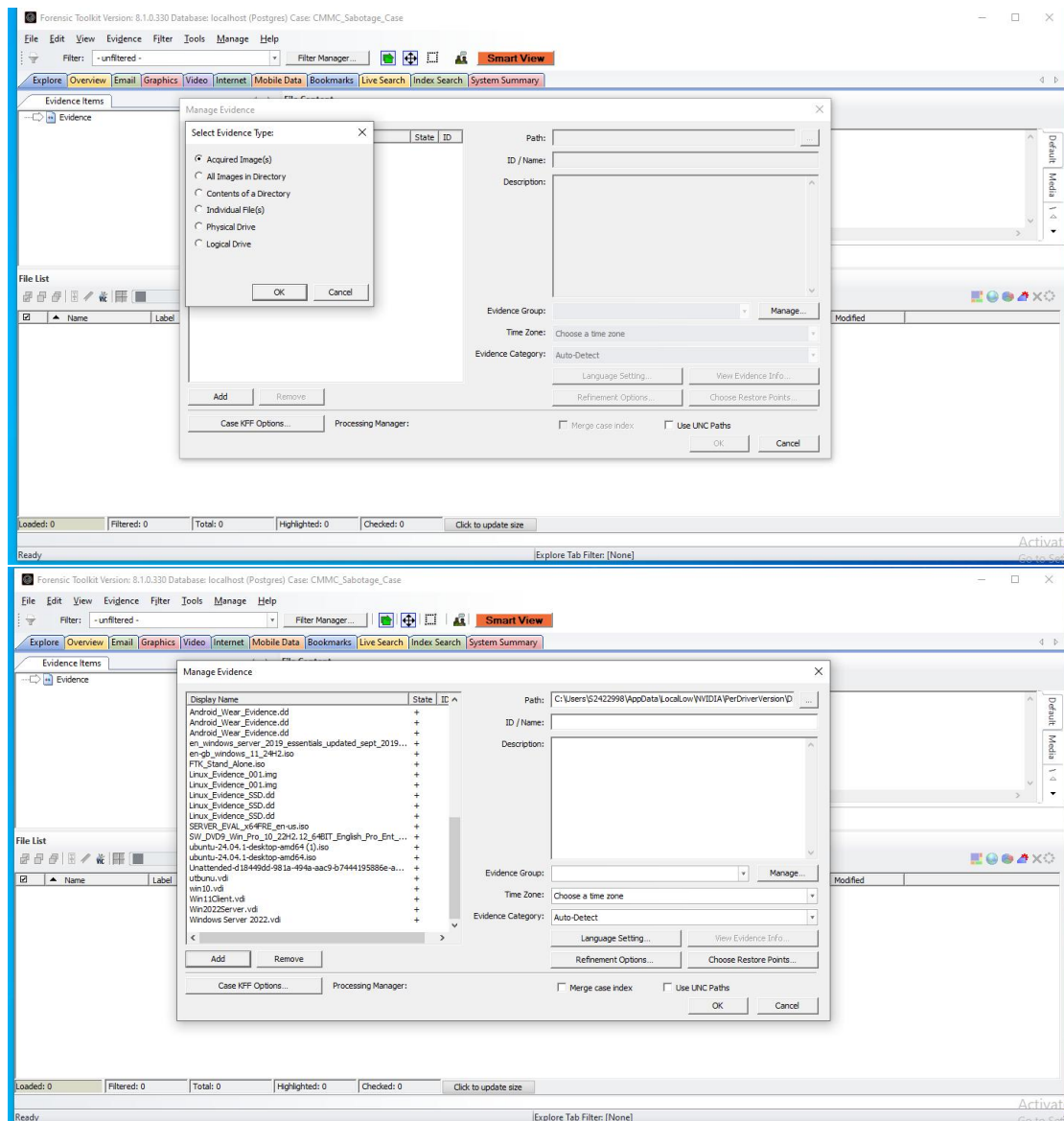
Download all the evidence file which be given by the shared OneDrive, obtain an image of Rich Daley's computer. Log in the FTK by using the account and the password given by the teacher and add an Administer User which called Troy Simpson and give the Troy all the permission of the User Roles.



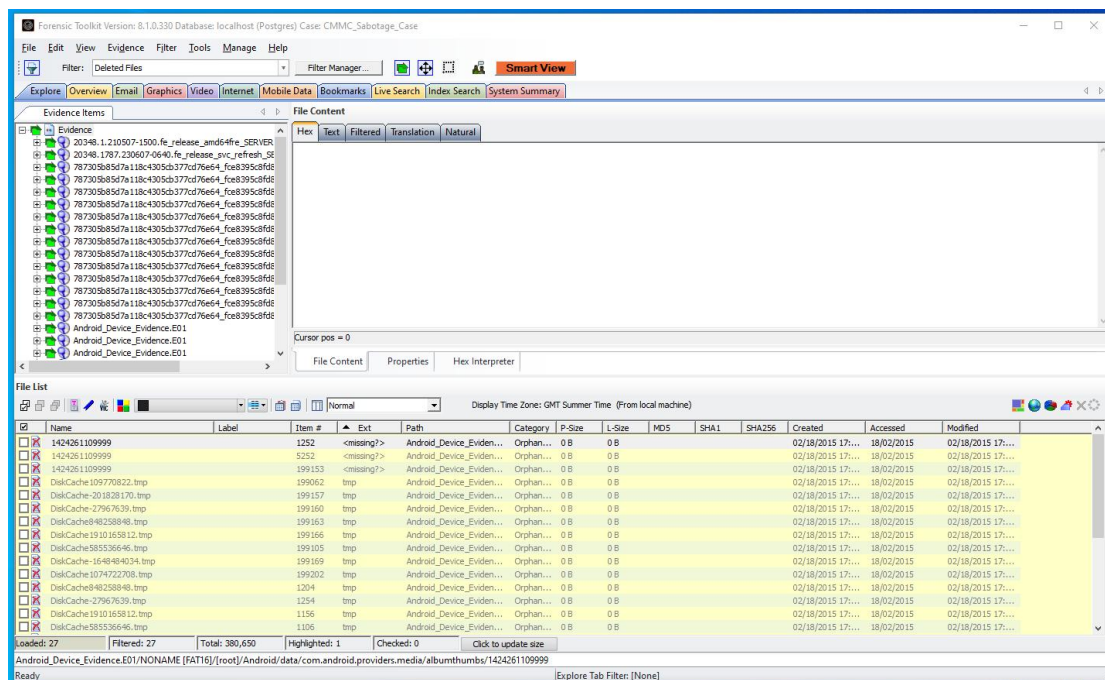
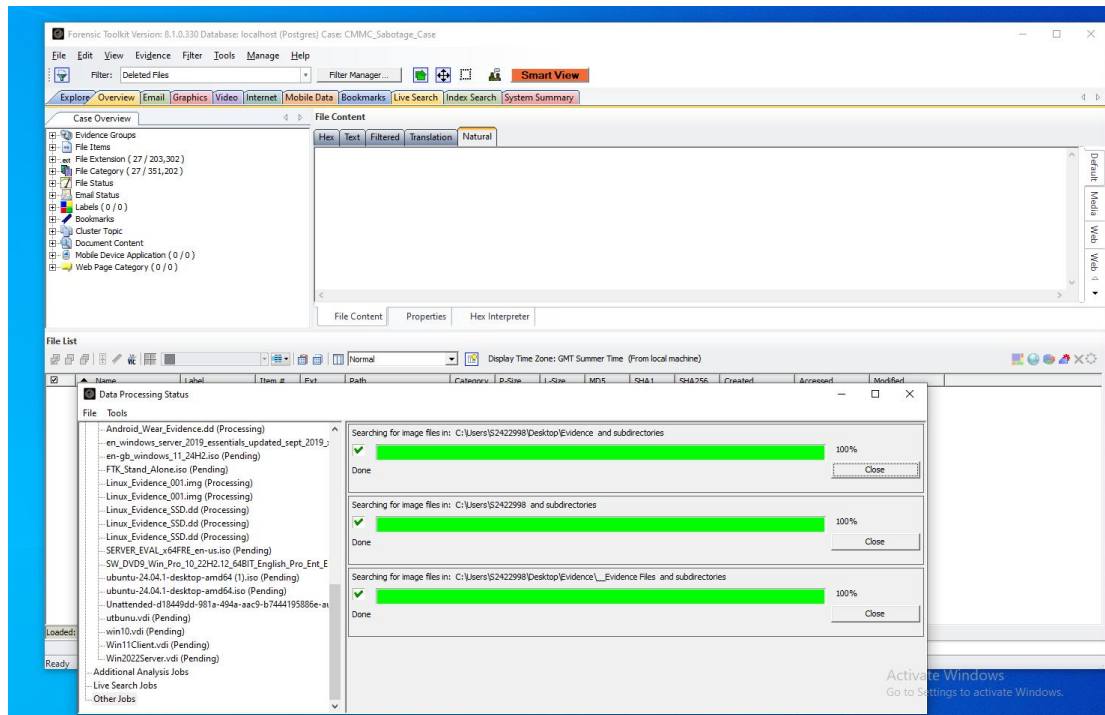
Add a new Case and title it 'CHNC_Sabotage_Case', fill the reference and write some brief description of the Case. Then, give it the Description File and Case Folder Directory.

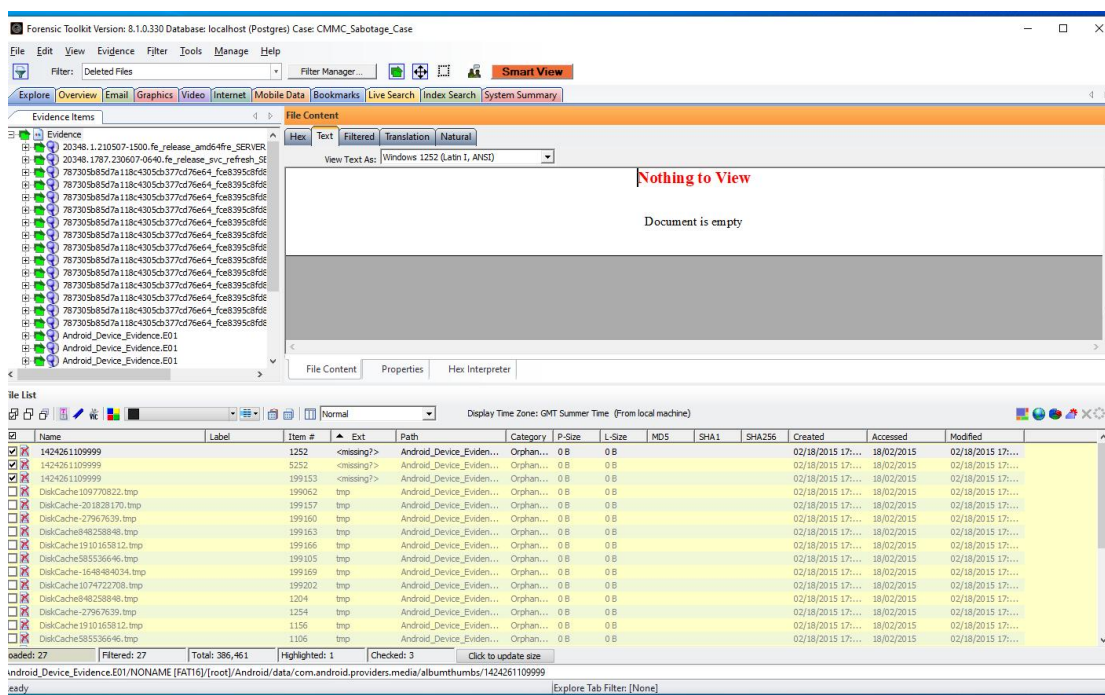


I use "all images in Directory" feature, add all extracted evidence files were imported into the case. FTK completed automatic indexing successfully.

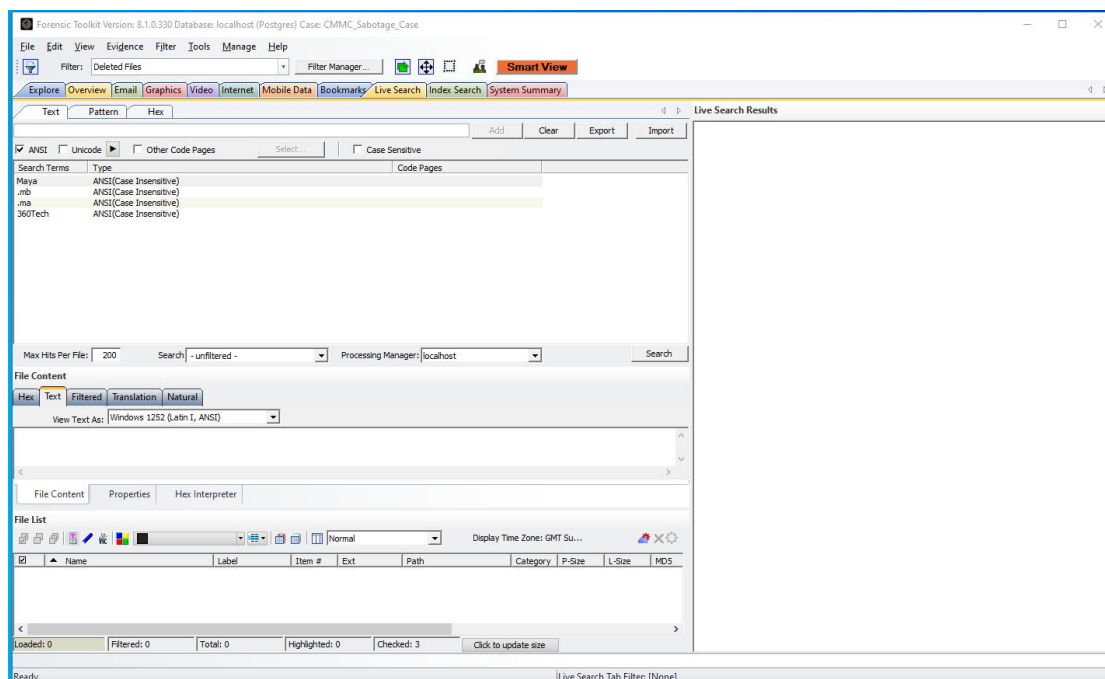


After successfully importing all the evidence files and completing the automatic indexing, I first tried to enter the 'Explore' module to check the 'Deleted Files', and found that there were indeed deleted files in the system, but most of them were marked with the extension 'missing?'. This means that the structure of these files has been corrupted, with header information or directory indexes missing, and the original format cannot be recognised properly. In this case, it is usually not possible to directly determine whether the file is the target design or not, but these remnants can still be used as preliminary clues for further analysis.

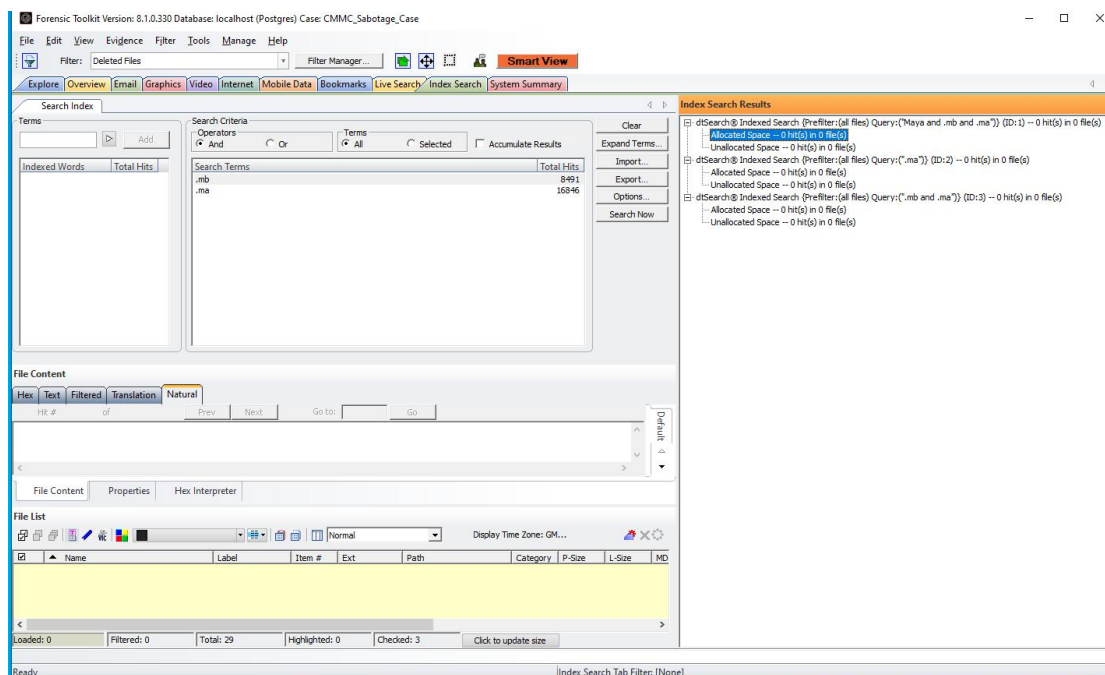
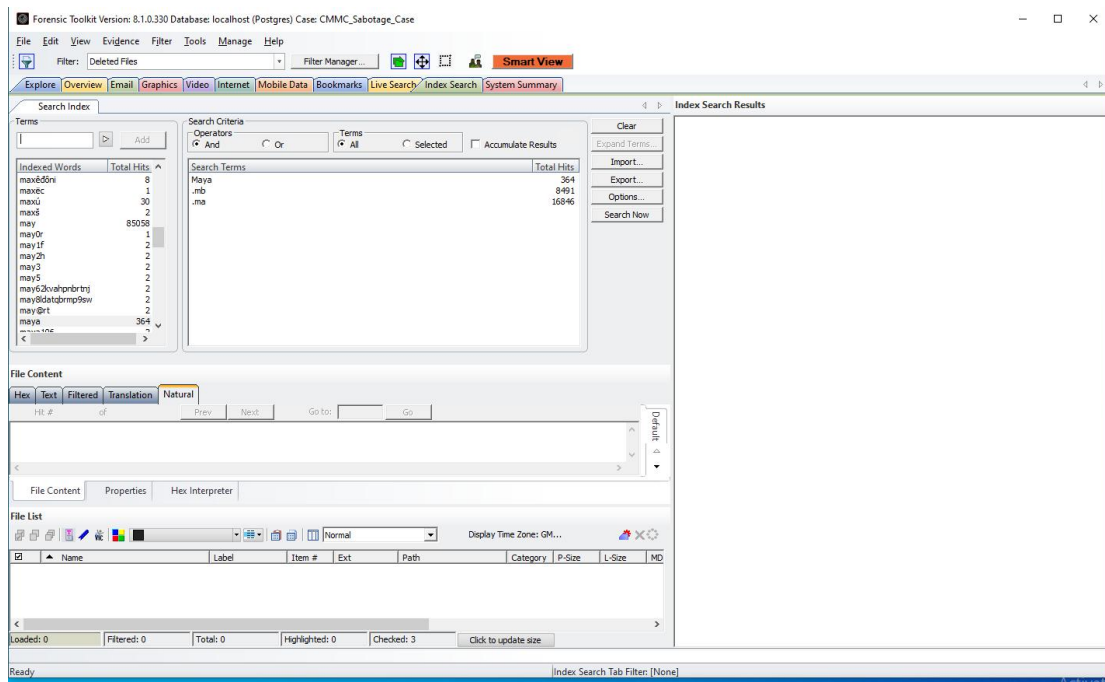




I then tried to use FTK's 'File Status' filter to focus on Unallocated Space, Slack Space and Fragment blocks. These areas could theoretically have data left over from before they were deleted or overwritten. During this process, I turned on the file preview function to see if I could restore some of the images or Maya-related file fragments, but most of the data could not be recovered due to fragmentation or unstructured content.



Based on this, I continued to use FTK's built-in 'Index Search' function to try to locate potential content through keyword search. Considering that the target files may involve terms such as 'Maya', '.mb', '.ma' etc., I used multiple keywords to search for them. However, only a few strings were found in the index results that were relevant to the search terms, and there were no recognisable design files, suggesting that the data may have been completely overwritten.



Even though I could not locate the complete target file, I still made an attempt to recognise the fragments, i.e. extracting the original data blocks from the unallocated space by using FTK's 'Carving' function, in the hope of recovering the complete or partially visible content from them, PDF, DWG, etc., so I set a variety of file extensions as target types for scanning. As a result, some headless image fragments were extracted, but none of them had design logic or engineering data structure, and it was impossible to judge that they were related to the target design files. After completing the initial analysis and screening, I used the built-in reporting functionality provided by FTK to archive and summary the entire case process. Through the 'Report' function, I selected all key modules to ensure that all operations, evidence paths and concluding information involved in the analysis process were included for subsequent review, comparison

and legal use. The report was automatically generated in PDF format and recorded all the evidence I found, the module operation and the summary of the recovered files, so that it is convenient to refer to it when investigating again in the future.

After several rounds of attempts, the findings at this stage are as follows:

A large number of files marked as 'Deleted' were found on the disk, and some of the file extensions were no longer recognisable, so it was initially judged that there might be traces of human deletion. Design files may have been completely erased.

Autodesk Maya-related files such as '.mb' or '.ma' were not found intact in any logical volume, indexed area or unallocated space, and GUI-type output files (e.g. PSD, PNG, ASP.NET, etc.) were not recognised and may have been permanently overwritten or moved.

Since the company does not perform regular backups of Rich's work systems, the current analysis is limited to the only disk image captured, which means that if the original data has been overwritten, it is virtually impossible to restore it by technical means.

Technical bottlenecks at the current stage and recommendations for further operations:

Although FTK is equipped with powerful file recovery and analysis functions, in this case, it is difficult to recover the contents of the target files through traditional disk forensics because the files have been deleted more thoroughly and may have been overwritten. But, based on the current results, we can take the following further steps to improve the investigation:

Memory Forensics:

If we can obtain Rich's memory image files (e.g.: raw/.lime format) from his last boot state before leaving the company, we can use tools such as Volatility to analyse his runtime information, such as the design software that had been opened, the path of the most recently opened files, the temporary directory where the files were automatically saved, and possibly even intercept the file transfer channel or login records. Although this type of data is not currently available, if the CMMC has a similar event in the future, it can be prioritised to retain the memory image.

Registry and System Log Deep Dive:

In the event that the target file is not located, we can turn to the system registry and event logs to look for recent file deletions, USB device access logs, remote access history, unusual account activity, etc. Although these circumstantial evidences cannot recover the files themselves, they may provide strong support for the subsequent pursuit of responsibility or litigation.

Network Behaviour and Transmission Path Analysis:

If the company has enabled traffic monitoring devices or VPN access log systems, we can try to match Rich's network connection behaviour in the last week before he left the company, and find out whether there are any abnormal IP connections, records of sensitive file uploads, or access to third-party online storage platforms.

User Trace Reconstruction:

In addition to FTK, we can also combine Autopsy tool to forensically examine the file opening

history, Timeline, shortcuts, Recent Files directory, etc.,so as to determine whether the user has recently operated the target design files,and even if the files are no longer in the local area,we can still confirm the existence of the files through the operation traces.

Social and Email Investigation Suggestions:

If there is legal authority or internal review authority,it is recommended to review Rich's corporate email communications,especially searching emails with'360tech'as the keyword,to look for evidence of potential transactions or contact information to support further tracing of the direction of the leak.

Summary:

Currently, the target design files cannot be recovered through FTK's comprehensive analysis,but it has been able to confirm the existence of file deletion behaviour on the device. Some data may have been overwritten and cannot be recovered. But then we can investigate further with other computer forensic tools.I have used FTK to generate a corresponding report, which provides a list of the evidence I have found, which can be used as a reference for further investigation.