
Journal of Informatics and Web Engineering

Vol. 4 No. 2 (June 2025)

eISSN: 2821-370X

Analysis of Forensic Disk Imaging Tools for Data Acquisition and Preservation

Michelle Chee Ern Lim¹, Brandon Chen Hong Chow², Le Ying Lim³, Tarini A/P
Shanbagamaran⁴, Darren Lim Yong Jun⁵, Ngu War Hlaing^{6*}, Ahmad Sahban Rafsanjani⁷

^{1,2,3,4,5,6,7}Faculty of Engineering and Technology, Sunway University, 5, Jalan Universiti, Bandar Sunway, 47500 Petaling
Jaya, Selangor, Malaysia

*corresponding author: (nguhlaing@sunway.edu.my; ORCID: 0000-0003-3412-1620)

Abstract – The identification, preservation, analysis, and presentation of electronic evidence to support legal or organizational inquiries constitute the discipline of digital forensics, which is crucial to contemporary investigations. A crucial component of forensic inquiry, disk imaging guarantees precision, dependability, and legal defensibility. To preserve the original evidence, disk imaging makes an identical, bit-by-bit duplicate of a digital storage device, capturing hidden data, deleted material, and active files. Given the critical role of disk imaging in forensic investigations, selecting the right tool is crucial for accuracy, efficiency, and compliance with forensic standards. This study assesses widely used tools, including AccessData FTK Imager, Guymager, X-Ways Forensics, OSForensics, and FTK Imager, to help researchers and industry professionals choose the most suitable option for their investigative needs. This research examines the usability, imaging speed, supported hashing techniques, supported output formats, and other aspects of each tool to assess their suitability for usage in various forensic scenarios. The shows that X-Ways Forensic is among the greatest imaging tools because of its wide range of supported operations, fast imaging speed, and format compatibility. The result of hash verification, perfectly matched with source data, again establishes the capability of AccessData FTK Imager, FTK Imager, Guymager, X-Ways Forensics, and OS Forensics to ensure forensic soundness. Its capability to generate a detailed report with comprehensive drive geometry and file segmentation establishes its applicability in forensic workflows. Besides, the time consumed for processing shows its applicability in time-critical investigations too.

Keywords—Digital Forensics, Cyber Crime, Digital Image Forensics, Forensic Investigation, Disk Imaging Tools, Digital Evidence

Received: 07 January 2025; Accepted: 26 March 2025; Published: 16 June 2025

This is an open access article under the [CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) license.



1. INTRODUCTION

Despite the availability of various forensic disk imaging tools, challenges remain in terms of efficiency, compatibility, and integrity verification. Some tools struggle with handling large volumes of data, while others lack support for advanced encryption or emerging storage technologies. Additionally, differences in imaging speed, hash verification methods, and usability create inconsistencies in forensic investigations. This study evaluates and compares forensic disk imaging tools to address these gaps, providing insights into their effectiveness for data acquisition and preservation. We systematically evaluate the performance and capabilities of five widely used disk imaging tools, analysing key factors such as imaging speed, supported hashing algorithms, output formats, and system compatibility. We assess the performance of these tools using real-world forensic

evidence, including compromised storage devices from cybersecurity incidents and data recovery cases. This ensures a practical evaluation of their efficiency in handling damaged, encrypted, and large-volume data sources encountered in actual investigations. We highlight the strengths and limitations of each tool, providing forensic practitioners with insights into their applicability in different investigative contexts, including cost-effectiveness, ease of use, and adherence to ISO/IEC 27037 forensic standards. This study aims to conduct a comparative analysis of five prominent forensic disk imaging tools—FTK Imager, Guymager, X-Ways Forensics, OSForensics, and AccessData FTK Imager. The evaluation focuses on their performance, usability, data integrity mechanisms, and forensic soundness to assist investigators in selecting the most appropriate tool for different forensic scenarios.

2. BACKGROUND AND RELATED WORK

Digital forensics is an investigation which is done on electronic devices at crime scenes [1]. Digital forensics is the process of examining and analysing computing devices to collect and save evidence that can be used in court. The main goal is to investigate carefully, keep a record of all the evidence [2], and find out what happened on the device and who is responsible. Digital forensics tools are now commonly used by investigators and analysts [3, 4]. Forensic analysts usually follow these steps. They first isolate the device to prevent accidental damage or tampering. Then, they create a digital copy of the device's storage. The original storage is securely stored to keep it unchanged. Analysts use specialized tools and software to examine the copy. They look for hidden, deleted, encrypted, or damaged files, including unused storage spaces.

Digital forensics plays a key role in solving crimes involving computers, like phishing or bank fraud, and crimes where evidence might be stored on a computer, like money laundering or child exploitation [5], [6]. Memory forensics is a specific type of investigation focused on analysing a computer's memory (RAM) [7]. It is especially useful for detecting advanced cyberattacks that do not leave traces on the hard drive. The different types of digital forensic are shown in Figure 1.

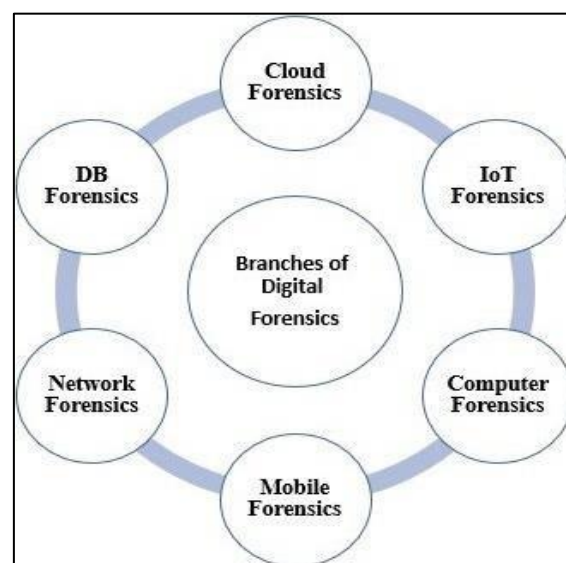


Figure 1. Different Types of Digital Forensics [8]

Forensic science involves four main steps which are preparation, collection, analysis and reporting. Preparation involves assembling the necessary tools to carry out forensic investigations. This phase helps investigators determine the aim and scope of the investigation. This is followed by the collection phase, where all the data is acquired from the source device by using forensics tools. Disk imaging occurs during this phase. Next, the analysis step involves searching for files and logs in a system. This phase aids in analysing the details acquired and recovering deleted files. Finally, the reporting phase, which involves detailed documentation of the forensic investigation. The process, steps, timeline and images should be reported in this phase for future reference [9].

Digital devices consist of internal and external storage devices. It is important to copy and extract necessary information from them, because they may contain data that will be useful for forensic investigation. There are different types of disk imaging tools to use to acquire data from digital devices. The disk imaging tool can leave an impact of integrity and reliability in this process [10]. The five widely used disk imaging tools are FTK Imager, Guymager, X-Ways Forensics, OSForensics and AccessData FTK Imager. The best tools to use for forensic investigation can be determined by comparing and analysing these tools. This paper's three main goals are to:

compare the features, performance, and limitations of various forensic tool types; implement and analyse each tool's use and impact on disk imaging; and evaluate hashing algorithms and functions to ensure data integrity in disk imaging.

2.1 Categories of Forensic Tools

Collecting institutions, such as archives, frequently handle and process data from raw digital sources like hard drives and removable storage devices. These sources often contain valuable contextual information as well as private and sensitive data, including content, file details, and system metadata. Effectively identifying and managing this supplementary information is crucial for meeting donor or submission agreements, establishing provenance, and ensuring future access. However, there is a lack of standard procedures for processing and analysing digital media. Disk imaging means creating an exact copy of the original media combined with automated image analysis can help address these challenges. By incorporating digital disk imaging into their workflows, collecting institutions can better preserve the authenticity, integrity, and provenance of digital materials.

In [11], several digital forensic analysis tools were examined, highlighting that pattern recognition techniques are highly effective during the analysis phase of digital forensics. These recognized patterns help identify features that contribute to the development of numerous digital forensic tools. As a result, these tools are not only essential for preserving and analysing evidence but also play a crucial role in resolving conflicts that arise during the execution phase. In [12], various techniques for live and dead forensic analysis were discussed. The study highlights the essential commands provided by different digital forensic tools such as Wireshark, Autopsy, OSForensics, TrueCrypt, FTK Imager, and SANS SIFT, creating a user-friendly environment to assist investigators. Additionally, it emphasizes the collection of information through live analysis, which avoids data loss caused by halting the target system.

In [13], it was noted that criminals often attempt to destroy evidence by deleting, damaging, or overwriting files on hard drives. The study primarily focused on methods to recover this destroyed data. Recovery efforts were carried out using various tools, including Wireshark, Autopsy, TrueCrypt, FTK Imager, OSForensics, X-Ways Forensics, and SANS SIFT. Researchers in [14] explored the features, limitations, and applications of digital forensic tools, comparing them with other tools to assist investigators and users in utilizing advanced forensic solutions for their investigations.

In [15], a machine learning approach was utilized alongside a proposed scheme to detect abnormal packets and attacks. The study found that the Naive Bayesian classifier achieved the highest accuracy compared to other classification methods. Amato et al. [16] employed Natural Language Processing (NLP) techniques to examine digital forensics evidence. Wu et al. [17] explored the latest developments and capabilities of digital forensics tools in the current environment. Cosic et al. [18] introduced a method for constructing a new intelligence-driven digital forensics model aimed at enhancing storage preparedness. Hemdan and Manjaiah [19] proposed a practical model for cloud digital forensics, known as the Cloud Forensics Investigation Model (CFIM), designed to analyse crimes occurring within the cloud from a forensic perspective.

Costantini et al. [20] suggested a framework for implementing AI applications in digital forensics, particularly during the analysis phase. Krivchenkov et al. [21] provided an overview of current AI-based digital forensics methods aimed at improving forensic investigations. Mohammad and Alqahtani [22] examined various machine learning techniques and their effectiveness in identifying evidence through file system tracking, with the algorithms demonstrating promising results.

Alhawi et al. [23] studied network traffic to detect Windows ransomware using machine learning and achieved a Total Form (TF) accuracy of 97.1% with the decision tree approach. Srinivasan et al. [24] introduced a method for describing text using Natural Language Processing to identify spam emails. Sachdeva and Ali [25] proposed a model for categorizing attacks in cloud environments through machine learning techniques integrated with digital forensics. Sarker [26] presented a model for managing intellectual cybersecurity, utilizing AI techniques to enhance the efficiency of cybersecurity analysis compared to traditional security methods. With the rapid advancement of technologies, selecting appropriate digital forensics methods and frameworks has become crucial.

Singh et al. [27] implemented a Digital Forensic ReaFdiness (DFR) approach to ensure compliance with IEC/ISO ethical standards. Sun et al. [28] introduced a model using Online NLP for forensic investigations, comparing various digital forensics tools across categories like computer forensics, network forensics, OS forensics, live forensics, database forensics, and email forensics. This comparison helps investigators easily select the appropriate tool for their needs.

In this paper, the evaluation process for FTK Imager, Guymager, X-Ways Forensics, OSForensics, and AccessData FTK Imager was meticulously planned to guarantee that the experiment accurately and reproducibly mirrored actual forensic situations. The experiment used several combinations of specialized software and hardware configurations that are typical in forensic investigations.

The imaging was set to create raw format images, segmented to optimize file storage and transport. This is because very large single-file disk images are often difficult to manage in environments that place limits on file size. Besides, segmentation permits more manageable transfers and storage of image files, especially in those cases where limited storage is available, or cloud solutions are being used.

Hashing was part of the whole imaging process, with MD5 and SHA-1 used for hash algorithms to validate data integrity. MD5 is an internationally recognized algorithm running quite fast, providing a unique fingerprint of data, while SHA-1 gives a slightly stronger method to ensure the reliability of the check [29]. Both were chosen because they are internationally accepted under forensic practices, meaning the authenticity of the imaged data could be asserted in both investigations and before the courts. These algorithms make sure that the imaging is forensically sound and instil confidence that nothing could change or corrupt the data.

3. RESEARCH METHODOLOGY AND ANALYSIS

The methodology for evaluating FTK Imager, Guymager, X-Ways Forensics, OSForensics, and AccessData FTK Imager was carefully structured to ensure that the experiment replicated real-world forensic scenarios while maintaining precision and reproducibility. The experiment made use of various combinations of specialist hardware and software setups, which are representative of common forensic investigations.

3.1 Experimental Setup

The system combination included a high-end PC with 32GB of RAM, an Intel i7 CPU, and SSD storage. These standards were designed to facilitate efficient processing throughout the imaging process, hence eliminating any bottlenecks caused by hardware restrictions. The experiment also used a 32GB microSD card as the primary storage media. This type of removable storage is extremely common in digital forensics since most consumer electronics make use of them. Hence, this is very suitable for realistic investigative scenario simulations.

Pre-imaging preparation of the microSD card involved the creation of some 24GB of random files in the following format such as text documents, images, videos, and archives. The goal of this step was to represent some real-world use scenarios, which meant the imaging would face a lot of file types and structures. Next, 33% of these files were deleted to set up an environment with partially fragmented and deleted data. Such preparation was necessary to check the forensic tools for their ability to work with fragmented data, the most common problem in any digital investigation.

The output was set to raw format with dd, which was selected because the raw format is readable by the widest range of forensic analysis tools. Raw format is the standard in forensic imaging, as it produces a strict bit-by-bit copy of the original media without adding metadata and compression, thus making the imaged data universally accessible by other forensic tools [30]. The use of raw(dd) also simplifies integrity verification since the output has no proprietary components that would obscure or otherwise change the original form of the data.

3.2 FTKImager

Exterro created the forensic imaging tool FTKImager, which is well known for its dependability and effectiveness in producing forensic photographs. This maintains data integrity while allowing users to obtain bit-for-bit copies of storage medium. FTK Imager features a Graphical User Interface (GUI) that is easy to use and intuitive. It ensures interoperability with many forensic analysis tools by supporting a variety of image formats, including SMART, EnCase (E01), dd, and Advanced Forensic Format (AFF). Additionally, the application can test data integrity using hashing techniques like MD5 and SHA-1.

The FTK imager is available for download from the official AccessData website and runs on the Windows operating system. The user can start imaging activities after downloading and installing the FTK Imager [31]. Users may also choose a storage medium with this tool, like a 32GB SD card or any other storage device. The *Create Disk Image* option allows the user to build a forensic image after selecting a storage medium. FTK Imager offers choices for acquiring particular files and folders, a logical drive, or a physical drive.

Users can also adjust several parameters, including the hashing algorithm, file segmentation size, and output format. Users can start the imaging process by clicking the start button once they have configured the parameters and set the image's destination path. A progress bar outlining the operation's status, including the hashing verification, will then be displayed by the software. After the imaging procedure is finished, FTK Imager produces an extensive report that contains important metadata for upholding the chain of custody and guaranteeing the evidence's forensic soundness. Furthermore, segmented picture files in the designated format (image.dd.001, image.dd.002) are produced by FTK Imager.

Additionally, FTK Imager can view the data without changing it, which can help the investigator find and identify pertinent evidence more rapidly. The forensic integrity of the photographed data is guaranteed by the hashing function, giving assurance that the evidence won't alter during the procedure. Investigators prefer it because of its versatility and compatibility with other forensic instruments. To sum up, FTK Imager is a strong and dependable program that offers an easy-to-use way to obtain and save forensic disk images.

The data collection and analysis steps are shown in Figure 2.

- a. Open the *FTK Imager* after installing on Window-based forensic workstation
- b. Click on *File*, then choose *Create Disk Image* to start the process
- c. Select the type of evidence
- d. Choose the output image format
- e. Initiate the image process by clicking *Start*
- f. Wait for the image process to complete
- g. After the image process is complete, verify the hash value to ensure data integrity

For the Exterro FTK Imager findings, the imaging process was conducted with details and attention to provide data integrity and efficiency. The acquisition began at 17:16.42 and was completed at 17:50.23, total of 33 minutes and 41 seconds. During the period, Exterro FTK imager demonstrated the ability to create a segmented forensic image while maintaining the integrity of the data throughout the process

The imaging process produced a total of twenty-one segments, labelled from Exterro_dd.001 to Exterro_dd.021. Each segment was generated and stored in the designation location, which allows the file sizes to be optimized for storage and transfer. Exterro FTK Imager prioritizes the data integrity by utilizing its built-in hashing. The MD5 checksum for the original media was calculated as 3968a79a3f8e855f3de9f63ccf9e9a38, and for SHA-1 checksum was cb283b24e510ab1b6f9d0c8b41f3a263bb664bf7. These hash values were generated during the imaging process and later verified in the validation phase. The verification began at 17:48.16 and finished at 17:50.01, confirmed that the hashes of the source and the created image matched perfectly. This ensured that no data corruption or tampering occurred.

Efficiency and dependability are demonstrated by Exterro FTK Imager. It proved that it could manage a storage medium's imaging while upholding strict data integrity guidelines. This tool's segmentation support and documentation features make it ideal for forensic investigations. Exterro FTK Imager is a reliable option for forensic imaging and evidence preservation because of its combination of these features.

3.3 Guymager

An open-source program called Guymager enables users to copy disks and photos, which are frequently utilized in forensic investigations. A Graphical User Interface (GUI) is included in Guymager, making it simple to use while creating and managing forensic disk images. Guymager supports a wide variety of image formats, such as dd, Expert Witness Format (EWF), and Advanced Forensic Format (AFF). To guarantee that the cloned disk's integrity is preserved, Guymager additionally offers hash function computations, enabling forensic investigators to produce high integrity work.

Guymager is a forensic tool that runs only under the Linux Operating System, to download this user can proceed to the link <https://guymager.sourceforge.io/> and follow their downloading instructions or user could also use Linux distributions such as Kali Linux that comes in-built with tools such as Guymager. Upon opening Guymager users will be prompted with an interface that lists down all the currently detected partitions and storage mediums, users can then select the storage medium such as the 32GB SD card being used in the experiment to be cloned.

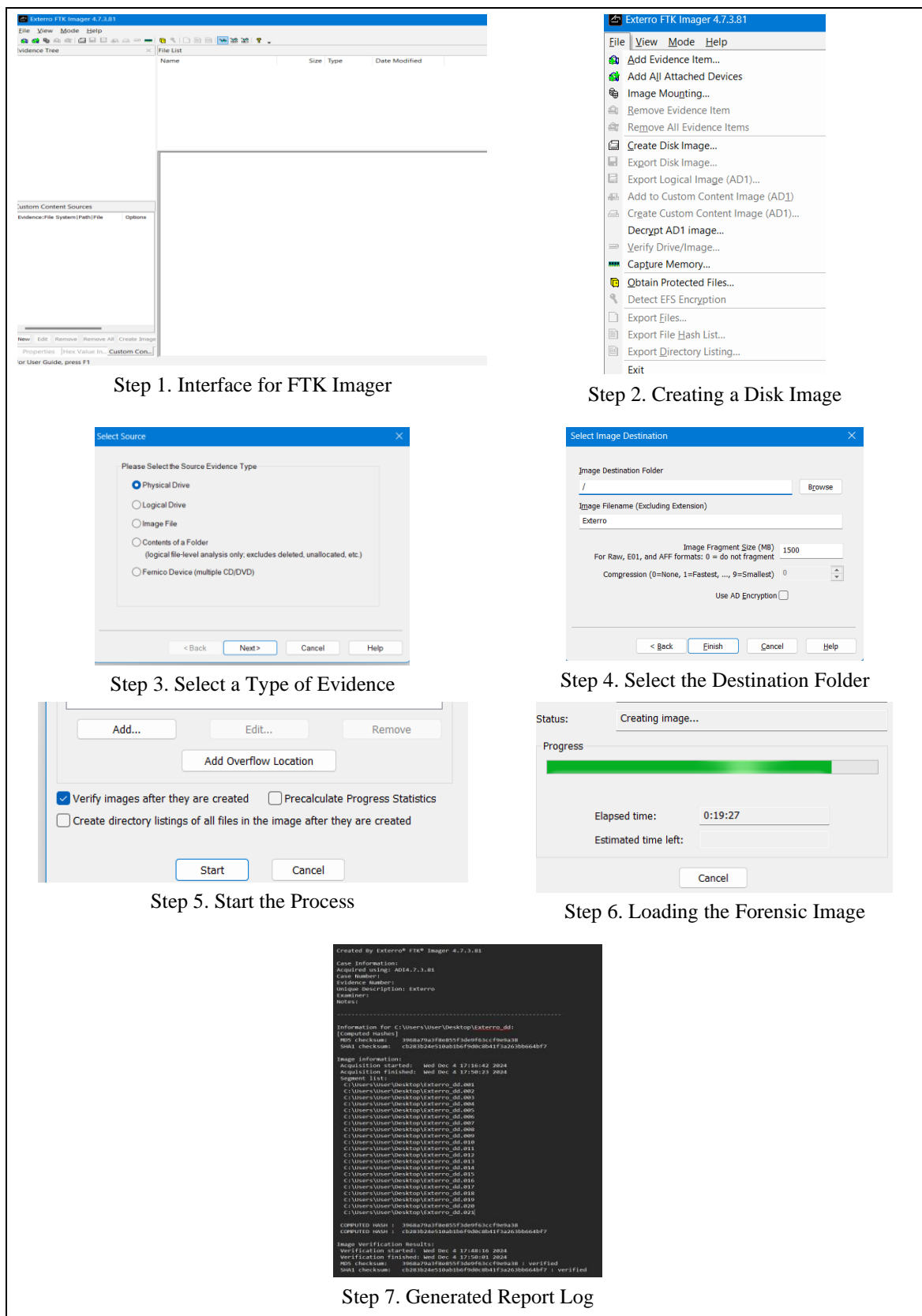


Figure 2. Data Collection and Analysis using FTK Imager

Upon clicking on the selected storage medium, a selection will be prompted to choose between acquire image and clone device. After that, users will be prompted to choose which type of formatting that would desire and how large each section of partition will be, in this prompt of the GUI users can also select the type of hashing algorithm to be generated. After selecting where the image will be cloned to the user can click on start and wait for the image to be

cloned. Upon completion an indicator bar will show 100% indicating its completion. The steps-by-steps process are shown in Figure 3.

The data collection and analysis steps are shown below:

- a. Open the Guymager application after installing or using Linux distributions such as Kali Linux.
- b. Select the storage medium that wished to be cloned or acquired the image from
- c. Select the type of file format wished to be used
- d. Select the file destination to be cloned to
- e. Set the file size of each single partition split which is set to 1500 MB to maintain the consistency between different tests
- f. Select the types of hashing algorithm to be generated for integrity check, in this experiment MD5 and SHA1.
- g. Wait for the completion of the image acquisition.
- h. Upon completing the image acquisition, users can view the average speed for acquisition.
- i. An auto-generated report that is labelled .info is generated and contains the hash, and their respective information all listed in it. The .info file can be opened with any text editor including notepad, nano and cat command

The findings help to provide a better understanding of the performance of Guymager with all recorded metrics being recorded in the .info file. Guymager demonstrated reliability and efficiency throughout the entire imaging process. The acquisition which took place only used a total of 12 minutes and 20 seconds to perform the imaging. Among the 12 minutes and 20 seconds, 9 minutes and 4 seconds was the actual imaging time while the remaining 3 minutes and 16 seconds were used to perform verification. The verification recorded a speed of up to 55.95 MB/s while the verification speed clocked in at 156.08 MB/s. The imaging process was smooth, and no resulting bad sectors were encountered and a total of twenty-one sectors were generated.

Guymager also prioritized data integrity by providing hashing capabilities which generated checksums for the hashing algorithms below which are MD5, SHA1, and SHA-256. The original media produces identical hashes for both sources and image files which ensure the absence of file corruption or file tampering. Specifically, the MD5 hash was 3968a79a3f8e855f3de9f63ccf9e9a38, the SHA- hash was cb283b24e510ab1b6f9d0c8b41f3a263bb664bf7, and the SHA-256 hash was 84c27d224050792dc5d559cedf95eb6bb6e92d83516ab8fa57a27a7b81363693. These verified values ensure the forensic soundness of the process.

During the imaging process, some detailed information of the device was captured which includes that the device size was 31.9 GB or (31,914,983,424 bytes) and was confirmed to be an ATA device with sector size of 512 bytes but further details such as logical or physical sector, cylinders head, and more were not extractable from Guymager.

The entire process of Guymager's image acquisition process has been meticulously collected and documented including the operation, handling of image creation, hash verification and segment generation were all logged. This provides transparency ensuring that no data was manipulated at any point of the data acquisition which is an important process for forensics to ensure the credibility of the evidence.

3.4 X-Ways Forensic

X-Way Forensic is an integrated Computer Forensic software developed by X-Ways Software Technology AG and can perform tasks such as disk cloning, imaging, read file systems and partition, identify lost or deleted partitions and more. Its many different features and applications make it one of the most thorough and comprehensive forensic tools accessible. Users must download X-Way Forensic and buy a product license before they can start using it.

After that, extract the files to the location of your choosing. Since the application is portable and may be run straight from the extracted directory, there is no need for a formal installation procedure. Once the main software has been extracted, download the viewer component separately, making sure that the 64-bit version corresponds to the 64-bit version of X-Ways Forensics, if that is the case. The viewer component should be placed in the proper subfolder, such as \viewer for 32-bit or \x64\viewer for 64-bit [31].

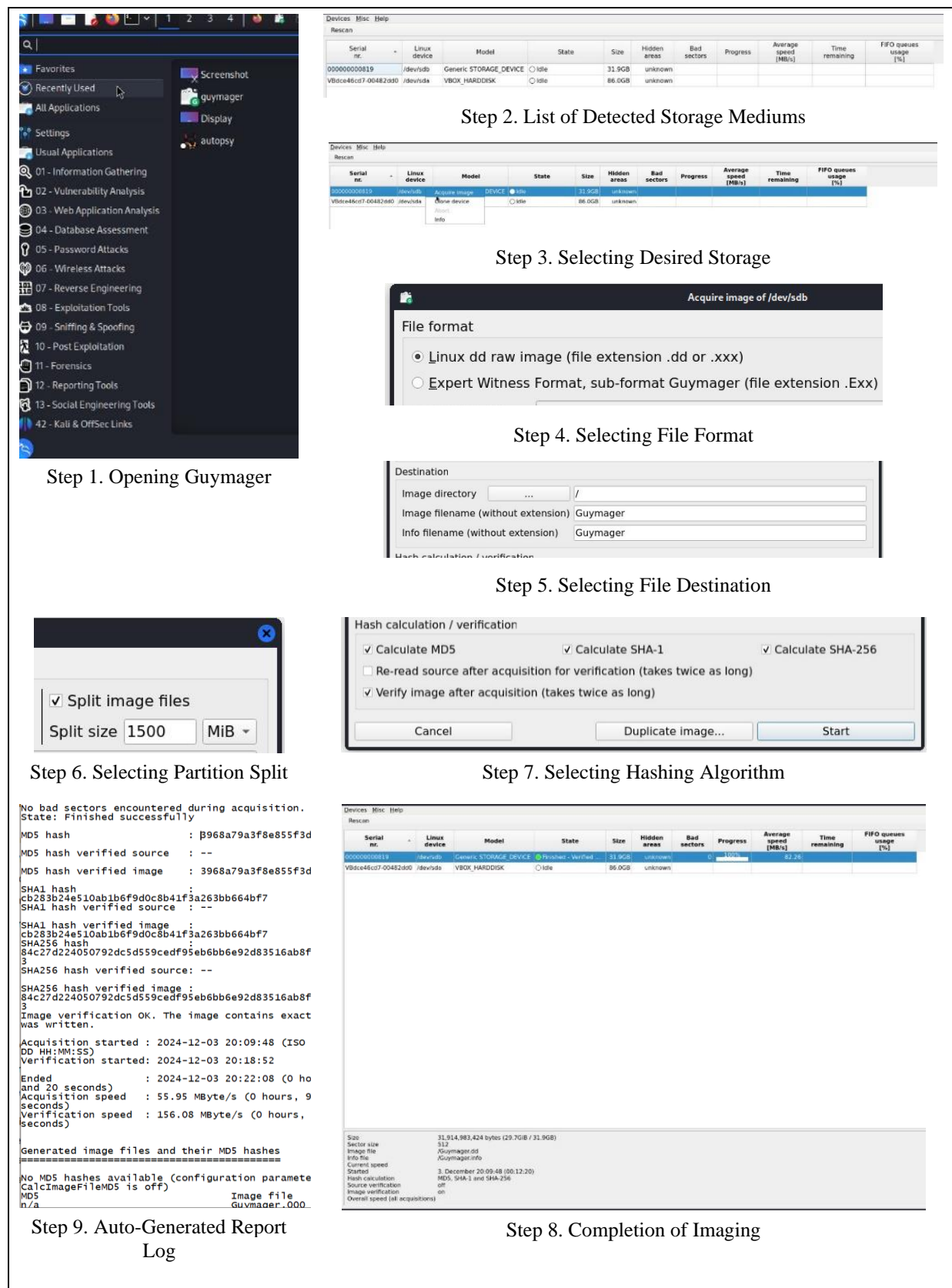


Figure 3. Data Collection and Analysis using Guymager

X-Ways Data can be collected, stored, and examined by forensic. Obtaining a forensic picture utilizing the imaging or cloning capabilities and storing it in a raw or e01 format with metadata is the first stage in the data acquisition process. Next, we can calculate hash values such as MD5 or SHA-256 during acquisition to confirm the authenticity of the imaged disk. In real world forensic scenarios, investigators would maintain a chain of

custody by documenting every step in an activity log and creating multiple backups in secure locations. This helps ensure that the evidence and image collected are legitimate and administrable in court.

X-Ways Forensic is also capable of analysing data which can be done by loading the evidence object into the case and refine the volume snapshot to extract file system details, metadata, and deleted files. To help find useful evidence or files easier, X-Ways forensic has a filter and search function in the directory browser to narrow the scope by file types, timestamps, or attributes, and conduct simultaneous or logical searches to locate specific evidence. Besides that, X-Ways Forensic can also provide advanced features such as metadata extraction, encryption detection, image content analysis, and still image capture from videos which can be used to find any hidden information.

All the functions provided by X-Ways Forensic will also provide hash comparisons of files of interest confirm authenticity and integrity. Besides that, X-Ways Forensic can also be used to generate a detailed case report documenting the evidence, steps taken, and findings, while preserving logs and hash values which can help other investigators recreate the investigation process, thus making the evidence collected more authentic and reliable. For real forensic investigations, X-Ways Forensic has a write blocker function that helps protect the original evidence by preventing any modification or editing to be done to the original evidence [31].

X-Ways Forensic is a paid licensed tool that requires RM5,469 per year for 1 account thus, we were unable to obtain the product and perform the data acquisition and analysis [32]. However, based on extensive research and the product's official documentation, we have outlined the step-by-step procedures for acquiring, preserving, and analysing data using X-Ways Forensics. While we could not implement the process ourselves, the outlined procedures can ensure reproducibility and adherence to professional standards.

Steps to acquire data using X-Ways Forensic [33]:

- a. Install X-Ways Forensics by extracting the files to a directory.
- b. Download and place the viewer component (e.g., 64-bit edition) in the designated directory (\viewer or \x64\viewer).
- c. Launch X-Ways Forensics and create a new case from the Start Centre. Specify paths for storing case files, temporary files, and evidence snapshots.
- d. Add an evidence object such as a physical drive, image file, or logical volume. Use the *Interpret Image File as Disk* feature if necessary to handle raw image files.
- e. Clone the source drive or create a disk image using the imaging tools. Save the image in .e01 format or raw format for compatibility.
- f. Ensure the hashing feature is enabled to compute hash values (e.g., MD5, SHA-256) during acquisition for data authenticity.
- g. Store the acquired disk image and its associated metadata (hash values) in a secure location.
- h. Recalculate and compare hash values of the image file to ensure it matches the original data.

X-Ways Depending on the circumstance, forensic software may be used for a variety of purposes. It is a practical tool with many capabilities that can be used to do forensic investigations [34]. All things considered, it may offer a thorough examination of the evidence and produce a report that includes all the pertinent details, guaranteeing that the evidence gathered is admissible in court.

We were unable to get the case-specific data since we couldn't launch and use the X-Ways Forensics program itself. X-Ways Forensic can, however, produce a dd raw disk image file with a bit-by-bit replica of the original drive provided it is used correctly. In addition, X-Ways Forensic will provide a hash value for both the generated dd disk and the original drive.

The dd drive is a perfect duplicate of the original drive as these hashes can be compared and should match. Additionally, X-Ways Forensic will provide an acquisition record with metadata pertaining to the actual imaging procedure. This can contain information like timestamps, hash values, and the model, serial number, and imaging tool parameters of the source device.

In addition, X-Ways Forensics may produce a thorough report outlining the results if it is utilized for data analysis. File system structures, recovered deleted files, keyword search results, metadata analysis, and proof of user activity are a few examples of the data that may be included in this report. It can also record timestamps, hash values, and detected artifacts such as registry entries, email contents, and browsing history. Because the reporting tool is adjustable, users can add or remove particular facts according to the case's needs.

3.5 OSForensics

OSForensics is a digital forensic tool, developed by PassMark Software and it is an open-source tool. It analyses electronic devices for forensic investigation. Some of the features that OSForensics offers are identifying suspicious files, disk imaging, collecting information from disk, file recovery and hash verifications. OSForensics can perform deep scans, analyze systems and detect hidden or deleted data and promotes a detailed investigation, aiding the investigators with forensic investigation. It is user-friendly software which provides reporting options, making it suitable for both beginners and well-trained forensic investigators. OSForensics supports various formats for disk imaging, such as, RAW Image (dd) and Advanced Forensic Format (AFF). These are the versions available for free trial of OS Forensic. There are more formats offered in Premium version, where users will have to pay for it.

To utilize OSForensics, users must install and download it from the website through the link <https://www.osforensics.com/download.html> and follow the instructions to complete the installation process. Upon completion, users can access the tool, and the GUI interface allows them to utilize the software seamlessly. After initiating the software, users can select the *Create Forensic Image* option to create a disk duplicator for the disk they want to duplicate. Users can select the source drive, output destination, and hash verification types. The source drive could be physical or logical according to the drive they would like to create a disk image for. The hash algorithms in OSForensics Free Trial available are MD-5, SHA-1 and SHA-256.

After the selections have been done, users can click the *create image* button to start copying and verify the disk selected. Once it is done, the status bar will show *Completed* along with the amount of time it took to complete the disk imaging. Steps to acquire data from OSForensics are as shown below together with figures as shown in Figure 4 and Figure 5.

- a. Open the OSForensics software after installation is completed. A pop-up box is shown as in the image below. Click the Free Trial Version as it will be used for this experiment. The free and Premium version serves limited/ upgraded features.
- b. Next, it will lead to GUI interface, and at the left column, click the *create forensic image* tab. Once clicked, the interface will display. Click the *add* button to create a new case.
- c. Once the add button is clicked, the image settings will pop out. Select the intended source drive to do disk imaging. In this case, the microSD card as the physical drive. As shown below, select *PhysicalDrive1*. Next, click the ellipsis button beside the target file section. This allows users to select the destination of the image file. The formatting for the image can be chosen as well. In this case, it will be RAW image (*img). Click *Save* to proceed to the next step.
- d. Next, add a description for the file such as *OSForensics_dd*. Followed by selecting the has function. The hash functions that have been chosen for this experiment are *MD5* and *SHA-1*. Make sure to tick the *Verify Image File after Completion* box to ensure integrity.
- e. After all the selection processes are completed, the case will be displayed on the *create disk image* tab. Clicks *create image* at the bottom of the information displayed.
- f. In this experiment, OSForensics displays a pop-up message stating a warning for this imaging process. As shown below, it states there are over *1000* bad blocks. If *yes* is clicked it will continue with the imaging process and zero fills the bad blocks. If *no* is clicked it will show error and will not be able to proceed with imaging.
- g. For demonstration purposes *no* was clicked, and the result is as shown.
- h. To proceed with the experiment, *yes* was clicked. When the system starts running, it will display information such as the status of disk imaging, copy method, disk size, speed, data read, unread data, primary hash and secondary hash.
- i. Once imaging is successfully completed, it will display the information as shown below. It includes the status of completion and time taken to complete copying and verifying process of the disk image.
- j. The output of the imaging will be shown in two documents which are text and image file as shown below. In this experiment the destination location chosen was the Desktop, so it is easier to view.
- k. Could not mount the dd file, as the disk image file is corrupted. Due to the large amount of zero fill bad block that happened, the disk imaging process does not match the original source data, rendering it fully unusable.

As for the text file (txt), it is an auto-generated report which contains case information and hash functions. It is shown that the checksum source and checksum image are identical which shows strong indication of data integrity.

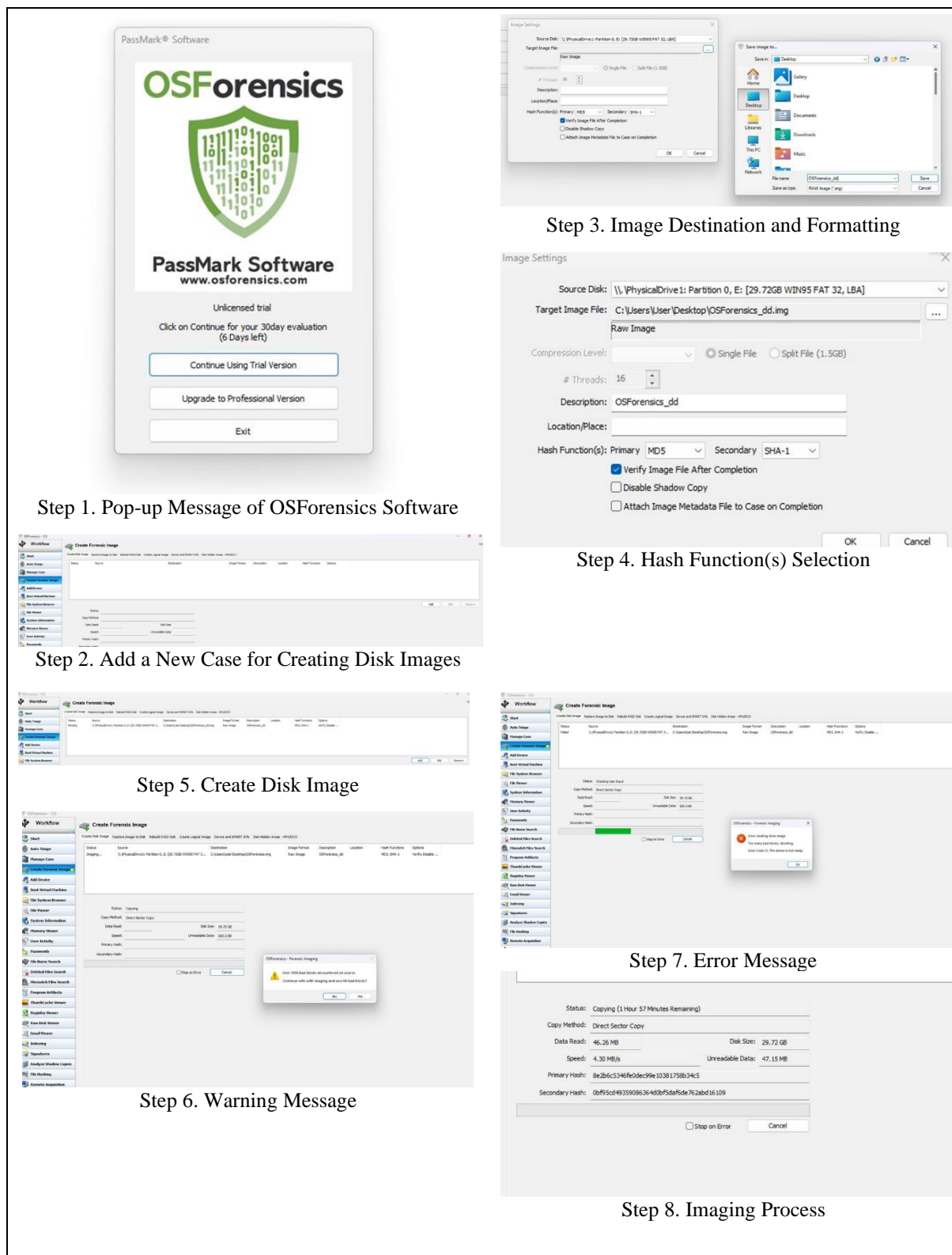


Figure 4. Data Collection and Analysis using OSForensics (Steps 1 – 8)

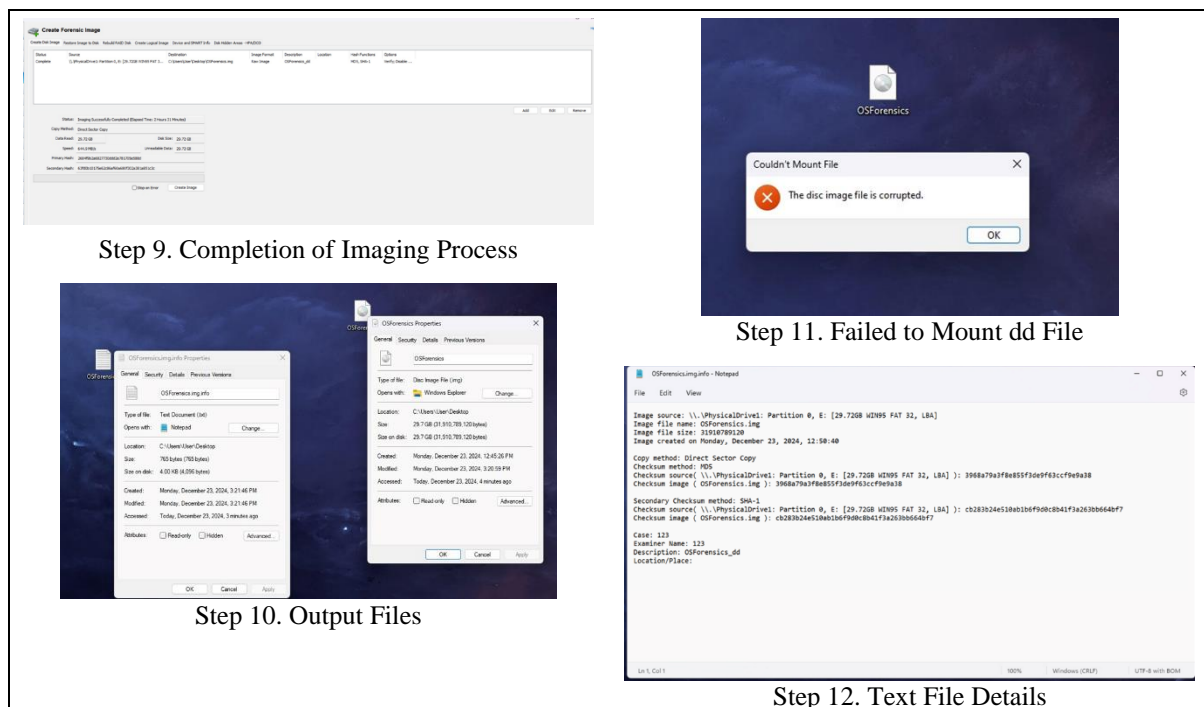


Figure 5. Data Collection and Analysis using OSForensics (Steps 9 – 12)

The disk imaging process took 2 hours 31 minutes to complete. The imaging process faced several issues which significantly impacted the overall process and its outcome. The first issue is that there were no segments of images created. This segmentation feature is only available in the premium version. Segmentation feature allows us to split data into manageable chunks for analysis and storage. Since OSForensics trial version does not have the feature, it was not able to create disk image with segmentations. Additionally, there were errors in imaging due to the presence of bad blocks on the source drive. As shown in the data collection and analysis section, the microSD card as the physical drive consists of one thousand bad blocks as scanned by OSForensics. These bad blocks caused the tool to encounter unreadable data, which leads to corruption of disk image files. As shown in the data collection and analysis section, the .dd image file created was invalid and could not be mounted due to corruption. This error shows that OSForensics appeared to be particularly sensitive to bad blocks.

However, the imaging process incorporated hashing mechanisms to ensure data integrity. OSForensics allows users to choose only two hash options as a primary and secondary hash function. In this experiment, MD5 and SHA-1 were chosen. The checksum of source using MD5 method was 3968a79a3f8e855f3de9f63ccf9e9a38 and SHA-1 method was cb283b24e510ab1b6f9d0c8b41f3a263bb664bf7. These checksums matched with the generated hashed for the image file. This ensures the integrity of disk image, even though the corrupted file rendered the hashes less meaningful in this situation. As a conclusion, the imaging process was affected by the issues of sensitivity to bad blocks. The corruption of disk images leads to the inability to mount the .dd file. However, the hash functions worked well in this process, but due to the issue faced, it made the hash function less meaningful.

3.6 AccessData FTK Imager

AccessData® FTK® Imager v.4.3.1.1 represents a robust yet compact forensic imaging application, engineered for the generation of precise bit-by-bit duplications of storage media, thereby maintaining the integrity of evidentiary material. AccessData FTK Imager accommodates multiple formats, including dd, SMART, E01, and AFF, rendering it suitable for use with an array of forensic analysis tools. The tool's capabilities in segmentation and hashing contribute to the dependability and organization of forensic images, even within extensive investigative contexts [30].

To utilize AccessData FTK Imager, individuals are required to download and install the software from the official AccessData website. After installation, the program provides a user-friendly graphical user interface that facilitates its usage, especially for those with little forensic experience. Users may start the imaging process by selecting the *Create Disk Image* option after starting the software. Through pinpointing the source drive, whether physical or logical, and identifying output format, and then hashing algorithms like MD5 or SHA-1, AccessData FTK Imager

allows users to precisely acquire data. In addition, the software is capable of segmentation, enabling output image to be cut into segments that are smaller, thereby making systems that are limited regarding file size and available storage manageable.

Steps to acquire dd file using AccessData FTK Imager:

- a. Open *AccessData FTK Imager* and click on *Create Disk Image* under the upper left corner *File*.
- b. Select *Physical Drive* as the evidence type.
- c. Select the microSD card as the physical drive. In this case, it is *PHYSICALDRIVE1*. This initial setup ensured that the imaging tool accessed the intended device without errors.
- d. Next, create an image destination. Make sure to click on *Verify images after they are created* to ensure the integrity of the process.
- e. The image type was configured to produce raw (dd) format images. This image format was selected because it is widely supported by multiple forensic examination tools and can generate a bit-by-bit, identical replica of the source media.
- f. Fill in the evidence information as needed.
- g. Select a destination where the image file will be saved, the image filename, and the image fragment size. The Segmentation option, which splits the resultant disk image into files of 1.5GB each, was enabled. This is because the size of some of the images is very big and it is very hard for storage and transport, especially on systems that have restrictions on the size of a file.
- h. Press the *Start* button once the image destination is created.
- i. The dd file is now creating in progress.
- j. The dd file is now created and it takes 6 minutes and 26 seconds.
- k. A total of twenty-one sequentially named files were created from the imaging labelled as *AccessDataFTKImager_dd.001* to *AccessDataFTKImager_dd.021*.
- l. A text file that includes all the information of the acquisition such as segment lists, computed hashes, and image verification results is generated. Where the imaging process was completed, the hash values of the source drive and imaged files were checked against each other to ensure the integrity of the imaging process, which required confirmation that corruption or alteration did not take place in the process.

The steps to acquire dd file using AccessData FTK Imager are shown in Figure 6 and Figure 7 respectively.

The efficiency and reliability of AccessData FTK Imager were demonstrated within the whole imaging process. The acquisition process starts at 08:32:41 and ends at 08:39:07, which takes about 6 minutes and 26 seconds. The imaging operation was error-free and created twenty-one segments of images. All segments were in raw format (dd), thus assuring the compatibility of these segments with a wide array of forensic tools. Its segmentation feature turned out to be perfect in dividing the image into manageable file sizes that simplify storage, transfer, and analysis.

During the actual process of imaging, FTK Imager carried out very strong data integrity validation through implemented hashing mechanisms. The original media had an MD5 checksum of 3968a79a3f8e855f3de9f63ccf9e9a38 and a SHA-1 of cb283b24e510ab1b6f9d0c8b41f3a263bb664bf7. These are matched against the generated hashes for the imaged files to confirm that no data was altered or corrupted through the imaging process.

FTK Imager captured the physical details of the source drive as accurate. Identification of the microSD card resulted in 3,880 cylinders, 255 tracks per cylinder, and sixty-three sectors per track. Thus, the size is approximately 30,436MB with a sector count of 62,333,952. These detailed metrics give confidence in the reliability and accuracy of the imaging that has taken place and further pinpoint how precise a tool FTK Imager is for forensic purposes.

In sum, imaging went without any glitches or complications. Since the imaged format was raw (dd), the data structure was bit-for-bit identical to that on the source drive, thus ensuring forensic soundness. As with all tools, verbose output made it easier to report comprehensive details about every step of the process, including imaging timestamps, hash verification, and segment lists, among other things, enabling reproducibility and transparency.

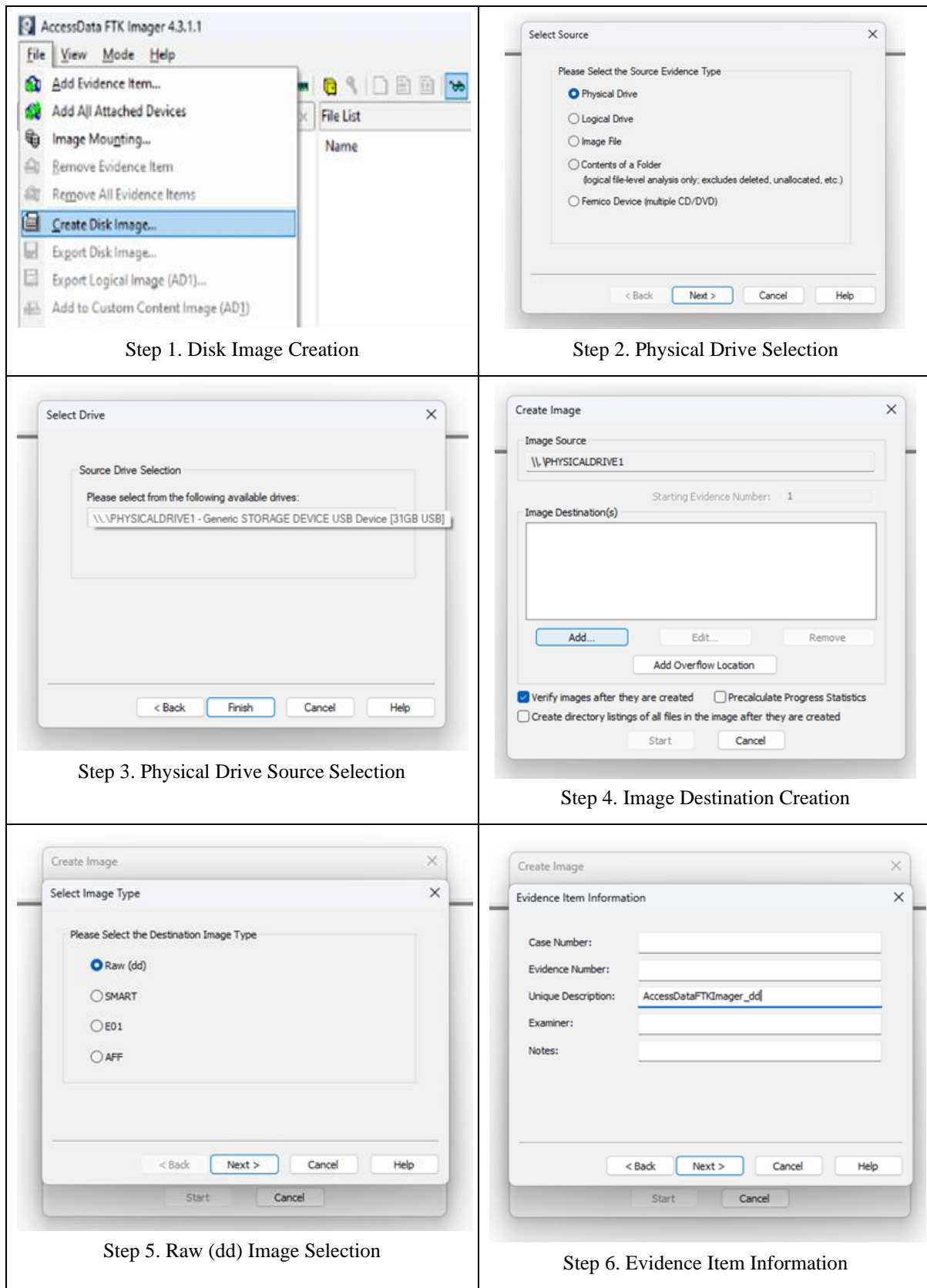


Figure 6. Data Collection and Analysis using AccessData FTK Imager (Steps 1 – 6)

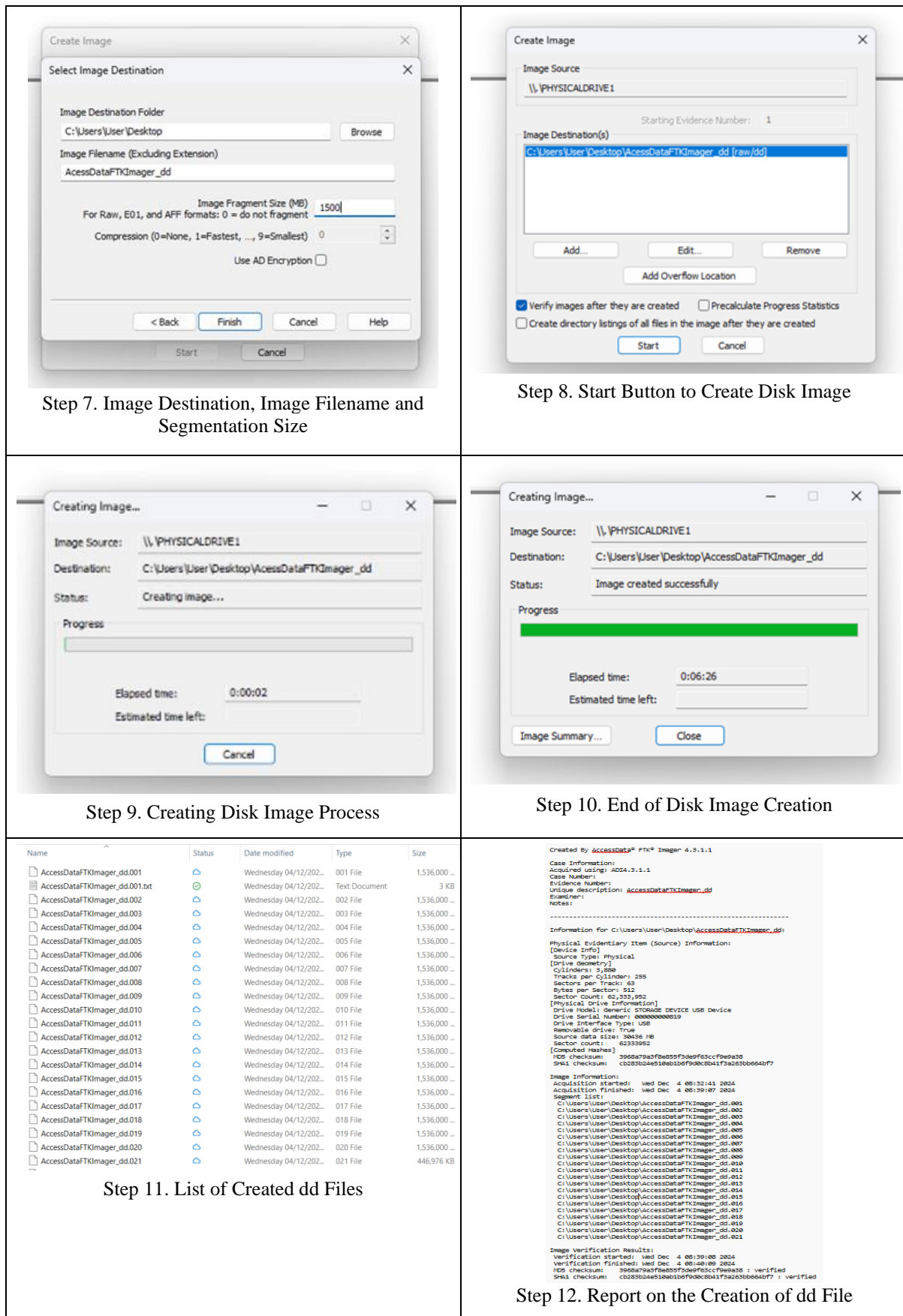


Figure 7. Data Collection and Analysis using AccessData FTK Imager (Steps 7 – 12)

4. RESEARCH DISCUSSIONS

4.1 FTKImager

Exterro FTK Imager is a useful tool in digital forensics because it strikes a compromise between usability and sophisticated forensic imaging capabilities. Because of its simple user interface, the tool keeps performance standards high while making imaging easier for investigators. Accessibility for forensic experts is guaranteed by its interoperability with Windows-based operating systems. Furthermore, Exterro FTK Imager is a cost-free solution, which appeals to businesses on a tight budget.

Its hashing capabilities, which include MD5 and SHA-1, are among its characteristics. To guarantee the integrity of the forensic picture, these hashing methods are applied both during and after the imaging procedure. By comparing the resulting hashes with the original data, it is confirmed that no corruption or manipulation took place during collection. This guarantees that the data is legally defensible and improves the imaging process' credibility. A range of output formats, including Raw (dd) and EnCase (E01), are also supported by the utility. The forensic community generally accepts these formats, which makes it possible to use them with other forensic tools and streamline the analysis procedure. Additionally, Exterro FTK Imager makes it possible to divide big disk pictures into smaller segments, which is very helpful for transmitting and keeping evidence when there are storage or hardware constraints.

Exterro FTK Imager's capacity to generate thorough logs and reports is another asset. These reports provide information including segmentation lists, imaging timestamps, and hash values. The tool's output complies with chain-of-custody regulations, giving investigators the audit trail they need for admissibility in court. Exterro FTK Imager is only compatible with Windows, thus experts using Linux who would prefer open-source alternatives are not able to use it. Furthermore, sophisticated hashing algorithms like SHA-256, which are widely used in forensic processes, are not supported by Exterro FTK Imager. One may argue that the lack of additional hashing options and native Linux support are constraints that address more specialized use cases.

Exterro FTK Imager consistently performs well in terms of imaging speed, especially for small-to-medium-sized drives. Exterro FTK Imager ensures that evidence is precisely maintained during capture by striking a balance between speed and data integrity. All things considered, Exterro FTK Imager is a reliable and effective forensic imaging instrument. It is a popular option for forensic investigations because of its user-friendliness, thorough reporting, and compatibility with popular formats. For digital forensic experts working in a Windows environment, it remains a dependable option even though it might not meet needs like Linux compatibility or extremely quick imaging of huge disks.

4.2 Guymager

Because users just need to specify the storage media and are frequently just a few clicks away from finishing the imaging process, Guymager offers an intuitive user interface with a reduced learning curve. Guymager is also completely open source, which makes it more user-friendly and freer to use because there are many tutorials available. Besides that, Guymager also has a decent imaging speed, making it suitable to handle smaller to medium sized drives. Nevertheless, Guymager stands out as it includes a separate verification check to ensure that all parts of the acquisition were done successfully which often reduces the imaging speed, nevertheless this flaw is balanced out by its tendency to provide extra checks. Next is Guymager's ability to produce hashes, similarly to most imaging tools Guymager also can produce hashes which include the three main hashing used which are MD5, SHA-1 and SHA-256. These hashes are produced for the original copy and the clone itself and if both matches, it means that the bit-by-bit replica is successful which can ensure the integrity of the work done.

Guymager provides an understandable amount of data formats which primarily are the dd format, the AFF format and the EWF format which provides compatibility for the general forensics use cases. Guymager also provides a detailed logged report of what steps have been taken, how long the imaging lasted, the operating system used along with the hardware details and other detailed information of the imaging process. This auto-generated log of information not only eases the user in generating the necessary information for imaging to ensure the quality of work, but it also helps to enhance the credibility of the provided evidence as the detailed log generates information about everything which user could have an oversight if the report was done manually.

Lastly, the main benefit but also the limitation of Guymager is that it is fully Linux-based, which only allows it to be done on Linux Operating Systems. Its strengths lie in that not many imaging tools are created for Linux-based OS but rather Windows which allows Guymager to stand out as one of the main go-to choices for Linux users. This

is because not only is Linux compatible, but it also performs decently as it is open source. Nevertheless, this strength is also its weakness as most users are Windows-based and Guymager is only created for a very niche market of Linux users.

4.3 X-Ways Forensic

X-Ways Forensics has a user interface that has a steep learning curve due to its large variety of functions. This means that it is more suitable for professionals and not beginner friendly. Users will need training before they can master and use all the functions of X-Ways Forensic. However, the tool's sophisticated features and capabilities make it one of the most effective and practical tools for forensic inquiry once users become acquainted with it.

Additionally, when compared to other imaging tools, X-Ways Forensic offers a fast-imaging speed. Large drives can be handled with ease, and its imaging speed depends on a number of variables, including write-blocker usage, source drive state, and hardware performance [35]. Overall, when compared to other imaging programs, X-Ways Forensic can image a disk more quickly.

Furthermore, X-Ways Forensic supports common hashing methods like MD5, SHA-1, and SHA-256. These techniques generate hash values for the source disk and the forensic picture both during and after the imaging procedure. Matching hash values preserve the credibility and dependability of the evidence produced by confirming that the picture is an identical bit-for-bit reproduction of the original.

In addition, a wide variety of output formats are supported by X-Ways Forensic. This covers raw forensic image formats such as DD (dd, .img), which are popular because of their ease of use and wide range of compatibility. Additionally, EnCase formats (.e01, .ex01), which are renowned for their sophisticated metadata and compression capabilities, are supported. The FTK image format (ad1) from AccessData, the SMART forensic format (.s01), and the proprietary container format (.ctr) from X-Ways are further proprietary formats. Additionally, the program works with open formats like AFF (.aff, .afm, .afd), which provide flexibility for various forensic requirements.

X-Ways Forensic is a helpful tool for forensic investigations since it can provide a variety of output formats and is interoperable with other forensic programs, which facilitates the investigation process. Since X-Ways Forensic supports most of the widely used forensics tools, the wide range of supported output formats also makes it simpler for other investigators to duplicate the discoveries.

In addition, X-Ways Forensics facilitates the division of photos into more digestible, smaller segments. When moving evidence across computers or dealing with restricted storage capacity, this capability is quite helpful. Segmentation guarantees that extensive research may continue without sacrificing storage or performance limitations.

The hash between the original disk and the imaged disk is then automatically calculated and compared by X-Ways Forensics, which further supports verification. This increases the forensic evidence's dependability and suitability for use in court by preserving its authenticity and integrity. This keeps the evidence intact and makes it more legally defensible.

The fact that X-Ways Forensic can only be used with Windows-based operating systems and needs administrator credentials to install and run is one of its primary drawbacks. Other operating systems are not supported. Finally, this instrument's expensive licensing, which costs RM5,469 for a single account annually, makes it less accessible to users than other tools. This is another drawback of this tool in comparison to others. Because of its many features, X-Ways Forensic remains one of the top forensic investigation tools despite the limitations.

4.4 OSForensics

The results of disk imaging process using OSForensics allow us to identify the strength and weakness of this tool used for forensic investigation purposes.

The identification of bad blocks in the source drive using the tool can cause the imaging to fail. These bad blocks that have been identified can cause imaging tools to have difficulty in reading data accurately, leading to damaged, incomplete or corrupted image files. OSForensics is particularly sensitive to bad blocks compared to other tools. Other tools were able to successfully create disk images without encountering bad block issues. The sensitivity of

OSForensics made it difficult to read the data, hence resulting in failure to mount the .dd file. This suggests that OSForensics should acquire more robust-handling mechanisms to better manage bad sectors.

Next, the lack of support for segmentation is one of the limitations of the free trial version of the tool. Segmentation is a crucial step in disk imaging as it allows us to divide data into manageable chunks. These segmented data help to carry out analysis for the imaging process. Especially dealing with large drives or unseen corrupted files, it is important to utilize the segmentation feature, as it will be easy to manage the chunks later. The absence of this feature made it complicated for storage of resulting images and hindered the usability for subsequent analysis.

The use of the hash algorithms demonstrated the effort to ensure data integrity throughout the imaging process. The checksum of source and image were matched in this experiment, which shows that the verification of source and image are completed and matched successfully. While the hash values indicated the integrity of data processed, the corruption of the disk image rendered hashes less relevant. The statement has been made so, because the image could not be used for effective analysis.

In conclusion, the imaging tool used which is OSForensics performed its basic functions, to complete the disk imaging, but faced a lot of issues and produced an outcome that is not usable. The lack of segmentation features and sensitivity to bad blocks poses challenges that are not encountered in other tools. The limitation in using trial version made other tools to be more effective for this experiment. Improvements such as segmentation can be solved by using premium version, and for future investigations OSForensics should adopt a robust error handling method.

4.5 AccessData FTK Imager

The findings of this research have been able to highlight the strengths of AccessData FTK Imager in the digital forensic investigation domain. The segmentation feature proved to be a standout capability, allowing the tool to comfortably handle big storage devices while maintaining the integrity of data. This feature proves very useful when constraints either at storage or transfer levels require the use of smaller file sizes.

The hash verification results, which perfectly match the source data, further establish the forensic soundness assurance by FTK Imager. Supporting its applicability within forensic workflows, this tool provides the capability to generate reports that are detailed in their drive geometry and file segmentation. Additionally, efficient processing time highlights its suitability for time-sensitive investigations.

Besides that, FTK Imager adds great value in the field of automated reporting for forensic workflows. Such logs developed while imaging include but are not limited to details about the device geometry, hash values, and segmentation details, and these provide a very strong chain of custody of any digital evidence. This allows for transparency and ensures that whatever activities are performed on imaging are reproducible and verifiable if challenged by the court.

In turn, the research showed some weaknesses, though FTK Imager has very strong hashing, it could be further improved by the inclusion of support for advanced hashing algorithms, like SHA-256 and SHA-512, which are increasingly being adopted in forensic workflows. Compared to other forensic imaging tools, FTK Imager presents itself as very practical for investigators because it is easy to use and broadly supports multiple formats. The performance regarding forensic soundness corresponds to industrial benchmarks, thus having a role as the cornerstone in digital forensic workflows.

5. SUMMARY OF DISK IMAGING TOOLS

The methods used in this experiment, and its findings, have direct application in the real world of digital forensic investigations. The fact that the image is in raw format means that the forensic analyst has a full bit-for-bit image of the original drive on which all the data concerning deleted files and unallocated space is stored. Forensic analysis encompasses anything from recovering deleted files to looking for hidden data on the storage medium. Verification of the integrity of data by hashing mechanisms like MD5 and SHA-1 ensures that imaged data is forensically sound and admissible, an important basis on which cases in court can proceed.

In practical forensic scenarios, the techniques employed in this study can be applied to a variety of investigations. The segmentation feature in AccessData FTK Imager, FTK Imager and X-Ways Forensics is very useful in situations where evidence needs to be transferred across systems that have file-size limitations. For example, older

operating systems with file-size limitations or constrained cloud storage platforms. Besides that, the ability to create raw format images in dd format allows an examiner to use multiple forensic tools to perform more in-depth analysis, such as recovering deleted files using specialized recovery software. The comparison table is shown in Table 1. Consider a scenario where one needs to examine a removable storage device said to contain illicit materials. An examiner can use AccessData FTK Imager, FTK Imager, Guymager, X-Ways Forensics, and OS Forensics to forensically image the microSD card. That way, analysis can be done on an imaged copy, thus preserving the original evidence. This will ensure the integrity of the original evidence is preserved for court purposes. Moreover, being able to verify the hash values before and after will ensure that evidence has not been tampered with during the acquisition process.

Table 1. Comparison of Disk Imaging Tools

Feature/Tool	FTK Imager	Guymager	X-Ways Forensics	OSForensics	AccessData FTK Imager
Ease of Use	User-friendly GUI, intuitive workflows	Simple GUI, suitable for Linux users	Advanced interface with a steep learning curve, suited for experienced professionals.	User-friendly GUI, straightforward workflow.	User-friendly GUI, intuitive workflows
Imaging Speed	Efficient and consistent	Moderate, varies by hardware (12 minutes and 20 seconds includes verification)	Highly efficient imaging process, optimized for faster speeds on compatible hardware.	Slow, not as the other tools in this experiment. (2 hours 31 minutes)	6 minutes and 26 seconds (efficient and consistent)
Hashing Support	MD5, SHA-1 (SHA-256 not supported)	MD5, SHA-1, SHA 256	Supports MD5, SHA-1, and SHA-256	MD5, SHA-1 and supports SHA-256	MD5, SHA-1 (SHA-256 not supported)
Output Formats	Raw (dd), E01	Raw (dd), EWF	Raw (dd, .img), E01, .ad1, .ctr, .s01, .aff	Raw (dd), AFF	Raw (dd), SMART, E01, AFF
Segmented Images	Supported (customizable)	Supported (less customizable)	Supported (customizable)	Limited segmentation	Supported (customizable)
Verification Support	Automated hash verification	Hash verification available	Automatic hash calculation and verification	Automated hash verification	Automated hash verification
Platform Compatibility	Windows	Linux	Windows	Windows	Windows
Price	Free and Open Sourced	Free and Open Sourced	Licensed and cost RM RM5,469 per year for 1 account	Free and Open Sourced	Free and Open Sourced

For instance, in a case requiring an investigation into corporate espionage in terms of unauthorized data transfer, AccessData FTK Imager, FTK Imager, Guymager, X-Ways Forensics, and OS Forensics has the capabilities to perform detailed reporting and hashing allowing investigators to show that critical evidence-say, residual network logs or traces of deleted files-were on the imaged device without destroying its evidentiary integrity. Linking the results of this experiment to these scenarios makes it clear that AccessData FTK Imager, FTK Imager, Guymager, X-Ways Forensics, and OS Forensics are important constituents of modern digital forensic investigations.

The result of hash verification, perfectly matched with source data, again establishes the capability of AccessData FTK Imager, FTK Imager, Guymager, X-Ways Forensics, and OS Forensics to ensure forensic soundness. Its capability to generate a detailed report with comprehensive drive geometry and file segmentation establishes its applicability in forensic workflows. Besides, the time consumed for processing shows its applicability in time-critical investigations too.

5.1 Findings

The methods used in this experiment, and its findings, have direct application in the real world of digital forensic investigations. The fact that the image is in raw format means that the forensic analyst has a full bit-for-bit image of the original drive on which all the data concerning deleted files and unallocated space is stored. Forensic analysis encompasses anything from recovering deleted files to looking for hidden data on the storage medium. Verification of the integrity of data by hashing mechanisms like MD5 and SHA-1 ensures that imaged data is forensically sound and admissible, an important basis on which cases in court can proceed.

In practical forensic scenarios, the techniques employed in this study can be applied to a variety of investigations. The segmentation feature in AccessData FTK Imager, FTK Imager and X-Ways Forensics is very useful in situations where evidence needs to be transferred across systems that have file-size limitations. For example, older operating systems with file-size.

limitations or constrained cloud storage platforms. Besides that, the ability to create raw format images in dd format allows an examiner to use multiple forensic tools to perform more in-depth analysis, such as recovering deleted files using specialized recovery software.

Consider a scenario where one needs to examine a removable storage device said to contain illicit materials. An examiner can use AccessData FTK Imager, FTK Imager, Guymager, X-Ways Forensics, and OS Forensics to forensically image the microSD card. That way, analysis can be done on an imaged copy, thus preserving the original evidence. This will ensure the integrity of the original evidence is preserved for court purposes. Moreover, being able to verify the hash values before and after will ensure that evidence has not been tampered with during the acquisition process.

For instance, in a case requiring an investigation into corporate espionage in terms of unauthorized data transfer, AccessData FTK Imager, FTK Imager, Guymager, X-Ways Forensics, and OS Forensics has the capabilities to perform detailed reporting and hashing allowing investigators to show that critical evidence-say, residual network logs or traces of deleted files-were on the imaged device without destroying its evidentiary integrity. Linking the results of this experiment to these scenarios makes it clear that AccessData FTK Imager, FTK Imager, Guymager, X-Ways Forensics, and OS Forensics is an important constituent of modern digital forensic investigations.

The result of hash verification, perfectly matched with source data, again establishes the capability of AccessData FTK Imager, FTK Imager, Guymager, X-Ways Forensics, and OS Forensics to ensure forensic soundness. Its capability to generate a detailed report with comprehensive drive geometry and file segmentation establishes its applicability in forensic workflows. Besides, the time consumed for processing shows its applicability in time-critical investigations too.

6. CONCLUSION

In conclusion, in this research, testing against five of the commonly used which are FTKImgaer, Guymager, X-Ways Forensics, OSForensics and AccessDataFTK Imager were performed. The test was conducted by using a common computer which has the same specifications to perform the test. An external 32 GB SD card was used to simulate the storage medium that needed to be cloned. A few comparison metrics were collected for all five imaging tools which included, ease of use, imaging speed, hashing algorithms, output formats, segmented images, verification, platform and price. It can be concluded that among the top performers for most categories was AccessDataFTK Imager. Hence, for the general users AccessDataFTK Imager provides the best performance as compared to its counterparts but in special case scenarios other choices may be deemed as more suitable. Such scenarios include requiring specific uses of the imaging tool and are not limited to budget, users may select X-Way Forensics as a better alternative instead. Another scenario that other tools may deem suitable is if the device used for cloning is Linux based. The Guymager is the only option among the five which is catered for Linux OS. This study evaluates each tool in terms of ease of use, imaging speed, supported hashing algorithms, supported output formats and more to evaluate how each tool can be used in different forensic situations. The result of the evaluation indicates that X-Ways Forensic is one of the best tools for imaging due to its large variety of functions and supported formats but requires a paid license for full access to its features.

ACKNOWLEDGEMENT

We thank the anonymous reviewers for the careful review of our manuscript.

FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this article.

AUTHOR CONTRIBUTIONS

Michelle Chee Ern Lim: Researched about X-Ways Forensics
Brandon Chen Hong Chow: Researched and completed disk imaging for Guymager
Le Ying Lim: Researched and completed disk imaging for AccessData FTK Imager
Tarini A/P Shanbagamaran: Researched and completed disk imaging for OSForensics.
Darren Lim Yong Jun: Researched and completed disk imaging for FTK Imager
Ngu War Hlaing: Supervised the research group and wrote the paper
Ahmad Sahban Rafsanjani: Introduced the research topic idea

CONFLICT OF INTERESTS

No conflict of interest was disclosed.

ETHICS STATEMENTS

Our publication ethics follow The Committee of Publication Ethics (COPE) guideline.
<https://publicationethics.org/>



REFERENCES






- [1] A. Alazab, A. Khraisat, and S. Singh, "A review on the Internet of Things (IoT) forensics: challenges, techniques, and evaluation of digital forensic tools," *IntechOpen eBooks*, Feb. 2023. doi: 10.5772/intechopen.109840.
- [2] S. Al-Juboori and S. Jimoh, "Cyber-Securing Medical Devices Using Machine Learning: A Case Study of Pacemaker," *Journal of Informatics and Web Engineering*, vol. 3, no. 3, p. 271, 2024. doi: 10.33093/jiwe.2024.3.3.17
- [3] N. A. Almubairik and F. A. Khan, "Systematic Literature Review on Wearable Digital Forensics: Acquisition Methods, Analysis Techniques, Tools, and Future Directions," *IEEE Internet of Things Journal*, 2024. doi: <https://doi.org/10.1109/JIOT.2024.3485027>.
- [4] J.-J. Chin, "Editorial: Artificial Intelligence and Cybersecurity in Pervasive Computing," *Journal of Informatics and Web Engineering*, vol. 3, no. 3, pp. 208–213, Oct. 2024. doi: 10.33093/jiwe.2024.3.3.13.
- [5] A. S. Rafsanjani, N. B. Kamaruddin, M. Behjati, S. Aslam, A. Sarfaraz, and A. Amphawan, "Enhancing malicious URL detection: A novel framework leveraging priority coefficient and feature evaluation," *IEEE Access*, 2024. doi: 10.1109/ACCESS.2024.3412331
- [6] A. S. Rafsanjani, N. B. Kamaruddin, H. M. Rusli, and M. Dabbagh, "Qsecr: Secure qr code scanner according to a novel malicious url detection framework," *IEEE Access*, vol. 11, pp. 92523-92539, 2023. doi: 10.1109/ACCESS.2023.3291811.
- [7] K. M. Salih and N. Dabagh, "Digital forensic tools: A literature review," *Journal of Education and Science*, vol. 32, no. 1, pp. 109.0-124.0, 2023. doi: 10.33899/edusj.2023.137420.1304.
- [8] M. Khanafseh, M. Qataweh, and W. Almobaideen, "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 8, 2019. doi: 10.14569/ijacsa.2019.0100880.
- [9] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," *IEEE Access*, vol. 10, pp. 11065-11089, 2022. doi:10.1109/ACCESS.2022.3142508.

- [10] R. G. Arias, J. B. Higuera, J. J. R. Granados, J. R. B. Higuera, and J. A. S. Montalvo, "Systematic Review: Anti-Forensic Computer Techniques," *Applied Sciences*, vol. 14, no. 12, p. 5302, Jun. 2024. doi: 10.3390/app14125302.
- [11] S. Sachdeva, B. Raina, and A. Sharma, "Analysis of digital forensic tools," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 6, pp. 2459-2467, 2020. doi: 10.1166/jctn.2020.8916.
- [12] C.-H. Yang and P.-H. Yen, "Fast deployment of computer forensics with USBs," in *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*, 2010: IEEE, pp. 413-416. doi: 10.1109/BWCCA.2010.106.
- [13] K. Parveen and G. Haider, "Digital Investigations: Navigating Challenges in Tool Selection for Operating System Forensics," *International Journal for Electronic Crime Investigation*, vol. 8, no. 1, pp. 79-92, 2024. doi: 10.54692/ijeci.2024.0801189.
- [14] J.-U. Lee and W.-Y. Soh, "Comparative analysis on integrated digital forensic tools for digital forensic investigation," in *IOP conference series: materials science and engineering*, 2020, vol. 834, no. 1: IOP Publishing, p. 012034. doi: 10.1088/1757-899X/834/1/012034.
- [15] A. Abirami and S. Palanikumar, "Proactive network packet classification using artificial intelligence," in *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities*: Springer, 2021, pp. 169-187.
- [16] F. Amato, G. Cozzolino, V. Moscato, and F. Moscato, "Analyse digital forensic evidences through a semantic-based methodology and NLP techniques," *Future Generation Computer Systems*, vol. 98, pp. 297-307, 2019. doi: 10.1016/j.future.2019.02.040.
- [17] T. Wu, F. Breitingner, and S. O'Shaughnessy, "Digital forensic tools: Recent advances and enhancing the status quo," *Forensic Science International: Digital Investigation*, vol. 34, p. 300999, 2020. doi: 10.1016/j.fsidi.2020.300999.
- [18] J. Cosic, C. Schlehuber, and D. Morog, "Digital forensic investigation process in railway environment," in *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2021: IEEE, pp. 1-6. doi: 10.1109/NTMS49979.2021.9432658.
- [19] E. E.-D. Hemdan and D. Manjaiah, "An efficient digital forensic model for cybercrimes investigation in cloud computing," *Multimedia Tools and Applications*, vol. 80, pp. 14255-14282, 2021. doi: 10.1007/s11042-020-10358-x.
- [20] S. Costantini, G. De Gasperis, and R. Olivieri, "Digital forensics and investigations meet artificial intelligence," *Annals of Mathematics and Artificial Intelligence*, vol. 86, no. 1, pp. 193-229, 2019. doi: 10.1007/s10472-019-09632-y.
- [21] A. Krivchenkov, B. Misnevs, and D. Pavlyuk, "Intelligent methods in digital forensics: state of the art," in *Reliability and Statistics in Transportation and Communication: Selected Papers from the 18th International Conference on Reliability and Statistics in Transportation and Communication, RelStat'18, 17-20 October 2018, Riga, Latvia 18*, 2019: Springer, pp. 274-284. doi: 10.1007/978-3-030-12450-2_26.
- [22] R. M. A. Mohammad and M. Alqahtani, "A comparison of machine learning techniques for file system forensics analysis," *Journal of Information Security and Applications*, vol. 46, pp. 53-61, 2019. doi: 10.1016/j.jisa.2019.02.009.
- [23] O. M. Alhawi, J. Baldwin, and A. Dehghantanha, "Leveraging machine learning techniques for windows ransomware network traffic detection," *Cyber threat intelligence*, pp. 93-106, 2018. doi: 10.1007/978-3-319-73951-9_5.
- [24] S. Srinivasan, V. Ravi, M. Alazab, S. Ketha, A. M. Al-Zoubi, and S. Kotti Padannayil, "Spam emails detection based on distributed word embedding with deep learning," *Machine intelligence and big data analytics for cybersecurity applications*, pp. 161-189, 2021. doi: 10.1007/978-3-030-57024-8_7.
- [25] S. Sachdeva and A. Ali, "Machine learning with digital forensics for attack classification in cloud network environment," *International Journal of System Assurance Engineering and Management*, vol. 13, no. Suppl 1, pp. 156-165, 2022. doi: 10.1007/s13198-021-01323-4.

- [26] I. H. Sarker, "Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects," *Annals of Data Science*, vol. 10, no. 6, pp. 1473-1498, 2023. doi: 10.1007/s40745-022-00444-2.
- [27] A. Singh, A. R. Ikuesan, and H. S. Venter, "Digital Forensic Readiness Framework for Ransomware investigation," in Springer eBooks, 2018, pp. 91–105. doi: 10.1007/978-3-030-05487-8_5.
- [28] D. Sun, X. Zhang, K.-K. R. Choo, L. Hu, and F. Wang, "NLP-based digital forensic investigation platform for online communications," *Computers & Security*, vol. 104, p. 102210, Jan. 2021. doi: 10.1016/j.cose.2021.102210.
- [29] G. Al-Asad, M. Al-Husainy, M. Bani-Hani, A. Al-Zu'bi, S. Albatienh, and H. Abuolien, "Comparative assessment of hash functions in securing encrypted images," *Engineering Technology & Applied Science Research*, vol. 14, no. 6, pp. 18750–18755, Dec. 2024. doi: 10.48084/etasr.8961.
- [30] A. Alshammari, "Detection and Investigation Model for the Hard Disk Drive Attacks using FTK Imager," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 7, Jan. 2023. doi: 10.14569/ijacsa.2023.0140784.
- [31] L. Lau, "Book Review: The X-Ways Forensics Practitioner's Guide," *The Journal of Digital Forensics, Security and Law*, Jan. 2014. doi: 10.15394/jdfsl.2014.1188.
- [32] H. Kang et al., "Android-Based Audio Video Navigation System Forensics: A case study," *Applied Sciences*, vol. 13, no. 10, p. 6176, May 2023. doi: 10.3390/app13106176.
- [33] N. A. H. Haldar, "Advances in digital forensics frameworks and tools," *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*, vol. 165, 2020. doi: 10.4018/978-1-7998-2466-4.ch010
- [34] S. Fleischmann, "X-Ways Forensics/WinHex Manual.," ed: X-Ways Forensics Computer Forensics Integrated Software, 2012.
- [35] S. A. Gyimah, "X-Ways Forensics Platform For Digital Forensics Examiners," *Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics*, pp. 353-356, 2022.

BIOGRAPHIES OF AUTHORS

	<p>Michelle Chee Ern Lim is a motivated and aspiring cybersecurity enthusiast currently pursuing a bachelor's degree in information technology, specializing in Computer Networking and Security. She is passionate about cybersecurity and dedicated to honing her technical skills while applying theoretical knowledge to real-world challenges. With a strong interest in network security and ethical hacking, she seeks opportunities to gain hands-on experience and contribute to the ever-evolving field of cybersecurity. She is eager to stay ahead of emerging threats and make a meaningful impact on industry. She can be contacted by email: 21050349@imail.sunway.edu.my</p>
	<p>Brandon Chen Hong Chow is a dedicated cybersecurity student with a strong academic interest in network security, penetration testing, and incident response. His research focuses on identifying vulnerabilities, analysing cyber threats, and developing effective security strategies. He is particularly interested in ethical hacking, risk assessment, and incident response. Through academic coursework and independent study, he explores emerging cybersecurity challenges and defence mechanisms. He actively participates in research initiatives and security competitions, aiming to contribute to the advancement of cybersecurity practices and policies. He can be contacted by email: 21056429@imail.sunway.edu.my</p>

	<p>Le Ying Lim is a dedicated cybersecurity student with a strong academic interest in network security and pursuing a bachelor's degree in computer Networking and Security. His research focuses on identifying vulnerabilities, analysing cyber threats, and developing effective security strategies. He is particularly interested in ethical hacking, risk assessment, and red team operations. Through academic coursework and independent study, he explores emerging cybersecurity challenges and defence mechanisms. He engages in research initiatives and security competitions; he strives to contribute to the development of advanced cybersecurity practices and policies. He can be contacted by email: 21030002@imail.sunway.edu.my</p>
	<p>Tarini A/P Shanbagamaran is a third-year student at Sunway University, pursuing a degree in Information Technology, specializing in Computer Networking and Security. She is passionate about cybersecurity and is keen on exploring digital forensic tools. With hands-on experience in forensic tools, she aims to contribute to the field of cybersecurity. She has also attained the Fortinet Certified Fundamentals in Cybersecurity and Fortinet Certified Associate in Cybersecurity. She actively pursues industry certifications to expertise in advanced cybersecurity disciplines. She can be contacted by email: 21046347@imail.sunway.edu.my</p>
	<p>Darren Lim Yong Jun is a student specializing in computer networks and security, with a strong passion for cybersecurity. He is particularly interested in red team operations, focusing on ethical hacking, penetration testing, and offensive security. Constantly learning and exploring advancements in cybersecurity, he aims to sharpen his skills in adversary simulation and security assessments. With a deep curiosity for digital threats and vulnerabilities, he is committed to contributing to a safer and more resilient cyber landscape. He can be contacted by email: 21056874@imail.sunway.edu.my</p>
	<p>Ngw War Hlaing earned her Bachelor of Engineering (B.Eng.) and Master of Engineering (M.Eng.) degrees from the University of Malaysia Sabah (UMS), in 2018 and 2019, respectively. She completed her doctoral degree in 2023 at Universiti Teknologi Malaysia (UTM). She is also a registered Graduate Engineer under the Board of Engineers Malaysia and is recognized as a Professional Technologist by the Malaysia Board of Technologists. Currently, she is a full-time lecturer at the Faculty of Engineering and Technology, Sunway University. She can be contacted by email: warhlaingn@sunway.edu.my</p>
	<p>Ahmad Sahban Rafsanjani obtained his PhD in network security and his master's in information security from Universiti Teknologi Malaysia (UTM), Malaysia. He is currently Programme leader and senior lecturer at the Department of Smart Computing and Cyber Resilience, Faculty of Engineering and Technology, Sunway University, Malaysia. He has published several research papers in journals and conference proceedings, and his areas of interest include network security, data hiding, cryptography, IoT security, and malware analysis. He can be contacted by email: ahmadsahban@sunway.edu.my</p>