International Journal of Education & Well-Being
Volume 2, Issue 2, 2024, 108-122

ISSN: 2980-3489

DOI: 10.62416/ijwb-41

Research Article

Recieved: 18/05/2024 Accepted: 21/07/2024 Published: 15/08/2024

Handling Data Security in Education

Deshira Imeri-Saiti[1], Mentor Hamiti[2], Jehona Asani[3]

Imeri-Saiti, D., Hamiti, M., Asani, J. (2024). Handling Data Security in Education. *International Journal of Education & Well-Being*, 2(2), 108-122. https://doi.org/ 10.62416/ijwb-41

Abstract

Digital forensics is a new science and follows the rapid changes in the computer environment, expanding into many disciplines, which turns it into a very challenging field that requires the continuous development of methodologies and tools to counter the ever-newer changes in cybercrime. The research subject refers to the analysis and challenges of digital forensics, tracking of hard drives, recovery of deleted files from the hard drive, their quality after recovery, and the possibility of creating forensic images on physically damaged hard drives. The research is based on digital forensics and tracking of all hard drives by creating digital images and analyzing forensic images FTK Imager and Autopsy 4.15.0. The research concludes that the number of files allocated to a forensic image does not play a role in the duration of report generation during the creation of forensic images using FTK Imager. Unlike allocated files, unanalyzed files in a forensic image are directly proportional to the duration of generating reports for forensic images through FTK Imager. Also, in conclusion, it is worth noting that FTK Imager cannot generate a forensic image when the hard drive is physically damaged. This research paper investigates the integral relationship between data security and data recovery even after deletion, highlighting the importance of digital forensics in hard drive security management to protect sensitive information and maintain regulatory compliance, which should also find the right place in education. Educational institutions must balance early education on data permanence and recovery with ensuring students have foundational digital knowledge before introducing complex security concepts.

Keywords: Hard drives, Digital forensics, FTK Imager, Autopsy, Data confidentiality, Education.

Eğitimde Veri Güvenliğinin Yönetimi

Deshira Imeri Saiti[1], Mentor Hamiti[2], Jehona Asani[3]

Özet

Dijital adli bilişim, bilgisayar ortamındaki hızlı değişimlere paralel olarak gelişen ve birçok disiplini kapsayan yeni bir bilim dalıdır. Bu durum, dijital adli bilişimi oldukça zorlu bir alan haline getirir ve sürekli olarak metodolojilerin ve araçların geliştirilmesini gerektirir. Araştırmanın konusu, dijital adli bilişim analizi ve zorlukları, sabit disklerin izlenmesi, silinmiş dosyaların sabit disklerden geri getirilmesi, geri getirilen dosyaların kalitesi ve fiziksel olarak hasar

[1] Faculty of Contemporary Sciences and Technologies, South East European University, North Macedonia, d.imeri@seeu.edu.mk, ORCID: 0009-0003-4533-7862

[2] Faculty of Contemporary Sciences and Technologies, South East European University, North Macedonia, m.hamiti@seeu.edu.mk, ORCID: 0000-0002-5622-1182

[3] Faculty of Contemporary Sciences and Technologies, South East European University, North Macedonia, j.asani@seeu.edu.mk, ORCID: 0009-0004-2626-890X

Address of Correspondence/Yazışma Adresi: d.imeri@seeu.edu.mk

görmüş sabit disklerde adli görüntülerin oluşturulma olasılığını kapsamaktadır. Araştırma, dijital adli bilişim ve tüm sabit disklerin dijital görüntülerinin oluşturulması üzerine odaklanmakta ve adli görüntülerin analizi FTK Imager ve Autopsy 4.15.0 yazılımları kullanılarak yapılmaktadır. Araştırma, FTK Imager kullanılarak adli görüntülerin oluşturulması sırasında dosya sayısının rapor üretme süresini etkilemediğini ortaya koymaktadır. Atanan dosyaların aksine, adli görüntülerde analiz edilmemiş dosyalar, FTK Imager aracılığıyla adli görüntülerin raporlarının oluşturulma süresiyle doğrudan orantılıdır. Ayrıca, FTK Imager'ın fiziksel olarak hasar görmüş bir sabit diskten adli bir görüntü üretemediği sonucuna ulaşılmıştır. Bu araştırma, veri güvenliği ile veri kurtarma arasındaki bütünsel ilişkiyi incelemekte ve silinmiş olsa bile veri kurtarmanın önemini vurgulamaktadır. Dijital adli bilişimin sabit disk güvenlik yönetiminde hassas bilgilerin korunması ve düzenleyici uyumun sağlanması açısından önemine dikkat çekmektedir. Bu konuda eğitimde erken dönem veri kalıcılığı ve kurtarma eğitimi ile öğrencilerin temel dijital bilgilerini sağlamlaştırma arasında bir denge kurulmalıdır.

Anahtar Kelimeler: Sabit diskler, Dijital adli bilişim, FTK Imager, Autopsy, Veri gizliliği, Eğitim.

Introduction

Digital forensics is a separate discipline of forensic science and in different fields, it requires different approaches, different tools, and specialized education and training. Digital forensics threads are characterized by relatively small equipment capacity and relatively small amounts of information. This allowed the entire hard drive to be copied to another drive. The copy was used to analyze the content and to use the same material as evidence.

The rapidly growing Internet technology can give rise to cybercrimes committed by attackers, where various types of digital devices are being used to carry out an attack. To detect such criminal activity, the criminal investigator must use various data recovery methods and a practical framework (Salunkhe, Bharne, & Padiya, 2016). There are different types of forensic tools according to Salunkhe et.al. (2016), namely (FTK), free software, techniques, and tools that are available for the forensic investigation of files such as "Decision Tree" for the generation, storage, and analysis of data obtained from the log files which are presented as evidence in the forensic analysis of the files. There are different types of forensic applications of data analysis according to Hassan (2019), namely application-specific forensics (e.g. web browser forensics), file system forensics (NTFS, FAT, EXT), hardware forensics, multimedia forensics (text, audio, video and images) and memory forensics.

Digital forensics tools allow the recovery of deleted files or fragments of files that can help reconstruct the key events of a case, where deleted files can be easily recovered by checking the file names of deleted files kept in file directories. Still, it is not uncommon for deleted file names to be reused before any changes are made to the "metadata" (Boddington, 2016). According to Prasanthi (2016), from the tools that are free for computer forensics, namely for disk tools and data capture, the relevant tools are used: Arsenal Image Mounter; DumpIt; EnCase Forensic Imaging; Encrypted Disk Detector; EWF MetaEditor; FAT32 format; Web Forensics Acquisition; FTK images; Guymager; Live RAM Capturer; NetworkMiner; Nmap; Magnet RAM Capture; OSFClone; OSFMount; Wireshark; Disk2vhd. Also Autopsia according to sleuthkit.org (2021) is an easy-to-use, GUI (graphical user interface)-based program that allows you to efficiently analyze hard drives and smartphones. It has a plug-in architecture that allows you to find additional modules or develop custom modules in Java or Python.

Kent, Chevalier, Grance, & Dang (2006) describe the basic stages for conducting digital forensics as collection, examination, analysis, and reporting. According to Arnes (2018), the process of digital forensics is divided into 5 successive, but also iterative phases, where the first phase is the identification of possible sources of evidence from digital devices; Then, collecting digital data by copying the source; Next, examining the raw data, giving it structure, so it is easier to process and understand; Then the analysis, where we seek to gain a better state and identify the digital objects that would ideally be evidence and finally, we present them to a court or any other entity of interest.

Special focus is given to the aspect of digital forensics and hard drive tracing. In particular, the analysis of the challenges of digital forensics, the tracking of hard drives, the recovery of deleted files from the hard drive, their quality after recovery, as well as the possibility of creating forensic images on physically damaged hard drives, has been examined.

Literature review

Digital forensics of disk images

In the study by Breitinger & Baggili (2017), a total of 715 cybersecurity articles from 2010 to 2015, from conferences and journals related to data usage, were analyzed. First Breitinger & Baggili categorized the origin of data (i.e., computer generated, experiment generated, or real world). They analyzed its availability and finally, the different types of data (e.g. malware, disk images, etc.), where the results show that most datasets are generated by experiments (56.4%) followed by real-world data (36.7%) and the other hand, 54.4% of articles use existing data. The Real Data Corporation, Digital Corpora (2019) is a collector of raw data extracted from data storage devices that are purchased on the secondary market around the world, where many studies have shown that hard drives, mobile phones, USB sticks, and other devices that hold data are often discarded by their original users without cleaning the data first and upon purchasing these devices and extracting their data. According to data from digitalcorpora.org (2021), the data extraction from the devices consists of 1,289 images of hard drives ranging in size from 500 MB to 80 GB; 643 images of flash drives (USB, Sony Memory Stick, SD, and others), ranging from 128 MB to 4 GB; 98 CDROMs and a total of 70 TB of data (uncompressed).

According to Moch & Freiling (2009), there are several ways to obtain interesting images from the hard disk for training digital investigators, where the first and most obvious way is their construction or manual approach and in this case, an instructor carefully prepares a floppy disk or hard disk image with separate files and artificial evidence, and the resulting image is then distributed to students online or on a USB. The second approach involves a special form of "real" cases, that is, those produced using honeypots, while briefly, a honeypot is a computer that is connected to the network so that it can be attacked and compromised. The third approach is called the second-hand approach, which consists of acquiring a large amount of second-hand hard drives and giving them to students for analysis. This approach is also suitable for raising awareness among students about the value of their data since the evidence found is in a sense "real" and this approach has a high motivation factor.

The first step in generating synthetic data is to define use cases for the data, for example, in a digital forensics class where students will be tested on their knowledge of hard drive analysis, they will need to search disk images for traces of malware or recover fragments of multimedia data using relevant tools (Yannikos, Graner, Steinebach, & Winter, 2014). Disk images can be created in a reasonable amount of time manually or through scripting. The second step in the generation process is to specify a real-world scenario. Such an example is a computer used by many individuals who usually install and uninstall software, download, copy, delete, and overwrite files, while the third step is to create a model to match the file and serve as the basis of a simulation, which is also the last step.

Hard drives and features

The ever-increasing number of hard drives is mainly due to the rapid advancement of technology, where visual inspection technology in the hard drive industry includes the latest progress and developments in computer vision technology of hard drives (HDD) (Muneesawang & Yammen, 2015). Although their storage comes in many forms, hard drives are the richest sources of digital evidence on computers, where even modern technological machines have hard drives and can be connected to external controllers with a CPU, RAM, and high-capacity hard drives, and data can be stored, erased and can help digital investigators deal with hard drives as a source of evidence (Casey, 2011). HDD drives come in two forms, fixed (internal) and external, where the first (fixed) is located inside the computing device, while the external HDD can be connected to the computing devices via a USB or eSATA cable. HDD devices store data on platters, where a hard drive can have a set number of platters; Drives with capacities less than 500 GB will contain only one platter, while larger capacity drives may have anywhere from one to five platters, depending on the HDD's physical size, capacity, manufacturer, and model (Hassan, 2019). The capacity of a hard disk can be calculated by multiplying the number of cylinders, heads, and sectors by 512 bytes each (Casey, 2011). All file systems used by Windows are organized by hard drives based on cluster size (a cluster consists of several sectors), where the cluster size represents the smallest amount of disk space that can be used to hold a file and depends on the file system used and the size of a partition and varies from 4 to 64 sectors (Hassan, 2019).

According to (EC-Council, 2009) some characteristics that distinguish the different types of hard drives are the capacity of the hard drive, the interface used, the speed of rotations per minute, search time, access to time, and timing of transfer; while according to the data density on a hard disk, there are three types: track density: (the space between tracks on a disk), area density: (the number of bits per square inch on a platter) and bit density: (one bit per track length unit). The two most common form factors of contemporary HDDs are 3.5-inch for desktop computers and 2.5-inch mostly for laptops, while HDDs are connected to systems via standard interface cables such as PATA (parallel ATA) cables, SATA (Serial ATA), USB or SAS (Zlatanov, 2015).

In recent years, similar to flash memory, SSDs have appeared, which have no moving parts (or platters) and store data in a series of NAND flash cells or microchips (NAND is composed of a group of transistors similar to that used in RAM). According to Hassan (2019), SSD also uses some kind of controller (which is an embedded processor) to determine how to store, retrieve, and memorize data. Despite the advantages of speed, silence, and lower power consumption of the SSD type, the HDD will remain in widespread use for many years to come.

Hard drive forensics

A typical investigation involves seizing a hard drive and other media, such as USB drives; making forensic copies; evaluating evidence; and submitting a report. For example, a forensic analysis of a 6 TB drive can take several days or weeks. This means that based on experience, the forensic laboratory manager can estimate how many cases each investigator can handle and when they can expect a preliminary and final report on each case (Nelson, Phillips, & Steuart, 2019). Computer storage devices (such as hard drives or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may attempt to conceal incriminating evidence;

he or she may store it at random with misleading file names and this prompts the investigating authorities to examine all the stored data to determine which particular files are evidence or instruments of crime (Sammons J., 2012).

Forensics tools were born in DOS, and over the years, Windows hard drives used a variety of file systems, including FAT16, FAT32, New Technology File System (NTFS), Resilient File System (ReFS) and others, where most DOS-based tools could not read NTFS drives, in addition, the popularity and spread of the Xbox required investigators to be familiar with the FATX file system (Nelson, Phillips, & Steuart, 2019). This means that for evidence stored on a hard drive, there are defined methods and best practices for acquiring and interpreting data. When retrieving data from a hard drive, it is important to remove the drive, connect it to another computer through a write blocker, and make an exact bit-for-bit copy of the hard drive (Arnes, 2018). Physical acquisition, also known as a bit-stream image, in this method, a bit-for-bit, sector-by-sector copy of a hard disk is generated. File system metadata, deleted files, deleted file fragments, and unallocated space will also be captured using this method, where the resulting image will be a complete duplicate of the source (copy of correct); in other words, if we are taking a forensic image of a 500 GB hard drive, the resulting image will be exactly 500 GB, unless compression is used during the acquisition process. This is the most commonly used method in investigating captured data that is stored in an image file, while the second method is to copy the data (bit-for-bit) from the source disk to a newer disk that has the same storage capacity or slightly more (Hassan, 2019). Alternative approaches advance one step further, i.e., complete reconstruction of the disk image in a forensically sound manner, i.e. in the proposed system, where the data image is not accessed through a copy entire bit-for-bit, but it gives the same forensically sound disk image to the investigator. The acquisition result can be verified by comparing the hash of the recreated disk image with the original one. To reconstruct the disk image, three components of binary data are needed, which are: file data, block-level slack space, and the third is unallocated disk space, where this reconstructed image can then be verified against the original drive by comparing their hash values (Du, Ledwith, & Scanlon, 2018).

Digital forensics tools can fall into many different categories, including database forensics, disk and data capture, email analysis, file analysis, file viewers, internet analysis, mobile device analysis, network forensics, and registry analysis. In addition, many tools fulfill more than one function simultaneously, and a significant trend in digital forensics tools is “wrappers”—one that package hundreds of specific technologies with different functionalities into one overarching toolkit (Zbrog, 2024).

A physical extraction can be performed using keyword searches based on file terms provided by the investigator and examining unallocated space, i.e., space available on a system because it has never been used or because the information in it has been deleted. Logical extraction, on the other hand, involves searching for and retrieving evidence from the situation in which it is located about the system of record in a computer operating system, which is used to maintain records of the names and locations of files that are stored in a storage device such as a hard drive (Prakash & Duhan, 2020).

Method

In this research, in correlation with the forensics of four Sata-type hard drives, we created digital images of the hard drives through FTK Imager software. Generated images were analyzed using Autopsy 4.15.0 software. The main objectives that have been elaborated are the analysis of digital forensics challenges, the tracing of hard drives, the recovery of deleted files from hard drives, their quality after recovery, the analysis of the recovery of files from damaged hard drives, as well as recommendations for improvement compared to theory and newly implemented systems. In this study, the FTK Imager tool was used, with the help of which the images of the four tested hard drives were created.

A disk image is defined as a computer file that includes the contents and structure of a data storage device such as a hard disk, CD, phone, tablet, RAM, or USB. The disk image consists of the actual contents of the data storage device, as well as the information necessary to replicate the structure and layout of the device's contents.

This differs from a normal backup because, in it, the integrity of the exact storage structure remains intact, which is essential in maintaining the integrity of a forensic investigation. Suppose the structure of the prepared documentation (file) and its contents cannot be verified to be the same as the original intended model. In that case, the integrity of the evidence is at risk and may be inadmissible in a court proceeding (Frauenhoffer, 2018).

We researched the images of four external hard drives using FTK Imager. The hardware devices used to create the forensic images are the *Tableau eSata Forensic Bridge*, hard drive 1, hard drive 2, hard drive 3, and 4, shown below. The *Tableau eSata* Forensic Bridge is a portable write blocker that enables the forensic acquisition of SATA hard drives.

From the report generated after the creation of the image, we can see the specification of the hard drive for which the forensic image was created, the information on the creation of the image - the start and end of the same showing the day, month and year as well as the period of the start and completing the creation of the forensic image of the hard drive. In the first report, we also find data for the verification of the created image, as well as data on MD5 and SHA1, which represent cryptographic hash functions on the hard disk.

In this research, for the analysis of digital images created through the digital forensic tool FTK Imager 4.3.1.1, the digital forensic platform Autopsy 4.15.0 was used. Through this forensic image analysis tool, four hard drives were analyzed and compared between them. Namely, the general block diagram illustrating the digital forensic process involving the hard drives using FTK and Autopsy.

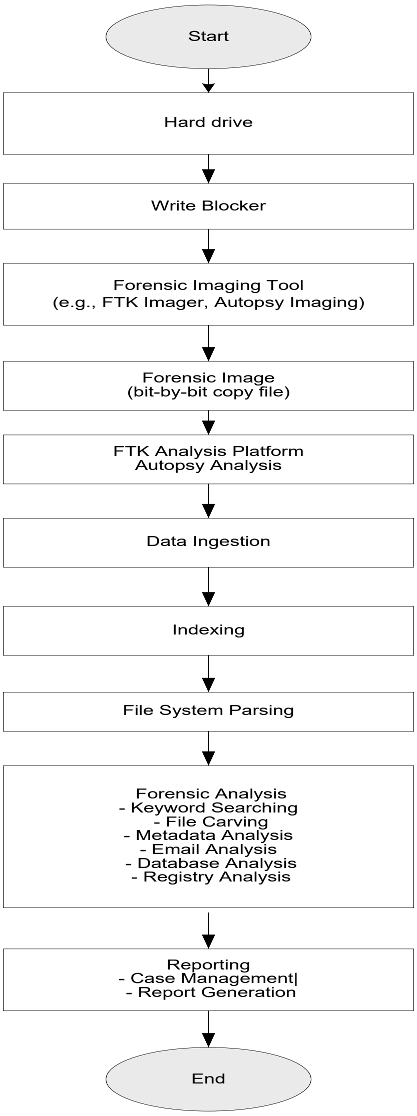


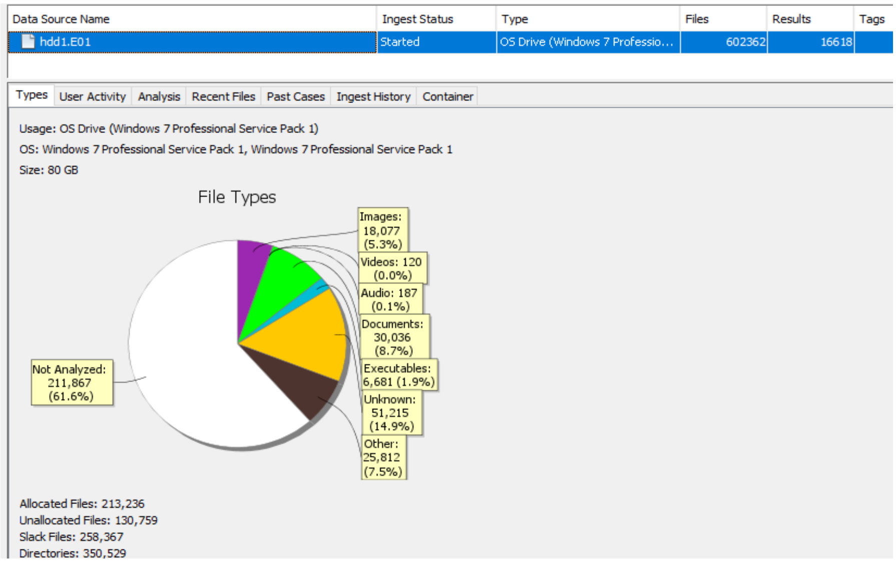
Chart 1. General block diagram

Comparing and analyzing the hard drives for digital forensic investigations using tools like FTK and Autopsy involves a systematic approach to ensure thorough examination and comparison of digital evidence. Here are the main steps guide: Preparation, Initial Analysis with FTK, Analysis with Autopsy, Cross-Tool Analysis and Correlation, Reporting and Documentation, and Considerations.

Results

Digital forensics poses significant challenges in tracing hard drives, recovering deleted files, and analyzing data from damaged drives. The process begins with creating images of the hard drives using tools like FTK Imager and analyzing the created images with Autopsy, providing a snapshot of the digital evidence. However, challenges arise during file recovery, where the quality of retrieved data can vary due to factors like fragmentation and overwrite patterns. Despite the capabilities of tools like FTK Imager, ensuring the integrity and completeness of recovered files remains a persistent challenge.

The figures below are a summary of the data source of a hard disk and present the categorization of files in certain categories such as the categories images, videos, audio, documents, executables, unknown, and others. Below we find figures 1, 2, 3, and figure 4 which present the data source summary graphs for hard drives 1, 2, 3, and 4.



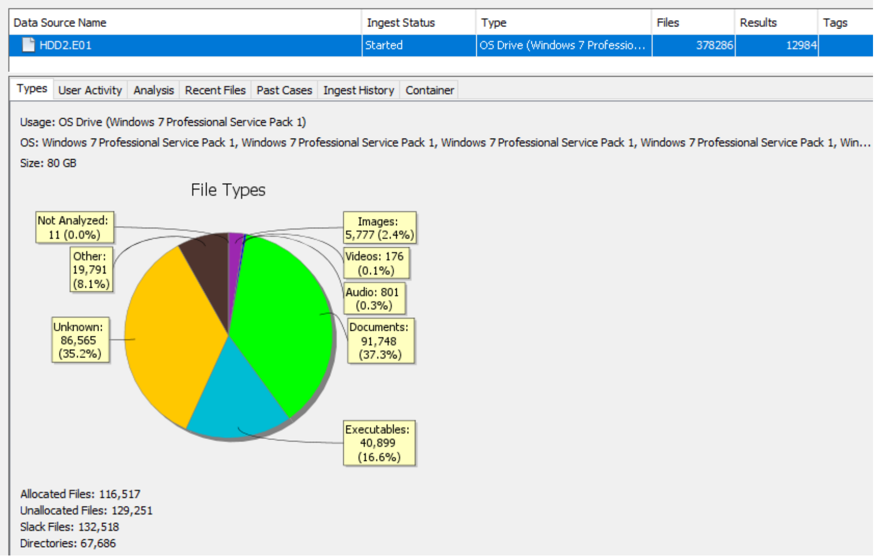
Data Source Name	Ingest Status	Type	Files	Results	Tags
hdd1.E01	Started	OS Drive (Windows 7 Professio...	602362	16618	

Usage: OS Drive (Windows 7 Professional Service Pack 1)
OS: Windows 7 Professional Service Pack 1, Windows 7 Professional Service Pack 1
Size: 80 GB

Allocated Files: 213,236
Unallocated Files: 130,759
Slack Files: 258,367
Directories: 350,529

Figure 1. Data sources summary of Hard-drive 1

In Figure 1, it can be seen that the analysis of the content of hard drive 1 after creating the forensic image. From this image, we can see that hard disk 1 contains 211,867 (61.6%) not analyzed files, 18,077 images (5.3%), 120 videos, 187 audio, 30,036 (8.7%) documents, 6,681 (1.9%) executables have been detected. , 51,215 (14.9%) unknown files, and 25,812 (7.5%) other. There are 213,236 allocated files, 130,759 unallocated files, 258,367 slack files, and 350,529 directories.



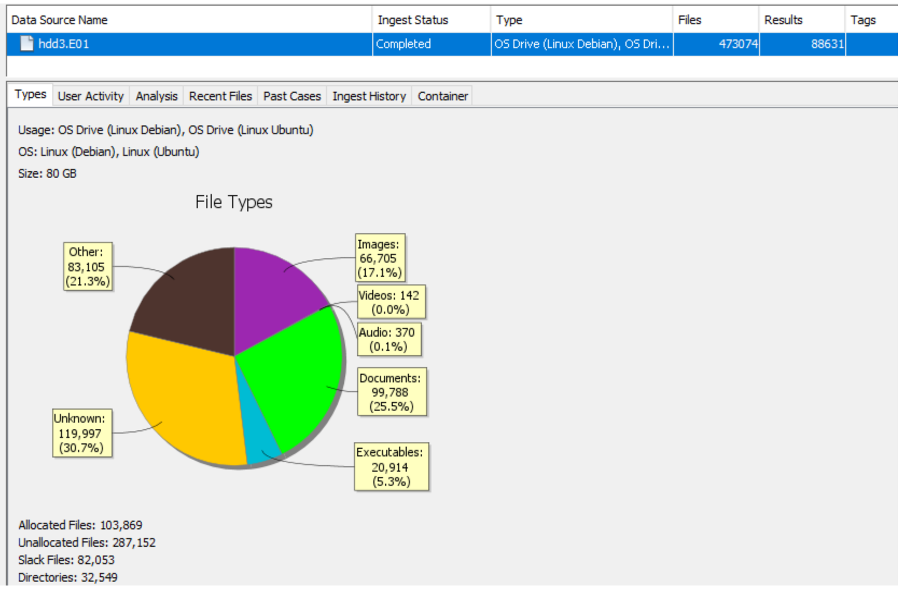
Data Source Name	Ingest Status	Type	Files	Results	Tags
HDD2.E01	Started	OS Drive (Windows 7 Professio...	378286	12984	

Usage: OS Drive (Windows 7 Professional Service Pack 1)
OS: Windows 7 Professional Service Pack 1, Windows 7 Professional Service Pack 1, Windows 7 Professional Service Pack 1, Windows 7 Professional Service Pack 1, Win...
Size: 80 GB

Allocated Files: 116,517
Unallocated Files: 129,251
Slack Files: 132,518
Directories: 67,686

Figure 2. Data sources summary of Hard-drive 2

In Figure 2, it can be seen that the analysis of the content of hard drive 2 after creating the forensic image. From this image, we can see that hard drive 2 contains 11 not analyzed files, 5,777 images (2.4%), 176 videos, 801 audio, 91,748 (37.3%) documents, and 40,899 (16.6%) executables have been detected. , 86,565 (35.2%) unknown files and 19,791 (8.1%) other. There are 116,517 allocated files, 129,251 unallocated files, 132,518 slack files, and 67,686 directories.



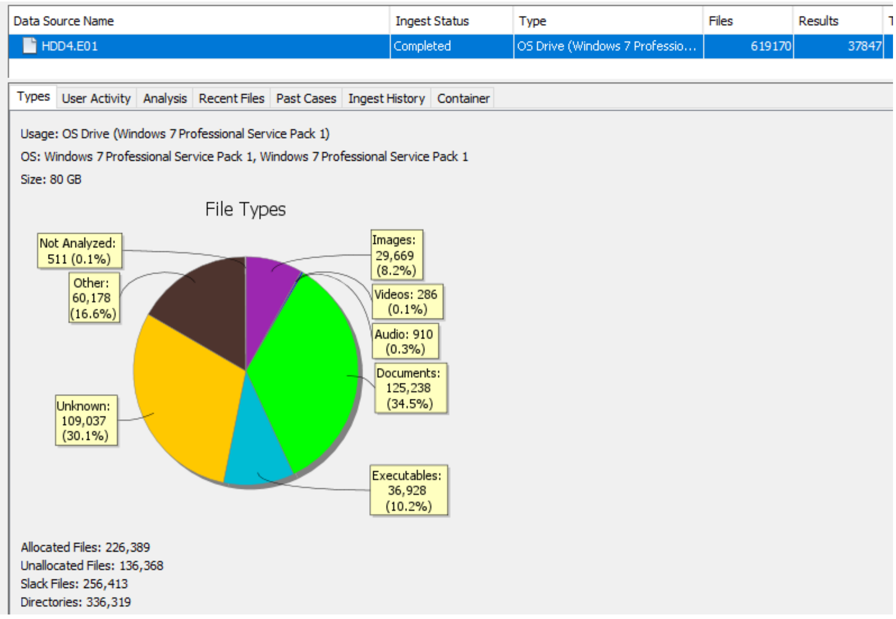
Data Source Name	Ingest Status	Type	Files	Results	Tags
hdd3.E01	Completed	OS Drive (Linux Debian), OS Dri...	473074	88631	

Usage: OS Drive (Linux Debian), OS Drive (Linux Ubuntu)
OS: Linux (Debian), Linux (Ubuntu)
Size: 80 GB

Allocated Files: 103,869
Unallocated Files: 287,152
Slack Files: 82,053
Directories: 32,549

Figure 3. Data sources summary of Hard-drive 3

In Figure 3, it can be seen that the analysis of the content of hard drive 3 after creating the forensic image. From this image, we can see that hard drive 3 contains 66,705 images (17.1%), 142 videos, 370 audio, 99,788 (25.5%) documents, 20,914 (5.3%) executables have been detected, 119,997 (30.7%) unknown files and 83,105 (21.3%) other. There are 103,869 allocated files, 287,152 unallocated files, 82,053 slack files, and 32,549 directories.



Data Source Name	Ingest Status	Type	Files	Results	T
HDD4.E01	Completed	OS Drive (Windows 7 Professio...	619170	37847	

Types User Activity Analysis Recent Files Past Cases Ingest History Container

Usage: OS Drive (Windows 7 Professional Service Pack 1)
OS: Windows 7 Professional Service Pack 1, Windows 7 Professional Service Pack 1
Size: 80 GB

Allocated Files: 226,389
Unallocated Files: 136,368
Slack Files: 256,413
Directories: 336,319

Figure 4. Data sources summary of Hard-drive 4

In Figure 4, it can be seen that analysis of the content of hard drive 4 after creating the forensic image. From this image, we can see that hard drive 4 contains 511 not analyzed files, 29,669 images (8.2%), 286 videos, 910 audio, 125,238 (34.5%) documents, 36.928 (10.2%) executables have been detected, 109,037 (30.1%) unknown files, and 60,178 (16.6%) other. There are 226,389 allocated files, 136,368 unallocated files, 256,413 slack files, and 336,319 directories.

From Figures 1, 2, 3, and 4, we can see that hard disk 3 has the most unallocated files, 287152. Based on the data source summaries for hard drives 1, 2, 3, and 4, it results that Hard drive (1) has the most unanalyzed files in total, with 61.6% or 211,867 files (Figure 1).

If we compare the data source summaries through the Autopsy software for hard drives 1, 2, 3, and 4 and the reports generated through FTK Imager for hard drives 1, 2, 3, and 4, we can conclude that however hard drive 4 has the most allocated files (226 389), the report generated for the hard drive 4 through FTK Imager was generated for a shorter period (33 min), compared to the reports generated through FTK Imager for hard-drives 1,2 and 3. Hard drive 1 has the most unanalyzed files, while the generation of the report through FTK Imager was carried out for a longer period (34 min 49s) compared to hard drives 2,3 and 4.

In Table 1, chart 2, and Chart 3 are visible the details about allocated files, unallocated files, slack files, and directories for hard drives 1, 2, 3, and 4 as well as generating and verifying reports for hard drives 1, 2, 3, and 4 compared to the data source summary for hard drives 1, 2, 3, and 4.

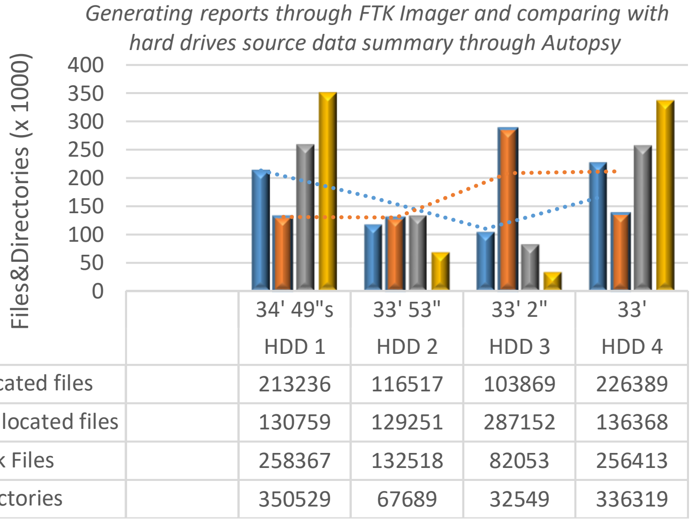
Table 1. Generating and verifying reports for hard drives 1, 2, 3, and 4 compared to the data source summary for hard drives 1, 2, 3, and 4

HDD	**Report generation through FTK Imager**	**Verification of report through FTK Imager**	**Allocated files**	**Unallocated files**	**Slack Files**	**Directories**
HDD 1	34 min 49 s	15 min 25 s	213236	130759	258367	350529
HDD 2	33 min 53 s	9 min 6 s	116517	129251	132518	67689

HDD 3	33 min 2 s	11 min 3s	103869	287152	82053	32549
HDD 4	33 min	12 min 10 s	226389	136368	256413	336319

Based on this analysis, from Table 1 we can see the number of files allocated to a forensic image does not play a role in the duration of report generation during the creation of forensic images through FTK Imager.

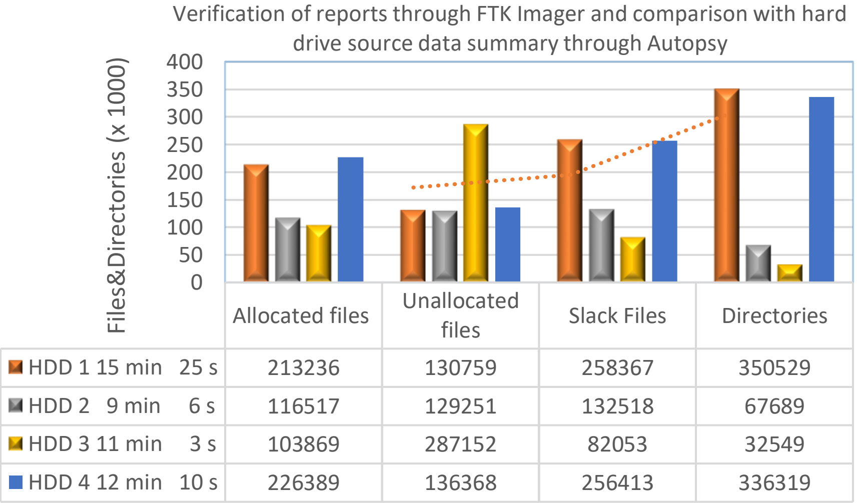
Compared to allocated files, the unanalyzed files in a forensic image are directly proportional to the duration of generating reports for forensic images through FTK Imager.



	34' 49"s HDD 1	33' 53" HDD 2	33' 2" HDD 3	33' HDD 4
■ Allocated files	213236	116517	103869	226389
■ Unallocated files	130759	129251	287152	136368
■ Slack Files	258367	132518	82053	256413
■ Directories	350529	67689	32549	336319

Chart 2. Report generation for hard drives 1, 2, 3, and 4 compared to data source summary for hard drives 1, 2, 3, and 4

From chart 2, it can be seen that the time for generating reports for hard drives 1, 2, 3, and 4 for allocated files, unallocated files, slack files, and directories.



	Allocated files	Unallocated files	Slack Files	Directories
■ HDD 1 15 min 25 s	213236	130759	258367	350529
■ HDD 2 9 min 6 s	116517	129251	132518	67689
■ HDD 3 11 min 3 s	103869	287152	82053	32549
■ HDD 4 12 min 10 s	226389	136368	256413	336319

Chart 3. Report verification for hard drives 1, 2, 3, and 4 compared to data source summary for hard drives 1, 2, 3, and 4

From chart 3, it can be seen that the time for verification reports for hard drives 1, 2, 3, and 4 for allocated files, unallocated files, slack files, and directories.

Creating a forensic image on a physically damaged hard drive

According to the analysis of Solodov et.al., (2021) who have taken in their research 14 discs for analysis and the same were subjected to fire damage, water damage, but also various shocks and vibrations, after the obtained results have reached some conclusions.

Solodov et. al., (2021) defined that the possibility of successful data recovery in the case of HDDs and SSDs with signs of damage should not be excluded based on the visual appearance of the device. It is important to complete the data recovery within a short time. Selective data recovery is a preferred method.

In this study, after creating four forensic images for hard drives 1, 2, 3, and 4, was also tested forensic image creation on the physically damaged hard drive, concluding that through the imaging tool digital forensics FTK Imager cannot generate a forensic image when the hard drive is physically damaged.

Conclusions and Recommendations

FTK Imager and Autopsy 4.15.0 tools were used in connection with digital forensics, tracing hard drives, and creating and analyzing forensic images. Also of great importance is the inclusion of the Tableau eSata Forensic Bridge device, which is a portable write blocker that enables the forensic acquisition of SATA hard drives. Through the Autopsy tool, for analysis of forensic images, all deleted files can be returned, or only some of the files that are of interest to the party can be tagged. The quality of deleted files even after recovery remains high.

The number of files allocated to a forensic image does not play a role in the duration of report generation when creating forensic images through FTK Imager. Unlike allocated files, unanalyzed files in a forensic image are directly proportional to the duration of generating reports for forensic images through FTK Imager. In this study, after creating four forensic images for hard drives 1, 2, 3, and 4, forensic image creation on the physically damaged hard drive was also tested, in which case it was concluded that through the imaging tool digital forensics FTK Imager cannot generate a forensic image when the hard drive is physically damaged.

As a conclusion and recommendation, it can be said that the open source tools for creating and analyzing forensic images FTK Imager and Autopsy 4.15.0 are very efficient in tracking hard drives, but they cannot create and analyze forensic images of physically damaged hard drives, therefore tools that enable magnetic reading of physically damaged hard drives must be used. The evaluation of open-source and proprietary forensic software at the heart of the analysis process must be considered carefully. The cost and benefit of each software suite should match the form and function in an accredited laboratory forensic space. Configuration control of any open-source software poses legal challenges and accreditation challenges if the software is operated out of scope (Alexander, 2022).

Ensuring data confidentiality on hard drives is paramount in safeguarding sensitive information from unauthorized access. Encryption techniques, such as AES or BitLocker, offer robust protection by encoding data, making it indecipherable without the correct decryption key. However, in forensic investigations, skilled professionals utilize specialized tools and techniques to extract data from hard drives, even if encrypted, to uncover evidence for legal purposes. This delicate balance between privacy and investigative necessity underscores the complexity of maintaining confidentiality while enabling lawful access to crucial information stored on hard drives.

The dilemma faced by educational institutions regarding whether to inform students that "delete" does not mean permanent deletion is multifaceted. On one hand, early education about data permanence and recovery using free and open-source software could foster a greater awareness of digital responsibility and data security among students. This proactive approach might enhance students' understanding of the digital footprint they leave behind and promote better data-handling practices. On the other hand, delaying this information until later stages might ensure students have a foundational knowledge of digital systems before delving into more complex concepts like data recovery. However, this reactive approach may leave students temporarily unaware of critical security practices. Balancing these considerations requires a nuanced approach, integrating data security education progressively while ensuring students are equipped with essential knowledge and tools at appropriate stages of their educational journey.

Declarations

Acknowledgements: Not applicable

Authors' contributions: Authors DIS and MH made significant contributions, especially in the preparation of the introduction, method and discussion sections, in the recordings, in the writing of the abstract and summary. Also, depending on the changes in the general narrative and composition of the article. Author JA analyzed and commented on the studies. All three authors reviewed and approved the article.

Competing interests: The authors declare that they have no competing interests.

Funding: Not applicable

Ethics approval and consent to participate: No ethics committee is required.

References

Alexander, Brandon (2022). Evaluation of Open-Source & Proprietary Forensic Software Tools. ISSC621: Computer Forensics. APUS. DOI: 10.13140/RG.2.2.3484416006

Arnes, A. (2018). Digital Forensics. John Wiley & Sons Inc.

Boddington, R. (2016). Practical Digital Forensics. Packt Publishing Ltd.

Breitinger, C. G., & Baggili, I. (2017). Availability of Datasets for Digital Forensics–and What is Missing. Cyber Forensics Research and Education Group (UNHcFREG), Tagliatela College of Engineering, ECECS, University of New Haven, 300 Boston Post Rd., Westhaven, CT 06516, USA.

Digital Corpora. (2019). Accessed 04 22, 2019 [Online] Available at: https://digitalcorpora.org/corpora/disk-images/real-data-corpus

Digitalcorpora.org. (2021). Accessed 06 30, 2021 [Online] Available at: https://digitalcorpora.org/corpora/disk-images/real-data-corpus

Du, X., Ledwith, P., & Scanlon, M. (2018). Deduplicated Disk Image Evidence Acquisition and Forensically-Sound Reconstruction. 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (pp. 1674-1679). 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).

EC-Council. (2009). Computer Forensics: Hard Disk and Operating Systems, Volume 2. Cengage Learning.

Frauenhoffer, M. (2018). Medium. Retrieved 08 11, 2020 [Online], Available at: https://medium.com/@Frauenhoffer/how-to-create-a-forensic-image-with-ftk-imager-6fb8ee07fb2d

Hassan, N. A. (2019). Digital Forensics Basic. New York: Apress.

http://sleuthkit.org/. (2021). Accessed 06 30, 2021 [Online] Available at: https://sleuthkit.org/autopsy/docs/user-docs/3.1/quick_start_guide.html

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. Retrieved from Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50875

Moch, C., & Freiling, F. C. (2009). The Forensic Image Generator Generator (Forensig2). In IT Security Incident Management and IT Forensics, 2009. IMF'09, Fifth International Conference. IEEE, 78-93.

Muneesawang, P., & Yammen, S. (2015). Visual Inspection Technology in the Hard Disk Drive Industry. ISTE Ltd and John Wiley & Sons, Inc.

Nelson, B., Phillips, A., & Steuart, C. (2019). Guide to Computer Forensics and Investigations: Processing Digital Evidence. 2019, 2016 Cengage Learning, Inc.

Prakash, N., & Duhan, D. R. (2020). COMPUTER FORENSIC INVESTIGATION PROCESS AND JUDICIAL RESPONSE TO THE DIGITAL EVIDENCE IN INDIA IN LIGHT OF RULE OF BEST EVIDENCE. International Journal in Management and Social Science, Volume 08, Issue 05.

Prasanthi, B. V. (2016). Cyber Forensic Tools: A Review. International Journal of Engineering Trends and Technology (IJETT) – Volume-41 Number-5.

Salunkhe, P., Bharne, S., & Padiya, P. (2016). Data analysis of file forensic investigation. International Conference on Signal Processing, Communication, Power and Embedded Systems (SCOPES), 372-375.

Sammons, J. (2012). Forensics, The Basics of Digital: the primer for getting started in digital forensics. Syngress is an imprint of Elsevier.

Solodov, D., & Solodov, I. (2021). Data recovery in the case of fire-damaged Hard Disk Drives and Solid-State Drives. Forensic Science International: Reports

Yannikos, Y., Graner, L., Steinebach, M., & Winter, C. (2014). Data Corpora for Digital Forensics Education and Research. In IFIP International Conference on Digital Forensics, (pp. 309–325). Springer.

Zbrog, Matt (2024). A GUIDE TO DIGITAL FORENSICS AND CYBERSECURITY TOOLS. Accessed 07 16, 2024 [Online] Available at: https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools

Zlatanov, N. (2015). Hard Disk Drive and Disk Encryption. Black Hat. Amsterdam: IEEE Computer Society.