BOOK CHAPTER | Interference-Free Data Storage

Storing Forensic Data Against Interference

Amenuveve Gracious Adzogbley
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: graciousgra@gmail.com

ABSTRACT

Digital forensic investigators face a wide range of inquiry goals, such as dealing with cybercrime. Digital forensic tools are no different. Different digital traces were examined on persistent storage devices (SSDs, SD cards, and USB drives), volatile memory snapshots, and network captures. A large realistic, timely training data is required to train experts, improve the forensic tools and keep their knowledge and capabilities up to date. However, there is a significant gap in digital forensic training data due to many factors such as privacy, secrecy, data protection, and intellectual property rights. Multiple frameworks for generating realistic digital forensic data sets have been proposed in recent years. None of these frameworks offers a comprehensive strategy for creating digital forensic tools, for relevant traces, from many sources.

Keywords s: Data Storage, Cybersecurity, Cybercrime, Protection, Forensics, interference.

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Amenuveve Gracious Adzogbley (2022). Storing Forensic Data Against Interference SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 7-14. www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P2

1. INTRODUCTION

As digitalization progresses, companies and individuals face several difficulties and dangers to their security. To overcome the obstacles, well-trained forensic professionals are required to reconstruct the full sequence of actions on current devices and operating systems following a crime and locate the culprits' traces. To stay up to date with the complexity and variety of today's forensic investigation, forensic professionals often require substantial training data encompassing a wide range of illegal behaviors to sharpen their abilities and test their digital forensic tools. The law enforcement sector has a pressing need to verify the dependability of computer forensic technologies. A methodology is needed to ensure that forensic tools generate accurate, consistent and objective test results. The National Institute of Standards and Technology's (NIST) Computer Forensic Tool Testing (CFTT) built a method for testing computer forensic tools by developing generic tool specifications, test methods, test criteria, test sets, and test hardware.

The results provide information for toolmakers to improve their tools. Users can make informed decisions about acquiring and using computer forensic tools, and interested parties can better understand a tool's capabilities. The technique of recovering and investigating data saved on digital devices is known as digital forensics. It also refers to hardware and software tools used by specialists to recover data without losing it. The purpose of digital forensic technology is to prepare and extract evidence from computers and mobile systems [1]. Digital forensics applies to any device that stores data (computers, laptops, cellphones, memory cards, and external hard drives). In the next section, we will go over data storage devices, including what they are, how they are utilized, and the advantages in digital forensics [1].

The following is a breakdown of the forensics procedure:[1].

1. Identification
2. Preservation
3. Collection
4. Examination
5. Analysis
6. Presentation

Types of data acquired in computer forensics

What follows elucidates the types of data acquired in computer forensics

Persistent data: This is data stored on a local hard drive (or another device) and retained when the computer is turned off [1].

Volatile data: This is a type of data stored in memory and is lost when the computer loses power, which are the two forms of data [1]. Experts in operating systems and file systems, data recovery, cloud computing, and other areas of forensics are available to manage this material. They study hard drives or hard-disk images from various operating systems and give an interface for analysing files and extracting and storing information or data acquired in an electronic format.

Fig 1: Forensic Evidence Storage
Source: https://online.norwich.edu/academic-programs/resources/computer-forensics-ultimate-guide-starting-career-emerging-field

Forensics and Data Storage

In today's world, numerous devices save data. Some are outdated, yet they still hold data and may require data recovery. The most well-known are listed below:[1].

Solid State Disks (SSD)

Solid-state disks (SSDs) use flash memory chips to store data (called NAND flash memory). /SSD stores data electronically rather than magnetically. Thus, there are no moving parts to break. SSDs have the advantage of being smaller, lighter, and use less power than hard discs. It comes in a variety of shapes depending on the number of chips and how they are assembled. They are more expensive, but they read and write data faster. One disadvantage is that there are no indicators that a total drive failure is imminent. Hard discs in desktop and laptop computers can be replaced with them. When trying to recover information lost from SSD discs, traditional forensic methods fail, hence new ways have been developed. A magnetized medium is used to store data in the magnetic material. In this category, there are three types of storage devices namely: [1].

Floppy disks: It contains a Soft magnetic disk called a floppy disk used for transmitting data, storing, and backup up small amounts of data. They are susceptible to heat, dust, and magnetic fields, which is a significant disadvantage. Flash memory, optical discs, and external hard drives have been mainly replaced by floppy discs [2].

Hard drives: They contain hard magnetic platters that store and retrieve digital information. They have the largest capacity and are more accessible and inexpensive than SSDs. One disadvantage is that they consume more energy and produce more noise when in use than SSDs. A hard drive is susceptible to damage when shaken or dropped due to its moveable, mechanical elements. Even after the power supply is turned off, data is stored on these drives. Data can be recovered from hard drives using data carving techniques or a commercial data recovery application. Cloning a hard drive to an image file is another forensic recovery option. This method is more practical, although it is dependent on the size of the source hard drive and the equipment employed.

Magnetic tapes: These tools look like audio cassette tapes. Because of their large capacity, they are ideal for archiving, affordable and long-lasting. These are extremely slow when compared to a hard drive. Data can only be accessed by winding the tape. The majority of data is downloaded to magnetic tapes for long-term storage. Because data is magnetically stored, tapes must be kept away from any magnetic fields at all times. Because they must be read linearly from the beginning to the conclusion of the tape, they differ in the way data is recovered. This significantly lengthens the time it takes to do forensic recovery. One use of magnetic tape that still exists is tape vaulting for the storage of physical records. In this process, technicians and other professionals back up digital data to magnetic tape to secure it in physical vaults as a redundant strategy in the event of disasters or other emergencies.[3]

Digital audio tapes: These are cassettes that digitally store audio information. Low cost and compact size are some clear benefits of using digital audiotapes, as well as the fact that they are stored on a computer rather than a reel-to-rear machine. These, on the other hand, can only be recorded and played back in one direction. Many of these tapes and their supporting hardware are no longer manufactured by large corporations, posing forensic recovery challenges[3]

Digital Linear Tapes (DLT): These are viable digital audiotape substitutes. They utilize a unique algorithm that allows for high-speed data retrieval and storage. Using 'longitudinal recording' techniques, these cassettes may store up to 35GB per cassette. These tapes are commonly used to back up servers in data centres and can be recovered quickly for forensic purposes [3].

SD Card: SD cards are perhaps the most commonly used alternative storage nowadays, and they're excellent because they're usually designed to work with a variety of devices. SD cards are designed for short storage and data transfer, but not for long-term storage.[1]

USB – For smaller files, a USB stick can still provide a good option if you want to carry something with you physically [1]

2. RELATED LITERATURE

Magnetic Tape: 'Tape is dead! Long live tape!' Were you around in the 80s when cassette tapes were all the rage? Many people still say 'mixed tape' sometimes when referring to playlists they make on Spotify or Pandora, or even CDs that they give to each other. Though the cassette tape has long since fallen out of favour, it was neither the first nor the last device to use magnetic tape for storage. A magnetic tape, in computer terminology, is a storage medium that allows for data archiving, collection, and backup. At first, the tapes were wound in wheel-like reels, but then cassettes and cartridges came along, which offered more protection for the tape inside. One side of the tape is coated with magnetic material. Data on the tape is written and read sequentially.

Finding a specific record takes time because the machine has to read every record in front of it. Most tapes are used for archival purposes, rather than ad-hoc writing and reading.[3]. Data is written into 'tracks' on the medium. Some run along the edge of the tape, which is called the linear recording, while others are written diagonally, which is called helical recording. Older magnetic tapes used eight tracks, while more modern ones can handle 128 or more tracks.[3]

Linear Tape File System

The Linear Tape File System (LTFS) mimics random access attributes of hard disks and has brought about a revolution in tape backup in the age of huge files and big data. By storing metadata about an object separate from the object itself, it increases access and retrieval times. LTFS is an open standard, meaning is not proprietary or owned by anyone. This allows different vendors, architectures, and systems the ability to use the technology [3].

Linear Tape File Systems have brought a huge leap forward in storage capacity. IBM and Fujifilm unveiled an LTO tape that can store up to 220 Terabytes of data! This is a significant increase over the technologies mentioned previously, and even from the prototype of LTFS [3].

Advantages and Disadvantages

Although magnetic tape is still viable when compared to hard discs, external drives, or even cloud storage, it lacks speed in data retrieval.[2]

Although there are fewer tape drives around than disk drives, tape drives still perform a valuable function. Although disk drives can be faster, smaller, and hold more data, a physical tape is much more mobile.

An organization can back up its data to tapes, remove them, and send them to off-site storage via courier; this is a critical step in disaster recovery. While disc drives can read and write data at fast speeds, tape drives are often used only for writing data. As a result, they're an excellent backup or archive tool [2]

3. IMPLICATIONS FOR PRACTICE, RESEARCH, POLICY CYBER SECURITY IN AFRICA

The British consulting firm Ovumone estimated that a billion people in Africa will have Internet access by 2022 [4]. Analyzing the trend of cybercrimes across countries, analysts have suggested 10–15% internet penetration as the threshold level for the generation of significant hacking activities [5]. Today, internet penetration rates in many African economies have already reached this level. Cybercrime is shifting towards the emerging economies. This is where the cybercriminals believe they can make a fortune with little hindrance. As expected, many African economies have become important sources as well as victims of cyber-threats.

According to Kenya – based IT and business advisory firm Serianu, cybercrimes cost African economies $3.5 billion in 2017. In that year, annual losses to cybercrimes were estimated for Nigeria at $649 million, and Kenya at $210 million. Likewise, according to the South African Banking Risk Information Centre (SABRIC), South Africa loses $157 million annually to cyberattacks [6].

Global Cyber-Threats From Africa

Cyberattacks that originated from African economies have a worldwide effect. It is reported in [7] that Africa's "Cyber [weapon of mass destruction] WMD" potentially poses a direct threat to the world. For instance, in 2010, 80% of PCs used in Africa were infected with viruses and malware [7]. Cybercriminals often use these unprotected computers to launch cyberattacks against targets all over the world. As a response, businesses from industrialized countries categorize online transactions originating from Africa as risky.

An annual survey of CyberSource released in 2006 ranked Nigeria as the world's riskiest country for online transactions. CyberSource's 2008 similar survey showed that 76% of the North American merchants rejected orders from Nigeria and 58% did so for Ghana [5]. Likewise, due to a large number of fraudulent clicks from Africa on Internet pay per click advertising, paid-search companies such as Overture have implemented "continental cut-off" services, which reportedly disregard clicks on adverting originating from Africa [7].

Measures at various levels to address cyber-threats

Several initiatives have been launched and carried out at various levels to improve the continent's cybersecurity landscape. The most important of these is improving regulatory quality [6]. According to a November 2016 report by the African Union Commission (AUC) and the cybersecurity firm Symantec, 11 countries in the continent had specific laws and provisions in place to deal with cybercrime and electronic evidence: Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia. Additional 12 countries had taken at least some legislative measures, albeit limited. Draft cybercrime laws had been prepared in many other countries and bills had already been presented to national Parliaments in some of the countries [6].

4. RESEARCH GAPS/FINDINGS

Based on the findings, this study finds that data deleted on hard disc drives can be fully recovered. However, data deleted on solid-state drives cannot be fully recovered using the Autopsy forensic tool but can be partially recovered using the ProDiscover Basic forensic tool. To better understand, data deleted from hard drives is not permanently deleted. Every file generated and kept on a hard drive has a pointer in the operating system. When a folder or file is deleted, it is just that the pointer is removed by the OS. This deleted data will still be present on the drive as long as new data is not overwritten on these data sectors. Therefore, data deleted on Hard drives can be easily retrieved using forensic tools and data recovery tools. [1].

When it comes to data deleted on SSDs it is different. Most modern SSDs support TRIM. Deleted files on drives that have TRIM enabled cannot be retrieved. SSD reads and writes data from flash cells. Data on flash cells cannot be overwritten. Hence to write data, flash cells should be empty. As this study uses an external SSD, it is more likely that the TRIM command is disabled, resulting in not completely wiping the deleted files. The flash cells will not be wiped out if the TRIM command is disabled. In the case of an internal SSD, the TRIM is enabled by default, and the OS immediately wipes out the deleted data to increase the write speed to SSD for any future use. [1].

The other property which makes it difficult to retrieve deleted data is self-corrosion. SSDs have this property called self-corrosion. A process running in the background looks for unused data and wipes off flash cells permanently. So, when SSD image 2 is analysed in Autopsy, deleted data might have undergone self-corrosion, and only one file was retrieved. Whereas, as this study used an external SSD, TRIM was disabled by default, and deleted data was retrieved using ProDiscover Basic.

Thus, this study concludes, that data deleted on SSDs is wiped out due to self-corrosion of SSD and disabled TRIM command, to improve the read/write performance speed time, which was lacked by traditional HDDs.“If it takes one hour to write 10 GB data to your drive, it takes the same time to wipe out, rather than to save time Operating System removes the pointer and overwrites the deleted data sectors when needed.”[1].

5. CONCLUSIONS

There are many different storage devices used in computers and mobile phones in recent times. In particular, it is uncommon to see people without access to mobile phones at all times. Thus, such devices are an important source of forensic analysis in the event of a crime. Much of the work by forensic professionals focuses on building specific tools for specific storage devices. This trend certainly cannot continue due to different architectures used by different manufacturers in producing storage devices. Thus, in building forensic tools, the methodology should take into account devices of today and devices of the near future to achieve speed and efficiency in the work of a forensic professional.[1]

6. RECOMMENDATIONS

1. We recommend building forensic tools that take into account all types of devices and platforms (that is mobile, and computers) [8].
2. Forensic practitioners can no longer rely solely on specialized tools built for each potential evidence source. There are simply too many sources, changing too rapidly. Instead, we argue for the adoption of flexible, inference-based techniques that can be readily applied to a wide variety of different evidence sources without requiring significant manual work on the investigator's part. In essence: The traditional forensics approach of developing tools tailored specifically to each new digital evidence source is no longer tenable. Instead, inference-based techniques offer investigators a scalable means to quickly, accurately, and soundly extract information from diverse data sources, even if the exact underlying format is unknown [8].

Direction for future works

Future works/research can explore inference-based techniques for forensic analysis

REFERENCES

[1] Data Storage Formats & Digital Forensics: Devices & Types. (2018, August 5). Retrieved from https://study.com/academy/lesson/data-storage-formats-digital-forensics-devices-types.html.

[2] What Is a Floppy Disk? - Definition, Advantages & Disadvantages. (2015, September 6).Retrieved fromhttps://study.com/academy/lesson/what-is-floppy-disk-definition-advantages-disadvantages.html.

[3] Magnetic Tape for Data Storage: History & Definition. (2020, March 16). Retrieved from https://study.com/academy/lesson/magnetic-tape-for-data-storage-history-definition.html.

[4] https://www.consultancy.africa/news/30/africa-will-break-through-1-billion-mobile-internet-connections-by-2022.

[5] Kshetri, N. (2013). Cybercrime and cybersecurity in the global South. Basingstoke, U.K: Palgrave Macmillan: Houndmills.

[6kk] Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527

[7] Kshetri, N. (2010). The economics of click fraud. IEEE Security & Privacy Magazine, 8(3), 45–53.

[8] Walls, Robert J., "Inference-Based Forensics For Extracting Information From Diverse Sources" (2014). *Doctoral Dissertations*. 265.https://doi.org/10.7275/6040905.0 https://scholarworks.umass.edu/dissertations_2/265