ISSN Online : 2709-4030
ISSN Print : 2709-4022

Vol 6 No.1 2022

ANALYSIS OF DIGITAL DEVICES AND TOOLS INVOLVED IN DIGITAL INVESTIGATION

*Muhammad Asif Safdar, **Dr. Rashida Zahoor, ***Waqar Afzal

ABSTRACT

The crime, is no longer substantive, it can be executed without the weapons, by manipulating the technology available in the market, these crimes are commonly known as cybercrimes, the term cybercrime can be defined as crimes in which computer is object of crimes (hacking, phishing, spamming) or used as medium to commit the crime, the offenders manipulate these devices to commit the crimes, like accessing personal information, passwords and use them for malicious purposes. The war against these offences can only be fought with the equipment whether in substantive form or in soft, as it is a common phrase that "iron cuts iron", the digital devices when manipulated and compromised are subject to digital investigation and afterwards forensic examination, the footprints that the offenders left behind after commission of offence, can only be traced by using these tools and devices. There are numbers of software and hardware that are being utilized during the investigation of digital offence and in the forensic laboratories of almost every state to authenticate the evidence, collected during the course of digital investigation.

THE PROSPECTIVE FOUNTAINHEAD OF DIGIATL EVIDENCE

The devices through which the evidence can be collected are actually the sources of digital evidence, the evidence hide in several places in a computer. Computer's Hard disk is the primary sources of digital evidence, hard disk is the permanent storage in the computer, used to store computer's data (MerriamWebster, 2019). The information and data (in any form) along with the hard disk is considered as the evidence, hard disk can either be permanent or portable. There may be several files which can be collected from the hard disk like images, photos, video, and audio etc. are all admissible before the court of law on presentation. The question regarding the probable positions of hidden digital evidence in computer or another device is to be addressed ahead, there may be several positions on which one can find, seize and collect the hidden digital evidence, the probable list is as follow: Hard-Disk: hard-disk is the main source of computer storage, data is stored in the Hard-disk, and it is the primary memory of the computer in which the files are permanently stored. Hard-disk is considered as the most important source of data collection. It is mainly the part of the computer but now a days it is available in the form that can be attached externally with the computer and can be utilized in transmitting the huge data from one computer to another computer.

Removable Storage Devices: removable storage devices are the devices, that are handy to carry and utilized in transferring the little media quickly, there are thousands of removable storage devices, that are utilized for the above said purpose and is also considered during the course of digital investigation as a source of data or information and as a substantive piece of evidence, removable storage devices include a Compact Derive (CD), Digital Versatile Disk (DVD) etc. Pan/Flash/Thumb derives:

*Assistant Professor of Law, Gillani Law College, Bahauddin Zakariya University Multan
Assistant Professor of Law, Department of Law, Bahauddin Zakariya University Sub-CampusVehari **(Corresponding Author)
***B.A LL.B (PK), LL.M (UK), Advocate High Court

these devices are also handy and easy to carry, and used to carry data or information of light weight, pan derives are also subject to digital investigation as source and itself as evidence, even the investigator used these devices to carry and transmit the data from one place/from one destination to other. Memory Cards: memory cards are also very important, and played a vital role in storing the data in the usual digital devices like phone, smart phones, camera etc. Memory card is also having different types and is able to store data.

Digital handheld devices: these devices include the mobile phones, smart phones, cameras etc., these device provide the user an environment of communication, navigation, storage and many more, these devices are multifunctional and are also subject to digital investigation, these devices contain a variety of data and information, because of the variety available in usage, the data along with the device are the valuable evidence collected in digital investigation.

Networking Devices/tools are the tools that are responsible for the connection of one device/computer with other devices, there may be two kind of network connectivity one is through a wire which is known as cable based sharing and the other is wireless sharing in which the computers are connected with each other through wireless network, the only objective of networking is to connect more and more devices with each other to share the data or information with multiple computer at one click. These devices are also considered in digital investigation and also used as the source of and piece of evidence.

From the above discussion it is evident that the digital device in either kind is having prime importance in digital investigation, these devices are capable to store the data or information and provide the footprints of the offender to the investigator to collect the evidence contained by them.

TOOLS USED IN INVESTIGATION

Tool may be a device that aids in accomplishment of task (MerriamWebster, 2011). Tool is simply any instrument of simple piece pf equipment that one holds in hands to do a particular job (Collins dictionary, 2021). Digital forensic tools are defined as any device or combination of devices that is used to aid and assist the investigator or examiner in collecting and authenticating evidence in a digital forensic investigation. The term "tool" refers to any equipment or computer application that is used in digital inquiry or cybercrime investigation to gather, preserve, transform, and present evidence in digital format. Information Technology (I.T) played a vital role in this field, the investigation and the forensic examination could not be conducted without the enlightenment provided by I.T.

There are different classification of tools, subject to functionality, a general classification indicates that tools are commonly having two kinds, one is in shape of non-substantive like different software and other are devices themselves. The states of the world, through enactment and promulgations endorsed the evidence collected from digital devices as admissible piece of evidence, subject to the requirements. This paper discusses about the use of digital devices during the course of investigation of offences committed by manipulating the computer or digital devices and forensic examination of collected digital evidence, the preceding clause summarize the paper by giving overview of the techniques and devices used by the investigators and forensic examiner in the forensic laboratories.

There is minor distinction between digital investigation and digital forensic examination, as far as the definition of these two terms are concerned, one came to know that digital investigation is the collection of digital evidence from digital means with the help of digital means, knowledge, skills and expertise. Digital investigation/digital forensic investigation where the digital devices are used in light of knowledge, skill and expertise and the results be presented before the court of law, during the course of trial of offence, the confidence of collected evidence depends upon the authenticity of hardware and software, used during investigation and forensic examination (Carrier, 2016).

In the era of Information Technology (I.T.) everything is modernized and the outcomes of it can easily be seen in the current offences along with the procedure adopted during the course of investigation. It is well-known to investigate the offences having the evidence in digital shape, several countries have the enacted laws that gave the authority to the law enforcement and investigators to adopt the I.T. even in the investigation of non-digital/casual offences as well as it is also utilized in conducting inquiries in civil cases.

Through this piece of research, the researcher is interest to classify the devices/equipment (whether in shape of soft or hard form) used during the course of digital investigation and digital forensic examination.

There are several classifications and categories of the devices/equipment used in collection of digital evidence from digital crime-scene, from the previous researches it is evident that there are commonly two types of the equipment used in digital investigation, one is in soft form and can be termed as software and one is in substantive shape and can be termed as hardware.

The outcome of every investigation is collection of evidence, that are relevant to case in order to present the before the court of law during trial, to assist the court in decision. Whenever any person deals with the digital evidence, he must adopt general rules and procedural that are to be adopted meaning thereby that the procedure of collection may not change the shape or integrity of evidence, one who is well-familiar can only deals with the evidence and everything whether relevant or irrelevant should be seized, collected, documented and preserved by using the permissible and legitimate technology.

Before going into the intricacies, the evidence that is discussed in this article is briefly enlightened, the digital evidence commonly known as the electronic evidence is the data, information initiated just after commission of digital offence, these are basically the footprints left by the offender, and by following the footprints the investigator collect whatever he found from the crime-scene, the evidence collected from digital crime-scene is volatile, vague, perishable and fragile among all the evidence and the offence is having no boarder or jurisdiction (technopedia, 2021). The investigation requires excellence, knowledge, skill along with the precaution in the initiation, seizure, collection, preservation and transmission afterward authentication and conversion of the evidence into a shape presentable and admitted by the court of law.

Digital investigation is dependent on several tool, as it is primarily described that the evidence under consideration is not something in substantive form, and require the due care, excellence, knowledge and precaution. As far as the tools involved in digital investigation are concerned, there may have several kinds, but a simple classification is that there may be two kinds of tools one is in soft form hence called as Program and the other is in substantive form called the device/equipment.

Software is primarily a tool for law enforcement agencies and forensic professionals since it assists them in the identification, collecting, separation, transformation, storing, and decoding of data and information from the digital crime-scene during the course of an investigation into a digital offence.

Permanent data and transitory data are the two types of data that can be found on a computer or any other device. Permanent data is stored on a computer's hard drive, in a cellphone's storage or read-only memory (ROM), in a device that is used to store data, or in any other device. The data is present in its permanent form until it is compromised or deleted by a third party; on the other hand, data that is stored in Random Access Memory (RAM) is only present in its temporary form until the computer is turned off; it is only accessible when the system or a device is turned on, and as soon as it is turned off, the data is lost. All that is required is to capture temporary data throughout the time that the computer or other device is turned on.

Suppose you are interested in learning more about the available software on the market to assist and complement the investigation and forensic examination of digital offences. In that case, thousands of different types of software are available on the market used in the forensic analysis and investigation of digital crimes, some of which will be described in greater detail later on.

Each activity of the investigator and forensic examiner necessitates using a tool in the form of software or a device because the evidence they are collecting is not substantive evidence. The software commonly used in digital investigation and digital forensic examination includes backup software, copying software, authenticating software, encryption software, decryption software, editing software, recovery software, and an IP tracker. The backup software appears to be the software used to create backups of the files extracted from the computer or any other device and save them to a safe location. If we define backup software, it appears to us that it is the software used to create backups of the files extracted from the computer or any other device and save them to a safe place. In a forensic investigation, backup software is an application or programme that allows the investigator or forensic examiner to create exact copies of the data that can be recovered in the event of a complete deletion or formatting of the system. Investigators and forensic examiners use backup software to enable the backup of folders, files, documents, and other data and the entire server (Techopedia, 2021). Copier software is nearly identical to backup software in that it is used to copy an object from one location and paste/drop the object into another location where it cannot be modified. While the programme is available in software, the same is also available in the market in various forms such as photocopiers, printers, scanners, and other similar devices.

Authentication software is also a software, application, or process that helps to ensure and confirm a user's identity. It means that when a user attempts to access a system and obtains any information from it, the system stores and memorizes its identity in any shape. By using authentication software, the investigator or forensic examiner can track down the person who committed the crime by tracking down its id number.

Encryption software is the programme or application of an algorithm to readable text and converts it into text that is unfadeable in nature. Data is being encrypted by the investigator or forensic examiner to ensure secure storage and transmission of the information under investigation.

This is the programme or application that works in the polar opposite direction of encryption software; it is the reverse process of encryption; it is the process of decoding dates that have been encrypted into a secret format; this process is only used by those who have been authorized to do so by law enforcement authorities.

This type of software is also known as edition software, and it is designed to edit the information gathered during a digital investigation by the investigator. By employing this software, the investigator can divide the data into different sub-data and deal with specific/special data rather than a large amount of data in a single batch format.

Recovery software allows you to recover data from a storage device that has been erased, corrupted, or become inaccessible. The unique feature of this software is that it reviews, scans, identifies, extracts, and copies data from deleted, corrupted, and formatted sectors, as well as from a user-defined location on the storage device's internal storage media (Techopedia, 2020).

The final piece of software in question is the Internet Protocol tracker, which assists the investigator and the forensic examiner. It converts an I.P. address into a host name and provides the investigator with the location and other information about the person who approached the computer or server in question.

The software mentioned above is an example of a soft/program format tool that aids and assists the investigator during a digital investigation in the collection, separation, preservation, transformation, authentication, and transmission of the evidence collected, among other things. The digital investigation and inspection could not be started if these software programs were not used to do them.

As far as devices that are not in programme format but are utilized during investigations, these devices are in substantive form and are being used as a tool during investigations, as described above. Tool use is widespread in the modern era, and tools are used to reduce human effort in various tasks. The researcher should provide some examples of common tools that are used in the modern era, such as a drill machine, which is a tool used to drill complex objects to make holes in them; it has a specific task to prepare objects such as walls, wood, and roofs, among others. A plier is also a tool for tightening things together; its objectivity is tightening and attaching objects together. When it comes to investigating and forensically examining digital crimes, digital tools are just as essential and compelling as any other type of tool. Some digital tools are unique in their function, while others are used in multifunctional activities, and the tools are distinct from one another from almost every perspective. Some of the examples of digital tools are digital cam (used to capture the crime scene's images and videos), a couple of gloves that enable the investigator to deal with the scene with clean hands, evidence taps and flags, used to indicate the location of evidence, bags used to store the evidence in substantive form etc. The investigators and forensic examiners utilize several tools and equipment to collect and authenticate the evidence.

CONCLUSION

To complement digital investigation, the investigator used both soft and complex tools to gather information about the crime that was committed; after completion of digital investigation, the most important stage is initiated, which is forensic examination; here, the examiner attempted to determine the authenticity of the evidence, gathered by the investigator. After completion of digital investigation, the most crucial stage is initiated, which is forensic examination. Tools in digital investigation and forensic analysis played an important role because the negative use of technology gave rise to these crimes, and the investigation of these crimes can only be carried out through the use of these devices, just as the war against technology can only be waged through the use of technology.

REFERENCES

Carrier, B. D. (2016). No Title. Retrieved from www.digital-investigation.org/di_basis.html

Collins dictionary. (2021). No Title. Retrieved 1 November 2021, from collinsdictionary.com/amp/English/tool

MerriamWebster. (2011). No Title. Retrieved from https://www.merriam-webster.com/dictionary/tool

MerriamWebster. (2019). No Title. Retrieved from https://www.merriamwebster.com/dictionary/harddisk

technopedia. (2021). No Title.

Techopedia. (2020). No Title. Retrieved from https://www.techopedia.com/definition/1069/data-recovery

Techopedia. (2021). No Title. Retrieved from https://www.techopedia.com/definition/4229/backup-software