P-ISSN: 2709-6795	Annals of Human and Social Sciences	Oct-Dec 2022,Vol. 3, No. 3
O-ISSN:2709-6809	http://doi.org/10.35484/ahss.2022(3-III)21	[223-230]

Annals of Human and Social Sciences
www.ahss.org.pk

RESEARCH PAPER

An Appraisal on Digital Forensic and Computer Tools involved in Investigation process: The Case of Pakistan

[1]Dr. Muhammad Hammad u Salam* [2]Dr. Sardar M.A. Waqar Khan Arif
[3]Dr. Shujaat Ali Rathore

1. Lecturer, Department of CS & IT, Faculty of Engineering and Technology, University of Kotli, Azad Jammu and Kashmir, Pakistan
2. Assistant Professor of Law, Department of Law, Faculty of Social Sciences and Humanities, University of Kotli, Azad Jammu and Kashmir, Pakistan
3. Assistant Professor, Department of CS & IT, Faculty of Engineering and Technology, University of Kotli, Azad Jammu and Kashmir, Pakistan

***Corresponding Author** hammad.salam@uokajk.edu.pk

ABSTRACT

Cybercrime is conducted by manipulating the digital devices, the negative use of digital devices harms an individual or society. As it is primarily cleared that the digital evidence or the evidence that is not available in substantive form, can only be collected by using the tools, techniques, knowledge and expertise, here a question may be arises that whether there is a settled principle to follow while conducting the digital investigation. In this context, this article discusses the concept of digital forensic and computer tools used in the investigation process. This research is limited to the case of Pakistan. An analytical method of the research is followed. This paper concludes that as the digital investigation unlike the formal investigation is totally different having different techniques, different mechanism and different skills, the process and steps involved in digital investigation are pretty much same in rest of the world, but the standards and the legal backings are different in the countries.

Keywords: Computer Tools and Devices, Digital Computing, Forensic, Investigation Process, Pakistani Law

Introduction

The term “forensic” is obtained from a Latin word “forensic” that means forum or discussion. The origin and the legal definition of forensic is different (Tubrazi, 2017). Forensic science is defined as the science utilized to determine legal questions, science used in solving digital problems and criminal cases. Digital forensic is defined as the kind of forensic science that deals with method of recovery and investigation of the date that is in digital format, contains by digital devices like computer, mobile phones etc. It is basically a process by which scientific techniques and methods are applied during investigation (Collin, 2004). In primitive times it is specific to criminal litigation, but modern era enlightens its application and applicability on civil proceedings too.

Digital forensic stems from forensic science and it is now considered the most important branch of forensic sciences, it is the act applied by the forensic expert to deal with the evidence that is not tangible and is not seen by naked eye, as the casual substantive evidence. The experts utilize digital mind, knowledge, and excellency to recover the hidden material/evidence from the digital devices. It was limited to computer in the last decade but due to advancement in technology and diversity in digital devices and reliance of cyber criminals on digital devices. Digital forensic gained prime importance in the field of forensic sciences. Digital forensics may discuss the methodical recovery, storage, analysis, and presentation of digital information (Collin, 2004). It is a branch of the forensic sciences that deals with the analysis of digital evidence from digital sources Digital evidence is simply a product of a digital forensic process (Tubrazi, 2017).

Computer forensic/digital computing is the derivative of digital forensic and enlighten the evidence generated, hidden, and collected through computer and its authentication and production before the court of law. The whole process from start to end involves complications like it is initiated by the person who is the expert of the field irrespective of the formal investigation conducted by the police. The computer forensic from the very beginning involved diversity of the techniques like indication, detection, preservation, collection, transformation, replication, conversion etc. accuracy matters in the investigation of digital offences, if anyone of the step is not performed as per the real spirit or may loss the whole crime scene because the digital offence is the fragile evidence among all forms and demand special care, excellency, knowledge, care and experience to be taken up and if the same is conducted with the real spirit, one would find the accurate results.

Digital forensic in simple words is, to utilize scientific methods, techniques, and principles to extract the information (hidden object) from the computer and rest of other digital equipment or devices. If we look few decades back, we come to know that there was nothing but the computer which is the sole device from which the hidden information could be extracted and by which the access to information could only be possible. Now the environment is totally changed due to the influence on information technology on every field of life, every digital device can be utilized as tool in investigation.

The technology has gone through several advancements, but the principles and the capability to deal with the information are still ancient. There are hundreds of digital devices which are available in the market, have now been used to collect the evidence and from which the evidence is collected. There are two main roles that are being played by the digital devices in the current scenario; one is that the digital devices are the source of the digital evidence, it means that these devices have the capability to store the evidence and aid the investigator to extract the hidden information stored and saved by them, on the other hand these devices are now being used to collect the digital evidence available from the other device and aid the investigator in investigation of an offence. If we compare the technology with the methods of investigation, we come to know that the technology has evolved faster than the methods and techniques adopted in the forensic examination. Following are some common examples in which digital forensic is being utilized and executed (digital devices) these devices include computer, smartphones, tablets, flash drive, remote control, printer, scanner, automated systems like Automated Teller Machine (ATM) etc.

The digital investigation is only conducted by a man well-equipped with the knowledge of Information Technology (IT), he would be a good-skilled person, because it needs so many cares, diligence, knowledge, and skill to deal with the evidence that is not in substantive form. The investigator is well-versed with temperament and confidence, he must know where to speak and pause. The qualifications and disqualifications of the investigators in digital the investigations are the part of law available in the developed countries, because better investigation, better results need the best investigator to take up the case and conduct investigation. As the IT and its standards evolved from time to time, the diversity in the digital devices, cyber-attacks, undefined cyber world, and environment are the serious threat to the investigation and investigator of digital offence. The cyber/digital investigation is totally different from a formal investigation, as the formal investigation has some/almost all the stages that are to be followed during investigation of every offence, but here in case of digital offence, the investigation and its stages are distinctive and unique in almost every case.

The computer forensic and the forensic of all other digital devices are not very common like in the computer forensic the investigator's job is to;

- Keenly observe the computer apparent view of the crime-scene,
- Take the forensic image of whole crime-scene,

- The attributed location of the data available in the computer,
- Classification of the data available in the computer,
- The safe data available in computer,
- The damaged files present in different location in the computer,
- The deleted files and their destination,
- The kinds of software's available in the computer,
- The working programs of the computer,
- Where the forensic image and other available data is copied and stored,
- The detail of the devices and techniques that is to be used by the investigator,

These are the glimpses of the investigation and the job of investigator during investigation. The purpose of forensic investigation is to collect a complete set of data from the contaminated computer/ suspected computer and to assure that the data collected and seized by the investigator is saved and having no threat of contamination. The ultimate purpose of digital examination/ investigation is to collect the evidence and to process it as per the available provisions of law, to transform and transmit it into a form that can be produced before the court of law empowered to adjudicate the same.

Discussion and Analysis

The use of IT evolved from time to time and is a serious threat for existing standards for investigation, there are several kinds of digital forensic, some of them are very important to be highlighted and described, some important classifications of digital forensic are as follow:

Digital Computing

Digital computing is commonly called as computer forensic and is the most important kind among all. In simple words computer forensic may include identification, imaging, collection, storing, preservation, transformation, transmission, analyses, replication, authentication of data attributed to be present in a personal computer (PC), laptop and the storage partially or permanently attached with it, during investigation, to be presented before the competent court as a piece of evidence during trial.

Mobile/Cell Devices Forensic

After digital computing, mobile phone/devices forensic is having the prime importance, because the technology of computer and the technology involved in the mobile travel parallel with each other, mobile forensic is simply defined as the data or information accessed, collected, seized, copied, transformed, transmitted, preserved, shaped in which mobile phone is the object of investigation, it may include all the devices that are partially or permanently attached to mobile phones like a sim card, internet provider, tablets etc.

Network Forensic

Network forensic shortly termed as the net forensic and it is also most important kind, it usually elaborates the server/source of information, whereabouts of the information/attack, the intrusion and its position or door, causes of contamination, server, and its security.

Digital Snap or Image Forensic

Digital image, like the other digital information is the data that is saved there in the computer or any other digital device in form of snaps and images. Digital image literally

means the extraction of the digital snaps and to authenticate it from the original source, metadata (Discovery, 2019).

Digital Forensic of Audio and Video Forensic

This is also one the important kind of digital forensic, the terms audio and video is defined by several sources, video is hereinafter defined as "of or related to pictures that are seen in recordings or broadcast" and image is defined as the picture that is produced by camera, artist or monitor etc. Digital forensic of audio and video means the collection, storage, process, analyses, evaluation, and preservation of the evidence in the form of pictures and video, there are mainly to objectives of the above kind of forensic one is to authenticate whether it is genuine as is attributed and the other is to find out whether it is tempered or not (Intaforensic, 2019).

Digital Forensic of Memory of Device

The memory of the digital devices sometimes termed as memory analyses is the key to its importance because the memory is that vital part without which there will be no digital forensic. Memory is defined as the power or process to remember whatever one learned (Guardian, 2019). Memory forensic is the extraction of information from the random-access memory (RAM) of the computer, in today's time almost every device has the memory that can store the information more as compared to the memory of the devices in the old times.

Probable Steps of Digital Forensics

The digital evidence, its kinds and its importance are briefly explained in the previous chapters. The digital evidence is nothing without digital forensics and digital forensic is nothing without the digital forensic examiner. The role of digital forensic examiner is considered as the core role without which one cannot claim the admissibility of digital evidence. Digital forensic in simple words it relates to use of scientific knowledge and methods in involving crime. Forensic relates to the use of science in solving criminal investigation or settling legal cases (Medical dictionary, 2019).

As far as the probable steps, involved in the digital forensic examination of digital evidence is concerned, one may find the deviation, irrespective of the admissibility of digital evidence in the whole world, the steps involved in digital forensic examination and digital investigation are different in the world, as it is primarily discussed that the standards of digital evidence is not similar in the world, every country has its own legislation by which the law enforcement agencies deduce their powers to investigate the offences. The ambiguity may arises that: "what is the difference between digital investigation and digital forensic examination?" the answer to the said question is that, digital investigation as formal investigation refers to collection of evidence by the law enforcement agencies like in Pakistan "Police" is the agency that is empowered by the law to collect the evidence, Police is the investigation agency of Pakistan (The Police Act, 1861).

The digital investigation is conducted by the several agencies, investigation agency established by the Government of Pakistan through legislation or notification, like FIA , CIA, CTD etc. but not conducted by the investigator who investigate the formal offence in which formal evidence is dealt, investigation of digital evidence requires the specialist person, who is well-versed with the knowledge, technique, skill and rational of science, because every step has its own uniqueness and even a minor mistake can destroy the whole crime-scene. Digital forensic or digital forensic examination is also a process which begins after completion of digital investigation. Digital forensic examination is the process by which the authenticity of collected digital evidence is checked. Digital forensic is divergent from digital investigation but here one thing is common that is knowledge, skill, Excellency and rational.

Digital forensic examination is also the most important process which determine the authenticity of the evidence collected during digital investigation.

The process of digital forensic examination overlaps the digital investigation in several grounds, the most important among all is, the digital investigation is futile without the digital forensic examination, the courts are not duty-bound to rely upon the investigation or the report compiled and submitted by the Investigation Officers (IO), same fact is enlightened in several reported judgments but when the discussion about the report compiled and submitted by digital forensic examiner is concerned, the courts cannot refuse to entertain the same evidence, one of the big reason of non-negation is that whenever the court refuse a piece of evidence, it endorsed the reason of refusal but here the court usually have no reason of refusal.

Tools Involved in Digital Investigation and Forensics

Tool may be a device that aids in accomplishment of task, the meaning of tool in digital forensic is, the device used in the digital forensic to aid the investigator or expert to collect and authenticate the evidence. On explanatory note, tool is either a device or program, used in digital investigation or forensic to collect, preserve, transform, and present the evidence that is in digital form. The tools here are of two kinds:

Program/ software

Devices

Programs or software are tolls that are not in substantive form, it can be defined as the program that run in the computer and perform certain functions (Merriam-Webster, 2011). A software is a set of instructions and its associated documentation that tells a computer what to do or how to perform a task, software includes all different programs, on a computer such as application and operating system. In a simple view, software is basically a set of instructions that are given to computer, may have different forms and dimensions, to do a specific task, an example of the use of software is that whenever the investigator finds something in form of encryption (encryption secures online information, protected from daily attacks) he uses to adopt the decryption software's, to decode the encrypted data or information to use it on any forum, decryption is generally the reverse process of encryption. It is the process of decoding the data which has been encrypted into secret format (Decryption, 2019).

Software is basically the tool of law enforcement and forensic experts because it aids the law enforcement during the investigation of digital offence in identification, collection, separation, transformation, storing, decoding the data and information from the digital crime scene. Here a question arises that where to use the digital tools? The answer to this question is very much simple, the data available in computer or either device are of two kinds, permanent data, and temporary data. Permanent data is the data that is available in hard disk of the computer, in the storage or read only memory (ROM) of cellphone, in a device used to store the data or in any device. The data is there in permanent form until compromised or deleted by any person, on the other hand, the data that uses random access memory (RAM) to survive is in temporary form, the data stays until one switch-off the computer, it is only available when the system or a device is on, and whenever it is switched off, the data would be vanished. All you need is to collect the temporary data within the time when the computer or any device is on.

If one is curious about the software available in the market that aid and complement the investigation and forensic examination of digital offence, there are thousands of software that are available in the market that are being used in the forensic examination and investigation of digital offences. Every activity of the investigator and the forensic examiner,

need a tool in form of software of device because the evidence, that he is going to collect is not a substantive evidence; the software that are commonly used in digital investigation and digital forensic examination are “backup software”, “copier software”, “authentication software”, “encryption software”, “decryption software”, “editing software”, “recovery software”, “IP tracker”.

Every software has its own uniqueness and utility, if we define the backup software, it appears to us that, the software that is being used to create backup of the files extracted from the computer or any other device and save it to the safe place. Backup software is an application or program, utilized by the investigator or forensic examiner to enable backup of the folders, files, documents, and rest of other data, even the server as whole, backup software make exactly, the copy or clone of the data, that could be recovered in case of complete deletion or formatting of the system (Techopedia, 2019). Copier software is almost the same thing as the backup software, it is utilized to copy an object from one location and paste/drop to same to a position where it could not be manipulated, the program is available in shape of software, but the same is available in market in several shapes like photocopier, printer, scanner etc.

An authentication software is also a program, application or process that ensure and confirm a user identity. It literally means that the user that tried to access he system and obtained any source of information from the computer, its identity in any shape is stored and memorized by the system to whom, it accessed the information, by using the authentication the investigator or forensic examiner tried to find the person who was engaged in the offence by tracking its identity from the system or server. Encryption software is defined as the program or application of algorithm to readable text to convert it into the text that is unfadeable in nature. Data is being encrypted by the investigator or forensic examiner for secure storage and secure transmission. Decryption software is the program or application that work totally opposite of the encryption software, it is the reverse process of encryption, and it is the process of decoding the dates, which has been encrypted into secret format. The process is only adopted by the one who is authorized by the law enforcement to do so.

The edition software is also a program or application that is designed to edit the stuff that is being collected by the investigator during digital investigation, by using the editing software, the investigator classifies the data into different sub data, to deal with the specific/special data rather a data in form of bulk. Recovery software is a software to recover the deleted, corrupted, or inaccessible data from a storage or device. The speciality of this software is that it reviews, scan, identifies, extract and copy data from deleted, corrupted and formatted sectors or in a user-defined location within the storage device. The last concerned software is Interned Protocol (IP) tracker, it is also most important software that aids the investigator as well as forensic examiner, and it converts an IP address into a host name and provide location and other desired information about the one who approached the computer or server. These software’s are some of the examples of tools in soft/program format that aids and assist the investigator during digital investigation in collection, separation, preservation, transformation, authentication, and transmission of the evidence that is being collected. Without the use of these software the digital investigation and examination could not be initiated at all.

If one talks about the devices that are not in program format, and used in the investigation, the devices are in substantive form and used as tool in the investigation. In the modern era tools are very common in almost every field of life, tools are used to reduce human effort in specific task, the researcher needs to quote some examples of common tools that are being used in the modern time, a drill machine is a tool to drill the hard objects to make holes in them, it has a specific task to drill the objects like wall, wood, roof etc. the plier is also a tool to tight the objects, its objectivity is to tight and join the things with objects. The digital tools, like other casual tools are very much important and effective in

investigation as well as forensic examination of digital offence, some tools are unique in function but some of them are used in multifunctional activity, the tools are unique from each other in almost all perspectives.

In initial stages the tools are being utilized to collect the information to complement digital investigation, the investigator used the soft as well as hard tools to gather information about the offence that is happened, after completion of digital investigation, the most important stage is started which is forensic examination, here the examiner tried to determine the authenticity of the evidence, gathered by the investigator during digital investigation.

Conclusions and Recommendations

From the above discussion it is concluded that the Digital forensic or forensic examination is basically a technological science that deals with initiation, identification, investigation, preservation, transportation, authentication, and presentation of digital evidence that have been collected from a computer or any other digital device during digital investigation. The investigator of digital offence and forensic examiner are the unique, educated, and well-versed persons having the knowledge, education and skill of digital investigation and forensic examination. In rest of the word a program/degree is offered in this field, and the one, who qualify the same would go for digital investigation and forensic sciences.

There are several fields in which they must invest their time some of the fields are cyber-security, digital technology in forensic sciences, problem solving in cyber-net etc. After the education and research, there are several skills that must be adopted by the person interested to be a part of forensic or investigation team. He must be a self -motivated person having the capability to solve the problem and analyse the issue with an eye different with a casual person, because the field demands the ultimate effort. Computer and IT expertise are also mandatory to be possessed, every step and stage is only complemented by using the computer and other digital device, almost every functionality of the computer in shape of hardware and software must be addressed by the person. In simple words the man must be a Master of Computer, IT and other computer related studies. The last and the most important character that must be available in the forensic examiner is the application of skill, it is the very practical step, during the investigation and forensic examination may be used effectively for further progress.

References

Antawi-Boasiako, A. 2017. 'A model for digital evidence admissibility assessment'. Vol 511 IPIF International Conference on Digital forensic. < https://link.springer.com/chapter/10.1007/978-3-319-67208-3_2> (Last accessed: 08 April 2022).

Collin, P.H. 2004. Dictionary of Law, 4th edn. 127.

"Decryption" deft.org < https://www.defit.org/decryption/> (Last accessed: 20 January, 2022).

"Digital audio and video forensic" Inta forensic. Online at: < https://www.intaforensics.com/digital-forensics/audio-video-forensics/> (Last accessed: 10 March, 2022).

"Digital Forensic" Medical Dictionary. Online at: < https://medical-dictionary.thefreedictionary.com/forensics> (Last accessed: 12 January, 2022).

"Encryption" internetsociety < https://www.internetsociety.org/issues/encryption/> (Last accessed: 31 February, 2022).

"Forensic" Merriam-Webster. 2011. Online at: < https://www.merriam-webster.com/dictionary/forensic> (Last accessed: 15 May, 2022).

"Image forensic" Discovery. Online at: < https://qdiscovery.com/what-is-a-forensic-image/> (Last accessed: 10 April 2022).

"Memory forensic" Digital guardian. Online at: < https://digitalguardian.com/blog/what-are-memory-forensics-definition-memory-forensics> (Last accessed: 10 March, 2022).

The Police Act. 1861. s2.

Tubrazi, S. J. 2017. The Law of digital forensic. March.