Nizami *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003(Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 1 January-March 2018

Introduction to Digital Forensics and Commonly Used Technologies

Syeda Marrium Nizami[1], Gulfraz Naqvi[2] and Tayyaba Sultana[3]
Lahore Garrison University
mariyum002@yahoo.com, gulfraz.naqvi@gmail.com, tayyabaanwar66@gmail.com

Abstract:

In this paper importance and usage of digital forensic is discussed. As the world is developing and moving towards technology new and better ways or investigation should be introduced. Investigating methods like foot prints are used but with old technology. The new method that is still not commonly used is discussed for awareness. The growth of cybercrime is increasing with advanced methods, to overcome this problem investigation teams should be given special trainings. This will not only reduce the crime but also precious time and money of investigation department.

Keywords: digital forensic, cyber, crime, technology, investigation.

1 Introduction

The description, restoration, examination and performance in court of related data taken from electronic devices such as Systems and mobile phone are included in Digital or computer [1] forensics. That data evolve into digital affirmation bestowed in court outlined to gather people in time and space to create origin for offence against the law. Example if a wife poisoned her husband and killed him. After arresting the suspect the police will examine her computer to view her online activities and the web pages that deal with poison. In this way police will reach to the evidence. Digital proof is not important. If it points to believe on the changes in crime the accused will face the punishment.[2] In some cases it can point the accuse to pay financial damage. And the crime department that testifies in court about digital proof can be the difference between justice dressed and justice declined.

2 Digital Forensic a scientific process

Digital Forensics can be defined as “Digital forensic is an application of computer science and investigative procedure for legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeat-ability, reporting, and possible expert presentation.”

This scientific process contains the following terms:

2.1 Search authority

Search authority's examine the officers according to their work and abilities, and then assign then the cases. This is a very sensitive issue that is to be handled with care. Handing over the sensitive to an inexperienced and careless officer can lead to a big failure

2.2 Chain of custody

The process in which the evidence in documented collected and protected is called chain of custody. It is necessary for an evidence to be followed by chain of custody. When the evidences are found on the crime scene complete documentation is done including photography, note taking and sketching.

2.3 Imaging/hashing function

In an electronic crime hashing and imaging functions plays an important role in authenticating, discovering and examining the evidence. The arbitrary size data is converted to a fixed size using this function to quick data lookup as hash functions include hash tables.

2.4 Validated tools

Validated tool is an instrument used testing reliability of the results found where it is hard to trust the results. At such place reliability pays an important role. Then is validity that checks the capability of measure that is measured. The actual place to be examined is searched to find the criminal. After that is normative, that checks that is the information collected is true or not, by asking the same question from more than one person.

2.5 Analysis

The data is gathered using different tools. After gathering it is verified whether the collected information is true or not by using different functions then the analysis are made to reach the culprit.

2.6 Repeatability (Quality Assurance)

After the collecting the data and information, thee collected data is examined again and again so that if there is any false information that can be corrected immediately. This step plays an important role as a small mistake can result a heavy loss.

2.7 Reporting

Reporting means after analysis the reliable and valid data is grouped together in the form of a report that can be presented to the senior officers for discussion. This report is also useful for future cases, it can help the new officers to over look the old cases that happened before and how they were solved.

2.8 Possible expert presentation

As this whole investigation is not that easy, so after all the steps are followed to find the result at the end in this step the experienced experts make presentation that shows the evidences and the past cases for better results.

3 Forensic Computer and Digital Forensics

3.1 Working of forensic investigators

The analysis of digital data and solving computer related problems are done by forensic computer investigators and digital forensic experts. As the name implies forensic investigators investigate the crimes of hacking the source of hacking and the recovery of data. Their job includes the recovery of lost data, tracking hackers, collecting the evidences, making an investigation report, handling the electronics, teamwork and cooperation with detectives. Internal and external investigation is also done by the forensic investigators.

3.2 Education skills and Salary

Forensic investigators are sometimes fulltime or part time haired by the government and private sectors to investigate the hacking attack. It is necessary for the investigator to have a vast [3] knowledge regarding computer hardware and software. They must be familiar with the operating system, BOIS, Linux, Mac OS and windows. The education they required college education and specialized degree programs that are easily available in universities. They can major in the subjects like computer criminology. The reverent experience and knowledge regarding computer studies and hacking is acceptable for becoming a forensic investigator. Information technology, computing, criminal investigation, digital forensic experts certified hacking programs and criminology is suffice for forensic investigators. Their work is to interpret the data catch the hacker and recover the maximum loss that is possible. The salaries of forensic investigators are too high as it is a growing industry and the growth or usage of computers in rapidly increasing day by day. The per year wages of forensic investigators working in government or private sectors reaches up to fifty thousand dollar. They also work for private industries and firms on contrast so they need to be very expert in their jobs. They are not as regular because an [4] investigator can earn money per hour so working all the time is not necessary for them. Forensic investigators have different type of mood they enjoy problem solving and investigating. They never give up because they are so sure about their skills and knowledge in digging deep into a computer system. They are confident that come what may they will find a solution to that problem. [5]

4 Research Challenges

Research challenges describe the impact of forensic research in today’s life. Starting with the forensic tool, visibility and search model employed on it. Forensic researches are very expansive so new method should be introduced with the new technology produces better results on lower cost. There are two main problems with the today’s forensic tool

- These tools do not assist in investigation they were just designed to help investigator to find particular pieces of proofs.
- These tools do not investigate the crime committed on system or against the system; they just work against people where systems are used as proof.

Condition of today’s tool is that it was created to solve a pornography case not hacking one. [6] They are created to find proof where the control of proof in the crime itself. Today’s system can work on the case that contains data in terabytes but it cannot assemble that terabytes data into a report. These tools do not have the history of cases which is very helpful in new cases. Today’s tool needs changes in it to improve investigation and exploration. Because they are playing an important role in cyber defence and intelligence so their proper working is the basic necessity.

5 New research method

If the researchers are to be physically and mentally meaningful digital forensic in the coming era it needs to become more effective better related and better financially supported. These regular tools of the researchers are absorption and modularization. The important factors in cyber [7] researches are:

5.1 Computer forensic

Computer forensics or cyber forensics is defined as the use of investigative and analysis techniques, to gather evidence, to preserve evidence from any computing device in such a way that it can be presented to the court of law.

5.2 Network Forensics

Network forensics deals with the collection and analysis of packets over a network. It is collected for the purposes of information gathering, legal evidence, or intrusion detection. These packets are analysed and evidence is extracted in a scientific way to be support the investigation and if necessary, to present in the court of law.

5.3 Mobile forensics

The investigation process that is carried on mobile phone devices like PDAs, GPS, SIM cards, tablets etc. The process of Mobile forensics seems simple but it's not less complex than computer forensics. Same as computer forensics it starts from gathering electronic data for legal proceedings till the presentation of findings to the court of law. The process ranges from getting the data which is physically present on the device to the data which is deleted, this includes all the pictures, video, SMS, logs that are available on phone and anything which is deleted.

5.4 Digital forensic image

The bit by bit, sector by sector copy of a storage device is called forensics image, this copy everything that's within the storage device from a very small size file in Kilo bytes (KBs) to huge files in TB (Tera Bytes), the data in this copy includes all types of files and folders that are within the system. Moreover, this copy contains the slack spaces, free spaces or unallocated spaces that are within the hard drive, and the story doesn't ends here, it contains all the files that are visible and all files that are not visible, the files that were once part of the system or were installed or anyway existed in the system, indeed these files are the ones that were deleted anyway, but were not overwritten by any other data.

Forensics image is one of the most important element of computer forensics investigation. As soon as forensics image is taken from the place of incident, its hash value is generated, so that when its presented in court for legal proceeding the value should match the hash value of actual evidence so that process of litigation could be carried out.

5.5 Digital audio/video forensic

Audio forensics is defined as the process of acquiring, analysing, and evaluating sound recording gathered from any sound tracking source such as voicemail recordings, answering machines, telephone calls or any audio file present in tape or any medium which could be presented to court of law as an evidence for legal proceedings. Whereas video forensics refer to the investigation carried out on the evidence gathered in form of video. The video evidence could be from any source it could be from any CCTV footage from any mobile phone video recording or any video which could be presented to court to deal with legal matters.

5.6 Memory forensic

The process of analysing the memory is called memory forensics. Memory is analysed by checking the data that’s within the memory dump of the computer or in the volatile memory. When an investigation is carried out on a system, the experts usually take the memory dumps, so that they can keep record of the data which couldn’t be found in hard drive. Capturing of process running on RAM is also called live acquisition.

5.7 Computer technology skills

Digital forensic is study is technical field that can be understood by working on computer science and studding its background. A deep study of how technology works and what is its importance is important quality of a forensic investigator. A person is called a great forensic investigator who knows computer programming languages, knowledge of technology and networking, ways to interact with digital systems.

5.8 Cyber security

Solving the cyber issues like hacking cyber attack on firms this all belongs to the cyber crime so dealing with these issues called cyber security. The people deal in the cyber security is very intelligent and smart because to solve these issues one need to me very technical. Cyber security team consists of mentally strong members who enjoy problem solving.

5.9 Wireless Forensic

It’s a disciple within computer forensics, and specifically within network forensics field. The term wireless forensics was initiated by Marcus Ranum in 1997. The core purpose of this type of forensics is to collect, analyse and present the evidence gathered from network traffic to court of law. The evidence collected for wireless forensics can range from plain data to wide range of data collected from wireless technologies such as Voice over Internet Protocol (VoIP). The process of wireless forensics includes capturing of data that is transmitted over a network, analysing the network logs to unveil any abnormality that is within the network, monitor the source of the packet which may be the cause of attack.

While carrying out investigation on wireless network the security expert must keep this in mind that the same principle of computer forensics is applicable here as well, in which he has to identify evidence, preserve the evidence, and then he must make his analysis on it, which can be put to report form for further proceedings of the findings.

5.10 GPS Forensic

GPS stands for Global Positioning System. GPS devises plays a meaningful role in crime investigation to find the evidences. GPS information in GPS Forensic cases can provide such evidence that can turn over the whole plan of criminal. Today GPS is used in almost all mobile phones like smart phones, PDAs, tablets, etc that can provide the investigator with the location of criminal, first journey, last journey, current location, date and time, deleted data and even the details of mobile phones that are paired.

5.11 Malware Detection System

One of the necessity of systems these days is to have a malware detection system. Malware is mixture of basically two words malicious, and software. Malwares are widely used by the hacker for several means, there are some malwares which just corrupts the files, or delete the files, whereas there are some malwares which enters the system to encrypt the files that are within the systems, depending on the situation to which malware is designed. The situation where files are encrypted the hackers ask for ransom. So there is a need of system that should detect this malicious software in order to make our data protected, and data transmission more secure. There are several renowned organisation working days and nights to come up with system which can detect malwares, and could make processes smoother.

5.12 Password Recovery

Since 1998 the security forces electronic crime department and law enforcements are working together work on a serious issue that is to develop software that can recover the password. Password recovery software is not an ordinary thing. Sometimes a system having all the important and meaningful evidences are protected with a strong password that can be opened by the user only. But today the digital forensic researchers and investigators have made such software that can recover the password like Passware Kit Enterprise, Encryption Analyzer Professional, Passware Kit Forensic, Search Index Examiner etc. The password recovery can also be done without using software; there are also some techniques for this purpose.

5.13 Stenography

The art of hiding data within data is called steganography. Among many other encryption techniques, steganography is the one which is widely used to protect data.

In modern world steganography is widely practiced by hiding data within images, video, audio files etc.

5.14 Data recovery from serious damaged hard drive

To conduct an exclusive investigation the most meaningful evidence that can simplify the case is deleted data. Time age retrieving the lost data was almost impossible. But today the digital forensic methodologies make this impossible task possible. They have introduced with the techniques that can recover the lost and important data. Criminals always clean all the evidences that can be caught and the most important is the crime related information. The easiest task was to delete the data permanently from the drive and the criminal is safe. But this system is totally changed today by the help of digital forensic techniques the deleted or lost data can be easily retrieved.

6 Conclusion

This papers explains the concept of digital forensics and the type of technologies available to analyse a digital evidence collected by forensic team. Digital evidences are becoming increasingly important with the passage of time. In modern days many crimes are being solved with the help of digital evidences. It is very important to analyse the digital evidences carefully and reach to a conclusion through a scientific process.

Governments in most of the countries have passed laws pertaining to digital evidence. In Pakistan, Prevention of Electronic Crime Act (PECA) was approved by national assembly in August, 2016. Proper implementation of digital evidence analysis procedures and choice of right technologies ensures the proper conclusion of an investigation.

This paper explains the digital forensics evidence processing process and some of the technologies available to process the evidence.

7. References

[1] I.D.E.A.L. Technology Corporation. STRIKE (System for TRIaging Key Evidence), http://www.idealcorp.com/; 2010.

[2] Kanich Chris, Kreibich Christian, Levchenko Kirill, Enright Brandon, Voelker Geoffrey M, Paxson Vern, Savage Stefan. Spamalytics: an empirical analysis of spam marketing conversion. Commun ACM 2009;52(9). ISSN: 0001-0782:99e107. https://www.forbes.com/sites/laurencebradford/2017/04/29/6-skills-required-for-a-career-in-digital-forensics/#606402307fa6

[3] Lyle Jim. The CFReDS project, http://www.cfreds.nist.gov/; 2008. McCanne Steven, Jacobson Van. The bsd packet filter: a new architecture for user-level packet capture. In: Proceedings of the USENIX Winter 1993 conference. Berkeley, CA, USA: USENIX Association; 1993. p. 2. https://www.thebalance.com/digital-forensics-job-and-salary-information-974469

[4] Mocas Sarah. Building theoretical underpinnings for digital forensics research. Digit Invest 2004;1:61e8. Nance Kara, Hay Brian, Bishop Matt. Digital forensics: defining a research agenda. In: Proceedings of the 42nd Hawaii international conference on system sciences; 2009 https://www.interworks.com/blog/bstephens/2016/02/05/what-digital-forensics

[5] Nicholas Mikus. An analysis of disc carving techniques. Master's thesis, Naval Postgraduate School, March 2005. http://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3

[6] Opinion by Chief Judge Kozinski. 11860 us v. Comprehensive Drug Testing, Inc, http://www.ca9.uscourts.gov/datastore/opinions/2009/08/26/05-10067eb.pdf; August 2009. https://www.thebalance.com/digital-forensics-job-and-salary-information-974469

[7] Pollitt Mark, Nance Kara, Hay Brian, Dodge Ronald C, p Craiger Phili, Burke Paul, Marberry Chris, Brubaker Bryan. Virtualization and digital forensics: a research and education agenda. J Digit Forensic Pract 2008;2(2). ISSN: 1556-7281:62e73.

[8] Pollitt Mark M. An ad hoc review of digital forensic models. In: Proceedings of the second international workshop on systematic approaches to digital forensic engineering (SADFE'07); 2007. https://www.thebalance.com/how-to-become-a -digital-forensic-examiner-974633

[9] Saltzer Jerome H, Frans Kaashoek M. Principles of computer system design: an introduction. Morgan Kaufmann;
2009. Sencar Husrev, Memon Nasir. In: Identification and recovery of jpeg files with missing fragments, vol. 6; 2009, http://www. frws.org/2009/proceedings; 2009.

[10] Shelton Donald E. The 'CSI Effect': does it really exist? NIJ J March 2008;259, http://www.ojp.usdoj.gov/nij/journals/259/csieffect.htm.

[11] Turnbull Benjamin, Taylor Robert, Blundell Barry. The anatomy of electronic evidence aˆ quantitative analysis of police e-crime data. In: International conference on availability, reliability and security, (ARES '09); March 16e19 2009. p. 143e9. Fukuoka. Using purpose-built functions and block hashes to enable small block and sub-file forensics. In: DFRWS 2010,
2010. https://www.thebalance.com/digital-forensics-job-and-salary-information-974469

[12] Wood Charles Cresson, Banks William W, Guarro Sergio B, Garcia Abel A, Hampel Viktor E, Sartorio Henry P. In: Garcia Abel A, editor. Computer security: a comprehensive controls checklist. John Wiley & Sons; 1987. https://theconversation.com/footwear-forensics-device-could-catch-criminals-who-put-a-foot-wrong-54984