ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

A Study on Concepts of Digital Forensics

Suman Kumari [1], Aeshwarya [2]

PG Student, Department of Computer Science, K. L. Mehta Dayanand College, Faridabad, Haryana, India [1]

PG Student, Department of Computer Science, K. L. Mehta Dayanand College, Faridabad, Haryana, India [2]

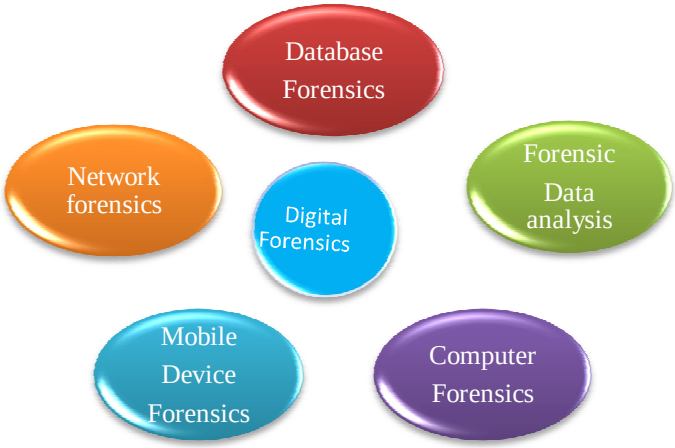
ABSTRACT: With the growth in technology, many security methods have arrived. But still crime rate is increasing and many professionals commit such cases which needs forensics investigation. In this paper we have discussed the Digital Forensics and the evidences which plays a major role to solve any case. Digital Forensics works in all the cases including computers or any digital device which used to commit crime or involved in such activities.

KEYWORDS: Forensics, technology, evidences, tools and techniques

I. INTRODUCTION

Today's era can be called as an age of information. In this age, most of the data is stored digitally. Security becomes an important issue but we can't also neglect the crimes using technologies today. Security techniques also become a challenge when it comes to investigation about the crime, if occurs. A Digital Forensics is a process to investigate using science and technology to examine the digital objects to answer the questions in the court of law about the events that occurred. Examination of digital objects requires careful methods and technical skills. Before starting any Investigation, some important questions must kept in mind such as Why the investigation is needed and the proper planning for investigation. Planning must ensure about feasibility. If the cost of the investigation being carried out is very much high than there will be no benefit of that.

Types of digital forensics



ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Aim of Digital Forensics:
Aim of Digital Forensics is to collect evidences and extract information from them to answer questions like What, Where, When, Who, Why[1].

Need for DF models :
Digital Forensics is an important tool in case of crimes related to computers. The process of Investigation must be done with proper well defined phases to reach the goal. There is need of models to work in in a systematic way to achieve the following [2]

- Determining the guilty person/parties
- Bringing perpetrators to justice
- Prevention of further malicious events
- Improving the prevention mechanism
- Improving security standards
- Increasing awareness about digital environment

Choosing the inappropriate investigation process may lead to incomplete or missing evidence or data[3].

II. PHASES OF WORKING

Digital Forensics works in a well defined manner. There are many models to define the process of Investigation and presenting them before law in court. All processes consists of some phases. The four main parts in which working is done are as follows:

1. Acquisition
2. Identification
3. Evaluation
4. Admission

   According to these phases the process starts with the acquisition of the objects and then the evidences are identified. Based on each and every evidence, examination is done to know what had happened. These evidences are presented in the court.

What can be the digital evidences?
According to the National Institute of Justice, “Digital evidences should be examined only by those trained specifically for that purpose”. Evidences that may be gathered digitally includes :

- Digital audio
- Digital video
- Cell phones
- Digital fax machines
- Computer documents such as files, spreadsheets or email
- Transactions
- Images
- Internet history, etc.

Electronic data can be easily changed, damaged or erased if handled improperly. Some of the evidences could be invisible to the naked eyes so proper tools are needed to acquire them.

How digital devices are collected?
On the scene, chargers, cables, peripherals, manuals, thumb drives, cell phones, hard drives are examined using different tools and techniques. Mobile Devices are turned off immediately which preserves cell tower location with call logs. Batteries are removed to prevent any change in data. Stand alone Computers are seized by turning off their connections. Equipments like copiers, scanners, security cameras, caller ID units are seized. Wireless devices and

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

original media are isolated and submitted to laboratories. Thus preventing contamination and proceed with the investigation.

III. CHALLENGES

Digital Forensics practitioners face some of the most challenging problems in computer science including big data analysis, natural language processing, cyber security etc. Additionally, the lengthy processes to create laws does not help much. Based on all the problems which occurs in investigation, the challenges can be divided into three major categories as shown below :[1]

1. Architectural
2. Legal and Administrative
3. Technical

Besides being many challenging situations, the investigation is carried out using back up systems, GPS systems, photos posted on social media, and many of the applications. Many phones in the market looks like company's phones but have local IMEI number which is a measure problem for forensics department.

IV. WHICH CASES NEEDS FORENSIC INVESTIGATION?

Today criminals are like technology professionals. In this information age the physical crimes are also associated with technology. Forensic Investigation can assist in a wide range of cases:[1]

- Child abuse cases
- Corporate policy violation
- Criminal Damage
- Financial Investigation
- Industrial Investigations

V. CYBER SECURITY VS DIGITAL FORENSICS

Both of the fields are strongly related with each other but still has distinct challenges and requires different skills. We can easily remember the difference between the two by thinking of the terms “before” and “after”. Cyber security is concerned with preventing illegal access to data(before any attack). Digital Forensics is about investigating after a crime.

VI. FUTURE SCOPE

Forensics department becomes a Window to past[4].It examines the objects and shows what had happened. Need of tools and techniques must be fulfilled as early as possible. Govt. has taken many steps in this field. In future, some more techniques need to be developed to solve the cases which grows with the technology. Environment is becoming more digital with the time and so security becomes the hot topic to keep our personal information safe from being misused. Cyber security has given rise to techniques such as steganography, biometric security which sometimes itself becomes a challenge to digital forensics. Digital evidences could be invisible to the eye. So there is a need for proper training to use the tools to acquire such evidences.

VII. CONCLUSION

Digital Forensics covers investigation of all devices capable of storing digital data. This process needs technical skills and proper training in that field. Labs must be provided with adequate tools and techniques needs a regular update with technology to get a good result in required time period. Awareness must be spread about changing technology

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

environment to reduce such cases. Lack of awareness also invites criminals to commit such crimes in which they are not caught easily. These days Forensics is not only restricted to law agencies, more and more private organizations are also including forensic department for overall security purpose.

REFERENCES

[1] Erik Miranda Lopez, So From Moon and Jong Hyuk Park, "Scenario Based Digital Forensics Challenges in Cloud Computing", MDPI Symmetry Article, Vol. 8, Issue 10, 8(10),107, 2016
[2] Ravneet Kaur, Amandeep Kaur, "Digital Forensics", International Journal of Computer Applications, Volume 50- no. 5, pp(0975-8887),2012
[3] Prius S. Patil, Prof. A. S. Kapse, "Survey on Different Phases of Digital Forensics Investigation Models", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, ISSN(2320-9798), 2015
[4] Simson Garfinkel, "Digital Forensics Research: The Next 10 years", Digital Forensic Research Conference
[5] Dr. Swati Mehta, "Cyber Forensics & Admissibility of Digital Evidence", The practical Lawyer, section 65-B, 2012
[6] K. Sridharan, Saktheeswari, "A Case study on cyber crime in India", International Journal of Power Control Signal & Computation, Vol. 4, No. 2, pp 123-129, 2013
[7] Cornell Walker, "Computer Forensics: Bringing the evidence to Court"
[8] Pankaj Gupta, Jaspal Singh, AnterpreetKaurArora, ShashiMahajan, "Digital Forensics - a technological Revolution in Forensic Sciences", J Indian Acad Forensic Med., vol. 33, no. 2, ISSN 0971-0973, 2011