ORIGINAL RESEARCH PAPER
Volume - 10 | Issue - 12 | December - 2021 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

CYBER FORENSICS-AN OVERVIEW

Forensic Science

Dr. G. B. Aravind Associate Professor and Coordinator, Forensic Science, Department of Forensic Medicine and Toxicology, JSS Medical College, JSS Academy of Higher Education and Research, Mysuru.

ABSTRACT

Cyber space has given several opportunities for enhancing quality of our lives in several ways. It has also given opportunities for criminals and those who intend to have an adventure with the law. Cyber Forensics is used to investigate and detect these. Technological growth has brought in an array of Cyber forensic disciplines, which enable the law to be enforced on the offenders. Forensic work involves the thorough knowledge of science and as well as the laws applicable, both to penalize violations and the procedural aspect.

KEYWORDS

Cyber Space, Cyber Forensics, Law, Offenders.

INTRODUCTION

Cyber space is a constantly expanding area, with emerging technology and applications. While this has facilitated the ease of living, it has also provided opportunities for the individuals, who have predatory tendencies and also those who wish to have a misadventure with the law. Cyber security offers certain element of prevention. Despite of this, a strong mechanism for investigation, detection and prosecution of a cyber-criminal serves as a greater deterrent. Cyber Forensics is the key to these.

Forensic science is the application of scientific knowledge to the law in order to examine clue materials seized in a crime scene or a suspect to fill in the missing links.

Cyber Forensics is therefore the application of investigation and analysis techniques, in relation to a computer, network or any device. Cyber Forensics is the procedure of identifying, preserving, collecting, analyzing and presenting the electronic evidence, in a legally acceptable form[1]. In another perspective, it is the process of application of the laws of a nation to the Computers or devices and Cyberspace.

Investigation

In cybercrime cases, the nature of the offence is such that the offence is committed in one place and the effects can be felt elsewhere. Fundamentally, the crime scene can be considered the apex of an inverted pyramid, that expands to encompass the Five 'W's and 1 H, ie., What? Who? Where? When? Why? and How? are to be systematically found out.

Cyber or Digital forensics is regarded as one of the fields that have shown a high growth rate in this century. It involves investigation of cybercrime, collection of computer based evidence of criminal activity. It uses scientifically developed protocols, which discovers and reconstructs events or sequences of events of the offences. The pertinent part of the science is that, electronic evidence, though latent or invisible, cannot be totally erased or removed, short of physically destroying the entire device[2].

It is universally understood that the diversity exists based on experiences. Also the tools and technology available in recognizing electronic evidence are equally varied. Standardization is arrived at for recognizing the electronic evidence. The examination protocol is similar to conventional Forensic Science. However, the task is complex, as technological versions of the hardware and software are changing along with testing methodology. Therefore a consensus that a four step procedure has to be followed for the collection and analysis of electronic evidence from a computer, computer system of a computer network has more or less evolved, which are as following:

1. Identification of Evidence: Perhaps, one of the most important stages, where the separation from other data is made. Locating and recognizing the method of stored data is made during this. It is also important to understand and execute the most appropriate means to retrieve and preserve the offensive electronic content.
2. Preservation: the offensive content so located has to be preserved, as far as possible in the original state. The difference between electronic evidence preservation and other Clue material collection in conventional forensic science is with the storage medium. Certified sterile media is made use for the collection of electronic evidence can be stored as a copy of the original, without any alteration to the original source. Creation of a copy or 'mirroring' of the data is made.
3. Analysis: analysis of the retrieved electronic evidence is made here. This is to identify the relevant information to the offence. The chain of events within the device or network is recreated 'bit-by-bit'. The media of the devise logs and chronicles every function. All information that have been erased or deleted can still be retrieved or recovered.
4. Presentation as evidence: Using the information as admissible proof in a court of law is the final stage. The implication as to the findings of the functions mean should be in a manner of presentation in simple terms that can be understood by a court of law. At the same time, the information should remain credible by being technically sound and also legally acceptable.

Two distinct components exist in cyber forensics. The first or computer forensics is the area where the gathering of evidence from the device, where the offence is either said to be have committed from or the effects of the offence felt. The focal concerns in computer forensics is in imaging or mirroring storage media, retrieval of deleted files, searching of slack and free space. Next is the preservation of collected information for litigation purposes. There are several forms of commercial or customized computer forensic tools are available.

The second component, the 'network forensics' is the more technically challenging aspect. It gathers electronic evidence that has been spread across the network, which is large and complex as well. This form of evidence is transient in nature and may not be preserved within permanent storage media. It deals primarily with an in-depth analysis of computer network intrusion evidence. The current commercial intrusion analysis tools may not be adequate to deal with today's networked, distributed environment. Customized software performs the recreation of the activities by the offender(s) and victim(s) prior to, at the time and subsequent to the incident. Hence, in a networked, distributed environment, it is imperative this type of examination of victim information systems on almost continuous basis[3].

Sequence Of Cyber Forensic Work:

After seizure of the evidence, the following are the steps taken to acquire and examine the data from the suspect device, in the laboratory:

Acquisition: TrueBack should work both in computer-to-computer acquisition through a parallel port link between the suspect computer and trusted workstation or through drive-to-drive (local mode) acquisition in the trusted workstation environment. TrueBack will now boot the computer (either the suspect computer of the trusted forensic workstation) and conduct a self-authentication check on the booting software. This option could be exercised both at the scene of crime (when computer forensic analysts are called at the scene of crime) or at the computer forensic laboratory (when in rare circumstance the hardware is seized without hashing and sent to the laboratory)

The focus of a Cyber Forensic Expert is mainly on active data, latent data and archival data. Active data is one that is currently available. It must be visible and can be understood using applications within a device. These might also be protected by passwords or encryption. Examples are word processor files, spread sheets, files and directories, Social Media and email content, database programs, system files, history files, temporary internet files, cookies, recycle bin and the like.

Latent data is in the form of deleted files, memory dumps and similar data which reside in swap files, temporary files, printer spool files, metadata, shadow file etc. They are also called as ambient data or volatile data. It requires an expert talent to bring to light the latent data using specialized tools and techniques.

Archived data includes that has been stored or backed up to external storage media such as tapes, CDs, DVDs, external hard disks, pen drive, zip disks, network servers or the internet. All care has to be taken while analyzing the content, as the backup peripheral devices does not have all the information. It is prudent to perform forensic analysis on original source media, mainly because backups do not store latent data[4].

The Guiding Principles of computer forensics can be expressed as the five 'A's

- Admissibility: Pertains to Legal admissibility. Every stage of the procedure from the point of the information of the offence till the submission of the evidence at the Court must be diligently documented;
- Acquisition: copying the evidence without altering or damaging the original;
- Authenticate: That the copy is identical to the source data, during the time of investigation;
- Analysis: Forensic Examination of the data while retaining its integrity and
- Anticipate the unexpected.

These principles are designed to facilitate a forensic examination of device media and enable the expert to testify in court as to their handling of a particular piece of evidence. The results must be replicable. This is due to the fact that any qualified expert who also examines the evidence using the same tools and methods employed will secure the same results[4].

Forms Of Cyber Forensics:

1. Disk Forensics: It is the extraction of data/information from storage media by searching for active, deleted files and also from unallocated and slack space, within the device.
2. Network Forensics: This is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic. While the main aim in many instances may be for the purpose of information gathering for the purpose of surveillance for malware and heuristic content, it can also serve as a form to gather legal evidence or intrusion detection. It deals with volatile and dynamic information; hence it is also called Pro-active forensics.
3. Wireless Forensics: It is a sub-part of network forensics. It is used to provide the tools required to collect and analyze the data from wireless network traffic. Voice over Internet Protocol (VoIP) Wi-Fi technologies.
4. Database Forensics: It studies and examines databases and their related metadata. A forensic examination of a database may relate to the timestamps that apply to the row (update time) in a relational table being inspected and tested for validity in order to verify the actions of a database user.
5. Malware Forensics: It deals with analysis and identification of malicious codes; to study their payload, viruses, worms, Trojans, Keyloggers etc.
6. Mobile Phone Forensics: This is one of the fastest growing area and perhaps the most varied, both in terms of the hardware and as well as the software versions. This is due to the number of manufacturers of the devices and the frequent up gradation of the technology. It examines and analyzes mobile devices that have been used in offences also. It is made use of to retrieve phone and SIM contacts, call logs (Dialed, Missed & Received), incoming and outgoing SMS/MMS, Audio, videos, paired device history and social media activity, along with geolocation and calendar information etc.
7. GPS Forensics: Also called SatNav Forensics, is a relatively new discipline with the fast paced world of Mobile Device Forensics. It is used for examining and analyzing GPS devices to retrieve information such as TrackLogs, TrackPoints, WayPoints, Routes, Photos, audio etc.
8. Social Media Forensics: Deals with recovery and analysis of Social Media Platforms and also emails including deleted messages, calendars and contacts.
9. Memory Forensics: Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.
10. E-Discovery: E-Discovery is the process of evaluating solutions for organization. A defensible e-Discovery process is repeatable, systemized and meets the legal requirements for proper handling and admissibility of electronic evidence. Email archiving can be a useful complement e-Discovery. An ideal e-discovery process identifies, collects, preserves, processes, reviews and produces relevant electronically stored information. Relevant information may be found in unmanaged, unstructured, semi-structured or structured data sources dispersed across networks on desktops, laptops, servers, share drives, removable storage media and other devices[6].

Legal Procedure:

Two systems exist, with respect to admissibility of evidence. European Union follows the principle of free introduction and free evaluation of evidence. The ease of introduction of the electronic evidence is available. In common law countries, there are laws of the procedure which provide with specific provisions which regulate the proof of an actor prove a document or its contents. This is characterized to a great extent by procedures that require oral and adversarial procedures, implying that all evidence introduced in a court of law has to withstand the scrutiny of the prescribed legal procedures with reference to its admissibility. Thus, all information collected during investigation cannot be termed as evidence. The rules of evidence presuppose that they have the following five properties:

1. Admissibility: It is the basic rule, as evidence must be admissible in a court for its use. It is governed by various legal requirements, which have to be complied with and a failure to do so is as good as not finding anything in the investigation at all.
2. Authenticity: It has to be proven in a court that the evidence what it purports to be is related to the offence in question, in a relevant manner. If the evidence cannot be authenticated in relation to the matter in question, it would nullify the use of that fact as evidence, and render it as irrelevant.
3. Reliability: The evidence that is brought forth to the court for presentation must be reliable. The methods of collection, the testing and examination of it and the analysis and interpretation should be procedurally valid and should not cast any doubt as to its authenticity and veracity.
4. Believability: The evidence so presented, should be completely believable. In addition to it the evidence must be clearly understood also by the court of law. It must be clear and lucid as the presiding officer of the court cannot be an expert in the field and too much of technological jargon may hinder its believability.
5. Completeness: electronic evidence must be in a position to prove the guilt of the perpetrator and also the innocence of others that are in question in relation to an accusation. In must be complete in the sense it must act in a culpatory and an exculpatory manner and be important to prove the matter in question.

These properties apply equally in the presentation of electronic evidence in a court of law. The Indian Evidence Act provides for evidence to a fact in Oral or a Documentary form. Electronic evidence should be in the form of material or Testimonial evidence or of an expert.

CONCLUSION:

Cyber Forensics is the amalgamation of the knowledge of Computer Sciences, Laws, Criminology and Forensic Science. Providing Electronic Evidence in a legally admissible form, by fulfilling the scientific criteria and as well as the requirements of the laws of the land. Cyber criminals do tend to use the vulnerability and gullibility of their victim, or with the sheer use of technologies. Hence, it is regarded as the most challenging, yet emerging field.

REFERENCES:

[1] Computer Forensics, US-CERT Department of Justice, US, Washington D.C.
[2] Bomisetty, Tamma and Mahalik "Practical Mobile Forensics (2014); Packt Publishing Birmingham and Mumbai

[3] Britz, Marjarie "Computer Forensics and Cyber Crime: an Introduction" (2013) Third Edition, Pearson Education Inc. New Jersey.
[4] Marcella and Greenfield "Cyber Forensics—A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes" (2002) AUERBACH PUBLICATIONS A CRC Press Company.
[5] Singh, Omveer, "Cyber Forensics: Introduction and First Responder" (2013) Additional Director (In-charge, Cyber Forensics Lab) Cyber Forensics Lab, Indian Computer Emergency Response Team (CERT-In) Department of Information Technology Ministry of Communications & Information Technology, Government of India, New Delhi.
[6] Vidya S Cyber-Forensics-The Basics CERT- Conference 2016.