www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 115.254.44.5 on dated 24-Apr-2019

Cyber Forensic: Introducing A New Approach to Studying Cyber Forensic and Various Tools to Prevent Cybercrimes

B. Vanlalsiama*
Nitesh Jha**

Abstract

With the advancement of technology world today Cyber-crimes, ethical hacking and various internet-based-crimes jeopardizes single or groups of internet users around the world. Even the greatest of the nations suffered being a victim of cyber-crime. However due to lack of digital evidence and methodology of cyber forensic the alarming crime remained unstoppable and will continue to last. The evolution of such crimes increases the need of implementing a proper and structural methodology for the study of cyber forensic to facilitate the inspection of cyber-crime and bring them to court.In this paper we adopted several phases, methodologies, including policies and educational system and combine into one effective procedures along with the powerful tool to work coordinately and to accommodate each phases after the completion of their own task. This paper serves as an enhancement of current tools and technique for the purpose of finding the accurate layers for specialization, certification, and education within the cyber forensics domain. It also highlights the importance and need of Cyber forensics tools to increase its toughness and the ability to combat this persistent threats. This paper focuses on briefing of Cyber forensics, various phases of cyber forensics, handy tools which will helps in the finding and bring the intruders in the court of law for judgment.

Keywords: Cyber Crime, Digital Evidence search Kit. Ethical hacking, Resource Centre for Cyber Forensic

Introduction

Cyber forensic play a vital role in solving crimes. the collection of forensic evidence serve an important key role that sometimes it is the only way to establish or exclude any case between suspect and victim or crime scene, eventually to establish a final verdict. As Internet technologies associate with us into everyday life, we come close to realizing new and existing online opportunities. One such opportunity is in Cyber forensics, unique process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted which helps in investigation process. The American Heritage Dictionary defines forensics as “relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law” [1].

According to the National Crimes Record Bureau, 4,231 cyber-crimes were registered under the IT Act and cyber-crime-related sections of the Indian Penal Code (IPC) during 2009-11. A total of 1,184 people were arrested under the IT Act for cyber-crimes, while 446 people were arrested under IPC sections. At least 157 cases were registered for hacking under the IT Act in 2011, while 65 people were arrested. Although a very large number of cyber-crimes probably go unreported, this statistics give us some idea about prevalence of cyber-crime in the country. This is making cyber forensics increasingly relevant in today’s India. The CID’s cybercrime cell recorded a massive 202% jump in cybercrime cases in 2014 compared to the year before. While the total number of cybercrime cases recorded in 2014 is 675, the figure stood at 334 in 2013.

B. Vanlalsiama*
MCA: 4th Semester
B-46, Chanakya Place, Janakpuri, New Delhi
Nitesh Jha**
MCA: 4th Semester,
C-39, Sagar Pur, Jankapuri, New Delhi

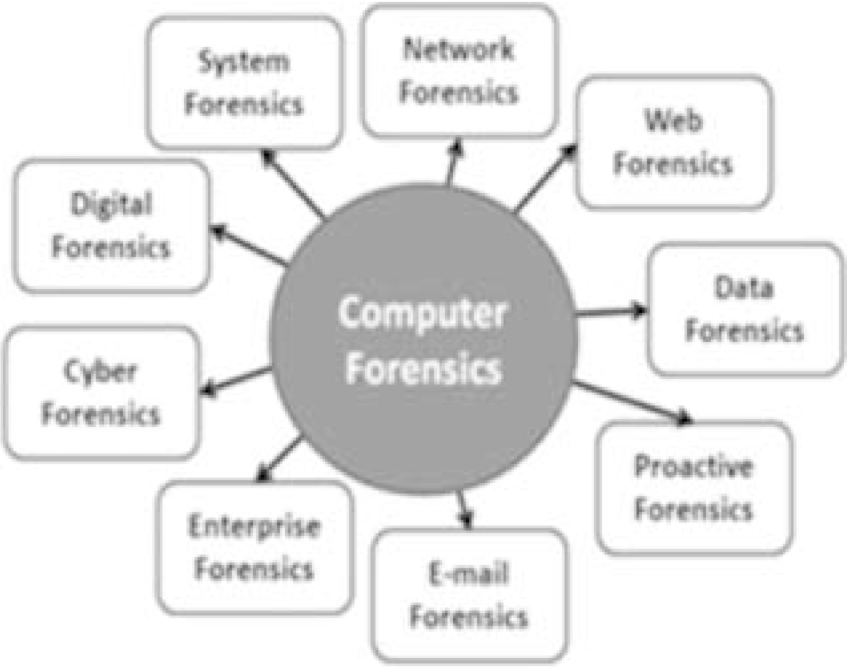

Figure 1. Status of Cyber-crime in India

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 115.254.44.5 on dated 24-Apr-2019

Taking the picture of India. Majority of the people in the country are unaware of such crime and keeps to the duty of police or investigator alone. Its initiative work in combating cybercrime remain still ineffective. Due to the unskilled or less knowledge of the investigator these crimes continue to emerge year after year. From the current scenario one can draw a hypothesis as If proper training and awareness regarding the importance of tackling cyber-crime is not recommended possibly India will suffer more than other countries in a coming decade.

Cyber forensics activities commonly include [1]

- The collection and analysis of computer data
- The identification and acknowledgement of suspect data
- The examination and of suspect data to determine details such as origin and content
- The presentation of computer-based information to courts of law
- The application of a country's laws to computer practice.

The existing methodology consists of the 3 A's:

- Acquire the evidence without altering or damaging the original
- Authenticate the image
- Analyze the data without modifying it. [2]

Using the Internet, hacker finds an opportunity to hack or perform illegal action because we all know one person sitting in a room can hack a person bank account living in another country. Since the introduction of inter-networking, hacker or intruder's action against theft, hack, and phishing have increased tremendously. It is essential that high security is maintained. It is however simply cannot be compromised. Hacker also begin to spark a better idea by using anti-forensic tool to commit a crime to hide away his/her identity. Due to this many organization were establish such as Resource Centre for Cyber Forensic (RCCF) in India to combat these kinds of crimes.

Overview of RCCF

- It offers various Cyber Security auditing services
- Consultancy for ISMS Auditing
- Cyber Forensic Analysis, Training and Laboratory Development
- Malware Analysis
- Vulnerability Assessment and Penetration Testing of Web Applications and Networks [3]

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 115.254.44.5 on dated 24-Apr-2019

Overview of tools available

Tools are mainly used for collecting digital evidence pertinent to different areas like disk forensics, network forensics, device forensics, live forensics, enterprise forensics, photo forensics and virtualized environment forensics. Some of the various tools presently used are as under:

Disk Forensics Tool: Suite with Disk imaging (True Imager), Data recovery and analysis (Cyber Check), S/W for tracing sender of e-mail, Forensic Data Carving (F-DaC), Forensic Registry analysis (F-Ran) and Forensic Thumbnail extraction (F-Tex) tools.

Network Forensics Tool: Suite with Network Session Analyzer (NeSA), Forensic Log Analyzer and S/W for tracing sender of e-mail

Mobile Device Forensics Tools: Software solution for acquisition and analysis of mobile phones, smart phones, Personal Digital Assistants (PDA) and other mobile devices (Mobile Check), s/w for analyzing Call Data Records of various service providers (Advik) and forensic solution for imaging and analyzing SIM cards (SIMXtractor)

Live Forensics Tool (Win Lift): Software solution for acquisitions and analysis of volatile data present in running Windows systems

Portable Forensics Toolkit: TrueTraveller is a portable forensics toolkit. [4]

A New Approach

As with any other crime scene, suspects leave behind trace evidence of their actions when using computers to commit a crime. Gathering evidence from a computer can be challenging, but valuable, because every operation that an each person carries out on a computer leaves behind a record that is usually dated. Finding and preserving that evidence requires careful methods as well as technical skill. Information on a computer system can be changed without a trace, the scale of data that must be analyzed is vast, and the variety of data types is enormous. Just as a traditional forensic investigator must be prepared to analyze any kind of piece of information or fragment, no matter the source, a forensic investigator must be able to make sense of any data that might be found on any device anywhere on the suspect boundary or areas. However, computer traces can also be misinterpret and, without the proper approach, files containing valuable evidence can be lost. Therefore the field of cyber forensics, still in its infancy, possesses a strong need to educate with the best training kit to equip the personnel with the latest knowledge and information.

Policies that enhance cyber forensic

1. Accurate data collection

Every policy adopted must fulfill the enterprise or organization requirement. Each enterprise's goal is to collect accurate and precise information to which the investigation could be performed and transform into useful evidence to capture the intruders. Since the misleading of information may have a huge impact on the current status of the investigation. One must keep in mind, presenting accurate data play a key role in the findings.

2. Education

Despite the changes, cyber-crime investigation in the state needs improvement. "Majority of the personnel handling cyber-crimes in the state have not studied computer science during their graduation or post-graduation. Though they are still doing their best, we believe that recruitment of B Tech graduates and post graduates with M.Sc., M.Tech or MCA degrees will immensely improve investigation standards and result in effective crime prevention,"

With technology playing a signification role in our day-to-day affairs, electronic data analysis like cellphone data analysis has become a part of even the traditional crime investigation process.

Surveillance and analysis of social media and cellphone data has become an integral part of prevention and investigation of terror and communal cases. It is a high time that cyber forensic education is prioritize with the same level of other line of education or even higher than that.

3. Forming forensic team

According to Robert Graham, a response team should include members from upper management, Human Resources, the technical staff, and outside members. The upper management member can ensure that the decisions made by the forensic team are balanced with

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 115.254.44.5 on dated 24-Apr-2019

the overall goals and best interests of the enterprise and that the decisions of the team have appropriate weight. Because of the personnel issues involved, there should be a member from human resources department. There should also be a member of the Information Technology (IT) staff on the forensics team. Security issues are often handled separately from normal IT activity. In such a case, the forensics team should work hand in hand with the IT department [6546456]

4. Role of investigator

One of the key factor to investigation is the way of investigating. Approach has been made this paper actually focus on Reactive and Proactive Investigations. Intuitively, reactive investigations attempt to solve crimes that have already occurred; this is the most frequent type .Proactive investigations attempt to deal with crime prior to the victimization, rather than after it has exacted harm on an individual, a corporation, or society.

5. Cyber forensic and law enforcement

A basic level understanding of computer forensics, at the very least, is an essential knowledge area for all law enforcement officers. Investigators need to know when information on a computer might have a nexus to a crime, how to write an appropriate warrant to seize and search a computer, and how to gather and search cyber evidence. Prosecutors and judges need to better understand the role of digital evidence — and the laborious task of a proper and thorough computer forensics exam. High technology crime task forces have already been formed in the larger metropolitan areas where this is a particularly serious problem, but the problem is actually far more widespread than just the big cities. Even a patrol officer who is not involved in computer crimes needs to know what actions to take when a computer is discovered at a crime or arrest scene. [5]

Overview of Methodology Used

It has studied that so many methodology for cyber forensic are currently being carried and applied in law enforcement. Even though many tools and various techniques has deployed we came to learnt that so many cyber-crimes cases remain pending and left unsolved. With the existing methodology and technique in this paper we form a special blended methodology which abbreviate as VIAR and its phases are discussed below:

a. Verification.

The first phases in this blended-methodology is to verify that an incident has taken place. Determine the breadth and scope of the incident, assess the case. What is the situation, the nature of the case and its specifics? This preliminary step is considered paramount important because will help determining the characteristics of the incident and defining the best approach to identify, preserve and collect evidence.

b. Information acquisition.

The next step is followed by taking notes (legal document) and describing the system you are going to analyze, where is the system being acquired, Outline the operating system and its general configuration such as disk format, amount of RAM and the location of the evidence. During this step is also important that you prioritize your evidence collection and engage the business owners to determine the execution and business impact of chosen strategies

c. Analysis of information.

After the evidence acquisition you will start doing your investigation and analysis in your forensics lab. Start by doing a timeline analysis. This is a crucial step and very useful because it includes information such as when files were modified, accessed, changed and created in a human readable format, known as MAC time evidence. The data is gathered using a variety of tools and is extracted from the metadata layer of the file system. Limited examination covers the data areas that are specified by legal documents or based on interviews. This examination process is the least time consuming and most common type. Partial examination deals with prominent areas. Key areas like log files, registry, cookies, e-mail folders and user directories etc., are examined in this case of partial examination. This partial examination is based on general search criteria which are developed by forensic experts.

d. Reporting Results.

The final phase involves reporting the results of the analysis, which may include describing the actions

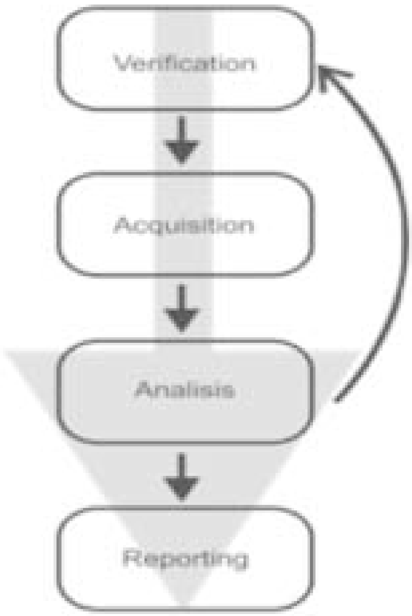

Figure 2. Phases of cyber forensic

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 115.254.44.5 on dated 24-Apr-2019

performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process. Reporting the results is a key part of any investigation. Consider writing in a way that reflects the usage of scientific methods and facts that you can prove. Adapt the reporting style depending on the audience and be prepared for the report to be used as evidence for legal or administrative purposes. The scientific method used in this phase is to draw conclusions based on the gathered evidence. This phase is mainly based on the Cyber laws and presents the conclusions for corresponding evidence from the investigation.

The above figure depict phases of cyber forensic. It is arrange in terms of stack resembling a top down approach. The top most phase is the first to be executed followed by acquisition and so on. To enhance cyber forensic phases unlike the existing phases, in this paper we make this phases iterative to ensure all the information gather and document are accurate. This eliminate the need of re-examination.

Cyber Forensics Tools

The main objective of cyber forensics tools is to extract digital evidence which can be admissible in court of law. Electronic evidence (e-evidence, for short) is playing a vital role in cybercrimes. Computer forensics tools used to find skeletons in digital media. To reduce the effect of anti- forensics tools the Investigator is likely to have the tools and knowledge required to counter the use of anti-forensics techniques [17]. Sometimes collection of digital evidence is straightforward because intruders post information about themselves from Facebook, Orkut, Twitter, Myspace and chat about their illegal activities. A subpoena, rather than special forensics tools, required obtain this information; these e-mails or chats from social networks can be admissible as evidence. [6]

Overview of DESK

To achieve all the phases being introduced we adopted one of the greatest tool called. Digital Evidence Search Kit (DESK). Desk machine is the computer used by a law enforcement agent and the subject machine is the personal computer of the suspect. The two machines communicate with each other using a serial (RS-232)

The main operations of DESK are provide by two software components in the DESK system:

- A text pattern file which contains search keywords, in Chinese and/or English, to be searched for on the subject machine, and
- Hash value databases that contain 'fingerprints' of file systems that enable file integrity verification. [7]

DESK search methods

The first important feature of DESK is the search function. It is used to search for files on the subject machine that contain pre-defined search keywords. Pre-defined search keywords are words that are relevant to a particular crime case. For instance, in a bank corruption crime, the pre-defined text patterns may contain names of different banks. The patterns can either be in English or in Chinese, or combinations of both. For Chinese patterns, different encodings of Chinese, such as Big5, GB (2312) and Unicode UTF16, are supported.

There are three main kinds of search operations:

Physical search: Physical search performs a search of the patterns of each physical sector of the subject machine's storage system. By using a physical search, cybercrime evidence purposely stored in unused sectors in the storage

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 115.254.44.5 on dated 24-Apr-2019

system can be discovered. Moreover, it provides a way for searching files independent of the specific file system. The disadvantage is that physical search, due to its lack of knowledge about the file system, can only search data within individual physical disk sectors

Logical search: Logical search makes use of the information about the file system. Conceptually, a file is a continuous sequence of bytes and the file system takes care of placing portions of the sequence into different sectors (not necessarily contiguous) while maintaining the logical contiguity of the contents of a file. A file can have a size larger than that of a disk sector. Sometimes a search pattern for a file may be split across two sectors. In these cases, the pattern cannot be found by a physical search, but can be found by a logical search.

Deleted file search: The third kind of search is the deleted file search. In most file systems, file deletion is typically accomplished by modifying only a few bytes of the file system. The contents of a deleted file are still in the storage system provided that it has not been overwritten. Therefore, patterns in a deleted file can still be found until “deleted” disk sectors are overwritten by other new files. DESK is able to search the sectors of files that have been deleted but not yet overwritten. [8]

Conclusion

Computer related crime is growing as fast as the Internet itself. Today, enterprises focus on implementing preventative security solutions that reduce vulnerabilities, with little concern for systematic recovery or investigation. We propose six categories of policies that will enable or facilitate after-the- fact action that can reduce the impact of computer crime and can deter computer crime from occurring. Some of the policies that we propose are simple actions that responsible network managers already engage as a matter of system reliability or as part of a disaster recovery procedures. The focus on computer and network forensics distinguishes these policies from backup and recovery needs. The procedures for cyber forensic require systematic application and detailed documentation, else the information may not be admissible in court. Further, backup and recovery procedures routinely ignore temporary information and other important sources of potential evidence.

Moreover, cyber forensic is much broader than just providing ready sources of potential evidence. .As people get more and more comfortable with computers, and technology advances, society becomes more computer dependent. In an era where everything from the stock market to air traffic control is managed by computers, security becomes a survival issue. In today’s society, computer crime is a serious problem. Preventive measures are not enough anymore, we must find a way to catch and prosecute computer criminals, and computer and network forensics is the gateway to archive it.

We should not leave everything to computer forensics experts. If we are going to find a solution to the computer crime problem, it will be through a collaborative effort. Everyone from individual users, to company owners have to get involved. This paper proposes policies, methodology and tools to enhance the forensics of computer security by helping experts in the field do their job faster and more efficiently. It is up to the companies and users to adopt these policies according to their needs.

References

1. Plethora of Cyber Forensics
2. www.ijarcsse.com International Journal of Advanced Research in Computer Science and Software Engineering
3. http://www.cyberforensics.in/Aboutcdac.aspx
4. http://cdac.in/index.aspx?id=cs_cf_cyber_forensics
5. http://www.computerforensics.com/law enforce.html
6. http://www.icbse.com/careers/cyber-forensics
7. http://www.engpaper.com/a1/computer-forensics research-papers.html
8. http://articles.forensicfocus.com/2014/11/29/investigation-and-intelligence-framework-iif-an-evidence-extraction-model-for-investigation/
9. http://articles.forensicfocus.com/
10. http://countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8-steps/