Plethora of Cyber Forensics

N.Sridhar[1]
Research Scholar, Dept.of CS&SE
Andhra University, Visakhapatnam,
Andhra Pradesh, India,
neralla_sridhar@yahoo.com

Dr.D.Lalitha Bhaskari[2]
Associate Professor, Dept.of CS&SE
Andhra University, Visakhapatnam,
Andhra Pradesh, India,
lalithabhaskari@yahoo.co.in

Dr.P.S.Avadhani[3]
Professor, Dept.of CS&SE
Andhra University, Visakhapatnam,
Andhra Pradesh, India,
psavadhani@yahoo.com

***Abstract*— As threats against digital assets have risen and there is necessitate exposing and eliminating hidden risks and threats. The ability of exposing is called "cyber forensics." Cyber Penetrators have adopted more sophistical tools and tactics that endanger the operations of the global phenomena. These attackers are also using anti-forensic techniques to hide evidence of a cyber crime. Cyber forensics tools must increase its toughness and counteract these advanced persistent threats. This paper focuses on briefing of Cyber forensics, various phases of cyber forensics, handy tools and new research trends and issues in this fascinated area.**

Keywords- Cyber Forensics; digital evidence; forensics tools; cyber crimes.

I. INTRODUCTION

As Internet technologies proliferate 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. 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].

Computer forensics involves the identification, documentation, and interpretation of computer media for using them as evidence and/or to rebuild the crime scenario [2]. According to [3] computer forensics defined as the process of identifying, collecting, preserving, analyzing and presenting the computer-related evidence in a manner that is legally acceptable by court.

More recently, computer forensics branched into several overlapping areas, generating various terms [4] such as, digital forensics, data forensics, system forensics, network forensics, email forensics, cyber forensics, forensics analysis, enterprise forensics, proactive forensics etc., as shown in figure-1. Digital forensics is the investigation of what happened and how. System forensics is performed on standalone machines. Network forensics involves the collection and analysis of network events in order to discover the sources of security attacks. The same process applied on Web is also known as Web forensics. Data forensics major focuses on analysis of volatile and non-volatile data. Proactive forensics is an ongoing forensics and there is an opportunity to actively, and regularly collect potential evidence in an ongoing basis. Email forensics deals with one or more e-mails as evidence in forensic investigation. Enterprise forensics is named in the context of enterprise; it is primarily concerned with incident response and recovery with little concern about evidence. Cyber forensics focuses on real-time, on-line evidence gathering.

Forensics analysis deals with identification, extraction and reporting on data obtained from a computer system.

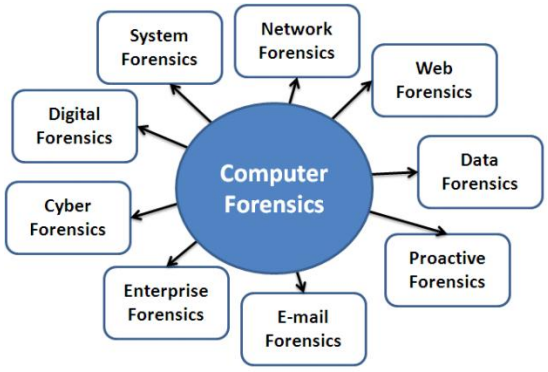

Figure 1: Various types of Computer Forensics

A. Cyber Crimes

In the 2008 CSI Computer Crime and Security Survey, it was noted that there is an average loss of $500,000 with corporations experiencing financial fraud (related to computing) and an extra average of $350,000 losses at companies that experienced "bot" attacks [5]. As per [6], the collecting digital devices in a forensically sound manner is becoming more critical since 80% of all cases have some sort of digital evidence involved in them.

With increased use of Internet in homes and offices, there has been a proliferation of cyber-related crimes and these crimes investigation is a tedious task. Cybercrime is typically described as any criminal act dealing with computers or computer Networks [7]. Cybercrimes can be classified into three groups [2]; Crimes directed against computer, crimes where the computer contains evidence, and crimes where the computer is used to commit the crime. Other names of cybercrime are e-crime, computer crime or Internet crime. Cybercrimes spread across the world with various names like worms, logic bombs, botnets, data diddling, mail bombing, phishing, rootkits, salami theft, spoofing, zombie, time bomb, Trojan horse etc.

Using the Internet, a person sitting in a Net cafe of a remote location can attack a computer resource in USA using

a computer situated in Britain as a launch pad for his attack. Challenges behind these situations are both technological and jurisdictional. Confidentiality, integrity and availability are the cardinal pillars of cyber security and they should not be compromised in any manner [2]. Attackers also begin using anti-forensic techniques to hide evidence of a cybercrime. They may hide folders, rename files, delete logs, or change, edit or modify file data [7]. To combat these kinds of crimes, Indian Government established Cyber Forensics Laboratory in November, 2003.

B. Overview of Cyber Forensics

Cyber forensics becoming as a source of investigation because human expert witnesses are important since courts will not recognize software tools such as Encase, Pasco, Ethereal as an expert witness [8]. Cyber forensics is useful for many professionals like military, private sector and industry, academia, and law. These areas have many needs including data protection, data acquisition, imaging, extraction, interrogation, normalization, analysis, and reporting.

It is important for all professionals working in the emerging field of cyber forensics to have a working and functioning lexicon of terms like bookmarks, cookies, webhit etc., that are uniformly applied throughout the profession and industry. Cyber forensics international guidelines, related key terms and tools are focused in the cyber forensics field manual [7].

The objective of Cyber forensics is to identify digital evidence for an investigation with the scientific method to draw conclusions. Examples of investigations that use cyber forensics include unlawful use of computers, child pornography, and cyber terrorism.

The area of cyber forensics has become prominent field of research because:

1) Forensics systems allow the administrator to diagnose errors
2) Intrusion detection systems are necessary in avoiding cyber crimes
3) Change detection can be possible with proactive forensics

Cyber forensics can be used for two benefits [9]:

1) To investigate allegations of digital malfeasance
2) To perform cause analysis

II. Phases of Cyber Forensics

Cyber forensics has four distinct phases: incident identification, acquisition of evidence, analysis of evidence, and reporting with storage of evidence [10]. Figure 2 shows various phases of cyber forensics process and each phase responsibility. The identification phase mainly deals with incident identification, evidence collection and checking of the evidence. The acquisition phase saves the state of a computer system that can be further analyzed. The analysis phase collects the acquired data and examines it to find the pieces of evidences. The reporting phase comprises of documentation and evidence retention.

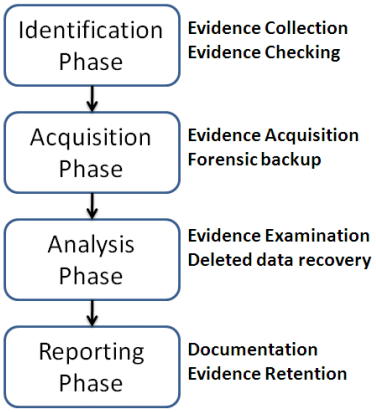

Figure 2: Phases of Cyber Forensics

A. Identification Phase

The identification phase is the process of identifying evidence material and its probable location. This phase is unlike a traditional crime scene it processes the incident scene and documents every step of the way. Evidence should be handled properly. Basic requirement in evidence collection is evidence must be presented without alteration. This requirement applies to all phases of forensics analysis. At the time of evidence collection, there is a need of thorough check of system logs, time stamps and security monitors.

Once evidence collected, it is necessary to account for its whereabouts. Investigators would need detailed forensics to establish a chain of custody, the documentation of the possession of evidence. Chain of custody is a vital part of computer forensics and the legal system [11] and the goal is to protect the integrity of evidence, so evidence should be physically secured in a safe place along with a detailed log. Figure 3 shows the evidence and chain of custody which is useful during incident investigation. Handling specific type of incidents like Denial of Service, Malicious Code, Unauthorized access etc are described in computer security incident handling guide [12].

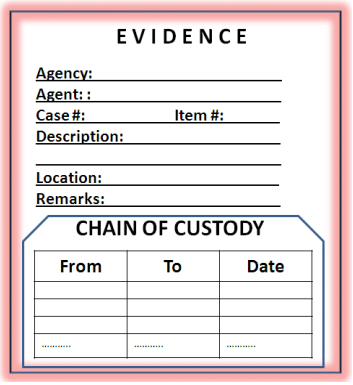

Figure 3: Evidence Form and Chain of Custody

B. Acquisition Phase

The acquisition phase saves the state of evidence that can be further analyzed. The goal of this phase is to save all digital values. Here, a copy of hard disk is created, which is commonly called as an image. Different methods of acquiring

data and their relative advantages and disadvantages are described in [13]. As per law enforcement community, there are three types of commonly accepted forensics acquisition: mirror image, forensics duplication and live acquisition.

Mirror images, bit-for-bit copy, involve the backups of entire hard disk. Creation of mirror image is simple in theory, but its accuracy must meet evidence standards. The purpose of having mirror image is evidence available in the case of the original system need to be restarted for further analysis.

A forensic duplicate, sector-by-sector, is an advanced method that makes a copy of every bit without leaving any single bit of evidence. The resultant may be single large file and must be an exact representation of the original drive at bit-stream level. This method is most common type of acquisition because it creates a forensic image of the e-evidence and it also contains file slack. In case of the small file overwrites a larger file, surplus bytes are available in the file slack. The forensic duplication process can be done with the help of tools like Forensic Tool Kit (FTK) imager, UNIX dd command, or Encase. Access Data's FTK is one of the powerful tools available and one of the promising features is the ability to identify steganography and practice of camouflaging data in plain sight.

It is often desirable to capture volatile information, which is stored in RAM; it cannot be collected after the system has been powered down. This information may not be recorded in a file system or image backup, and it may hold clues related to attacker. All currently running processes, open sockets, currently logged users, recent connections etc, are available in volatile information.

Generally, intruder takes steps to avoid detection. Trojans, keyloggers, worms etc., are installed in subtle places. One of such things to be considered in the acquisition process is rootkits, automated packages that create backdoors. An Intruders/hackers use rootkits to remove log files and other information to hide the presence of intruder. Mobile phones are become tools for cybercrimes, mobile phone evidence acquisition testing process are discussed in [14].

C. Analysis Phase

Forensic analysis is the process of understanding, re-creating, and analyzing arbitrary events that have gathered from digital sources [15]. The analysis phase collects the acquired data and examines it to find the pieces of evidences. This phase also identify that the system was tampered or not to avoid identification. Analysis phase examines all the evidence collected during collection and acquisition phases. There are three types of examinations can be applied for the forensics analysis; limited, partial or full examination.

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. Most time consuming and less frequent examination process are full examination. This requires the examiner to look each, and every possible bit of data to find the root causes of the incident. File slack inspection is done in this examination.

Some of tools used in the analysis phase are Coroner, Encase, FTK. The Coroner toolkit run under UNIX and EnCase is a toolkit that runs under Windows [7]. EnCase has the ability to process larger amounts and allow the user to use predefined scripts to pull information from the data being processed. FTK contains a variety of separate tools (text indexing, NAT recovery, data extraction, file filtering and email recovery etc.) to assist in the examination.

D. Reporting Phase

The reporting phase comprises of documentation and evidence retention. 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. There is a need of good policy for how long evidence from an incident should be retention. Factors to be considered in this process are prosecution, data retention and cost [12]. To meet the retention requirements there is a need of maintaining log archival [16]. The archived logs must be protected to maintain confidentiality and integrity of logs.

E. Forensics Methodology

The International Association of Computer Investigative Specialists (IACIS) has developed a forensic methodology which can be summarized as follows:

- ✓ Protect the Crime Scene, power shutdown for the computer and document the hardware configuration and transport the computer system to a secure location
- ✓ Bit Stream backup of digital media, use hash algorithms to authenticate data on all storage devices and document the system date and time
- ✓ Search keywords and check file space management (swap file, file slack evaluation, unallocated space)
- ✓ Evaluate program functionality, document findings/results and retain Copies of software

III. 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. A snapshot of the state of the art of forensic software tools for mobiles given in [18]. The process model for cellular phone tool testing had shown in [14]. Various cyber forensics tools and their description are provided in [7] some of them are:

1. The Coroner's Toolkit (TCT), is an open source set of forensic tools designed to conduct investigation UNIX systems.
2. Encase is the industry standard software used by law enforcement
3. The Forensic Toolkit (FTK) is very powerful tool but not simple to use.
4. I2Analyst is a different type of analysis tool, It is a visual investigative analysis software.
5. LogLogic's LX 2000 is powerful and distributed log analysis tool.
6. NetWitness and security intelligence, are network traffic security analyzer tools.
7. ProDiscover Incident Response (IR) is a complete IT forensic tool that can access computers over the network to study the network behavior
8. The Sleuth Kit is one of network forensics tools used to find file instances in an NTFS file

IV. Current Research

Cyber Forensics is sizzling topic of the current trends. Many researchers started doing intensive research in this current area. New directions in this field include authorship analysis, digital evidence collection and forensics investigation process, proactive forensics, intrusion detection systems with the help of honeypots, building evidence graphs, identifying usage of mobile phones in cybercrimes and hash function for preserving the integrity of evidence. The complete picture of Cyber Forensics in the form of Cyber forensics ontology which can be helpful for studying cyber forensics is given in [19]. Proactive forensics helps in the creation of preventive intelligence and threat monitoring besides post incident investigations.

Advantages and disadvantages of intercepting wireless network traffic as a means of locating potential evidence sources during evidence seizure are listed in [20]. Also in the same work the advantages and disadvantages of impairing communications to or from 802.11-based wireless networks during forensic seizure were discussed. High speed bitwise search model for large-scale digital forensic investigations using pattern matching board to search for string and complex regular expressions discussed in [21].

Various methods on how the evidential value of digital timestamps can be enhanced by taking a hypothesis based approach to the investigation of digital timestamp in his thesis work are proposed in the thesis [17]. Analysis of Instant Messaging in terms of computer forensics and intrusion detection is unexplored until now. Authorship classification used for forensics analysis or masquerade detection [22]. Creation of mobile software that runs on a mobile device and the goal is to aid crime scene personnel in the collection of digital devices during the course of an investigation is proposed by [23].

V. Conclusion

Cyber forensics is an emerging field in the 21st century. Detailed study of the field of cyber forensics is given in this paper. When analyzing cyber forensics, the process of doing so is different from the traditional forensics. In this paper, we described various computer forensics related definitions and phases cyber forensics and forensics methodology.

Various phases of the Cyber forensics have been discussed and each phase explored with their respective tools. Moreover, we mentioned different tools that are utilized in cyber forensics. Finally, we had shown the current research trends in this new era of cyber forensics; it still evolves and will remain a hot topic as long as there are ways to threaten data security.

References

[1] Kruse W.G, and Heiser J.G, *Computer Forensics Incident Response Essentials*, 2002, Addison Wesley Pearson Education, Boston

[2] Ibrahim M. Baggili, Richard Mislan, Marcus Rogers, *Mobile Phone Forensics Tool Testing: A Database Driven Approach*, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2

[3] Caloyannides, Michael A, Computer Forensics and Privacy. Artech House, Inc. 2001.

[4] Deepak Singh Tomar, Nikhil Kumar Singh, Bhopal Nath Roy, *An approach to understand the end user behavior through log analysis*, International Journal of Computer Applications (0975 – 8887) Volume 5– No.11, August 2010

[5] Svein Yngvar Willassen, Methods for Enhancement of Timestamp Evidence in Digital Investigations, Doctoral thesis at NTNU, 2008: 19

[6] Wayne Jansen, Rick Ayers, *Forensic Software Tools for Cell Phone Subscriber Identity Modules*, Conference on Digital Forensics, Security and Law, 2006

[7] Ashley Brinson, Abigail Robinson, Marcus Rogers, *A cyber forensics ontology: Creating a new approach to studying cyber forensics*, Digital Instigation, Elsevier, 2006

[8] Benjamin Turnbull, Jill Slay, *Wireless Forensic Analysis Tools for use in the Electronic Evidence Collection*, IEEE Proceedings of the 40th Annual Hawaii International Conference on System Sciences-2007 (HICSS'07)

[9] Hyungkeun Jee, Jooyoung Lee, and Dowon Hong, High Speed Bitwise Search for Digital Forensic System, Proceedings of world academy of science engineering and technology, volume 26, 2007.

[10] Angela Orebaugh and Jeremy Allnutt, *Classification of Instant Messaging Communications for Forensics Analysis*, The International Journal of Forensics Computer Science, 2009 (1), 22-28

[11] Ibrahim Baggili, Generating System Requirements for a Mobile Digital Device Collection System, European and Mediterranean Conference on Information Systems 2010, Abudhabi, UAE

Authors' Profile

N.Sridhar is a research scholar in Andhra University under the supervision of Prof.P.S.Avadhani and Dr.D.Lalitha Bhaskari. He received his M.Tech (IT) from Andhra University and presently working as Associate Professor in IT Department of GMRIT. He is a Life Member of ISTE. His research areas include Network Securiy, Cryptography, Cyber Forensics and Web Security.

Mrs. Dr. D. Lalitha Bhaskari is an Associate Professor in the department of Computer Science and Engineering of Andhra University. She is guiding more than 8 Ph. D Scholars from various institutes. Her areas of interest include Theory of computation, Data Security, Image Processing, Data communications, Pattern Recognition. Apart from her regular academic activities she holds prestigious responsibilities like Associate Member in the Institute of Engineers, Member in IEEE, Associate Member in the Pentagram Research Foundation, Hyderabad, India.

Dr. P. S. Avadhani is a Professor in the department of computer Science and Engineering of Andhra University. He has guided 7 Ph. D students, 3 students already submitted and right now he is guiding 12 Ph. D Scholars from various institutes. He has guided more than 100 M.Tech. Projects. He received many honors and he has been the member for many expert committees, member of Board of Studies for various universities, Resource person for various organizations. He has co-authored 4 books. He is a Life Member in CSI, AMTI, ISIAM, ISTE, YHAI and in the International Society on Education Technology. He is also a Member of IEEE, and a Member in AICTE.