ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

A Review on Cyber Forensics

[I]T.Jhansi Rani, [II]T.Swathi
[I,II]Assistant Professor, CSE, G.Pulla Reddy Engineering College (Autonomous), Kurnool. AP, India

Abstract
Computers have become an integral part of our lives. They have changed the way we work. Due to this cyber crimes are steadily increasing. Criminals have become to realize that if they want to keep doing their deeds they have to keep abreast with the times. Hence there is a need to pinpoint exactly what happened. The ability of exposing is called "cyber forensics". Cyber Penetrators have adopted more sophisticated 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 review paper focuses on briefing of Cyber forensics, various phases of cyber forensics, handy tools and new research trends in this fascinated area.

Keywords
Cyber Forensics, Digital Evidence Forensics Tools, Cyber Crimes

I. Introduction

Predators everywhere look for an opportunity to take advantage of innocent people at any given moment. Computers, in conjunction with the Internet, have given some of these predators a new tool with which to pursue their evil purpose. Due to the steady increase in instances of cyber terrorism, Internet fraud, and constantly evolving viruses, computer forensics has, and will increasingly, become more of a focal point for government and law enforcement. There are several steps and procedures that must be taken to reduce the risk of becoming a victim. There is also a plethora of tools available for use by trained individuals in the field of computer forensics. Some things can also be done to place a great deal of consequential fear in those who may be the culprits. One such way is Cyber forensics, a unique process of indentifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted.

Computer forensics involves the identification, documentation, and interpretation of computer media for using them as evidence and/or to rebuild the crime scenario [Arfid, 2005]. According to Garber [2001] 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.

A. Importance of computer forensics

Computer forensics has become an important part of the judicial process in recent months, the media reported numerous cyber attacks by criminals who know how hacking technique in computer network systems, with this in mind electronic evidence plays a more vital role in court to prove or disprove the actions of an individual in order to obtain a conviction. However, obtaining electronic evidence can be difficult and there may be problems of authenticity, digital evidence must be provided in a way that is admissible in a court of law. The exchange of information takes place every day on the Internet. While this may be convenient for us, it can also pose as an opportunity for criminals. Phishing, corporate fraud, intellectual property disputes, theft, breach of contract and asset recovery are some situations where computer forensics can be applied.

The main computer forensics advantage is its ability to search and analyze a large amount of information quickly and efficiently and to identify key pieces of data that can be used to assist in the formation of a legal case. Valuable data that has been lost, deleted by offenders can be recovered and used to form substantial evidence in court. A forensic expert recognized computer is able to produce in court data by reporting that was previously impossible. Another advantage is a forensic doctor can search the hard drive using different languages and is beneficial as cyber crimes easily cross borders through the Internet. It is important to remember that the evidence can not be captured once, so asking the right experts. More recently, computer forensics branched into several overlapping areas, generating a plethora of terms [Oliver et al, 2009] such as, digital forensics, system forensics, network forensics, web forensics, data forensics, proactive forensics, E-mail forensics, enterprise forensics, cyber forensics, etc. System forensics is performed on standalone machines. Network forensics involves 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 majorly 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. E-mail forensics deals with one or more e-mails as evidence in forensic investigation.

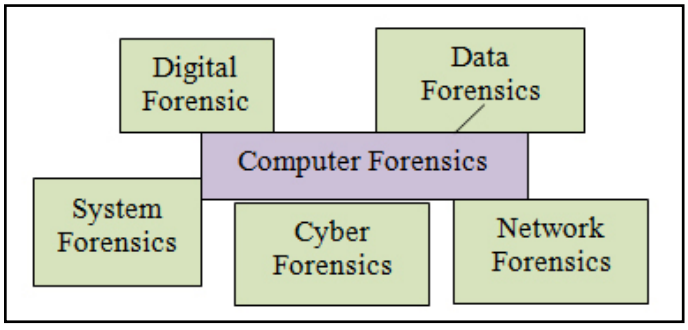

Fig. 1: Plethora of Computer Forensics

Cyber forensics focuses on real- time, online evidence gathering. Forensics analysis deals with identification, extraction and reporting on data obtained from a computer system.

With increase use of Internet in homes and offices, there has been a proliferation of cyber-related crimes and these crimes investigation is tedious task. Cyber crime is typically described as any criminal act dealing with computers or computer Networks [Marcella, Albert, 2008]. Cyber crimes can be classified into three

groups [Arfid, 2005]; Crimes directed against computer, crimes where the computer contains evidence, and crimes where the computer is used to commit the crime. Other names of cyber crime are *e*-crime, computer crime or Internet crime.

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 [Arfid, 2005]. Attackers also begin using anti -forensic techniques to hide evidence of a cyber crime. They may hide folders, rename files, delete logs, or change, edit or modify file data [Marcella, Albert, 2008]. 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 [Meyers and Rogers, 2004]. 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. Albert and Robert [2008] focused the cyber forensics international guidelines, related key terms, and tools in their field manual.

The objective of Cyber forensics is to identify digital evidence for an investigation with 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 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 [Whitman, Mattord, 2010]:

(1) To investigate allegations of digital malfeasance
(2) To perform root 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 [Cole, 2010]. 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.

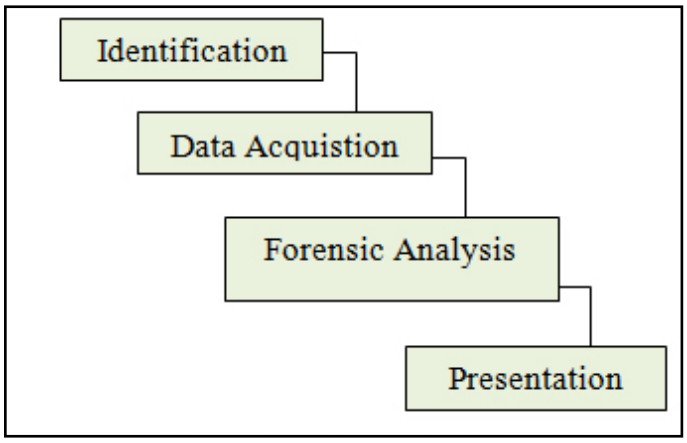

Fig. 2: Phases of Cyber Forensics

1. 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 process the incident scene and document 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 the 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 [McQuade and Samuel, 2006] and 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. Karen et al [2008] described handling specific type of incidents (Denial of Service, Malicious Code, Unauthorized access etc) in their computer security incident handling guide.

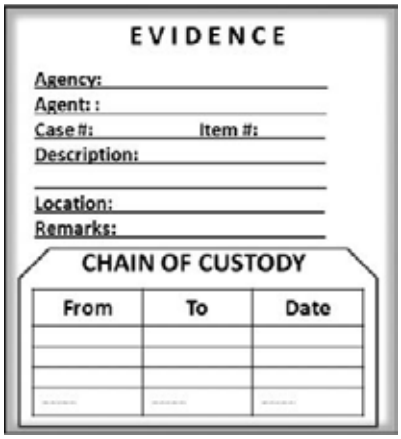

Fig. 3: Evidence Form and Chain of Custody

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. Kruse and Heiser [2002] described the different methods of acquiring data and their relative advantages and disadvantages. As per law enforcement community, there are three types of

commonly accepted forensics acquisition: mirror image, forensics duplication and live acquisition.

A Mirror image, bit-for-bit copy, involves 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 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 the evidence. The resultant may be single large file and must be an exact representation of the original drive at bitstream 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 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 more powerful tools available and one of the promising features is the ability to identify steganography, 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 backups 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. Intruders/hackers use rootkits to remove log files and other information to hide the presence of intruder. Mobile phones are become one of the tools for cyber crimes, mobile phone evidence acquisition testing process are discussed in [Baggili et al, 2007].

3. Analysis Phase

Forensic analysis is the process of understanding, re-creating, and analyzing arbitrary events that have gathered from digital sources [Caloyannides, 2001]. 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 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 is 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. [Marcella, Albert, 2008]. 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, E-mail recovery etc.,) to assist in the examination.

4. Reporting Phase

The reporting phase comprises of documentation and evidence retention. The scientific method is used in this phase 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 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 [Karen et al, 2008] (p 3-27). To meet the retention requirements there is a need of maintaining log archival [Tomar et al, 2010]. The archived logs must be protected to maintain confidentiality and integrity of logs.

5. 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 vital role in cyber crimes. 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 antiforensics techniques [Willassen, 2008]. 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. Jansen, Ayers [2006] gave a snapshot of the state of the art of forensic software tools for mobiles. Baggili et al [2007] had shown the process model for cellular phone tool testing. [Marcella, Albert, 2008] described various cyber forensics tools and their description, some of them are:

(1) The Coroner's Toolkit (TCT), is an opensource set of forensic tools designed to conduct investigation UNIX systems.
(2) The Forensic Toolkit (FTK) is very powerful tool but not simple to use.
(3) I2Analyst is a different type of analysis tool from those information security professionals are used to.
(4) LogLogic's LX 2000 is powerful and distributed log analysis tool.
(5) NetWitness, security intelligence, is a network traffic security analyzer tool
(6) ProDiscover Incident Response (IR) is a complete IT forensic

tool that can access computers over the network to study the network behavior

(7) The Sleuth Kit is one of network forensicstools used to find file instances in an NTFS file

IV. Current Research

Cyber Forensics is a sizzling topic of the current trends. Many researchers started doing intensive research in this current area. New directions in this field includes 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 cyber crimes and hash function for preserving integrity of evidence.

Turnbull and Slay [2007] listed the advantages and disadvantages of intercepting wireless network traffic as a means of locating potential evidence sources during evidence seizure. 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 [Hyungkeun et al, 2007].

Willassen [2008] in his thesis proposed 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. 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 [A. Orebaugh and J. Allnutt, 2009]. Baggili [2010] proposed the creation of mobile software that runs on a mobile device and goal is to aid crime scene personnel in the collection of digital devices during the course of an investigation.

V. Conclusion

Cyber forensics is an emerging field in the current trend. A survey of the field of cyber forensics is given in this paper. When analyzing cyber forensics, the process of doing so is different than the traditional forensics. In this survey paper we described various computer forensics related definitions and phases of cyber forensics and forensics methodology. The various phases of Cyber forensics have been discussed and each phase explored with their respective tools. It still evolves and will remain a hot topic as long as there are ways to threaten data security. Finally we had shown the current research trends in this new era of cyber forensics

References

[1] *A. Orebaugh and J. Allnutt, 2009, Angela Orebaugh and JeremyAllnutt, "Classification of Instant Messaging Communications for Forensics Analysis", The International Journal of Forensics Computer Science, 2009 (1), pp. 22-28.*

[2] *Arfid, 2005 Arfid Ahmed, 2005, "Have You Been Hacked"? A Primer to Cyber Security and Cyber Forensics, the Chartered Accountant, Dec 2005.*

[3] *Ashley et.al.,2006 Ashley Brinson, Abigail Robinson, Marcus Rogers, "A Cyber Forensics Ontology: Creating a New Approach to Studying Cyber Forensics", Digital Instigation, Elsevier, 2006.*

[4] *Baggili and Rogers, 2009. Ibrahim Baggili, Marcus Rogers, "Self-Reported Cyber Crime: An Analysis on the Effects of Anonymity and Pre-Employment Integrity", International Journal of Cyber Criminology, Vol 2, Issue 2, July-Dec 2009.*

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

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

[7] *Caloyannides, 2001 Caloyannides, Michael A, "Computer Forensics and Privacy". Artech House, Inc. 2001.*

[8] *Cole, 2010 Eric Cole, Ronald Krutz, James W. Conley, "Network Security: Bible", 2nd Edition, (2010), p.p 730 Wiley India Pvt. Ltd.*

[9] *Garber, 2001 Garber, L. 2001, "Computer Forensics: High-Tech Law Enforcement", IEEE Computer Society's Computer Magazine, 34 (1). pp. 22-27.*

[10] *Hougton, 2000 Houghton Miffin Company – The American Heritage Dictionary, 4th Edition, 2000.*

[11] *Hyungkeun et al, 2007 Hyungkeun Jee, Jooyoung Lee,and DowonHong, "High Speed Bitwise Search for Digital Forensic System", Proceedings of World Academy of Science Engineering and Technology, Vol. 26, 2007.*

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

[13] *Karen et al, 2008 Karen Scarfone, Tim Grance, Kelly Masone, "Computer Security Incident Handling Guide", NIST SpecialPublication pp. 800-61, (2008).*

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

[15] *Marcella, Albert, 2008 Marcella Jr., Albert J., "Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes". 2008. Taylor & Francis Group, LLC. Auerbach Publications. pp. 27-48 pp.77-85 pp.87.*

[16] *McQuade and Samuel, 2006 McQuade, Samuel C. "Understanding and Managing Cybercrime", (2006). Pearson Education, Inc. pp. 373-374.*

[17] *Meyers and Rogers, 2004 Meyers M, Rogers M, "Computer Forensics: the Need for Stand Ardization and Certification", International Journal of Digital Evidence, 2004.*

[18] *Oliver et al, 2009 Oliver De Vel, Alison Anderson, Mal Corney, George Mohay, "E-Mail Authorship Attribution for Computer Forensics", Applications of Data Mining in Computer Security, Springer (2009), pp. 230.*

[19] *Rogers, 2006 Rogers, M. (2006), "DCSA: A Practical Approach to Digital Crime Scene Analysis". West Lafayette, Purdue University.*

[20] *Tomar et al, 2010, 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 pp. 0975-8887) Vol. 5 No. 11, August 2010.*

[21] *[Turnbull and Slay, 2007, "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).

[22] Whitman, Herbert, 2010 Michael E. Whitman, Herbert J.Mattord, "Principles and Practices of Information Security", Cengage Learning (2010) pp. 426.

[23] Willassen, 2008, "Svein Yngvar Willassen", Methods forEnhancement of Timestamp Evidence in Digital Investigations, Doctoral thesis at NTNU, 2008: 19.