International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 173 - 178

A Review on Computer Forensics

Ms. Vishakha R. Bhadane
Assistant Professor, Dept of Computer Engineering
JESITMR, Nashik
e-mail: bhadanevishakha@gmail.com

Mr. Rahul C. Patil
Assistant Professor, Dept of Computer Engineering
JESITMR, Nashik,
e-mail:rahulpatil0830@gmail.com

***Abstract*—**Activities cyber crimes have become worse important part of everyday life in both the corporate world and the general public. The phenomenon of digital crime achieved what one might call the overwhelming factor. This explores the need for computer forensics to exercise effective and legal way, and describe the basic technical issues, and a reference point for further reading. It promotes the idea that competent practice in computer science and awareness of the fundamental laws of the retina for organizations today. This is an important topic for managers who need to understand how come a strategic element of computer science in the public information organization IT security. Network administrators and other IT security staff members need to understand the issues related to computer science. Those who work in the field of corporate governance, legal services, information technology, or find an overview of Sciences.

Keywords*-Computer Forensics, Digital Crime ,Security , Cyber Laws.*

*****

I. INTRODUCTION

Computer forensics is also known as Computer Forensic Science (CFS). It is a branch of digital forensic science pertaining to legal evidence in computers and digital storage media.

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence of a particular computing device in a manner that is suitable for presentation to a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible. Computer Forensics is the science of obtaining, preserving, and documenting evidence from digital electronic storage devices, such as computers, PDAs, digital cameras, mobile phones, and various memory storage devices . Everything must be done in a way designed to preserve the probative value of the evidence and ensure its admissibility in court proceedings.

Computer forensics involves the identification, documentation and interpretation of computer media for use as evidence and / or reconstruct the crime scenario [Arfid, 2005]. Garber [2001] computer forensics defined as the process of the identification, collection, preservation, analysis and presenting the elements related to the computer in a manner that is legally acceptable by the court. More recently branched into computer forensics several overlaps, generating a plethora of terms [Oliver et al, 2009], such as digital forensics, forensic system, network forensics, web forensics, data forensics, proactive forensics, forensic E-mail forensics company, cyber forensics, etc., as shown in Figure 1. Digital Forensics is the investigation of this happened and how. forensics system is performed on Autonomous machines. network forensics involves collection and network events analysis to discover the sources of security attacks. The same Process applied to the web is also known as web forensics. Data forensics majority focuses on analysis volatile and non-volatile data. forensics proactive is a forensic courses and there is a possibility of actively and regularly collect potential evidence in a ongoing basis. Email forensics deals with one or more e-mails as evidence in forensic investigations.

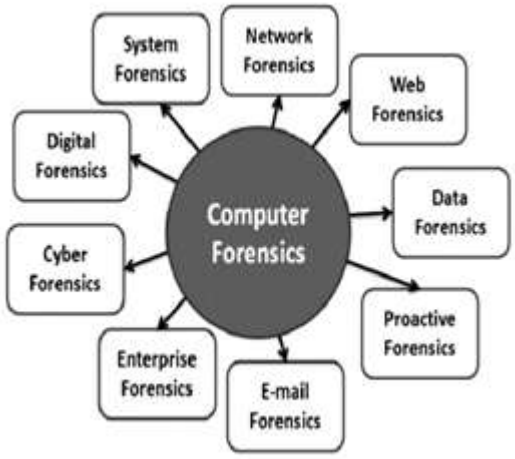

Figure 1. Plethora of Computer Forensics

Forensic Enterprise is appointed in the context of business; it is mainly related to the incident response and recovery with little concern evidence. Cyber Forensics focuses on real-time, on-line evidence collection. Forensics analysis is the identification, extraction and reporting data obtained from a computer system. Crimes of cyber crime in 2008 CSI Computer safety investigation, it was noted that there is a average loss of $ 500,000 with companies experiencing financial fraud (computer-related) and an additional average of $ 350,000 loss to companies attacks "bot" experienced [Baggili and Rogers, 2009] .114 International Journal of Computer Science, Systems Engineering and Information Technology Rogers [2006], the digital device collection in a forensic way sound is increasingly critical since 80% of all cases have some sort of digital evidence involved in them. The field of cyber forensics has become important research because: With the increase of Internet use in homes and offices, there has been a proliferation of crimes related to cyber and they investigate crimes is tedious. Cyber Crime is usually described as any crime operation with computers or computer networks [Marcella, lbert, 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 for commit the crime. Other names of cyber crime are crime, computer crime and Internet crime. Using the Internet, a

person sitting in a Net cafe a remote location can attack a computer resource United States using a computer located in Britain as a launch pad for his attack. Challenges behind these situations are both technological and jurisdictional. ONFIDENTIALITY, integrity and availability are cardinal pillars of cyber security and they should not be compromised in any way [Arfid, 2005]. Attackers also begin using anti-Forensic technology hide the evidence of a cyber crime. They can hide folders, rename files, delete logs, or modify, edit or modify the file data [Marcella, Albert, 2008]. To fight against these types crimes, the Indian government has created Cyber forensic laboratory in November 2003. We can also say that computer forensics is the science of forensics applied in a digital environment. But where a specialist in traditional forensics can collect and store fingerprints or other physical evidence, the specialist in computer forensics collects and maintains digital evidence.

This collection of digital evidence must be done by carefully prescribed procedures and recognized that the probative value of digital evidence is preserved to ensure admissibility in court proceedings. As the traditional forensics can involve people with different specialties, computer forensics even involves a multitude of professional specialties who work together to collect, store and analyze digital evidence[1].

II. PHASES OF CYBER FORENSICS

Cyber forensics has four distinct phases: the identification of the incident, the acquisition of evidence, analysis proof, and relations with the storage of evidence [Cole, 2010]. Figure 2 shows the different phases of cyber forensics process and each phase of responsibility. The identification phase deals mainly with problem determination, evidence collection and verification of evidence. The acquisition phase which saves the state of a computer system that can be further analyzed. The analysis phase collects acquired data and examines it to find the pieces of evidence. The phase comprises reporting documentation and preservation of evidence.

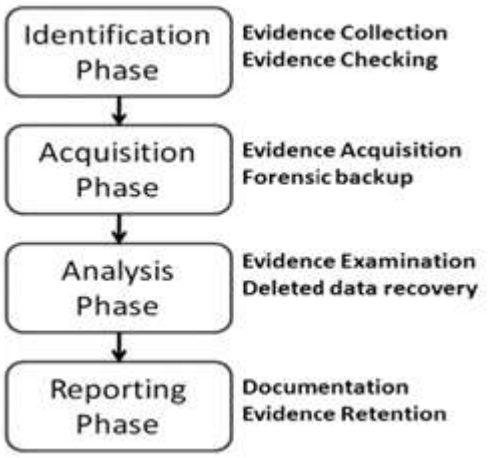

Figure 2. Phases of Cyber Forensics

A. Identification Phase

The identification phase is the process of identifying relevant evidence and its likely location. This phase is unlike a traditional crime scene, it deals with the scene of the incident and documenting every step of the way. The evidence must be handled properly. basic requirement for evidence collection is proof must vs Computer Forensics Computer Security will be presented without alteration. This requirement applies to all phases of the forensic analysis. At the time of collection of evidence, it is necessary to thorough checking system logs, time stamps and security monitors. Once the collected evidence, it is necessary to account for his whereabouts. Detailed forensic investigators would need to establish a chain of custody, documentation of the possession of evidence. Chain of custody is an essential part of computer forensics and legal system [Samuel McQuade and 2006] and the goal is to protect the integrity of the evidence, so that evidence must be physically secured in a safe place with a detailed log. Figure 3 shows the evidence and the chain of custody which is useful when the incident investigation. Karen et al [2008] described the handling specific types of incidents (Denial of Service, malicious code, unauthorized access, etc.) in their computer security incident handling guide.

Figure 3. Evidence Form and Chain of Custody

B. Acquisition Phase

The acquisition phase saves the state of the evidence that can be further analyzed. The objective of this phase is to save all the numerical values. Here is a copy of the hard disk is created, which is commonly referred to as an image. Kruse and Heiser [2002] described the various methods of data acquisition and their advantages and disadvantages. As for enforcement community law, there are three types of commonly accepted acquisition of forensics: mirror image, forensic duplication and acquiring live. A mirror image, bit for bit copy, involves the entire hard disk backups. Creating mirror image is simple in theory, but accuracy must meet the standards of proof. The purpose of having the mirror image is proof available when original system needs to be rebooted for later analysis.

Double judicial sector by sector, is an advanced method makes a copy of each bit without leaving a single bit of evidence. The resulting file can be alone and must be an exact representation of the original disc at the bit stream. This method is most common acquisition because it creates a forensic image of the e-proof and it also contains the soft file. For small file overwrites a larger file, the extra bytes are available in soft file. The forensic duplication process can be done with the help of tools like Forensic Tool Kit (FTK) images, the UNIX command or Encase. FTK data access is one of the most powerful tools available and one of the promising features is the ability to identify stenography, the practice of hiding data in order. It is often desirable to capture volatile information which is stored in the RAM; it can not be withdrawn after the system was turned off. This information can not be saved to a file system or image backups and can

detain the attacker linked indices. All running processes, open sockets, users currently connected, recent connections etc are available in the volatile information. In general, the hacker takes steps to avoid detection. Trojans, key loggers, worms, etc., are installed in subtle places. One of these things to be considered in the process of acquisition is root kits, automated packages that create back doors. Intruders / Hackers use root kit to delete the log files and other information to hide the presence of intruders. Mobile phones have become one of the tools for cyber crimes, mobile processes of acquisition of phone data test are discussed in [Baggili et al, 2007].

C. Analysis Phase

Forensic analysis is the process of understanding, re-creation, and analysis of arbitrary events gathered from digital sources [Caloyannides, 2001]. The analysis phase collects acquired data and examines it to find the pieces of evidence. This phase also identifies that the system has been tampered with or not to avoid identification. analysis phase examines all the evidence gathered during collection and acquisition phases. There are three types of tests can be applied to forensic analysis; review, partial or complete. Limited review covers areas of data that are specified by legal documents or based on interviews. This review process is less time and the most common type. Partial exam addresses important areas. Key areas such as log files, registry, cookies, email folders and user directories, etc., are examined in this case of partial examination. This partial examination based on general search criteria that are developed by forensic experts. More time and less frequent review process is a comprehensive review. This requires the examiner to look at every bit of data possible to find the root causes of the incident. File slack inspection is done this review.

Some of the tools used in the analysis phase are Coroner, Encase, FTK. Coroner toolkit running on UNIX and EnCase is a toolkit that works on Windows. [Marcella, Albert, 2008]. EnCase has the ability to handle larger quantities and allow the user to use predefined scripts to extract information from data being processed. FTK contains a variety of separate tools (text indexing, NAT recovery, data extraction, file filtering, email recovery etc.) to assist in the review.

D. Reporting Phase

The phase relationships includes documentation and preservation of evidence. The scientific method is used at this stage to draw conclusions based on the evidence collected. This phase is mainly based on Cyber Laws and presents the findings of evidence to the inquiry. There is a need for a good policy for how long the evidence of an incident should be retained. Factors to consider in this process is continuing, data retention and cost [Karen et al, 2008] (p 3-27). To meet the requirements of retention is required to maintain records of journal [Tomar et al, 2010]. Archived logs should be protected to preserve the confidentiality and integrity of newspapers.

E. Forensics Methodology

The International Association of IT specialists Investigation (IACIS) developed a legal methodology that can be summarized as follows:

- Protect the crime scene, the computer's power off and document the hardware and transpor the computer system to a secure location
- Bit Torrent backup of digital media, use hash algorithms for authenticating data on all storagedevices and document the date and time of the system
- Search keywords and check the file management of space (page file, the evaluation file slack, unallocated space)\
- Evaluate the features of the program, document the results / outcomes and retain copies of software

III. COMPUTER FORENSICS VERSES COMPUTER SECURITY

Computer Forensics is often associated with computer security, the two are different.

- *Computer Forensics* mainly the acquisition, proper preservation and analysis of digital evidence, usually after an access or unauthorized use occurred.
- *Computer security*, its main objective relates to the prevention of unauthorized access, as well as maintaining the confidentiality, integrity and availability of computer systems.

Information Security and Computer Forensics are free in the greater familiarity with Computer Forensics can lead to greater awareness of the importance of computer security in general, and appropriate procedural controls for access and use computers, networks, and other devices. Furthermore, in case of breach of security, much can be learned during the process the collection of digital data. This knowledge can be applied to improve the system of procedural controls, operations and staff capacity. [1]

IV. 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

to help in a case involving evidence on the computer base is crucial.

V. PREVIOUS WORKS OF COMPUTER FORENSICS

Digital Forensics was developed in the first Digital Forensics Research Workshop (DFRWS) in 2001 and has been defined as the use of derivatives scientifically and preservation method, the collection, identification, validation, interpretation and analysis of the documentation and presentation of digital evidence tested from digital sources in order to facilitate or promote the reconstruction of events considered criminals or helping to anticipate unauthorized actions shown to be destructive to a planned operations [5]. This formulation emphasizes the scientific nature of digital forensic methods, in a time when there was the transition from being a craft to a field and created a legitimate part of forensic science. Many versions of commercial open source software and high quality tools have long been in existence for conducting digital forensic investigations. Although their data processing capabilities vary because they are based on the image processing paradigm, where the original of the suspected target image is first obtained, including all the operations performed on this image. This tool has been referred to the live access tool because they provide a standalone environment to allow researchers to examine the digital evidence from the source [5].

A. Relevance of Digital Forensic

Digital Forensics was developed in the first Digital Forensics Research Workshop (DFRWS) in 2001 and has been defined as the use of derivatives scientifically and preservation method, the collection, identification, validation, interpretation and analysis of the documentation and presentation of digital evidence tested from digital sources in order to facilitate or promote the reconstruction of events considered criminals or helping to anticipate unauthorized actions shown to be destructive to a planned operations [5]. This formulation emphasizes the scientific nature of digital forensic methods, in a time when there was the transition from being a craft to a field and created a legitimate part of forensic science. Many versions of commercial open source software and high quality tools have long been in existence for conducting digital forensic investigations. Although their data processing capabilities vary because they are based on the image processing paradigm, where the original of the suspected target image is first obtained, including all the operations performed on this image. This tool has been referred to the live access tool because they provide a standalone environment to allow researchers to examine the digital evidence from the source [5].

VI. CHALLENGES OF DIGITAL EVIDENCE

Since electronic data is clearly different from the traditional paper documents, it is therefore necessary to be handled accordingly.

a) Types of Data

A modern computer typically stores vast amounts of data. Some of these data are active others may be residual or back up data.

b) Active Data

Active data is data created by the user such as customer information, inventory data, word processing documents or spreadsheets, programs and operating system files, including temp files .

I) META-DATA AND OTHER DATA

Many users are aware of important data held in data files. However, many users may not be aware of the other information on the files - including the creation time and the person creating it -which may also be useful in an investigation. This data is referred to as meta data. For example, one were to open a Microsoft Word © document and verify the properties (by clicking File, then click Properties on the top menu) could find a wealth of information, including dates and times documents was created, last modified, and printed, the number of revisions, the file size and the installation time. This meta data is stored in the document itself, can contain the history of the document, including all users who have modified and / or registered there, the directory structure of all machines, it was and stored on the printer names, it was printed.

II) OPERATING SYSTEM DATA

Data from the computer's operating system can be a rich source of information about what the user has done. From these data, a specialist in forensic medicine can retrieve information such as a user of websites visited; emails sent and received, etc. While access to the Internet, browsers keep records of websites visited by a user. If a user allows cookies, which are small files used by browsers to monitor, among other things, a user visits, cookies can be a valuable source of information about the user's Internet practices storing all kinds data, including passwords. These records can be recovered by forensic investigations if clear evidence of the sites the user visited is needed.

III) TEMPORARY FILES

When a user runs a program, for example, word processing, data can be temporarily stored on the hard drive. For example, Microsoft Word saves changes to a document at intervals defined in a separate file recovery, temporary when the ASR function is activated. These temporary files can allow dedicated access Computer Forensics documents not recorded by a user. This is something the "Bandit toothless" discovered in 1999. The thief, who had participated in 12 bank robberies in the San Diego area, wrote threatening notes on her computer. Although he broke his word processor without saving these notes, a forensic investigation of his computer yielded five notes of the request 3.

IV) Communications Data

Whenever a person uses a computer, mobile phone or --other device to communique, a digital trail is created That can yield information Regarding Whom the user Communicated with, What Was Discussed, When It Occurred, Who Was privy to it, what materials Were Transmitted, and-even Attempts to erase the record of That communication. All thesis Would Be Electronically Stored - Potentially and discoverable. Some of this data Resides In a user's computer --other goal under data resides in May Devices That form of the network share or are attached to the network Such As routers or intrusion detection systems. Companies providing good communications services, for example, Internet Service Providers (ISPs) Maintain communications logs That are Useful in investigative searches.

V) Tracking and Tracing through the Internet

Tracing and tracking of emails and other Internet communications is possible because the communication protocol which is based Internet communications, TCP / IP, assign a four-byte identifier for each device connected to the Net. This identifier is called an IP address. An IP address is

often represented as four decimal numbers separated by periods, such as 143.89.56.78. Each ISP is assigned an IP address range that, in turn, yields ("Leases") to its subscribers. Some subscribers have static IP addresses that never change while others receive different IP address each time they connect to the Internet (ie addresses dynamic IP "). ISPs retain log files that show which has been assigned a specific IP address on a date and a specific time. The IP address of the sender is usually in the header information that is sent with each email message. Therefore, the use of relatively simple network tools, it is possible to get the name and address of the ISP assigned IP address.

c) Residual Data

Most users assume that deleting files from a computer actually deletes files, but in fact the operating system of a computer keeps a directory name and location of each file. When a user deletes a file, the operating system does not delete the file data. Instead the operating system only indicates that space is available. The contents of a deleted file remains in place until specialized programs replace them. A person who knows how to access these areas but erased released degreased, and has the proper tools, can recover their content. residual data may also include portions of files spread across the drive surface or embedded in other files. These files are commonly known file fragments and unallocated data.

I) SLACK SPACE

Data can also be found in what is known as the soft area of a hard drive. Slack space is an area at the end of the space allocated to an unoccupied by data belonging to that file. For example a file 4Kilobytes (KB) in length can be allocated 32KB of disk space. The 28KB of space between the end of the file and the allocated space is the soft spot.

II) BACKUP DATA

Many commercial data and communications are kept on backup tapes regularly. Users can also create their own backups - for example, Microsoft Word © allows users to automatically save a backup copy of a document if the backup function is activated. The backup data typically consists of information copied on portable media (usually tapes, diskettes or CD) to provide users access to their data in case of system failure. The frequency of backups and the backup data in general are set by corporate policy if networked systems are normally stored on a routine schedule. Typically network backups only capture data stored in centralized storage systems, but not the data stored on the hard drives of individual users.

d) Sources of Data

An obvious source of data is the computer of a user; even potential sources of digital data in a computer is not always obvious. Although digital data obviously exist on the hard drive of a computer, digital data can also be located on media devices attached or inserted in a computer such as a CD ROM, floppy disks, backup tapes and memory cards and in the cache memories of the computer. Data can also be located on shared disks, also known as network drives or file servers. These shared disks act as centralized data repository for user data that can be considered as an electronic file room with indexed files to facilitate the access of individuals and groups. In many enterprise environments, users save their work data, including word processing documents, email messages, accounting and spreadsheet files on shared drives. Data can also be found in other places:

- Smart cards may contain valuable information that may be of use to a computer criminal.
- PDAs may be used to store password or other useful data.
- Mobile phone handsets reveal the callers' identities
- Whenever a person enters a building the building security system creates an electronic record

Even printouts from a computer, phone lists, access logs or procedural documentation may prove valuable in an investigation.

VII. LEGAL ASPECTS OF COMPUTER FORENSICS

Anyone overseeing network security must be aware of the legal implications of forensic activity. the security professionals should consider their policy decisions and technical actions under existing laws. For example, you must have a permit before to monitor and collect information on a computer intrusion. There are also legal ramifications with security monitoring tools. The judiciary is a relatively new discipline computing courts and many existing laws used to prosecute computer-related crimes, legal precedents and practices related to computer forensics are in a state of flux. The new court rulings are issued that affect how computer forensics is applied. The best source of information in this area is the United States Department of Justice website Cyber Crime. 4 The site lists recent court cases involving computer forensics and computer crime, and there are guides on how to present evidence from the computer to the court and what standards apply. The important point for forensics investigators is that the evidence must be gathered in a manner that is legally admissible in a court case. Increasingly, laws are passed that require organizations to preserve the confidentiality of personal data. It becomes necessary to prove that your organization complies with IT security best practices. If there is an incident affecting critical data, for example, the organization added a forensics capability to its arsenal will be able to demonstrate that he followed a solid security policy and potentially avoid or lawsuits regulatory audits. There are three areas of law related to IT security that are important to know. The first is in the United States Constitution. The Fourth Amendment 5 provides protection against unreasonable search and seizure, and the Fifth Amendment provides protection against self-incrimination. Although the changes were written before there were problems caused by people abusing computers, the principles apply to how computer forensics is practiced.

Second, anyone concerned with computer forensics must know how three U.S. Statutory

laws affect them:

- Wiretap Act (18 U.S.C. 2510-22)
- Pen Registers and Trap and Trace Devices Statute (18 U.S.C. 3121-27)
- Stored Wired and Electronic Communication Act (18 U.S.C. 2701-120)

Violations of any of these laws in practice of computer forensics could be a federal crime punishable by a fine and / or imprisonment. It is always advisable to consult your legal counsel if you are in doubt about the implications of any

forensics action on behalf of your organization. Third, the federal rules of the United States of proof by hearsay about, authentication, reliability, and the best evidence must be understood. In the US, there are two main areas of legal governance affecting the actions of cyber security related to the collection of network data:

(1) authority to monitor and collect the data and

(2) the admissibility of the collection methods.

Of the three areas above, the Constitution of the United States and US Statutory laws govern primarily the collection process, while federal rules of evidence are especially on admissibility. If system administrators have the technical skills and the ability to retain critical information related to a suspected security incident in a forensic manner and her are aware of the legal issues related to forensic medicine, they will be a great asset to their organization . If an intrusion lead to a court case, the organization with the ability forensics will be a clear advantage.

VIII. CURRENT RESEARCH

Cyber Forensics is a sizzling topic of current trends. Many researchers have started to do intensive research in this current zone. New directions in this area includes analysis of the author, collecting digital evidence and forensics investigation process, the proactive forensics, Intrusion detection systems using honeypot, build graphical evidence, identify the use of mobile phones in cyber crimes and hash117 Paper Survey Cyber Forensics function to preserve the integrity of the evidence.

Ashley et.al., [2006] given the full picture of Cyber Forensics in the form of Cyber Forensics ontology which can be useful for the study of cyber forensics. Forensics pro actively contribute to the creation of prevention intelligence and threat monitoring and more after incident investigations. Turnbull and Slay [2007] listed the advantages and disadvantages to intercept wireless traffic as a way to find potential sources of evidence during the seizure of the evidence. In the same work as the advantages and disadvantages of infringing communications from or 802.11 wireless base networks during the judicial seizure were discussed. High speed binary search model for large-scale digital forensic investigations using pattern matching edge chain looking at characters and complex regular expressions discussed in

[Hyungkeun et al, 2007].Willassen [2008] in his thesis proposed various methods on how the probative value of digital Timestamps can be improved by taking a hypothesis Digital investigation approach timestamp. Analysis of IM in terms of computer forensics and intrusion detection is hitherto unexplored. Attribution classification used for forensic analysis or masquerade detection

[A. Orebaugh and Allnutt J., 2009]. Baggili [2010] proposed the creation of a mobile application that runs on a mobile device and the goal is to help the crime scene personal collection of digital devices in the course of an investigation.

IX. CONCLUSION

Computer forensics is an emerging field in the 21 st century. A survey of the field of cyber forensics is given in this paper. When analyzing Computer 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 Computer forensics and forensics methodology. The various phases of Computer forensics have been discussed and each phase explored with their respective tools. Finally we had shown the current research trends in this new era of cyber forensics. It still evolves and will remain a ho topic as long as there are ways to threaten data security.

REFERENCES

[1] Mary Kay Brown and Paul D. Weiner, " Digital Dangers: A Primer On Electronic Evidence In The Wake Of Enron ", Pennsyl vania Bar Association Quarterly January, 2003

[2] Steven M. Abrams and Philip C. Weis, "Knowledge Of Computer Forensics Is Becoming Essential For Attorneys In The Information Age", New York State Bar Journal February, 2003.

[3] Jenkinson, B. L. (2005) The structure and operation of the master file table within a Windows 2000 NTFS environment, MSc Thesis, Cranfield University.

[4] Halboob, Waleed, Muhammad Abulaish, and Khaled S. Alghathbar. "Quaternary privacy-levels preservation in computer forensics investigation process." *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*. IEEE, 2011.

[5] Turnbull, B., & Slay, J. (2007, January). Wireless forensic analysis tools for use in the electronic evidence collection process. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (pp. 267a-267a). IEEE

[6] Brannon, Stephen K., and Thomas Song. "Computer forensics: digital forensic analysis methodology." *Computer Forensics Journal* 56.1 (2008): 1-8.

[7] Oatley, Giles, and Brian Ewart. "Data mining and crime analysis." *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 1.2 (2011): 147-153.

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

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

[10] Baggili, Ibrahim M., Richard Mislan, and Marcus Rogers. "Mobile phone forensics tool testing: A database driven approach." *International Journal of Digital Evidence* 6.2 (2007): 168-178.

[11] Baggili, Ibrahim. "Generating System Requirements for a Mobile Digital Evidence Collection System: A Preliminary Step Towards Enhancing the Forensic Collection of Digital Devices." (2010).

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

[13] Grance, Tim, Karen Kent, and Brian Kim. "Computer security incident handling guide." *NIST Special Publication* 800 (2004): 61.

[14] Marcella Jr, Albert, and Robert S. Greenfield, eds. *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*. CRC Press, 2002.

[15] Meyers, Matthew, and Marc Rogers. "Computer forensics: the need for standardization and certification." *International Journal of Digital Evidence* 3.2 (2004): 1-11.

[16] 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.

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

[18] *Ahmed, Arif. "Have You Been Hacked? A Primer to Cyber Security and Cyber Forensics." CHARTERED ACCOUNTANT-NEW DELHI- 54.6 (2005): 852.*