A Study of Digital Forensic Tools and its Process for Cyber Crime Investigation

[1]Vikas, Research Scholar, Faculty of Computer Science & Engineering, Jagannath University, NCR, Haryana.
2Harnamo Ram, Lecturer Computer Application, Guru Nanak Dev Institute of Technology, Rohini, Delhi
[3]Dr. Gaurav Aggarwal, Supervisor & Professor, Faculty of Computer Science & Engineering, Jagannath University, NCR, Haryana.

Abstract:

Computer forensics is the process of using the latest knowledge of science and technology with computer sciences to collect, analyze and present proofs to the criminal or civil courts. Network administrator and security staff administer and manage networks and information systems should have complete knowledge of computer forensics. The meaning of the word "forensics" is "to bring to the court". Forensics is the process which deals in finding evidence and recovering the data. The evidence includes many forms such as finger prints, DNA test or complete files on computer hard drives etc. The consistency and standardization of computer forensics across courts is not recognized strongly because it is new discipline.

It is necessary for network &System administrator and security staff of networked organizations to practice computer forensics and should have knowledge of laws because rate of cyber crimes is increasing greatly. It is very interesting for mangers and personnel who want to know how computer forensics can become a strategic element of their organization security. Personnel, security staff and network administrator should know all the issues related to computer forensics. Computer experts use advanced tools and techniques to recover deleted, damaged or corrupt data and evidence against attacks and intrusions. These evidences are collected to follow cases in criminal and civil courts against those culprits who committed computer crimes.

The survivability and integrity of network infrastructure of any organization depends on the application of computer forensics. In the current situations computer forensics should be taken as the basic element of computer and network security. It would be a great advantage for your company if you know all the technical and legal aspects of computer forensics. If your network is attacked and intruder is caught then good knowledge about computer forensics will help to provide evidence and prosecute the case in the court.

Keywords: Computer forensics, Digital forensics, Cyber security & Cyber-crime.

INTRODUCTION:

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. Computer forensics is also known as cyber forensics. It involves applying computer investigation and analysis techniques to solve a crime and provide evidence to support a case. It is the process of identifying, preserving, analysing and presenting the digital evidence in such a manner that the evidences are legally acceptable. By using cyber forensic tools it is very easy to probe the evidence. It involves various applications like analysing the quality of food and predicting the fire disasters etc.

Most of the first criminal cases that involved computers were for financial frauds which are now overcome by Biometric Smart Card. Energizing Cyber security with biometrics & Digital Forensics. Biological evidence also plays major role in crime investigation. It contains Deoxyribo Nucleic Acid (DNA), which connects an offender to a crime scene. It examines evidence from crime scenes to determine if biological material is present.Digital forensics engagement commonly is performed during a fraud investigation because the results can provide a direction as to what the suspects involved in the fraudulent act are likely to know, when they were likely to know it, the documents to which they had access, actions taken on these documents eg: copied on the pen drives or deleted from the email box], with whom they communicated, and whether they appeared to try to hide their actions. The Internet history, web-based email, lost or deleted files, logging and registry files are examples of data the forensic accountant can utilize as evidence in their engagements by using the digital forensic techniques.

Digital Forensics_Process:

TYPES OF DIGITAL FORENSICS

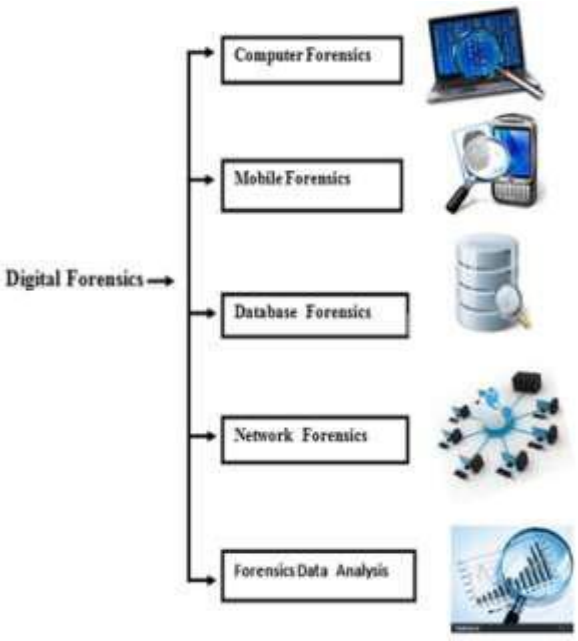

Fig.1 Types in Digital Forensics

A. Computer Forensics

Computer Forensics reveals the present stateof automatic data processing system and it obtains evidence from various media like computers, embedded systems, USB pen drives etc., It examines system logs and web history. Some of the artefacts can get from such investigations includes hidden, deleted, temporary and password-protected files, Sensitive documents and spreadsheets, File transfer logs, Text communication logs, Internet browsing history, Pictures, graphics, videos and music, Checking Event logs etc.

B. Mobile Device Forensics

It recovers digital evidence from a mobile device and investigates call logs and text messages (SMS/Email).It provides location information via GPS or cell website logs. It also investigates communication stores like BBM, WhatsApp, WebChat, etc. Phone number and service provider information can be viewed. History of Incoming and outgoing call logs,SMS, Emails, IRC chat logs, Contact details from address books and calendars are revealed. Security issues are more concerned here.

C. Network forensics:

Network Forensics monitors and analyses LAN/WAN/internet traffic (even at the packet level).It

Retrieves and analyses logs from a wide variety of sources. It determines the extent of intrusion and therefore the quantity of data retrieved.

D. Database forensics:

It is forensic study of databases and their data. Investigation is done on database contents, log files and in-RAM data. Many software tools are used to manipulate and analyse the data. This tools provides audit logging capabilities.

E. Forensic data analysis:

It deals with Investigation for financial frauds andcorrelating with financial documents. Working closely with Certified Fraud Examiners is carried.

Computer forensics work procedure or work process can be divided into 5 major parts:

Identification

The first process of computer forensics is to identify the scenario or to understand the case. At thisstage, the investigator has to identify the purpose of investigation, type of incident, partiesthatinvolved in the incidence, and the resources that are required to fulfill the needs of the case.

Collection

The collection (chain of custody) is one of the important steps because your entire case is based onthe evidence collected from the crime scene. Collection is the data acquisition process from therelevant data sources while maintaining the integrity of data. Timely execution of the collectionprocess is crucial in order to maintain the confidentiality and integrity of the data. Importantevidence may lost if not acted as required.

Examination

The aim of third process is to examine the collected data by following standard procedures,techniques, tools and methodology to extract the meaningful information related to the case.

Analysis

Since all five processes are linked together, the analysis is the procedure to analyze the dataacquired after examination process. At this stage, the investigator search for the possible evidenceagainst the suspect, if any. Use the tools and techniques to analyze the data. Techniques and toolsshould be justified legally, because it helps you to create and present your report in front of thecourt.

Reporting

It is the final, but the most important step. At this step, an investigator needs to document theprocess used to collect, examine and analyze the data. The investigation report also consists thedocumentation of how the tools and procedures were being selected. The objective of this step is toreport and present the findings justified by evidences. Every step mentioned above can be further divided into many parts and every part has its own standard operating procedures, we look into them in detail in the coming chapters.

LITERATURE REVIEW

Digital forensics is nearly 40 years old, beginning in the late 1970s as a response to arequirement for the service from the law enforcement community. The rise of computer crimes started in the 1980's meant that investigators began to look at computers as sources of proof. The Law enforcement began initial training efforts in digital forensics. In the year 1984 Computer Analysis and Response Team provided assistance to FBI field offices in the search and seizure of computer evidence as well as forensic

examinations and technical support for Federal Bureau of Investigation investigations. Establishment of Federal Law Enforcement Training Centre during this period.

In the year 1990's the usage of internet has started and increase in consumerization of technology has done. This means that technology is involved in crimes, and the rapid growth in Internet facilitated cyber attacks. International Law Enforcement Academy is established in 1995 to reduce crime,combat terrorism, and share in knowledge and training.

In the year 1997 Scientific Working Group on Digital Evidence (SWGDE) was established to develop standards in Forensics .The development standards by various law enforcement bodies has done during this period. There is little growth in private sector training and development. SANS Institute also came into.

Cyber crime exploded in the 2000's and the integration of technologies such as mobile devices expanded as primary sources of technological evidence exponentially and as well as the use of technology in criminality. Digital Forensic Research Workshop (DFRWS) development of research was developed in the year 2001.It is used to bring together researchers, industry, tool, academics, enforcement, and military to tackle the challenges in digital forensics science. Digital forensics evolved from investigative techniques to a full forensic science. There is significant development in the private sector with regards to training courses and programs in digital forensics. Development of formal academic programs at universities had come into around the world during this period.

There are several useful discussions found through-out the literature that examine and compare the many proposed models and frameworks of cyber-crime investigation, predominately focusing on digital evidence recovery (Beebe and Clark, 2005; Carrier and Spafford, 2003; O Ciardhuain, 2004; Perumal, 2009; Pollitt, 2007; Selamat et al. 2008).

- Ieong (2006) argues that many of the digital forensic inves-tigation processes have been developed by either traditional forensic scientists focusing on robust evidence handling or by technologists focusing on digital evidence capture, making it difficult for law enforcement practitioners to understand and apply.

- The models found throughout the literature provide a useful overview of the general technical investigation activities and are often based on rigorous scientific forensic procedures. However, investigating cyber-related crime requires a much broader understanding of the wider context specific to a criminal investigation before it can be established just how and what technology is relevant. Many of the models are abstract in the context of law enforcement investigation and are largely restricted to the examination of a definitive technical crime scene and the forensic recovery of digital evidence from established sources.

- In Bolagh and Pondelik have proposed a technique to recover the decoding keys from the dump of the live image of a volatile memory. Proposed approach works on windows and Linux with True Crypt is a free open source tool that performs on-the-fly disk encryption. The authors also suggested a method to decrease the size of dump image, especially in case when True Crypt is used for encryption, the size can be bounded to 1-2 MB only. However, the suggested technique bears a limitation that the image should be present nearby for forensic analysis. In addition, decoding keys are located through content search, and if certain data deterioration appear in a disk then it becomes impossible to extract keys. Advances in data encryption mechanics have made the job of cyber investigators really tough.

- In Maximilian Bielecki and Gerald Quirchmayr have described the strengths of an automated presentation and argumentation support system with a analysis of cyber criminals similar to the ones used in law enforcement work and also the description of a prototype based on an automatic forensic support system called Computer Forensic Analyzer and Advisor. Computer Forensic Analyzer and Advisor demonstrate an approach of a fully automated system that supports investigators by independently identifying malicious software and programs.

- In Yangbin Zhou and Keyu Jiang, have presented wiping electronic evidence. The system is start with collecting the related work and analyzes the organization‟s security policies and strategy, finding out the security level of the computer systems, the work situation for staffs the personnel secures awareness level, and etc. With the security level of this organization, ethical programmer can test the reaction of the organization to a hacking attack. According to the system, Developer and organization's managers should clearly know their organization's insufficiency in computer forensics filed.

RESEARCH OBJECTIVES:

1) To identify to nature of cybercrime.
2) To find out the forensic tool used for detection of the intensity of the cybercrime.
3) To find out the optimal tool for a cybercrime investigation.
   a) Comparative analysis of a crime by existing tools
   b) To review the analysis of cybercrime reports generated by deferent tools
   c) To present analysis reports in a manner that leads to legal evidence of the cybercrime.

RESEARCH METHOLOGY & TOOLS USED FOR ANALYSIS:

Computer forensics is the branch of forensic science in which evidence is found in a computer or digital device. The aim of computer forensics is to examine digital devices in a constructive way with the goal of identifying, preserving, recovering, analyzing, and presenting the evidence in a court of law.
Computer forensics uses a number of methods for investigation as per the guidelines of the law. Some of its methods are

- Cross Drive Analysis
- Live Analysis
- Deleted Files
- Stochastic Forensics
- Steganography

Computer forensics also uses some tools to perform investigations. Some of them are

- Digital Forensics
- Open Computer Forensics Architecture
- Caine
- X-Ways Forensics

- EnCase
- Registry Recon
- Volatility and many more…

These tools can be further classified into:

- Disk and Data Capture Tools
- Database Forensics Tools
- File Viewers
- Network Forensics Tools
- File Analysis Tools
- MacOS Analysis Tools
- Internet Analysis Tools
- Mobile Devices Analysis Tools
- Email Analysis Tools
- Registry Analysis Tools

Processes in Computer ForensicsEvaluation

In this process of evaluation, computer forensics experts are given instructions, clarification of those instructions if not clear, guidelines for performing activities, and allocation of roles and resources. Such a process includes proper instructions on how to prepare systems for collecting evidence and where to store evidence. Instruction on documentation is also given to help ensure the authenticity of the data.

The process of computer forensics needs proper steps to determine the details of a case. It includes the proper reading of case briefs, understanding every fact, and obtaining permissions to continue the case.

Collection

This process involves the labeling and bagging of evidence from the crime scene. Secure and safe transportation of material is also important. Data is transferred to the expert's system.

In this process, cyber forensics experts visit the crime scene and collect evidence that is helpful for the investigation of the crime. Documents are needed during and after this process and include detailed information on the evidence. In this process, copies of evidence are made so that no information is lost during the investigation process.

Analysis

Computer forensics experts use a variety of methods and approaches to examine the evidence. This can be done by using the various types of available forensic software. In this process, deleted data, sensitive data, recently used data, and all other important files, as well as programs, are examined. Analysis of evidence must be accurate and must be done within the allotted time; its details should be recorded properly. Experts analyze the evidence twice to verify the correctness of the results.

Presentation

This process involves the proper documentation of evidence and the examination process of evidence. It includes all the methods used

in the process, the techniques used, and coping. The securing and transferring of evidence is also included.

These tasks help experts present the details of an investigation whenever asked when, how, and where the crime happened. It helps experts determine the validity of the evidence. It also helps experts in solving crimes and supporting claims with evidence in a court of law.

CONCLUSIONS:

The field of digital forensics has become popular over the last few years as both the computer and the cellular market has expanded. With the increasing use of digital data and mobile phones, cyber forensics has become more prominent, even Cyber thefts are also increasing as day advances. This research will help to show few existing & popular digital forensics tools used by various law enforcement agencies in performing crime investigations. This field will enable crucial electronic evidence to be found, whether it was lost, deleted, damaged, or hidden, and used to prosecute individuals that believe they have successfully beaten the system.

REFERENCES:

1. Stefan Bolagh, MatejPondelik. “Capturing Encryption Keys for Digital Analysis”, In Proceedings 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems(IDAACS), pp. 759--763, Prague, 15-17 September 2011.

2. Dija S, Balan C, Anoop V and Ramani B. “Towards Successful Forensic Recovery of BitLockedVolumes”.In Proceedings 6th International Conference on System of Systems Engineering (SoSE), pp. 317--322, Albuquerque, NM, 27-30 June 2011.

3. Maximilian Bielecki and Gerald Quirchmayr,“A prototype for support of computer forensic analysis combined with the expected knowledge level of an attacker to more efficiently achieve investigation results”, International Conference on Availability, Reliability and Security, pp. no:696-701,2010.

4. Louis J. Bottino, “Security Measures In aSecure Computer Communication Architecture”, 25th Digital Avionics Systems Conference, 15 October, 2006.

5. CHEN Wei and LIU Chun-mei, “The Analysis and Design of Linux File System Based on Computer Forensic”, International Conference on Computer Design and Applications, vol. 2, 2010.

6. William J. Hatt, Edward A. VanBaak and Holly B. Jimison, “The Exploration & Forensic Analysis of Computer Usage Data in the Elderly”, 31st Annual International Conference of the IEEE EMBS Minneapolis, Minnesota, USA,2-9 September 2009.

7. Kyung-Soo Lim, Seung Bong Lee and Sangjin Lee, “Applying a Stepwise Forensic Approach to Incident Response and Computer Usage Analysis”, 2009.

8. Andrew Marrington, George Mohay, HasmukhMorarji and Andrew Clark, “A Model for Computer Profiling,”International Conference on Availability, Reliability and Security, page no: 635-640,2010.

9. Luís Filipe da Cruz Nassif and Eduardo Raul Hruschka, "Document Clustering for Forensic Computing: An Approach for Improving Computer Inspection", 10th International Conference on Machine Learning and Applications,pp. no:265-268,2011.

10. NatasaSuteva, Aleksandra Mileva and Mario Loleski, "Computer Forensic Analisys of Some Web Attacks", World Congress on Internet Security, pp. no:42-47,2014.

11. Govind Singh Tanwar and Dr. Ajeet Singh Poonia, "Live Forensics Analysis: Violations of Business Security Policy", International Conference on Contemporary Computing and Informatics pp. no: 971-976, 2014.

12. Yongge Wang and YuliangZheng, "Fast and Secure Magnetic WORM Storage Systems", Proceedings of the Second IEEE International Security in Storage Workshop, 2003.

13. Lijun Zhang, Yu Zhou, Jia Fan, "The Forensic Analysis of Encrypted Truecrypt Volumes", pp. 405-409, 2014.

14. Yangbin Zhou and Keyu Jiang, "An Analysis System for Computer Forensic Education, Training, and Awareness", International Conference on Computing, Measurement, Control and Sensor Network, page no: 48-51, 2012.

15. Chung-Huang Yang, Pei-Hua Yen, "Fast Deployment of Computer Forensics with USBs". In Proceedings of International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), pp. 413--416, Fukuoka, 4-6 November 2010.