International Journal of Current Trends in Engineering & Research (IJCTER)
e-ISSN 2455–1392 Volume 2 Issue 1, January 2016 pp. 1-5
Scientific Journal Impact Factor : 3.468
http://www.ijcter.com

Review on Computer Forensic

Dipak V Bhosale[1], Prajakta K Mitkal[2], Rupali N Pawar[3], Rajesh S Paranjape[4]
[1, 2, 3] *Computer Science and Engineering, Karmayogi Engineering College, Shelve-Pandharpur*

Abstract— Forensic the word which indicate the detective work, which searches for and attempting to discover information. Mainly search is carried out for collecting evidence for investigation which is useful in criminal, civil or corporate investigations. Investigation is applicable in presence of some legal rules.

As criminals are getting smarter to perform crime that is, using data hiding techniques such as encryption and steganography, so forensic department has become alert has introduced a new concept called as Digital Forensic, which handles sensitive data which is responsible and confidential.

Keywords— *Computer Forensic, Text mining, SaaS, PaaS, IaaS, Cyber crime*

I. INTRODUCTION

Computer Forensic is a science of obtaining, preserving and documenting evidence from digital storage devices such as computers, PDAs, digital cameras, mobile phones and various memory storage devices. Computer forensic is carried out in 4 main steps: Collection, Examination, Analysis and Reporting

a) Collection: The goal of first step is to identify, isolate, label, record and collect the data and physical evidence related to the incident being investigated, while establishing and maintaining integrity of the evidence.

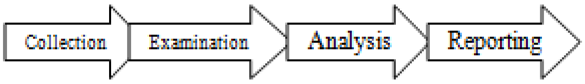

Figure 1. Computer Forensic process

b) Examination: Here identification and extracting the relevant information from collected data, using appropriate forensic tools and techniques.

c) Analysis: Analyze the results of the examination to generate useful answers to the questions presented in the previous phases.

d) Reporting: It includes finding relevant to the case, actions that were performed, Actions left to be performed and recommended improvements to procedures and tools.

Computer forensic is an art of discovering and retrieving information about a crime in such a way to make it admissible in court [1].

Computer forensic is also referred as forensic computing, in which electronic evidence are gathered [2].

II. LITERATURE REVIEW

2.1 Policies to enhance computer and Network Forensic

Policies are introduced so that on the basis of evidence found during forensic investigation, it may easy to identity the type of crime committed. In this paper the policies introduced are-

1) Retaining information, this consists of copy and retains application and local user files and Copy and retain computer and Network activity logs.

2) Planning the response, this consists of Establishing of a forensic team, Establishing an Intrusion response procedure and Formalizing of investigative procedure.

3) Training, this includes, Training of response team. Training of investigative team and Training for all Personnel that use computers.

4) Accelerating the investigation, this includes Prohibit personal file encryption, Prohibit disk scrubbing tools and file shredding software, Utilize data indexes and Utilize information fusion.

5) Preventing Anonymous activities, which consist of Onion routing, require date, time and user stamps in file, Use strong user authentication and use of strong access control mechanisms.

6) Protect the evidence, under this section the various activities carried out are Exercise rigid control over administrative access for systems housing potential evidence, Encrypting evidence files and connections and applying strong integrity checking technology. Using these six policies there can be decrement in computer crimes [1].

2.2 Forensics Computing- Technology to Combat Cyber crime

The process of gathering electronic evidence of a cybercrime is referred as forensic computing. This paper tells us to understand the various issues related to computer forensic evidence in point of view of court of law that to be presented. According to author the cybercrimes are unique in structure that can be represented mainly in three different ways that are,

1. They are skill intensive and technological
2. Have high degree of globalization
3. It is a procedural and jurisdictional issue.

As structure is represented, the author has also discussed the common purpose or what actually cybercrimes include as theft of telecommunication services, communication in furtherance of criminal conspiracies, Information piracy, counterfeiting, forgery, dissemination of offensive material, electronic money laundering and tax evasion, electronic vandalism, terrorism, sales and investment fraud, illegal interception of telecommunication and electronic funds transfer fraud.

To find out the cybercriminal the three different techniques are carried out that are Digital evidence recovery, cyber or intrusion forensics and forensic data analysis.An investigator plays an important role in investigation procedure, the steps should be followed as, Secure and isolation, recording the scene, conducting a systematic search for evidence, collecting and packaging of evidence and maintaining the chain of custody.

According to author there is no pure technological solution for this security related problem but combination of technological and non-technical aspects can be helpful to combat cybercrimes [2].

2.3 Latent Text Mining for Cybercrime Forensics

The main contribution in this paper is design, development and evaluation of a Latent Dirichlet Allocation (LDA), which is based on latent text mining model for cyber-attack forensics. To test model the data that is used from twitter and blog sites. The proposed approach consist of five layers that are Data collection layer, Data cleaning layer, Data mining layer, Learning and classification layer and Presentation layer.

1.For Data collection layer, generally autonomous information agents simulate human users and tap into private multilingual online social media to observe and collect cyber-attack related messages.

2.For Data cleaning layer, a text preprocessor is applied to pre-processing multilingual textual data such as word segmentation, stop word removal, stemming and part-of-speech tagging.

3.For Data mining layer, a linguistic feature extractor makes use of a set of pre-defined feature patterns and name entity recognition rules to extract explicit features from pre-processed messages.

4.For Learning and Classification layer, a machine learning classifier is deployed to produce cyber-attack predications based on an optimal set of latent and explicit features.

5.For Presentation layer, the manager employs a combination of texts, tables and graphs to present the cyber-attack predication results and visualize the casual relationship of cyber-attacks.

LDA mainly helps to increase the effectiveness, relevance in result rate in cyber-attack domain as compare to Intrusion Detection system, intrusion prevention system and anti-malware systems [3].

2.4 Calm before the storm: The Challenges of cloud computing in Digital Forensics

A cloud is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specific level of quality. The main three services are applicable for users that are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service(IaaS). Cloud can also be categorized according to level of deployment as private cloud, community cloud, public cloud and hybrid cloud. Digital forensic can be applicable in cloud also. According to author four principles were proposed by Association of Chief Police Officers in 2007 that are-

1.No action taken by law enforcement agencies or their agents should change data.
2.If any person needs to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3.An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved.
4.Person in-charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Enhanced Digital Investigation Process model consist of five major phases that are, Readiness phases, Deployment phases, Traceback phases, Dynamite phases and Review phases. In cloud environment the digital forensic carried out in steps that includes-

1.Identification, identifying an illicit event.
2.Preservation and collection, it provides sufficient storage capacity, chain of custody, media imaging, time synchronization, legal authority, approved methods, software and hardware and data integrity.
3.Examination and analysis, in which the recovery of deleted data, traceability, validation using hashing tools and event reconstruction takes place.
4.Presentation includes documentation of evidence and testimony.

Digital forensic community is an need in cloud environment as it is standard mechanism to evaluate frameworks, procedures and software tools [4].

2.5 Computer Forensic Analysis in a Virtual Environment

Computer Forensic analysis can be applied on virtual environment or virtual machine. Virtual machine is a software product which allows the user to create one or more separate environments, each simulating its own set of hardware and its own software. Main purpose of computer forensic is carried out for four phases that are Access, Acquire, Analyze, and Report. Virtual machine simulates some basic components since it not created to provide full support for a wide range of hardware devices. While applying computer forensic in virtual machine some basic rules that to be followed are: Minimal handling of the original, account for any change, comply with the rules of evidence and do not exceed your knowledge [5].

2.6 Forensic Methods for Detecting Insider Turning behaviors

Forensic approach is used for detection of evidences and study on that evidence for finding the criminal. Inadvertent acts by insiders may lead to serious consequences, so this paper focus on the different points to avoid the consequences. For avoiding this first focus should be on the background of the insider threats such as, insider must be an authorized. Insiders acting commensurate with the trust placed in them by the organization granting access are called as loyal. If any insider changes loyalties while retaining authority then that changed loyalty is called as “turning”. Rapid detection and response may be effective for detecting unauthorized and unusual act. Insiders turning usually undertake authorized acts and in many cases those acts are commonplace for the identified individual. The activity carried out for insider turning is subversion. According to hypothesis, by detecting subversion activities, investigators may gain the opportunity to develop suspicions of, observe precursors to and limit effects of, insiders who try to defeat attribution of their acts.

Next thing that to be focused is Background on relevant forensics approaches, it includes analysis, algorithmic approaches, and implementation of general theories. Forensic approach includes identification of redundant traces indicative of subversion and low base rates, Particularization, Individualization, and Addition of select redundant sensors and traces to enhance detection [6].

2.7 Digital Crime Investigation using various logs and fuzzy rules: A review

Digital forensic is field of investigation of computer crimes. The basic process carried is collection of evidence, examining that evidences, analyzing those evidences and finally reporting. Another thing that is considered is log files which have the entry related to incoming user and outgoing user. Log files are in text format so they can be read using notepad or any text editor. Log files consist of information such as date, URL, hostname, time, bytes, status and referrer. These information acts as major success for Digital forensic. Log files are again categorized into different types for easy analysis. Types are Network Device logs; it is used to perform communication in the network. Firewall logs, used to monitor the network's incoming and outgoing traffic. Web Server logs, used to maintain access logs and reports number of visitors, views, hits, most frequent visited pages. Next approach used in Digital forensic is Fuzzy rules. It works on basic mathematical concept of Set theory. The basic fuzzy operations used are Union, Intersection, and Complement. Using different basic approaches fuzzy rules and operations analyses the malicious activity and the attacker[7].

2.8 Techniques in Computer Forensics: A Recovery Perspective

Computer Forensic is also referred as media analysis, but after various arguments it is said that forensic computing is the more accurate term, especially because digital evidence is increasingly captured from objects, but not from computers. This paper includes various cases such as, knife found at crime scene is not the evidence of computer forensic but the blood stain of both the knife and the victims apparel by conducting appropriate chemical tests is the computer forensic evidence. Again in data manipulation various processes that transform the information in some way cannot be considered as computer forensic but operation including encryption or data compression or other type of encoding is the part of computer forensic. The major attempt done by victim is destroying the evidence that includes files. There are various types of attempts in destroying files such as destroying files through erasing, destroying files through overwriting, damaging hard drives, hiding the blocks, etc. Computer forensic team works on recovering the destroyed data. This work is done with the help of various tools such as, Drivespy, Encase, Forensic tool kit, I Look, Norton utilities, The Coroner's tool kit, XWays, TASK, etc. These tools as very helpful, though they are in process of automation and updating [8].

Computer Forensic is also referred as Digital Forensic that includes use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital source for the purpose of reconstruction of different events occurred at crime scene and for helping the anticipate unauthorized actions that disrupt the planned operations [9].The common issue found in crime investigation is destroying the data after performing the crime. So the first issue that to be occurred is recovering the lost or destroyed data, using forensic tools. Next issue is tracking the hacked data, so that the observation of activities can be done [10].Digital forensics plays an important role to reduce the rampant and unchecked usage of computer crimes through internet. Digital forensic analysis is divided into two categories that are dead or static forensic analysis and second is live analysis. The first category dead or static analysis includes analysis, where all target devices that are required in the analysis are shutdown. The second category, live forensic analysis includes finding the digital proof or evidence. The standard process carried out includes different phases such as, Acquisition, Analysis and reporting [11].

III. CONCLUSION

Computer Forensic is the source to find the evidence from the crime scene through the digital evidences. According to the survey of various authors the computer forensic is the mode through which the crimes are increasing. Since there are many different ways to hide the crime to the victim. Forensic team also has many different tools available to work on various types of crimes. Computer Forensic team works on basic process that includes identifying, collecting, preserving, analyzing and presenting. This process works very efficiently to detect the criminal. Mostly the best performance is given by the live forensic analysis techniques.

REFERENCES

[1] Alec Yasinsac and Yanet Manzano, “Policies to enhance computer and Network Forensics”, IEEE, 2001.
[2] Amarpreet Arora, Susheel Bhatt & Anamika Pant, “Forensics Computing-Technology to Combat Cybercrime”, IJARCSSE, volume 2 July, 2012.
[3] Raymond Y K Lau and Yunqing Xia, “Latent Text Mining for Cybercrime Forensics”, IJFCC, Vol 2 No. 4, August, 2013.
[4] George Grispos, Tim Storer and William Bradley glisson, “Calm before the storm: The Challenges of Cloud Computing in Digital Forensics”, IJDCF, Vol 4, Issue 2, 2012.
[5] Derek Bem, Ewa Huebner, “Computer Forensic Analysis in a Virtual Environment”, IJDE, Vol 6, Issue 2, 2007.
[6] Fred Cohen, “Forensic Methods for Detecting Insider Turning Behaviors”.
[7] Deepak Scholar, Hitesh Gupta, “Digital Crime Investigation using various Logs and Fuzzy rules: A Review”, IJARCCE, Vol 2, Issue 4, April, 2013.
[8] Bhanu Prakash Battula, B Kezia Rani, R Satya Prasad, T Sudha, “Techniques in Computer Forensics: A Recovery Perspective”, IJS, Vol 3, 2000.
[9] Mohd Taufik Abdullah, Ramlan Mahmod, Abdul Azim Ghani, Mohd Zain Abdullah, Abu Bakar Md Sultan, “Advances in Computer Forensics”, IJCSNS, Vol 8 No. 2, Feb 2008.
[10] Sonia Bui, Michelle Enyeart, Jenghuei Luong, “Issues in Computer Forensics”, May 2003.
[11] Shuaibur Rahman, M N Khan, “Review of Live Forensic Analysis Techniques”, IJHIT, Vol 8, 2015.