Exploratory Study of Cyber Crimes, Digital Forensics and It’s Tools

Giridhar V1, Prof. Clara Kannmani A2, Dr. S. Mohan kumar3
1Final Year CSE Student, 2Senior Assistant Professor, 3Associate Professor and R&D Co-ordinator, Department of Computer Science and Engineering, New Horizon College of Engineering, Bangalore, India

Abstract— The confidential perspective quintessence of data has got its unique importance in enlightening lives of innocents who were the victims of disastrous cyber attacks. upholding digital evidence involving enquiry to punish right criminal for right cause. This paper depicts the cybercrime topology with descriptive digital forensics forum and equipment tools in essence have been briefly analyzed. we convey the path of advancement in records ,their by leading to design of new equipment tools considering the impact of forensic tools used previously and continued usage of current one’s.

Keywords—Inculpatory; exculpatory; Industrial Espionage; evident data, digital forensics.

I. INTRODUCTION

A. Raise of cyber hazards

As theirs been an advancement in technology, though facing odds and hurdles in its carving path of striking height's to achieve fame and glide, has been limited by cyber crime. This intrusion is not the recent issue but has been since 1990's, this typology of cyber crimes made digital forensics to gain heights. Innocent people being the asset of world, unfortunately have become victims of cybercrimes and sniffing ,so digital forensics have become a part of life security. Since 1990,s the impact of cyber crime had horrified common man, One of the most well known crimes of mainframe era (1970's) is one-half cent crime, Banks commonly tracked money in accounts to third decimal place or more. In 2005-Identities theft (id and password) creating customers financially viable for $56.6 billion loss. In 2006-290,000 passports issued by UK government were stolen, their by giving as emergence for biometry.

In 1972, A notorious person, mark Abene opted making way into telephone systems using a normal telephone receiver. mafia boy was involved in most famous cracking attack in Canada’s history. In February 2000, his high profile break into Internet servers and launching of costly denial-of-service attacks on several highly dignified Web sites, including Amazon.com, eBay.com and Yahoo.com. Mitnick Kevin was imprisoned in February 1995 on a 25-count indictment that included charges of wire fraud and illegal acquisition of influential eminent data stolen from companies like Nokia, Motorola and Sun Microsystems.

B. Scenarios involved in cyber crime

- Employee Internet Abuse Via Indulging In Illegal Conduct.
- Data Leak/Data Breach I.E., Unauthorised Disclosure Of Corporate, Confidential And Valuable Information And Data (Giving Up Accidentally And Intentionally)
- Industrial Espionage Against Investigative Corporations (Corporate "Spying" Activities);
- Damage Assessment and Estimation For Catastrophe (Following An Incident-Planning)
- Criminal Fraud and Deceptive Cases
- Criminal Cases (Many Criminals Simply Store Information On Computers, Intentionally Or Unwittingly) and Countless Others.
- Copyright Violation Encouraging Fraudulent Pirate.

C. Digital data Importance and Its Impacts

- As there were so many attacks on data indulged with online transactions, there was a need to provide security which led to booming digital data security. Digital data is the evidence upholding against cybercrime to predict the suspect who has committed the crime. The branch of cyber technology dealing with investigating cybercrime called Digital forensics. It is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and preservation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations.
Roles of digital forensics is to Uncover at necessities then arrive at documentary evidence, proceeds and leads for deriving credentials and to Corroborate evidence discovered in other ways, their by Assisting in showing a pattern of events associating connection attacks on targeted victim computers.

Revealing an end to end path of event analysis, diagnose uncompromised attempts or situations, at last extract data that may be hidden, deleted or otherwise not directly available.

The Rules of Evidence: All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, are called "oral evidence".

All documents that are produced for the inspection of court are called "documentary evidence".

Path of digital evidence: physical context => Media + Logical context=> Data + Legal context => Information => Evidence

Physical context: must be definable in its physical form, i.e., it should reside on a specific piece of media.
Logical context: must be identifiable as to its logical position, i.e., where does it reside relative to the file system.
Legal context: must place the evidence in correct context. Evident with machine language, ASCII format. These form basic evidence against a suspect.
Advent of biometry against cyber theft made forensics to enhance, Biometry: “distinctive capture of uniqueness in Identity required subject”

D. Digital forensic process

The evidence must be Admissible, Authentic, Complete, Correct, Concrete, Reliable, Understandable and Believable. The process of understanding a seizure and handling of forensic examination leads to documentation.

Digital evidence Documentation involves following phases: Identification or preparation have to recognize incident, tools and techniques, search warrants and Authorisation, these mechanisms of investigator leads to get a yield of assurance for continued cybercrime probe. It’s the first phase of forensic process which has diversions to focus on identification, labelling, recording, recapturing and to acquire the data from possible relevant resources.

Search and seizure involves Recognize evidence, Collect evidence i.e., data and tools obtained based on incidence must be evaluated as evident data which is amassed together. collection is typically performed in timely periods to avoid likelihood of dynamic data loss.

Preparation involves Securing evidence, protecting the integrity of the evidence i.e., the evident data’s integrity and security must be ensured and properly encountered. The data from previous phases follow guidelines and procedures that preserve and enhance the integrity of data at this phase.

Examination involves Duplicating evidence. Recover the data i.e., this mechanism involves testing, investigating, evaluating, checking whether evident data is found to be original and being authentic. It also involves execution of active and alive evidence during check up or investigation, using tools recovery of data is being ensured. Processing large amount of data uses combination of automated and manual methods to access and extract data of particular interest.

Analysis involves Determine significance., Reconstruct fragments of data, Draw conclusions i.e., perceiving the essence of evidence, by integrating fragments of importance to yield weighted conclusion. Using legal judicious schemes and techniques compose impetus for further analysis and to implement reprocessing as per convictions to be taken care of.

Report involves Summarizing, Translating, Explaining conclusions i.e., finally, concept conclusion and its summary involved with explanations and translations for wider view of digital data appreciation. May include demonstrating the action at site, explaining the tools, protocols and procedures as per selection and definition, to determine or to predict what other activities need to be indulged with in order to achieve enhanced performance.

Using digital forensic techniques, one can corroborate and clarify evidence otherwise discovered in order to end up at correct conclusion. Generate investigative leads for follow up and verification in other ways i.e., focusing on both relevant and irrelevant gestures to reveal case highlights. It provides help to verify an intrusion hypothesis. It eliminates incorrect assumptions and get authentic info based on experience gained resolving by looking into case both sides.
II. FORENSIC TOOLS

The equipment involved in investigating suspicious entities theirs by finding out the cause and culprit for damage. Information technology, science, biomedical, networks, crime analysts perform investigative study with tools to detect culprit. Some of the top tools used in digital forensics are:

- The coroner's toolkit (TCT) Version 1.16, which is open source software with no GUI features, run on UNIX with command line interface knowledge. Scope of this tool is prominence. It has smart programs of security to recover related forensic data. [7]

- EnCase Forensics version 5.0, was most famous at times when its footstep was put forth in market. as it was GUI based with simple functions and operations with adequate and required documentation. For varied media, recovery was applicable having supported by many web applications. The price being $3000. The package provides scripting facility called Encrypt creating interaction using API with cyber related documents. [6]

- Forensic toolkit (FTK) version 1.61, had complete features of necessity with overwhelming program interface, had good documentation and also with USB pluggable hardware device with a cost of $1100. It scans forensic hard drive detecting deleted emails and recover password dictionary to crack encryption. It has disk imaging software which reconstructs evident image that was segmented and stored to access at necessities, based on MD5 hash value considering integrity check of data. the disk imaging app called FTK imager, these conclusions are drawn from [8]

- i2Analyst's Notes Version 6.0.55, is typically a different type of forensic tool which can import metadata from Encase also data from spreadsheet using CSV file. Used mostly in complicated cases or psychological dreadful crime investigations. Supporting documentation and helper tools of software with simplicity made it to take fame.

- LogLogic's LX 2000. it's marvellous tool for log registry and analysis in real time environment. It is highly expensive with cost of $50000, highly mature and operational with adequate documentation and has excellent interface bearing high learning curve.

- Mandiant first Response version 1.1: Freeware forensics audit tool with strongly built audit features. It's hard to understand features by sustaining with limited support and inadequate or constrained documentation. Activates the network computers to grab a snapshot before evidence commences. Its simplicity and organised view of recovery makes it famous.

- Net witness Version 6.0 is a type of network traffic security analyser which keeps track of adverse traffic rate by maintaining constant up and down congestion in packet relay, being a smart security managing tool. Automates and enhances the intruder detecting system's analysis process, balances load at traffic. it has good interface and costs up to $30000 with low scalability and inadequate documentation. Because of these cons its not entertained for large enterprises

- ProDiscover Incident Response version 4.55 is a absolute professional tool which access computers of interfacing networks. With its bright features its quite easier to use but well organised lay-out and documentation makes it to be used by an expert hand. Supports remote analysis of running processes, open files, open port and services running on open ports. It has full disk imaging capacity, ability to find hidden data, network data gathering, file metadata information, hash keeping are also prominent activities of this forensic tool.

- Sleuth kit and autopsy Browser tool is a freeware with proficient documentation and good support. It is efficient even in html environment having main platform of tool in UNIX OS but also can be used in non UNIX based platform. Support is much better even email based support and many active user forums are at hand. It is efficient with custom friendly tools or equipments.

- Emailing and web usage has spread across all minds from youngest to eldest imparting with individual interest or general interest, triggering hackers to hack against mailing crowd,[5] depicts eMailTrackerPro tool analyse header information of email examining source and multiple destinations their by tracking packet of case study.

- SmartWhoIs tool provides information about multiple IP addresses, hostnames or domains at a time,
The investigative study of any forensic approach, are dealt with equipments called forensic tools. The main confession or declaration strategy is to uphold or showcase optimised, cost effective and efficient tool in forensic tool field. comparative analysis among freeware and non-freeware software tools yielding economically, technologically, scientifically, manageably sound equipment at low cost with accuracy benefits is on focus. The exclusive tools at study Encase, FTK, sleuth kit with their system support formats, search features, indexing mechanisms etc. are described besides mentioning prototypes, results and conclusions are depicted in [3].

Digital forensic is a gliding field of competitive world. In spite of prescribing its impact, importance, upcoming forensic crisis, tactics of handling them etc.. the alternative analysis models are also focused. forensic visibility is denied due to encryption and cloud computing as storage and retrieval of docs somewhere at cloud server being tedious rendering no support for forensic analysis steps. Recent raise of RAM forensic that captures current state of running machine as a way forward technique than disk analysis reducing conservation of data layout from one version to another by making programmers to rely on current running programs. Along with these remarking [4] uphold risks, demands and results of forensic study needed

IV. CONCLUSION

The drastic upraise of technology making world small, social and friendly via social network media has made not only positive outbreaks but also negative. The main picture under focus is, securing individual personal evident documentary data and echoing impact and importance of tools used in cyber studies.

REFERENCES

[1] Anirban Banerjee, Dhiman Barman, Michalis Faloutsos and Laxmi N. Bhuyan “Cyber-Fraud is One Typo Away”


[9] Bernadette H. Schell and Clemens Martin “Contemporary world issues by Cybercrime”