International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 1 198 - 204

A Review on Digital Forensic Investigation Frameworks and Real World Cyber Crime Cases

N. Venkataramanan
Research Scholar,
P.G and Department of Computer Science
Periyar E.V.R. College (Autonomous)
Trichy, Tamilnadu, India
venkatramanan17.cs@gmail.com
venbhu65@yahoo.in

Dr. T. N. Ravi
Assistant Professor of Computer Science
Periyar E.V.R. College (Autonomous)
Trichy, Tamilnadu, India
proftnravi@gmail.com

***Abstract*—**At this modern phase of technology now it has turned out to be potential for public with fairly low practical talents to pinch thousands of pounds in a time in staying their homes. Therefore, all manufacturing firms, the competent commercial method governed through horizontal split-up of production developments, expert services and sales channels etc., (each requiring specialized skills and resources), in addition to that a good deal of business at expenses set by the market forces of quantity and claim. Accordingly, Cybercrime is no different; where it claims a floating worldwide market for skills, tools and finished product. Even it consumes its own money. The augmentation of cybercrime is in distinguishably associated to the ubiquity of credit card dealings and also for the online bank accounts. Cybercrime has developed a business and the demographic of the distinctive cybercriminal is fluctuating promptly, from bedroom-bound weed to the form of structured mobster more conventionally connected with drug-trafficking, coercion and currency decontaminating. The existing research hosts an organized and reliable methodology for digital criminological examination. As a result, the digital forensic science affords the tools, methods and technically upheld approaches that can be castoff to procure and explore the digital evidence. The digital forensic analysis need to be rescued to acquire the signals that will be recognized in the court of law. This study highlights on a organized and unswerving method to digital forensic analysis. In further, this research target sin categorizing the actions that enable and advance the digital forensic investigation practices. The top most cybercrime and prevailing digital forensic framework will be appraised and then the investigation will be assembled.

***Keywords*-** *Digital Forensic, Cyber crime, Investigation, Forensic Framework, data type*

*****

I. INTRODUCTION

In the recent years, Cybercrimes have mounted so significantly along with the circumstances have been superficially substituted by archaic, organized crime. The proliferation of technology maneuvers and supplementary tools; their omnipresent convention throughout the age, gender, socioeconomic and geographical boundaries; and, for many, a fictitious sense of information safety measures have been amalgamated to create an immaculate storm for cybercriminal movements [1].

In this existing situation, a cybercrime is demarcated as an envisioned action comprising the practice of computers or other technologies, and the criminal activity must proceed in a cybernetic situations, like as Internet [2] the segment of Cybercrimes has three elements: Devices and methods to perform a crime, Methodology or procedure for accomplishing the criminal plot — known as a vector. Therefore the Crime itself that is the final outcome of those tactics and happenings (a cybercrime is the ultimate objective of the criminal's activities).

The Virtual settings have grown into productive territory for cybercrime, with the amount of criminalities swelling each year laterally with the sternness of losses. But in 2011, online returns loss ensuing from duplicitous dealings were appraised to be $3.4 billion, up from $2.7 billion in 2010 [3] Economic losses are based only on swindle related with e-commerce and eliminate fraud concerning theft/loss of mobile devices and other types of cybercrimes.

Computer forensics appeared in reaction to the boom of crimes committed through the exploitation of computer systems either as a purpose of crime, a gadget deployed to consign a crime or a depository of proof associated to a crime. Computer forensics can be outlined in early in the year of 1984 when the FBI laboratory and other rule enforcement organizations started on developing several programs to scrutinize the computer verification. The researchers made an attempt in the field of Computer investigation and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have given that to generate the structure with the intention of conferring about the computer forensic science as a discipline together with the need for a consistent approach for further investigations[4].Digital forensics has been illustrated with the use of systematically derived and established techniques in the direction of the conservation, compilation, legalization, recognition, examination, elucidation and management of digital proof resulting from digital resources for the principle of assisting or totaling towards the rebuild of proceedings found to be criminal or assisting to predict the unconstitutional proceedings revealed to be disrupting for premeditated actions. The major component of digital forensics is the reliability of the digital proof. Digital evidence comprises of computer evidence, digital audio, digital video, Mobile phones, digital fax machines etc. The authorized surroundings need evidence

to have reliability, legitimacy, reproductively, non-interference and minimization [5].

In view of the fact, that the computer forensics is a comparatively new field which is used to balance the other forensic disciplines, and it can be sketched back in early 1920s, the enduring efforts to extend the investigation principles and to afford the composition for computer forensic investigations. This research paper endeavors to concentrate on the methodology of a computer forensic examination.

II. DIGITAL FORENSIC INVESTIGATION

In the previous segment, I have discussed the fundamental models of an examination and deployed the word forensic. It is to illustrate the term forensic firstly, we elucidate the definition noticeably and secondly described the application. The American Heritage Dictionary classifies forensic as an adjective and it is "connecting to the use of science or technology in the research field and its growth of information or proof in a court of law [6]." Consequently, it is to be measured forensic, a procedure must employ science and technology and the outcome ought to be competent to be employed in the court of law.

Due to growth of digital evidence, now technology is constantly required to progression the digital information and consequently the only dissimilarity between a forensic and a non-forensic examination of digital information is not the evidence can be provided in the court of law. A forensic examination is a process that deploys the science and technology to enhance the test theories, which can be penetrated into a court of law, to response the questions about proceedings that happened. In this proposed research I have discussed the necessities to enter digital evidence into a court of law. For instance, guidelines that are deployed by some U.S. courts to resolve the consistency of logical and methodological evidence [7].These guiding principles believe if the process has been printed, if it is commonly accepted by the society, if the procedure has been experienced, and if the procedure has a problem rate.

A. Digital Analysis Types

A digital examination could run into various plans of digital information and consequently there subsist numerous kinds of analysis. The different analysis brands are based on elucidation, or generalization, layers, which are common part of the data's design [8]. For example, consider the data on a hard disk, which has been designed with numerous interpretation layers. The lowest layer may restrain panels or other containers that are used for quantity administration. However, inside of each partition is information that has been structured into a file classification or database. The data in a file structure is construed to generate files that contain data in an application-specific design. In each of these layers have its own analyzing techniques and requirements. Moreover the examples for common digital analysis types include:

Media Analysis: The investigation of the data from a storage tool. This study does not reflect on any partitions or other working classification specific data configuration. If the storage tool deploys as a rigid size unit, such as an area, then it can be used in this investigation.

Media Management Analysis: The study of the administration system used to categorize the media. This classically grips the partitions and may include volume administration or RAID classifications that combine information from numerous storage devices into a single virtual storage device.

File System Analysis: The examination of the file system the data which is inside of a partition or disk. This characteristically involves dealing out the facts to dig out the contents of a file or to recuperate the contents of a removed file.

Application Analysis: The investigation of the data inside of a file. Files are produced by users and applications and the format of the contents are application specific.

Network Analysis: The analysis of the information through the communication system is the Network packets can be studied using the OSI form to interpret the unrefined data into an application-level flow. The Application study is a huge group of analysis methods since there are numerous application types. Some of the more common ones are listed below:

OS Analysis: An operating method is a function; even though it is a unique application since it is the primary one that is run when a computer launches. This analysis scrutinizes the design files and productivity data of the OS to resolve what events may have transpired.

Executable Analysis: Executables are digital substances that can cause events to transpire and they are repeatedly investigated during infringement study since the investigator needs to determine what proceedings the executable could be the source.

Image Analysis: Digital images are the objective of various digital examinations because some are illegal imports. This type of study looks for data about where the image was taken and who or what is in the image. In addition, the Image analysis includes investigating images for evidence of steganography.

Video Analysis: Digital video is used in safety cameras and in personal video cameras and webcams. The observations of on-line predators can sometimes engage digital video from web-cams. This type of analysis scrutinizes the video to identify the objects in the video and spot where it was shot.

B. Existing Digital Forensic Framework

1. Computer Forensic Framework

In early part of 1995[9] recommended a style for dealing with prospective evidence. The researcher plotted the computer forensic method for the access of documentary proof in a court of law. In further, he acknowledged that the process exploit must be conformed mutually to the law and science. This tactic has introduced four different steps that are recognized the precedent to the admission of any proof in court. The procedures are acquisition, identification, evaluation and admission as evidence. The outcome of these steps or processes is media (physical context), data (logical context), information (legal context) and evidence correspondingly.

2. Generic Investigation Framework

In 2001, The Digital Forensics Research Working Group [10] defined a generic study process that can be functionalized to all or the mainstream of study involves digital systems and networks. The procedures that defined at that time are recognition, safeguarding, compilation, assessment, investigation, presentation and decision. In this scaffold these kinds of processes are called as modules of task and individual tasks called essentials. This framework puts in positions a significant foundation for forthcoming prospects.

3. Abstract Digital Forensic Framework

However in 2002, [11] projected a structure called as a conceptual digital forensics structure based on DFRWS module contains eleven stages and they are recognition, preparation, approach technique ,conservation, compilation, assessment, investigation, presentation and returning proof. And it does well at affording the common framework that can be applied to classify the confrontations. This ample method affords numerous advantages as listed by the researchers such as mechanism for deploying the same structure for further prospect of digital technologies. On the other hand this structure is untied at any rate of appreciation where its third stage (the approach strategy) is to an extent a replication of its second stage (the preparation phase). As in the time of response to a notification of the incident, the recognition of the suitable procedure will possibly necessitate the resolve of methods to be used.

4. Integrated Digital Investigation Framework

In 2003, digital investigation method the framework is projected as [12] that based on the exploration process of substantial crime scene. This structure has sophisticated stages designed for the investigation of the material offense scene and it called as Integrated Digital Investigation Process (IDIP). The researchers illustrate that the digital offense scene as the practical setting produced by software and hardware where digital proof of an offense or event survival. Therefore, the structure systematizes the development into five groups consists of 17 stages. The groups are readiness stage, deployment stage, physical crime scene investigation stage, digital crime scene investigation stage and review stage. This emphasizes the modernization of the proceedings that led to the incident and highlights in appraising the whole task, hence ultimately building a system for quicker forensic investigations.

5. End to End Digital Investigation Framework

Its crutinizese very processes in DFRWS structure as a set and every actions taken as fundamentals of the class [13]. Then, he affirms to facilitate the six classes define the exploratory process. Consequently, he widens the methods into nine procedures in which he then known as End-to-End digital Investigation Process (EEDI). The subsequent nine procedures in EEDI ought to be implemented through the researcher with the intention of preservation, collection, examination and investigate digital proof. Moreover, he defined the significant actions in the compilation method such as to accumulate the images of effected computers, to gather logs of transitional devices principally those on the internet, to accumulate the logs of infected PC's along with to accumulate logs and data from intrusion recognition systems, firewalls, etc. Subsequently, he developed a formal demonstration of the nine steps deploying the Digital Investigation Process Language (DIPL) and Colored Petri net Modeling. This framework primarily highlighted on the analysis process to incorporate the proceedings from multiple locations.

6. Enhanced Digital Investigation Framework

Then in 2004, [14] improved the Integrated Digital Investigation Process Framework (IDIP) called Enhanced Digital Investigation Process Framework (EIDIP). EIDIP splits the explorations at the principal and derived crime scenes whereas portraying the stages like monotonous as a substitute of linear. In this study, they portrays the two supplementary phases which are sketched back and explode that hunt for to split the investigation into foremost offense scene (the computer) and the inferior offense scene (the physical crime scene). The primary intention of the augmentations is to renovate the two crime scenes concomitantly to evade unpredictability.

7. Event-based Digital Forensic Investigation Framework

Transporter and Spafford has projected a different structure for significant the Event-based Digital Forensic exploration Structure by identifying the non uniqueness Survey phase in IDIP and subsequently it is shortening the framework into Preservation, Search and Reconstruction phase [15]. This straightforward framework is based on the reasons and outcomes of events. The major objective of every phase is inimitable and the requirements can be defined. However, these three phases has not revealed the wholeness of each phases. Consequently, these phases are not lucid with the aim of this structure is sufficient for Digital forensic Investigation.

8. Extended Model of Cybercrime Investigation

The framework proposed by [16] has lucid steps to be taken throughout the investigation process starting from research of investigation procedure right after the crime is reported in anticipation of the case scattered. The model consists of different stages which he involve activities such as responsiveness, endorsement, forecasting, proclamation, exploration and recognize, compilation, transport, storage, investigation, hypotheses, presentation, proof/defense and dissemination. The framework also affords a foundation for the advancement of methods and tools to support the work of investigators. Therefore, this framework is most likely measured as the most complete to date [17].

9. Hierarchical Objective based Framework

[18] Proposed multi-tier method after they evaluated that the majority of preceding forensic models were single stratum process however in reality the method leaned to be multifaceted layers. They explicitly intend the numerous subtasks for the data investigation phase using survey extract and scan technique. The primary tier stages are research, episode retort, data compilation, data investigation, production and incident finality. In further, the data analysis stage is structured into the survey phase, extract phase and scrutinize in the second level stage. In the anticipated scaffold, the investigation task using the concept of goal-based tasks is introduced. As affirmed by the researchers, this structure affords the distinctive profits in the fields of expediency and specificity. As a result, these benefits can trounce the problems in the framework proposed by [12].

10. Forensic Process Framework

In 2006, forensics process projected by [19] four stages and they are compilation, assessment, investigation and reporting. The outcome for every stage is comparable to the premature method proposed by the research [9]. In this method, forensic process renovates media into proof either for law enforcement or an organization's domestic usage. Firstly, renovation crops up when poised data is investigated which abstracts data from media and renovates it into a design that can be administered by forensic tools. Formerly, the data is transmuted into statistics over and done with exploration and finally, the information is made over into proof during the reporting phase.

11. Investigation Framework

[17] Anticipated a new structure by amalgamating the prevailing frameworks to accumulate a reasonably complete framework. The proposed framework appeals on the capability of others in this research, [14] [12] [20] [21] [11] [16] it has emphasized two significant points; the knowledge of appropriate legal base precede to setting up the framework that is vivacious, meanwhile it will bear the complete analytical process; and the progression should consist of three phases (research, exploration and production) to convene the least amount of requests for the classification of the term "forensic". As a result, [17] I have proposed the framework by aligning the phases in the existing structure into the above three phases. In addition, this model fixes an authorized base as foundation to have strong understanding of what the legal necessities are; is recognized right at the commencement of investigation and appraise every following step or phase. In this structure, two necessities have been acknowledged as desirable at every side by side; that are the legal requirements of a explicit system and credentials of all the stages taken. The major benefit of this anticipated framework can be easily lengthened in consist of any quantity of supplementary phases required in forthcoming prospect.

12. Computer Forensic Field Triage Process Framework

The Computer Forensic Field Triage Process Model(CFFTPM) suggests the onsite or field method for affording the documentation, exploration and interpretation of digital proof in a short time setting starved of requirement on captivating the systems/media back to the test center for an in-depth investigation or obtaining a widespread forensic picture [22]. This structure obtained through the IDIP structure [12] and the Digital Crime/Offense Scene Analysis (DCSA) framework as established by [23]. The phases comprises in this model are forecasting, triage, client/customer profiles, History/timeline, web movements and case specific proof. This framework is a reinforcement of material world inspective approaches that have condensed into a formal process framework. The foremost benefit of CFFTPM is on its expediency and pragmatic caused by the fact that the framework was industrialized in contrary of most other DFIF. On the other hand, this structure is also not automatically pertinent in favor of the entire analytical circumstances.

The Universal Practice illustration for Confrontation and PC Forensics projected by [24] has acquainted with anew process framework to scrutinize the computer safety occasions and its objective is to merge both the concepts of Incident Response and Computer Forensics to progress the overall process of investigation. This framework engrossed prominently on the investigation and it entails Pre-Incident groundwork, Pre- Investigation, Investigation and Post-Investigation. Pre- Investigation section comprises of all steps and accomplishments that are implemented before the authentic investigation starts and Post-Investigation Stage is apprehensive on the transliterated report citations of the whole accomplishments during the examination. The concrete investigation obtains in the Analysis Phase. This methodology compromises a way to bear proper incident retort while applying ideologies are familiar through the Computer Forensics during the real investigation phase and it incorporating a forensic investigation into an Incident Response framework.

The three major problems have been examined from the above structures, which are methodized redundancies, area focus and framework qualities. For instance [11] and [14] have duplication process or accomplishments in their framework. [12] and [23] were highlighting on building a device for faster forensic investigations, however[13] [18] and [24] were focusing on the analysis process with the intention of achieving the proof and progress the overall method of investigation. [18] and [22] frameworks have the features of expediency, specificity and realistic which is more essential for examination process. All of these modules have their own strength; on the other hand till the moment where is not having individual method can be employed as a universal guideline for exploring all incidents cases. Consequently, the advance research is desirable to enterprise a general framework to flabbergast these disputes

III. REAL WORLD CYBER CRIME CASES

Cybercrime often has a global aspect. E-mails with illegitimate content often pass through a number of countries during the allocate from sender to recipient, or illegal content is stored outside the country [25] Within cybercrime investigations, close collaboration between the countries complication is very important [26]. The prevailing reciprocated legal support agreements are based on formal, complex and often time-consuming procedures, and moreover often do not cover computer-specific investigations. Setting up techniques for quick response to incidents, as well as requests for the worldwide coordination, is therefore vigorous [27].

Many countries base their mutual authorized assistance management on the principle of "dual criminality" [28]. Examinations on a worldwide level are commonly restricted to those crimes that are criminalized in all contributing countries. Even though there are numerous offences – such as the dissemination of child pornography that can be indicted in most authorities, regional differences play an essential role [29] the perfect example for the other kinds of unlawful content, such as hate speech. The criminalization of illegal content differs in various countries. Material that can lawfully be disseminated in one country can easily be illegal in another country. Presently, the computer technology in use is principally the same around the globe. Apart from language concerns and power adapters, there is very little dissimilarity between the computer methods and Mobile devices sold in Asia and those sold in Europe. An analogous position arises in relation to the Internet. As a result of regularization, the network protocols used in countries on the African continent are the same as those used in the United States Standardization empowers the users around the globe to access the same services over the Web.

A. Email Account Hacking

Nowadays Emails are escalated and being used for communal interaction, business communication and in web dealings. The majority email account holders do not precede the simple securities to protect their email account passwords. In Case of theft of email passwords and successive mismanagement of email ids are turned out to be very frequent.

The Situations:

1. The fatality's email id password is hacked and the account is subsequently distorted for transferring out the malevolent policy (virus, worm, Trojan etc...) to

community in the fatality's account book. The recipients of these viruses consider that the electronic message is coming from the familiar person and has the attachment. This affects their PC's with the malevolent code.

2. The victim's email id password is stolen and the Hackers attempt to extract funds from the Fatality. The victim is exposed that if he does not disburse the fund, the data comprised in the mail accounts will be distorted.
3. The Fatality's email id password is stolen along with outrageous mails are mailed to people through the victim's account book

The Rule

Situation 1: Segments 43 and 66 of Information Technology Act.

Situation 2: Sections 43 and 66 of Information Technology Act and section 384 of Indian Penal Code.

Situation 3: Segments 43, 66 and 67 of Information Technology Act and section 509 of the Indian Penal Code.

Who is Liable?

Situation 1: People who comprised the misuse the email account password and who are exploiting the email account.

Situation 2: Persons who have whipped the email account password and who are intimidating to exploit it.

Situation 3: People who have stolen the email id password and who are misusing the mail id.

The Motive

Situation 1: Business Espionage, awkward desire in being able to terminate valuable data belonging to outsiders etc.

Situation 2: illegitimate monetary profit.

Situation 3: Retribution, Covetousness, Abhorrence.

Modus Operandi

1. The tentative would mount key loggers in common PC's (such as cybercafés, airport lounges etc...) or the PCs of the victim.
2. The Credulous victims would login to their email accounts deploying the affected PC's.

The password of the Fatality's email accounts probably mail to the unknown.

B. Credit Card Fraud

Credit cards are universally being used for web booking of Flight and railway tickets and for other ecommerce dealings. Even though most of ecommerce websites have employed strong safety measures (like SSL, secure internet servers etc), in situation like credit card frauds are mounting up.

The Situation

The fatality's credit card information is stolen and distorted for making internet purchasing (e.g. airline tickets, software, contribution to pornographic websites etc).

The Law

Sections 43 and 66 of Information Technology Act and section 420 of Indian Penal Code.

Who is Liable

All people who have stolen the credit card data as well as those who have distorted it.

The Motive

Situation 1: The uncertain would accumulate key loggers in common desktops (such as cyber cafes, airport lounges etc) or the PC's of the fatalities. Credulous victims would use these corrupted computers to make web transactions. The credit card data of the victim would be mailed to the affected concerns.

Situation 2: Petrol bunk attendants, employees at wholesale shops, Board house waiters etc make a note of their data of the credit cards of the individual and it is used for erecting disbursement at these organizations. This data is sold to illegal persons where that can be distorted it for web forgeries.

C. Online Share Trading Fraud

Through the introduction of dematerialization of share markets in India, it has turned out to be compulsory for patrons to have demat accounts. In majority of the cases the net banking account is associated with the share marketing account. This has directed to the great number of web share marketing forgeries.

The Situation

Situation 1: The Fatality's account passwords are stolen and his accounts are distorted for making fake bank transfers.

Situation 2: The victim's account passwords are stolen and his share marketing accounts are distorted for creating illegal dealings that outcome in the victim facing losses.

The Law

Situation 1: Segments 43 and 66 of (Information Technology) IT Act and section 420 of Indian Penal Code.

Situation 2: Sections 43 and 66 of (Information Technology) IT Act and section 426 of Indian Penal Code.

Who is Liable?

Situation 1: All people who have stolen the account data in addition they have distorted it.

Situation 2: All people who have stolen the account data besides those who have distorted it.

The Motive

Situation 1: Illicit monetary profit

Situation 2: Retribution, covetousness, abhorrence

Modus Operandi

Situation 1: The conceive would establish the key loggers in public desktop's (such as cybercafés, airport lounges etc) or the PC's of the victim. Unsuspecting fatalities would employ these affected computers to login to their net banking and share marketing accounts. The passwords and other data of the victim would be mailed to the suspects.

Situation 2: Same as Situation 1.

D. Tax Evasion and Money Laundering

The numerous deceitful business people and money launderers (Hawala operators) are employing practical as well as material storage media for trouncing the data and records of their illegal trades.

The Situation

Situation 1: The conceive employs physical storage media for trouncing the data e.g. hard drives, floppies, USB drives,

mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc.
Situation 2: The conceive deploys practical storage media for trouncing the data e.g. email id's, Web briefcases, FTP sites, G space etc.

The Law
Situation 1: The prediction upon the case, requirements of the Income Tax Act and Impediment of Money Laundering Act will be valid.
Situation 2: The prediction upon the case, requirements of the Income Tax Act and Impediment of Money Laundering Act will be valid.

Who is Liable?
Situation 1: The individual who hides the data.
Situation 2: The individual who hides the data. If the operators of the practical storage proficiency do not incorporated in the investigation, subsequently they also turned out to be unfathomable.

The Motive
Situation 1: Illegitimate monetary profit
Situation 2: Illegitimate monetary profit

Modus Operandi
Situation 1: The conceive would obtain tiny storage strategies with bulky data storage abilities.
Situation 2: The conceive would unwrap free or paid accounts with Internet storage suppliers.

E. Theft of Confidential Information

Nowadays the majority of Business traders piled up their susceptible data in computer systems. This data is beleaguered by opponents, criminals and sometimes it has irritated the employees.

The Situation
Situation 1: The business proficiency obtains the data (e.g. tender quotations, business plans etc) employing the ride out or social industrializing. Formerly, he employs the data for the gain of his own industry (e.g. quoting lower rates for the tender).
Situation 2: Illegal person obtains the data by lacerating or social engineering and terrorizes to formulate the data to the public if not the victim reimburses him some amount.
Situation 3: A displeased worker whips the data and group mails sent to the victim's rivals and also send it to various websites and news channels.

The Law
Situation 1: Sections 43 and 66 of the Information Technology Act, section 426 of Indian Penal Code.
Situation 2: Sections 43 and 66 of the Information Technology) IT Act, section 384 of Indian Penal Code.
Situation 3: Sections 43 and 66 of the Information Technology) IT Act, section 426 of Indian Penal Code.

Who is Liable?
Situation 1: The individuals who whip the data besides the individuals who exploit the stolen data.
Situation 2: The individuals who whip the data besides the individuals who terrorized the victim and extract money.
Situation 3: The dissatisfied worker besides the individuals who guides him in stealing and dispensing the data.

The Motive
Situation 1: Illegitimate monetary profit
Situation 2: Illegitimate monetary profit
Situation3: Revenge.

Modus Operandi
Situation 1: The conceive might employ an expert hacker to rupture into the victim method. The hacker could also use social engineering techniques.

Illustration
A gorgeous woman went to meet the system administrator (sysadmin) of a reputed company. She interrogated the sysadmin for a "magazine article". Throughout the interview she flirted a lot with the sysadmin and whereas in the departure she "accidentally" left her pen drive at the sysadmin's room. The sysadmin repossess the pen drive and view that it confined many photographs of the lady. He did not comprehend that the photographs were Trojanized! Once the Trojan was in place, a lot of penetrating information was stolen very easily.
Situation: The sysadmin of a reputed industries received a beautifully packed CD ROM containing "security updates" from the company that developed the operating system that ran his company's servers. He installed the "updates" which in genuineness were Trojanized software. For 3 years later and a lot of confidential data was stolen from the company's systems!
Situation 2: Same as Situation 1.
Situation 3: The dissatisfied worker would frequently have direct or indirect access to the data. He can use his personal computer or a cyber café to extent the data.

IV. RESEARCH DIRECTION AND SUMMARY

Through this research that it is motivated with the rapid growth in computer scams and cyber crimes, in addition the investigation acquires the immense challenges to probe some of the open issues of digital forensic analysis. This document created with the discussion about digital forensic study methods. The various open problems have been identified in the research field of digital forensic

Subsequently the proposed work affords the Systematic Digital Forensic Investigation Model for network forensic which is extremely constructive in compilation of digital forensic study. And the major advantages of the research are mentioned below:

- This will facilitate in evidence dynamics and modernization of events by comprehending the properties of Individuality, Repeatability, Reliability, Performance, Testability, Scalability, Quality and Standards in the investigation of computer scams and cyber crimes (CFCC).
- It will afford as benchmark and indicating points for investigating cases of computer scams and cyber crimes.

- It will assist in the enlargement of universal solutions, which can foster the need of fast shifting and extremely volatile digital technological scenario.

The reliability and acceptability of digital evidence can be accomplished.

REFERENCES

[1] Report on "Understanding Cybercrime : Phenomena, Challenges and Legal Response", Telecommunication Development Sector, November 2014.

[2] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab & Steve Chon, "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime", International Journal of Cyber Criminology, Vol 8 Issue 1 January, pp.1-20, June 2014.

[3] Draft on "Comprehensive Study on Cybercrime", United Nations Office on Drugs and Crime, February 2013.

[4] Daniel B. Garrie, J. David Morrissy, "Digital Forensic Evidence in the Courtroom: Understanding Content and Quality", Northwestern Journal of Technology and Intellectual Property, Volume 12, Number 2, pp.122-128 (April 2014).

[5] Alastair Irons and Harjinder Singh Lallie, "Digital Forensics to Intelligent Forensics" , Future Internet, pp.584-596, 2014.

[6] Fakeeha Jafari and Rabail Shafique Satti, "Comparative Analysis of Digital Forensic Models", Journal of Advances in Computer Networks, Vol. 3, No. 1, pp.82-86, March 2015.

[7] Emilio Raymond Mumba and H. S. Venter, "Testing and Evaluating the Harmonized Digital Forensic Investigation Process in Post Mortem Digital Investigation", ADFSL Conference on Digital Forensic, Security and Law, pp.83-98,2014.

[8] Mohsen Damshenas, Ali Dehghantanha, Ramlan Mahmoud, "A Survey on Digital Forensic Trends", International Journal of Cyber-Security and Digital Forensic, The Society of Digital Information and Wireless Communications, pp.209-234, 2014.

[9] Rabail Shafique Satti and Fakeeha Jafari, "Domain Specific Cyber Forensic Investigation Process Model", Journal of Advances in Computer Networks, Vol. 3, No. 1, pp.75-81, March 2015.

[10] Pedro A. Baziuk, Selva S. Rivera, and Jorge Núñez Mc Leod, "Towards Human Taxonomy with Congnitive Generic Terms", Proceedings of the World Congress on Engineering 2014 Vol II, WCE 2014, July 2 - 4, 2014, London, U.K.

[11] Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal Digital Evidence* , 1 (3).

[12] Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence* , 2 (2).

[13] Stephenson, P. (2003). A Comprehensive Approach to Digital Incident Investigation. *Elsevier Information Security Technical Report*. Elsevier Advanced Technology.

[14] Baryamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process Model. Proceeding of Digital Forensic Research Workshop. Baltimore, MD.

[15] Carrier, B., & Spafford, E. H. (2004). An Event-based Digital Forensic Investigation Framework. *Proceedings of Digital Forensics Research Workshop*. Baltimore, MD.

[16] Ciardhuain, S. O. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence* , 3 (1).

[17] Kohn, M., Eloff, J., & Oliver, M. (2006). Framework for a Digital Forenisc Investigation. *Proceedings of Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference. South Afrika*.

[18] Beebe, N. l., & Clark, J. G. (2004). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Proceedings of Digital Forensics Research Workshop*. Baltimore, MD.

[19] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response, *NIST Special Publication 800-86*. Gaithersburg: National Institute of Standards and Technology.

[20] Casey, E. (2004). *Digital Evidence and Computer Crime* (2 ed.). Elsevier Academic Press.

[21] NIJ. (2002). Results from Tools and Technologies Working Group. *Goverors Summit on Cybercrime and Cyberterrorism*. Princeton NJ.

[22] K.Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. Proceedings of Conference on Digital Forensics, Security and Law, (pp. 27-40).

[23] Roger, M. (2006). *DCSA:Applied Digital Crime Scene Analysis*. In Tipton & Krause.

[24] Freiling, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. Proceedings of Conference on IT Incident Management and IT Forensics. Germany.

[25] Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management, 2005.

[26] Regarding the need for international cooperation in the fight against cybercrime, see: Putnam/Elliott, International Responses to Cyber Crime, in *Sofaer/Goodman*, Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35. pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf

[27] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141.

[28] International Cooperation in the Draft United Nations Convention against Transnational Crimes, UNAFEI Resource Material Series No. 57, 114th International Training Course, page 87 *et seq.*, available at: www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

[29] Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.