



Conceptual Approach of Cyber Crime Investigation Process Models

¹Khimsuriya Jayantilal B & ²Dr Vyas Dhaval Shashikant

¹Research Scholar & ²Research Guide

Department of Computer Science, C. U. Shah University, Wadhwan, Dist.: Surendranagar, Gujarat (India)

Abstract: *Cybercrime increase day by day as new technologies and ideas increase. In the present scenario the cybercrime increased rapidly high rate, as new computer technology in growing at massive high speed. For this reason cybercrime investigation process also becomes clumsier without a noble cybercrime investigation process model/framework. Such type of model / framework is important because it provides guidelines for appropriate investigation process of cybercrime. The aim of this paper is to study different types of models and study various steps that have been proposed by various investigators. There is comparative analysis to be done to find out which model is better for investigation.*

Key words: *cybercrime, investigation model, digital forensic, digital evidence.*

I. INTRODUCTION

Today computer technology is compulsory each and every part of the society or sector like banking, insurance, education, politics, and much more. As computer technology helpful in various stages of life, same way it has also some vulnerability. As computers are interconnected with each other to create a network and transmit huge amount of data through wire or wireless technology of the computer. These computer systems are liable for cyber crime related offences like

The World Wide Web was invented in 1989. The first-ever website went live in 1991. Today there are more than 1.2 billion websites. There are 3.8 billion Internet users in 2017 (51% of the world's population of 7 billion), up from 2 billion in 2015. Last year, Cybersecurity Ventures predicted that cybercrime will cost the world \$6 trillion annually by 2021, up from \$3 trillion in 2015¹.

The paper discuss about the initial models that have been developed previously and also latest investigative models.

II. LITERATURE REVIEW

Due to the variety of cases, e.g., cyber-attacks conducted by IT specialists, civil cases in a corporation, or criminal cases, different investigators tend to follow different methods in their investigative process. Computer crime is a huge criminal activity that continues to grow in its prevalence and frequency. This increase in criminal activity poses a strain on business organization, law enforcement and government. Hence the need of shift from document based evidence to digital/electronic evidence has necessitated a rapid reformulation of standards and procedures (Casey, 2002).

To overcome cyber crime, digital forensic can be referred back to as early as 1984, when the FBI began developing programs to examine computer evidence (Noblett et al., 2000).

The area of computer forensic is in its journey to become a recognized scientific discipline (Reith et al., 2002).

Carrier and Spafford (2003) proposed an investigation process known as integrated digital investigation process with the intention to combine various available investigative processes into one integrated model. The author introduced the concept of digital crime scene, which refers to the virtual environment created by software, and hardware where digital evidence of a crime or incident exists.

Ciardhuain (2004) proposed a model for cybercrime investigation that combines the existing models, generalizing them and extending them by addressing certain activities.

Beebe and Clark (2004) proposed a model known as a Hierarchical Objective-Based Framework for Digital Investigation and introduced the concept of objective-based tasks in which the investigative goals are used to select the analysis task.



Agawal et al. (2011) proposed the Systematic Digital Forensic Investigation Model (SRDFIM) that focused on investigation cases of computer fraud and cybercrimes.

Numerous process models have been proposed in the literature to date. Generally, each framework attempts to refine the standard methodology for a specific use case and each of these process models take a broadly similar approach.

2.1 About Models In Brief

Here, description of some selected model given below:

Model1: Computer Forensic Process by M. Pollitt

The methodology of this model is for dealing with digital evidence investigation so that the results of the investigation consistent and legally acceptable. This model consist four phases. The Acquisition phase define the evidence is acceptable and approved from authority. Identification phase identifies the components used in investigation. The Evaluation phase evaluates the case. The Admission presents the evidence in the prosecution.

Model2: Digital Forensic Investigation Model by Kruse & Heiser

This model consists of phases named Acquiring, Authenticating and Analyzing. This model was developed to resolve cyber crime. This model does not provide detailed information. There are only fundamental stages.

Model3: Abstract Model of the Digital Forensic Procedures by Reith, Carr, & Gunsh

In this model consist nine phases, Identification, preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation and Returning Evidence. The more different phases are preparation, Approach Strategy and Returning Evidence. The preparation phase followed by Approach Strategy in which physical and digital evidence properly preserved and secured. When the whole investigation completed the evidence should be returned.

Model4: An Integrated Digital Investigation Process by Carrier & Spafford

This model comprises various processes of investigation in to a single integrated model. The model starts with Readiness phase, means equipment and personnel are ready for investigation.

There are two types of readiness, Operation Readiness and Infrastructure Readiness. The Deployment phase indicates mechanism to detect and confirm an incident has occurred. The further phases are Detection & Notification and Confirmation & Authorization. Next is Physical Crime Scene Investigation phase indicates physical evidence is collected and analyzed. The sub phases are Preservation, Survey, Documentation, Search & Collection, Reconstruction and Presentation. The Digital Crime Investigation phase similar to Physical Crime Scene Investigation phase, only focus on digital evidence. The Review phase, find out the area of enhancement of the result.

Model5: Enhance Integrated Digital Investigation Process by Baryamureeba & Tushabe

This model based on Integrated Digital Investigation Process (IDIP) model. The trackback phase is different phase in this. It is allow the investigator to trace back all the different way the computer or device used by the criminal. There are readiness, deployment, trackback, dynamite and review phases. The work of readiness, deployment phase and review phases are as per previous discussion. The dynamite phase is identifying the potential of culprits to do the crime. it has Physical Crime Scene Investigation, Digital Crime Scene Investigation, Reconstruction and Communication sub phases.

Model6: Hierarchical, Objective Based Framework by Beebe & Clerck

This framework divided in tow tier framework, the first tier phases are preparation, incident response, Data Collection, Data Analysis, Presentation of Findings, and Incident Closure. The second tier phases are object base sub phases (OBSP).

Model7: Integrated Framework by Kohn, Eloff, & Oliver

In this proposed framework, there are three phases: preparation; investigation, and presentation. These phases are make generalize the framework. The aim of Preparation phase is to make standard policy, legal advice, documentation and planning. The investigation phase involve the activities like searching and identify the evidence on a computer system, collect, transport, storage, examine and analysis. The Presentation phase involves presenting the analysis and proves the analysis.

Model8: Computer Forensic Field Triage Process Model by K. Roger, Goldman, Mislán, Wedge & Debtota

This model defines as those investigative processes that are conducted within the first few hours of an investigation, that provide information used during the suspect interview and search execution phase. This model includes the phases named Planning, Triage, User usage profile, Chronology timelines, Internet and Case specific. There the Planning phase indicates proper planning. The Triage phase directly deals with actual crime. The Usage/User Profiles phase involves examination and analysis. The Home Directory activity indication the inspection of directory and sub directories. The File Properties activity check the ownership of objects. The File Properties activity examines the system registry. The Chronology/Timeline phase concentrates on expenditure and timeline of the investigation. The Internet phase includes various internet related inspection like email check. In this Browser Artifacts activity involve checking cookies, history etc. The E-mail Artifacts involves analysis of the email. The



Instant Messaging Artifacts activity contains checking of instant messages. The Case Specific Evidence phase specifics a particular case. This model does not implement in all investigation process.

Model9: Systematic Digital Forensic Investigation Model by Mr. Ankit Agarwal, Ms. Megha Gupta, Mr. Saurabh Gupta, Prof. (Dr.) Subhash Chandra Gupta

This model consists of eleven phases named Preparation, Securing the Scene, Survey & Recognition, Documentation of Scene, Communication Shielding, Evidence Collection, Preservation, Examination, Analysis, Presentation and Result.

Model10: new model for cyber crime investigation procedure by Yong-Dal Shin

This model consists of ten main phases. These phases are Readiness phase, Consulting with crime prolifer, cyber crime classification & Investigation, Priority decision, Damaged cyber crime scene investigation, Analysis by prolifer, Suspects tracking, Injurer cyber crime scene investigation, Suspects summon, cyber crime logical reconstruction and Writing report.

Model11: Generic Computer Forensic Investigation Model by Yunus Yusoff, Roslan Ismail and Zainuddin Hassan

In this model grouped various phases or activities of the previous developed models. The model is divided into five general group or phases. These phases are Pre-Process, Acquisition & Preservation, Analysis, Presentation and Post-Process phase. In Pre-Process phase concern with all of the activities needed to be done prior to the actual investigation, Acquisition & Preservation phase related to identify, collect, transport, store and reservation of data. Presentation phase related to documentation and presentation of the investigation to the authority. Post-Process phase, concern with appropriate closure of the investigation of the case. Analysis phase concern with forensic investigation process, analysis of data is done here.

Model12: Cyber Crime Investigation Model by Dr. Ajeet Singh Poonia

There are eleven phases in this model named Crime, Realization, Authorization, Audit planning, Auditing, Manage evidence, Hypothesis, Challenge analysis, Final report presentation, Updating policies, Report abstraction and dissemination. This model tries to capture all investigation procedure. The realization phase identifies that crime has been occurred. Authorization phase involves activities between investigator and victims. In audit planning phase all necessary preparation done. The Managing evidences phase manage the relevant evidences. The Hypothesis phase makes the hypothesis. The Challenge analysis phase involves proves the validated of hypothesis. The Final report presentation phase made a final reporting. The Updating polices phase involves updating of policies. The Report abstraction and Dissemination phase represent final report to the public.

Model13:Domain Specific Cyber Forensics Investigation Process Modelby Rabail S. Satti and Fakeeha Jafari

This model is domain specific to establish a policy and process follow of cyber forensic investigation. This model presented to address to the specific domain of university which is under government law. This model includes ten different phases named Establishment of institutional cyber forensics investigations SOPs,Strategic planning & scope definition, Cyber scene sealing, Evidence Collection (by Investigating Authorities), Evidence preservation, Extraction of Relevant Evidences, Evidence analysis, Presentation of analysis and findings, Archiving of Case History Records and Post-case review. This model is generic in nature. Digital investigation process is complex in nature when new phases are added in the process flow

Model14: Digital Forensics Investigation Model by Ch. Pavani

This model has four stages, stage one investigation preparation, stage two evidence acquisition, stage three analysis of evidence and stage four results dissemination. Each stage divided into sub stages. The sub stages define as too general for investigation and practical use.

Model15: Artificial Intelligence based Digital Forensic Framework by Parag H. Rughani

In this framework author represent conceptual framework used to assist automated tools and intelligent tools for digital forensic investigation process. This framework is based on machine learning concept. The framework is divided into three phases like Smart Acquisition, Smart Analysis and Smart Presentation. The Smart Acquisition involve AI forensic tool to acquire the whole image. The Smart Analysis involves reducing the large analysis time.Smart Presentation represent smart reporting tool used for representation. As stated in paper major limitation of this framework is its dependency on training data sets, another limitation is size of training data sets.

III. GAP ANALYSIS

Most of the exiting model does not cover major issues of cyber crime or the security threats that may affect investigation process.

A few of the models were found focusing on the part of the process of investigation only.

The existing models are concerned only on the processing such as collection and analysis. Although this is important and valuable, they are not enough to fully describe the investigation process in a way that help in investigation processing.



Many of the existing cyber crime investigation 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.

While many of the existing models can be seen to build upon each other by extending earlier approaches with the aim of becoming more complete and robust.

Many of the digital forensic investigation processes have been developed either by 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 major limitation of existing cyber crime investigation model is that it refers only to the forensic part of an investigation and issues such as the exchange of information with other investigators are not addressed.

The existing models do not cover all aspects of cyber crime investigation; they are not general enough to describe fully the investigative process in a way which will assist the development of new investigative tools and techniques.

Another drawback with the existing models is that they have given more stress on the collection and examination of the evidence, which is basically middle stage of the model. However, the earlier and later stages must be taken into account for a successful cyber crime investigation model.

IV. CONCLUSION

There are number of cyber investigation process model was proposed by various authors. Many of the existing cyber crime investigation 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. While many of the existing models can be seen to build upon each other by extending earlier approaches with the aim of becoming more complete and robust.

REFERENCES

1. 2017 Cybercrime Report, Steve Morgan, Editor-in-Chief, Cybersecurity Ventures
2. Reith, Mark, Carr, Clint, and Gunsch, Gregg "An Examination of Digital Forensic Models," *International Journal of Digital Evidence* (1:3), Fall 2002, pp 1-12.
3. Palmer, Gary L. "A Road Map for Digital Forensics Research - Report from the First Digital Forensics Research Workshop (DFRWS) (Technical Report DTR-T001-01 Final)," Air Force Research Laboratory, Rome Research Site, Utica, pp. 1-48. <http://ncrb.nic.in/>, —*Cyber Crimes*
4. Inikpi O. Ademu, Dr Chris O. Imafidon, Dr David S. Preston: "A New Approach of Digital Forensic Model for Digital Forensic Investigation". (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.12, 2011.
5. Yong-Dal Shin. "New Model for Cyber Crime Investigation Procedure". Journal of Next Generation Information Technology, Volume 2, Number 2, May 2011.
6. Sundresan Perumal: "Digital Forensic Model Based On Malaysian Investigation Process". IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.
7. Séamus Ó Ciardhuáin: "An Extended Model of Cybercrime Investigations". International Journal of Digital Evidence Summer 2004, Volume 3, Issue 1.
8. Ankit Agarwal, Megha Gupta, Saurabh Gupta & Prof. (Dr.) S.C. Gupta: "Systematic Digital Forensic Investigation Model". International Journal of Computer Science and Security (IJCSS), Volume(5): Issue(1): 2011, 118-131.
9. Baryamureeba and Florence Tushabe: "The Enhanced Digital Investigation Process Model". Institute of Computer Science, Makerere University P.O.Box 7062, Kampala Uganda
10. P. Stephenson, (2003) "A Comprehensive Approach to Digital Incident Investigation.", Information Security Technical Report, Vol. 8, Issue 2, pp 42-52.
11. N. L. Beebe & J. G. Clark, (2004) "A Hierarchical, Objective-Based Framework for the Digital Investigations Process", in Proceeding of Digital Forensic Research Workshop (DFRWS), Baltimore, Maryland.
12. M. Kohn, J. H. P. Eloff, & M. S. Olivier, (2006) "Framework for a Digital Forensic Investigation", in Proceedings of the ISSA 2006 from Insight to Foresight Conference, Sandston, South Africa.
13. Yuof, Shaib and Selamat (2008) "Mapping Process of Digital Forensic Investigation Framework", International Journal of Computer Science and Network Security, Vol.8 No. 10, October 2008.