IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 07, February 2019)

Analysis and Design a Model for Cyber Forensic and Digital Investigation

Hiteshkumar Gunvantbhai Patel
Research Scholar
Mewar University, Chhitorgarh,
Rajasthan (India)

Dr. Chandikaditya Kumawat
Professor of CSE
Mewar University, Chhitorgarh,
Rajasthan (India)

Dr. Jigar Patel
Director
Kalol Institute of Management,
Kalol, Gujarat, (India)

Abstract – **Computer forensics is important. The procedures are important to follow, because doing so ensures evidence will be admitted and suspects will be more likely to face the consequences if found guilty. Following these procedures also means using the proper forensic tools to analyze data correctly. The tools used depend on what is being analyzed. Smaller companies or an individual user might not need many resources to secure their computers but perhaps a big organization might need many different types of applications to monitor hundreds of computers and dozens of sub-networks. This might require a digital evidence bag for more efficient collection of data. Also, certain technologies would benefit from a digital evidence bag such as magnetic card readers due to specific programs associated with the device to operate and process information.**

This paper discussed some of the forensic software tools that CFSs use during their investigations. Four of these tools were evaluated with respect to their functionalities and effectiveness within the forensic investigation methodology. Finally, a discussion about these tools is given. The purpose of our approach is to highlight the shortcomings of current tools in order to provide suggestions for improvements. It is very important that CFSs are able to stay ahead of cyber-criminals through the use of forensic tools that allow them to reliably carry out their tasks within an investigation. We believe that if the suggested improvements to these tools are further researched, prosecutions of cyber-crimes will definitely increase.

Keywords – **ADFM, CDFM, CFFTPM, CFS, DFRWS, GCFIM, IDIP, SRDFIM, UDFIM.**

I. Introduction

Digital forensic tools and methodologies are major components of an organization’s disaster recovery preparedness and play a decisive role in overcoming and tackling computer incidents. Due to the growing misuse of computers in criminal activities, there must be a proper set of methodologies to use in an investigation. The evidence acquired from computers is fragile and can be easily erased or altered, and the seized computer can be compromised if not handled using proper methodologies. The methodologies involved in computer forensics may differ depending upon the procedures, resources and Target Company. Forensic tools enable the forensic examiner to recover deleted files, hidden files, and temporary data that the user may not locate.

A forensic investigator must focus on fundamental areas such as standalone computers, workstations, servers, and online channels. Investigation of standalone computers, workstations, and other removable media can be simple. Examination of servers and online channels, however, can be complicated and tricky. During investigations, logs are often not examined or audited. The investigator must realize that logs play a key role during investigations. They must be given due importance, as they could provide a lead in the case. Digital forensic methodologies consist of the following basic activities:

- Preservation: The forensic investigator must preserve the integrity of the original evidence. The original evidence should not be modified or damaged. The forensic examiner must make an image or a copy of the original evidence and then perform the analysis on that image or copy. The examiner must also compare the copy with the original evidence to identify any modifications or damage.
- Identification: Before starting the investigation, the forensic examiner must identify the evidence and its location. For example, evidence may be contained in hard disks, removable media, or log files. Every forensic examiner must understand the difference between actual evidence and evidence containers. Locating and identifying information and data is a challenge for the digital forensic investigator.

Various examination processes such as keyword searches, log file analyses, and system checks help an investigation.

- Extraction: After identifying the evidence, the examiner must extract data from it. Since volatile data can be lost at any point, the forensic investigator must extract this data from the copy made from the original evidence. This extracted data must be compared with the original evidence and analyzed.
- Interpretation: The most important role a forensic examiner plays during investigations is to interpret what he or she has actually found. The analysis and inspection of the evidence must be interpreted in a lucid manner.
- Documentation: From the beginning of the investigation until the end (when the evidence is presented before a court of law), forensic examiners must maintain documentation relating to the evidence. The documentation comprises the chain of custody form and documents relating to the evidence analysis.

II. TYPES OF CYBERCRIMES

The term cyber-crime can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represents the cybercrime as — Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data. The Internet space or cyber space is growing very fast and as the cybercrimes.

Some of the kinds of cybercriminals are mentioned as below:

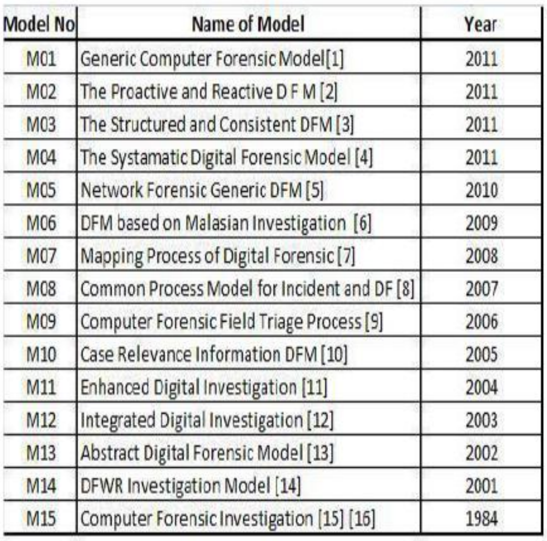
- Crackers: These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.
- Hackers: These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.
- Pranksters: These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.
- Career Criminals: These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs such as the Mafia. The greatest organized crime threat comes from groups in Russia, Italy, and Asia. "The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavoury alliances use advanced information technology and encrypted communications to elude capture."
- Cyber Terrorists: There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal to those addicted to drugs, alcohol, competition, or attention from others, to the criminally negligent.
- Cyber Bulls: Cyber bullying is any harassment that occurs via the Internet. Vicious forum posts, name calling in chat rooms, posting fake profiles on web sites, and mean or cruel email messages are all ways of cyber bullying.
- Salami Attackers: Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers, which deducts a small amount from the account of every customer.

III. PROPOSED MODEL ON FORENSIC INVESTIGATION

Since 1984 when the initial digital forensic model has been introduced, after that too many models has been described efficient methods to investigate a digital crime Scene. Now a days when crime takes place in form of digital devices it has been very crucial to identified the crime and justified the crime.

Although authors has been proposed very effective model or a framework to identify the crime level and digital evidence or digital data. It can be review that some models may be very reliable to take in practical approach and some may not be. At the very initial knowledge as a digital forensic investigator it has been experienced that it is so confusing to select the best model among them. Hence we have reviewed various latest digital forensic models, named given in Table 1 and then found that based on desired output one can summarized so many phases into some very effective and efficient phases. Using the comparison approach, we have developed a Comparative Digital Forensic Model which is based on bottom up approach. Using desired output from each and every phase of reviewed models, I have grouped the output and then identified the required phases to achieve those output.

Table 1: Digital Forensic Models



Model No	Name of Model	Year
M01	Generic Computer Forensic Model[1]	2011
M02	The Proactive and Reactive D F M [2]	2011
M03	The Structured and Consistent DFM [3]	2011
M04	The Systematic Digital Forensic Model [4]	2011
M05	Network Forensic Generic DFM [5]	2010
M06	DFM based on Malasian Investigation [6]	2009
M07	Mapping Process of Digital Forensic [7]	2008
M08	Common Process Model for Incident and DF [8]	2007
M09	Computer Forensic Field Triage Process [9]	2006
M10	Case Relevance Information DFM [10]	2005
M11	Enhanced Digital Investigation [11]	2004
M12	Integrated Digital Investigation [12]	2003
M13	Abstract Digital Forensic Model [13]	2002
M14	DFWR Investigation Model [14]	2001
M15	Computer Forensic Investigation [15] [16]	1984

The majority of organization relies deeply on digital devices and the internet to operate and improve their business, and these businesses depend on the digital devices to process, store and recover data. A large amount of information is produced, accumulated, and distributed via electronic means. Recent study demonstrates that in 2008, 98% of all document created in organization were created electronically. According to Healy (2008) approximately 85% of 66 million U.S. dollars was lost by organizations due to digital related crime in 2007. Panda labs (2009) show that in 2008, Ehud Tenenbaum was extradited from Canada on suspicion of stealing $1.5million from Canadian bank through stolen credentials and infiltrated computers. Williams (2009) states on cybercrime report, a complex online fraud which scammed over £1 million pounds from taxpayers in 2009.

This research focuses on a structured and consistent approach to digital forensic investigation procedures. The research questions for the research are formulated with the aim to map out a structured and consistent approach and guideline for digital forensic investigation. This research focuses on identifying activities that facilitate digital forensic investigation, emphasizing on what digital crimes are and describing the shortcomings of current models of digital forensic investigation.

A. Different Phases of Digital Forensics Investigation Models

A digital forensic is an investigation process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred. In 1984, the FBI Laboratory and other law enforcement agencies began developing programs to examine computer evidence. The procedure adopted in performing the computer forensic investigation has a direct influence to the outcome of the investigation. Digital forensics is the use of scientific methods for the identification, preservation, extraction and documentation of digital evidence derived from digital sources. The digital forensic process can be categorized into four different phases namely collection, examination, analysis and reporting. When introduced the initial digital forensic model in 1984, after that too many models has been described efficient methods to investigate a digital crime Scene. Now a days when crime takes place in form of digital devices it has been very important to identified the crime and justified the crime. Although authors has been proposed very effective model or a framework to identify the digital evidence or digital data.

a. DFRWS Investigative Model (2001)

G. Palmer held the 1st Digital Forensics Research Workshop (DFRWS) and proposed a general purpose digital forensics investigation process. It has 6 phases.

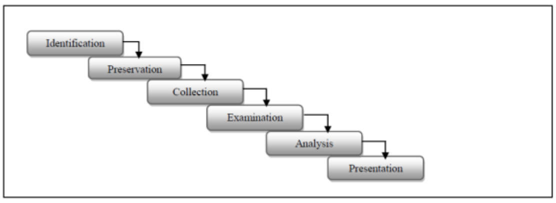


Figure 1: DFRWS Investigative Model

DFRWS Investigative model started with an Identification phase, in which profile detection, system monitoring, audit analysis, etc., were performed. It is immediately followed by Preservation phase, involving tasks such as setting up a proper case management and ensuring an acceptable chain of custody. This phase is crucial so as to ensure that the data collected is free from contamination. The next phase is known as Collection, in which relevant data are being collected based on the approved methods utilizing various recovery techniques. Following this phase are two crucial phases, namely, Examination phase and Analysis phase. In these two phases, tasks such as evidence tracing, evidence validation, recovery of hidden/encrypted data, data mining, timeline, etc., were performed. The last phase is Presentation. Tasks related to this phase are documentation, expert testimony, etc.

b. *Abstract Digital Forensics Model (ADFM) (2002)*

Reith, Carr & Gunsch, proposed an enhanced model known as Abstract Digital Forensic Model. In this model, there is three additional phases than DFRWS, thus expanding the number of phases to nine.

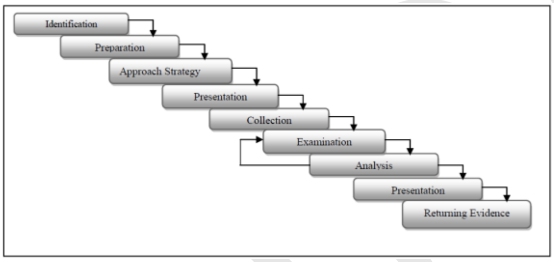


Figure 2: Abstract Digital Forensics Model

The 3 significant phases introduced in this model were Preparation, Approach Strategy and Returning Evidence. In Preparation phase, activity such as preparing tools, identify techniques and getting management support, were done.

Approach Strategy was introduced with the objective to maximize the acquisition of untainted evidence and at the same time to minimize any negative impact to the victim and surrounding people. In order to ensure that evidences are safely return to the rightful owner or properly disposed, the Returning Evidence phase was also introduced. The 1st phase in ADFM is Identification phase. In this phase, the task to recognize and determine type of incident is performed. Once the incident type was ascertained, the next phase, Preparation, is conducted, followed by Approach Strategy phase. Physical and digital data acquired must be properly isolated, secured and preserved. There is also a need to pay attention to a proper chain of custody. All of these tasks are performed under Preservation phase. Next is the Collection phase, whereby, data extraction and duplication were done. Identification and locating the potential evidence from the collected data, using a systematic approach are conducted in the next following phase, known as Examination phase. The task of determining the significant of evidence and drawing conclusion based on the evidence found is done in Analysis phase. In the following phase, Presentation phase, the findings are summarized and presented. The investigation process is completed with the carrying out of Returning Evidence phase.

c. *Integrated Digital Investigation Process (IDIP) (2003)*

Integrated Digital investigation process was proposed by Carrier & Spafford in 2003, to combine the various available investigative processes into one integrated model. The author introduces the concept of digital crime scene which refers to the virtual environment created by software and hardware where digital evidence of an incident or crime exists.

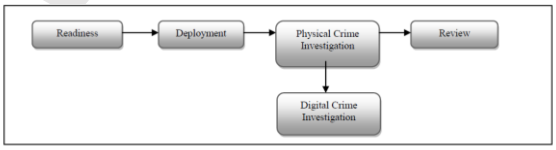


Figure 3: Integrated Digital Investigation Process

The process started with a phase that require for the physical and operational infrastructure to be ready to support any future investigation. In this Readiness phase, the equipments must be ever ready and the personnel must be capable to use it effectively. This phase is indeed an ongoing phase throughout the lifecycle of an organization. It also consists of 2 sub-phases namely, Operation Readiness and Infrastructure Readiness. Immediately following the Readiness phase, is Deployment phase, which provide a mechanism for an incident to be detected and confirmed. Two sub-phases are further introduced, namely, Detection & Notification and Confirmation & Authorization. Collecting and analyzing physical evidence are done in Physical Crime Scene Investigation phase. The sub-phases introduced are Preservation, Survey, Documentation, Search & Collection, Reconstruction and Presentation. Digital Crime Scene Investigation is similar to Physical Crime Scene Investigation with exception that it is now focusing on the digital evidence in digital environment. The last phase is Review phase. The whole investigation processes are reviewed to identify areas of improvement that may results in new procedures or new training requirements.

d. Enhanced Digital Investigation Process (2004)

Baryamueeba and Tushaba (2004) suggested a modification to Carrier and Spafford's Integrated Digital Investigation Model (2003). In the model, the authors described two additional phases which are trace back and dynamite which seek to separate the investigation into primary crime scene (computer) and secondary crime scene (the physical crime scene). The goal is to reconstruct two crime scenes to avoid inconsistencies.

e. Extended Model of Cybercrime Investigation

Ciardhuain (2004) argues that the existing models are general models of cybercrime investigation that concentrate only on processing of evidence in cybercrime investigation. The model shown provides a good basis for understanding the process of investigation and captures most of the information flows. Even though the model was generic, it concentrated on the management aspect.

f. The Systematic digital forensic investigation model SRDFIM (2011)

Agarwal and colleagues in 2011 proposed a systemic approach to digital forensic investigation. There are 11 phases in this model named Preparation, securing the scene, survey and recognition, documentation of scene, communication shielding, evidence (both volatile and non-volatile) collection, preservation, examination, analysis, presentation, result and review (Figure 4).

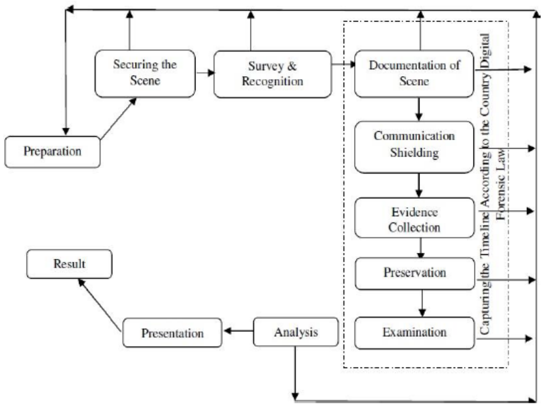


Figure 4: A Systemic Digital Forensic Investigation Model

g. Cyber Forensics Field Triage Process Model(CFFTPM)

This model was proposed by Rogers et al. in 2006 to provide an on-site field approach for identification, analysis and interpretation of digital data (evidence) bypassing the immediate need for bringing it back to lab. The model consists of 6 primary phases which can be further divided into 6 sub-classes. The process is claimed to be in compliance with the widely practiced forensic principles. This model emphasizes on the need to collect maximum informative evidence from the site at the earliest possible time, without support of digital forensic lab.

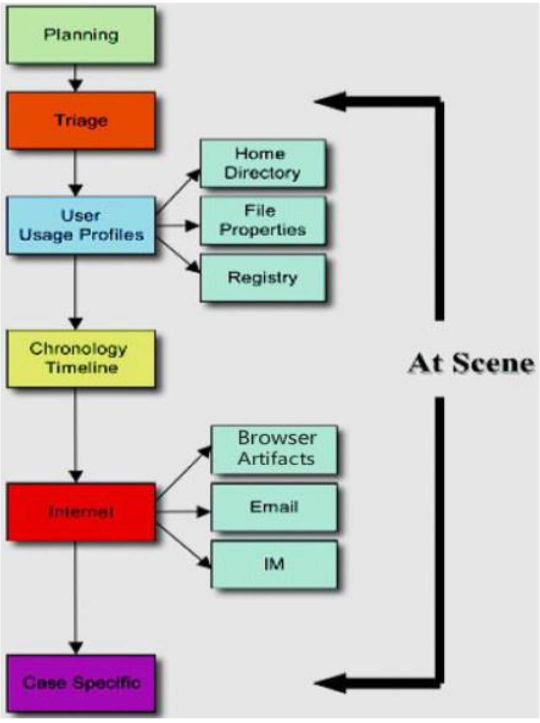


Figure 5: Cyber Forensics Field Triage Process Model (CFFTPM)

h. Generic Computer Investigation Model (GCFIM)

Recently Yunus Yusoff and his colleagues came up with a review of digital investigation models from 1985 till 2011. They examined the pre-existing models for sorting of common phases and then proposed a generic computer investigation model, consisting of 5 generic phases shown in Figure 6. Each of these generic phases represent the main phases present in most of the digital investigation models.

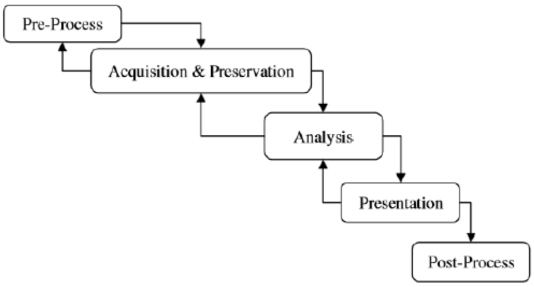


Figure 6: Generic computer forensic investigation model (GCFIM)

i. *Comparative Digital Forensic Model (CDFM)*

The CDFM is having 5 phases as given in Figure 7 describes the complete flow of the model like first phase Foundation which will establish a systematic plan for investigation, Secondly Accumulation & Conservation which will produce the crime type and level. The third phase is Inspection and Analysis which generate the authenticate evidence. Fourth phase is Presentation and Documentation which will explain proof to justify the case. And finally the Justification and disseminating the case which will generate the result. The next portion of study describes the detail working of model.

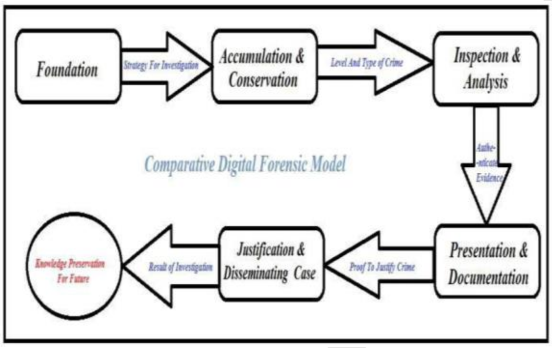

Foundation
Strategy For Investigation
Accumulation & Conservation
Level And Type of Crime
Inspection & Analysis
Authe- -nticate Evidence
Comparative Digital Forensic Model
Presentation & Documentation
Proof To Justify Crime
Justification & Disseminating Case
Result of Investigation
Knowledge Preservation For Future

Figure 7: Comparative Digital Forensic Model

j. *Universal Digital Forensic Investigation Model (UDFIM)*

The Universal Digital Forensic Investigation Model based on the comparison of all major previous Digital Forensic Models. I have reviewed various models as shown in table 1. Based on desired output required for different phases, I have proposed a new model with improvements.

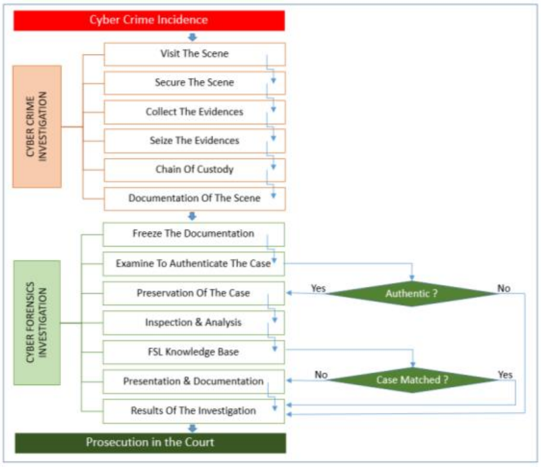


Figure 8: Universal Digital Forensic Investigation Model

B. Cybercrime Incidence Report and Forensics Investigation Process Flow

a. Cybercrime Investigation

Visit The Scene: As soon as any cybercrime incidence is reported, this is the first steps to follow. In this steps cybercrime investigator visits the place of crime.

Secure The Scene: When cyber security investigator has visited the scene, they need to secure that zone so as to prevent any possible modification or changes.

Collect The Evidence: After securing the crime zone, investigator need to collect all possible evidence of cybercrime. These may vary from a small memory card to server.

Seize The Evidence: Seizing of evidences are required to protect them from possible tempering or changes.

Chain of Custody: After seizing, all the seized evidences are taken into custody of in charge cyber security investigator.

Documentation of Scene: After completing the all steps till chain of custody, a comprehensive documentation is to be made by the investigator. This documentation contains all the vital information of the cyber security incidence and hands it over to cyber forensics investigation laboratory for further processes.

b. Cyber Forensic Investigation

Freeze the Documentation: Cyber Forensics Lab receives the complete documentation from investigator and freeze it immediately so as to ensure o data or information is manipulated till the case is resolved.

Examine To Authenticate The Case: In this step, Cyber forensic lab examines the complete document for authenticity of information and facts by cross verifying these details from sources.

Preservation of The Case: If the information provides found to be false the result documents are prepared accordingly and in other case, whole evidences are preserved via an additional copy cybercrime evidences and one will be sent to next higher steps for processing.

Inspection and Analysis: This is the main part of cyber forensics investigation process. Here various tool and techniques are used to analyze the data in volatile and non-volatile form, which available on any digital device.

FSL Knowledge Base: Forensics Science Lab (FSL) keeps track of all the forensics science cases solved in their knowledge base, which can be reused in perpetual case investigations. This will help a lot in swift disposal of many cyber forensics investigation cases.

Presentation and Documentation: The final investigation report of the FSL is used to prepare the final documentation of forensic study.

Result of The Investigation: The end result, which to be presented to the court of law is made in accordance with the guidelines of the court and provided to the prosecution authority.

Judgments from Court of Law: As we all know the decision of court is final. So, court goes through all the cyber forensic results provided by FSL and keep other cyber forensics laws and policies to take the final decision for cybercrime case.

IV. CONCLUSION

Many criminal investigations in today's technology rich society will involve some aspect of computer forensics discussed in this study. Any person undertaking to investigate such a case should be familiar with the basic technologies involved in gathering the information, how to properly gather the data, and how to ensure that the information will be valid as evidence during trial. In particular, it is important to be able to acquire, authenticate and analyze data stored in electronic devices, whether they run Unix or Microsoft operating systems. Furthermore, a competent investigator should understand the technologies involved in tracing and detecting the actions of a specific computer user. In the above pages, we have given an overview and brief introduction of each of these important aspects of digital forensics. Finally, it is important to avoid becoming a criminal by breaking the law while investigating criminal activities.

Based on the presented cyber forensic investigation processes, we are able to extract the basic common investigation phases that are shared among all models. The differences are in the content of each phase whereby certain scenario may require certain levels or types of details steps. Based on the grouping of the overlapping and similar phases, we have proposed a new model, Universal Digital Forensic Investigation Model. We hope that UDFIM can serve as the basic and high level investigation models for any future computer forensic investigation. It should also serve as a good starting point for the development of new computer forensic investigation methodology.

This work presents an overview of digital forensics models and concludes a novel framework for the future. The proposed model incorporates certain features of the past models to provide a new framework. In particular, the ontology of current computer technology in addition to abstraction layers of forensics science used to provide the structure of this model.

REFERENCE

[1] A.Agrawal, M. Gupta, S. Gupta and S. C. Gupta, "Systematic digital forensic investigation model," International Journal of Computer Science and Security (IJCSS), vol. 5, no. 1, 2011, pp. 118-131.

[2] Yasinsac, R. Erbacher, D. Marks, M. Pollitt, and P. Sommer, "Computer Forensics Education," Security & Privacy, IEEE, vol. 1, no. 4, pp. 15–23, 2003.

[3] Agrawal, A. Gupta, M. Gupta, S. Gupta, C. (2011) Systematic digital forensic investigation model Vol. 5 (1) Available (online): http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume5/Issue1/IJC S-438.pdf Accessed on 30th June 2011

[4] Armstrong, I. (2002) Computer Forensics Detecting the Imprint. SC Magazine.

[5] Arthur, K. K., & Venter, H. S. (2004). An Investigation into Computer Forensic Tools. ISSA. Pretoria: Information and Computer Security Architectures (ICSA) Research Group.

[6] Ashley Brinson, Abigail Robinson, Marcus Rogers, A cyber forensics ontology Creating a new appraoch to studying cyber forensics, Digital Investigation, 2006.

[7] Carrier (2001) "Defining digital forensic examination and analysis tools". Digital Research Workshop II. CiteSeerX: 10.1.1.14.8953.

[8] Carrier, "Open source digital forensics tools: The legal argument," stake Research Report, 2002.

[9] B.Carrier, E.H.Spafford. Getting Physical with the Digital Investigation Process, International Journal on Digital Evidence, Fall 2003, Volume 2, Issue 2.

[10] Bassett, R., Bass, L., & O'Brien, P. (2006) Computer Forensics: An Essential Ingredient for Cyber Security. Journal of Information Science and Technology, JIST 3(1)

[11] Benjamin Boeck, David Huemer, A Min Tjoa,Towards more Trustable Log Files for Digital Forensics by Means of "Trusted Computing" in 24th IEEE International Conference on Advanced Information Networking and Applications, 2010

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 7, Issue 07, February 2019)

[12] Bob Sheldon. .Forensic Analysis of Windows Systems,. from Handbook of Computer Crime Investigation: Forensic Tools and Technology, ed. Eoghan Casey. Academic Press, Bath, England 2002, p. 137-139.

[13] Brian Carrier. Defining Digital Forensics Examination and Analysis Tools Using Abstraction Layers. International Journal of Digital Evidence. Vol 1, Issue 4, Winder 2003.

[14] Brian Carrier. Defining Digital Forensics Examination and Analysis Tools. In Digital Research Workshop II, 2002.

[15] Bryant, R. 2008. Investigating digital crime. London: John Wiley & Sons Ltd.

[16] Byrd, M. 2004. Duty description to the crime scene investigator. Miami: Miami Dade Police Department.

[17] Eoghan (2004). "Digital Evidence and Computer Crime, Second Edition". Elsevier. ISBN 0- 12-163104-4.

[18] California High Technology Crime Advisory Committee (CHTCAC) 2000, Annual Report on High Technology Crime in California, California High Technology Crime Advisory Committee, Sacramento, CA, http://www.ocjp.ca.gov/pub_CHTCAC_annu1.pdf, visited 31 March 2000.

[19] Casey, E et al. HANDBOOK OF Computer Crime Investigation: Forensic Tools and Technology. Academic press, 2002. pp 53-71.

[20] Casey, E. 2004. Digital evidence and computer crime: Forensic Science, computers and the internet. 2nd edition. Florida: Academic Press.