Review of Digital Forensic Investigation Frameworks

Ritu Agarwal[1], Suvarna Kothari[2]

[1] Delhi Technological University, New Delhi, India.
ritu.jeea@gmail.com
[2] Delhi Technological University, New Delhi, India
suvarnakothari91@gmail.com

Abstract. Digital Forensic Investigation has seen a tremendous change in the past 25 years. From the age of early computers to the current day mobile devices and storage devices, the crime rate has also followed growth. With the diversity in crimes, frameworks have also been modified over time to cope-up with the pace of crimes being committed. The paper amalgamates all major approaches and models presented that have helped in shaping the digital forensic process. Each discussed model is followed by its advantages and shortcomings.

Keywords: Digital Forensics, models, review.

1 Introduction

Digital Forensics is "the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to facilitate the unauthorized actions shown to be disruptive to planned actions" [5]. With the advent of time, significant changes have been observed in the digital forensic process.

The statistical analysis based on trends from 2004 till present, of the papers from Elsevier journals, IEEE and magazine articles shows the frequency of articles published under Framework and Architecture are the least as compared to Challenges and Opportunity, Security and Privacy Issues and Cloud Forensic Investigation [25].This leads to much scope of future research being done on building a consistent and standardized framework for conducting digital investigation.

A concise survey on digital forensic models is being presented that may help researchers explore new ideas and provide new solution to challenges in the field. The literature review is divided into three phases: Phase1 consolidates papers from 1995 to 2003; Phase 2 combines papers from 2004 to 2007 and Phase 3 from 2008 to present. The paper tries to include major publications that have helped in shaping the digital forensic process.

K.J. Kim (ed.), *Information Science and Applications,*
Lecture Notes in Electrical Engineering 339, DOI 10.1007/978-3-662-46578-3_66

2 Literature Review

2.1 Phase 1:1995-2003

One of the earliest papers that clearly mapped the forensic process was given by Mark M. Pollitt [1] where he proposed four distinct steps "Acquisition, Identification, Evaluation and Admission as Evidence" so that evidence could be documented in the court of law. The result of these phases or methods is "media (physical context), data (logical context), information (legal context) and evidence". But except for this paper, people created guidelines that were focused on the details of the technology and a generalized process was not considered.

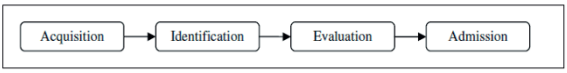

Figure 1: Computer Forensic Investigation Process

Farmer and Venema [2] gave steps as "secure and isolate, record the scene, conduct a systematic search for evidence, collect and package evidence, and maintain a chain of custody" which formed the foundation for further research but it was aimed at UNIX forensic procedures.

Mandia and Prosise [3] proposed a methodology which had step as "pre-incident preparation, detection of incidents, initial response, response strategy formulation, duplication, investigation security measure implementation, network monitoring, recovery, reporting, and follow up". This was advancement over the previous approach but was targeted for explicit platforms such as UNIX, Windows NT/2000 and Cisco Routers. The drawback is that other digital devices like mobile phones, personal digital assistants etc. are not addressed by this approach.

This was succeeded by the abstract model given by the U.S. Department of Justice [4] whose process included "collection, examination, analysis, and reporting". This is helpful as it attempts to shape a comprehensive process that will be valid for most electronic devices but the drawback is that analysis phase of this model is improperly defined and is ambiguous.

The Digital Forensic Research Workshop [5] was the first big consortium headed by the academic community rather than law enforcement. It worked towards developing framework that contains steps such as "identification, preservation, collection, examination, analysis, presentation and decision." In this framework, elements refer to individual tasks and classes of tasks are called processes. This framework lays foundation for future work.Working on this framework, many more models were proposed.

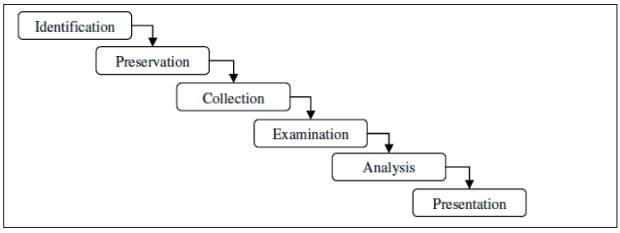

Figure 2: DFRDWS Investigative Model

The Abstract Digital Forensics Model [6] was one of them. It standardized the digital forensics process into nine components "identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, returning evidence." Categorizing of incidents can be done very well using this framework. This broad method has many advantages as proposed by the authors such as the same framework being applicable to forthcoming digital technologies. As we can see, the second step is almost the same as the third step.

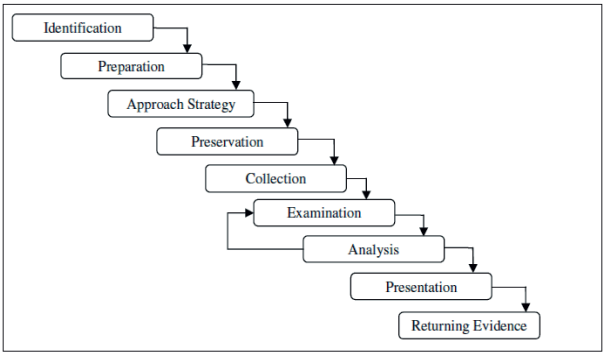

Figure 3: Abstract Digital Forensic Model

The Integrated Digital Investigation Model [7] proposed another model that consists of total of 17 phases generalized into five groups. It has "Readiness phase, Deployment phase, Physical Crime Scene Investigation Phase, Digital Crime Scene Investigation Phase and Review Phase". Physical crime scene was analysed using high level phases. High-level phases are used in this framework for the analysis of both the digital crime scene as well as the physical crime scene. This model covers all the cyber terrorism capabilities and the incidents that led to the events are also reconstructed. However, there are some shortcomings as well. It does not clearly differentiate amongst investigations at the suspect's scene and the victim's scene and moreover it seems impossible to make out whether a digital crime was committed or not unless some prior examination has been made.

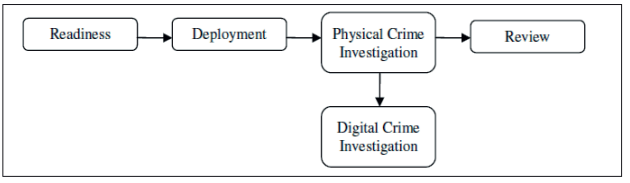

Figure 4: Integrated Digital Investigation Process

A Comprehensive Approach to Digital Incident Investigation [8] given by Stephenson sights class as a process of the DFRWS framework [5] elements of the class is called an action. The investigative process is divided into six classes. He then prolonged the processes into nine steps which formed the End-to- End digital Investigation Process (EEDI). The investigator performs these nine steps in order to "preserve, collect, examine and analyse digital evidence". Critical activities in the collection process were defined by him so as to "collect the images of effected computers, to collect logs of intermediate devices especially those on the internet, to collect logs of effected computers and to collect logs and data from intrusion detection systems, firewalls,

etc". Digital Investigation Process Language (DIPL) and Coloured Petri-net Modelling was then developed by him working on these steps. The principle focus of the framework was on analysis process and integrating events from different locations.

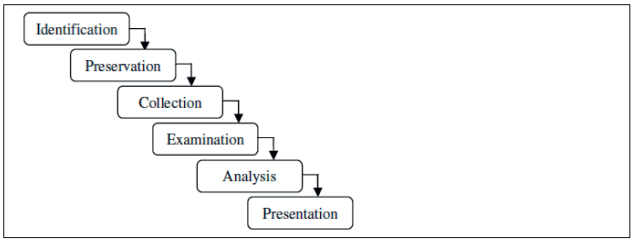

Figure 5: End-to-End Digtal Investigation Process

2.2 Phase 2: 2004-2007

The framework proposed by Ciardhuain [9] gave crisp steps for carrying out the process of investigation, beginning from the reporting of crime to the closure of the case. Phases called as activities in this framework have been defined as "awareness, authorization, planning, notification, search and identify, collection, transport, storage, examination, hypotheses, presentation, proof, defence and dissemination". A basis for the development of techniques and tools to assist in the work of investigators was provided by this framework. Therefore, this is the most complete framework till date.

Baryamueeba and Tushabe [10] made some additions to the Integrated Digital Investigation Model [7] and removed one of its disadvantages by showing clear difference between primary and secondary crime scene by adding two supplementary phases "Trace back phase and Dynamite phase". The aim was to recreate the two crime scenes simultaneously to avoid discrepancies. The primary and secondary crime scenes were separated by the framework while the phases were depicted as iterative instead of linear.

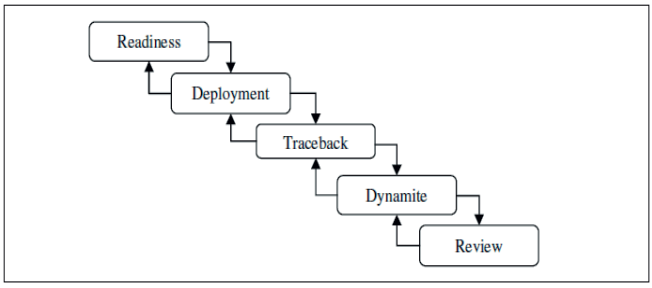

Figure 6:Enhanced Digital Investigation Process

In the Hierarchical Objectives based Framework for the Digital Investigations Process [11] by Beebe and Clark a multi tired model is proposed as opposed to the single tier approach being followed till now. It also introduces the objectives based task concept where analysis tasks are selected by investigative goals. Survey, extract and examine approach is suggested by the author to propose subtasks for analysis of data. The first tier comprises of phases "preparation, incident response, data collection, data analysis, presentation and incident closure". The second tier consists of "survey

phase, extract phase and examine phase" Concept of objective-based tasks is used for analysing tasks in this framework. As stated by the authors, exclusive advantages in the field of realism and specificity are offered by this framework.

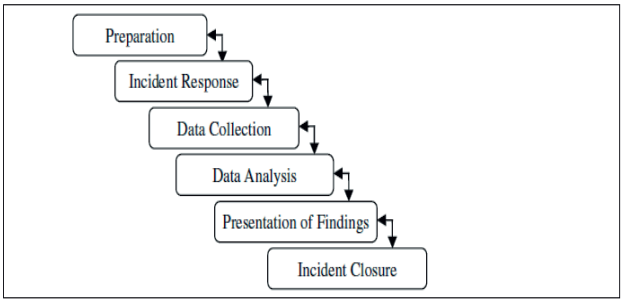

Figure 7: Hierarchical Objectives based Framework

In their 2004 paper, Carrier and Spafford [12] added events and event reconstruction to the digital forensic framework. Reconstruction is done using evidence so that hypothesis can be developed and tested. The framework comprises of three phases "Preservation, Search and Reconstruction Phase" and is based on sources and consequence of events. However completeness of each phase in not mentioned and it cannot be proven that this framework is satisfactory enough for investigation.

Rubin, Yun and Gaertner[13] carried on the work of Carrier[12][7] and Beebe [11] an introduced the concepts of seek knowledge, knowledge reuse and case-relevance. Seek knowledge refers to the investigative clues by which the analysis of data is driven. Case Relevance is "The property of piece of information, which is used to measure its ability to answer the investigative "who, what, where, when, why and how" questions in a criminal investigation" [13].The various levels of Case Relevance are "Absolutely irrelevant, Probably Irrelevant, Possibly irrelevant, Possibly Case-Relevant, Probably Case Relevant".

A paper on network forensics by Erbacher, Christensen and Sunderberg[14] brought up a number of grave matters as visualization of data in intrusion and network forensic situations. They suggested different aspects require different visualization techniques of examination but they also have to be combined.

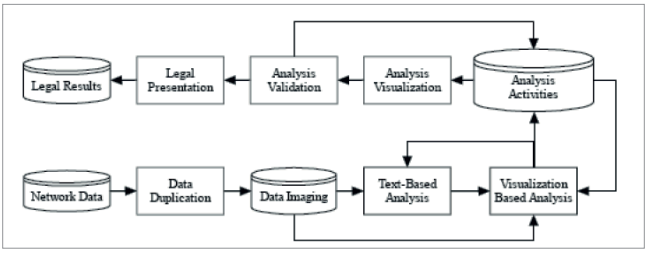

Figure 8: Visual Forensic Techniques and Processes

Kent, Chevalier, Grance and Dang[15] published a guide to Integrated Forensics into Incident Response where they have summarized the forensic process in four basic steps "Collection, Examination, Analysis and Reporting". This is very similar to [1].

Media is transformed into evidence by the forensic process in accordance with this framework either for an organization's inside usage or law enforcement. First, the data gathered from the media is transformed into a format that is readable by forensic tools. After the data has been collected, it is converted to information by the help of analysis and finally information is transferred into evidence in the phase of reporting.
The Computer Forensic Field Triage Process Model [16] was derived from IDIP Framework [7] and a process framework has been built that closely relates to the real world investigative methods. Hence it does not require the system to be taken back to the lab for examination instead the identification, analysis, and interpretation of digital evidence is done on the field itself. The phases contained within this framework are "planning, triage, usage/user profiles, chronology/timeline, internet activity and case specific evidence". This framework was unique since it was developed in reverse to most Digital Forensic Investigation Frameworks. The advantage of this model was its practicality and pragmatic nature but the drawback was that this could not be applied to all situations.

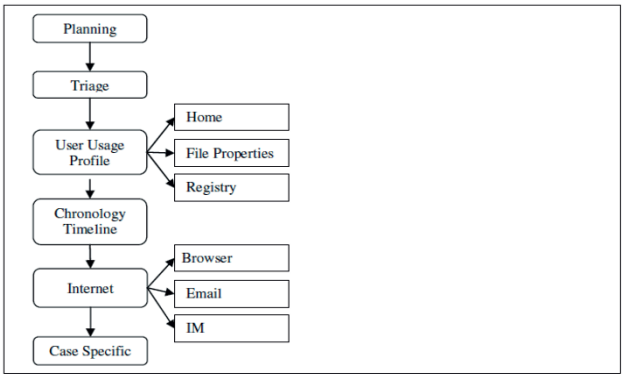

Figure 9: Computer Forensics Field Triage Process Model

In Framework for a Digital Forensic Investigation by Kohn, Eloff and Oliver [17] the aim was to merge the existing frameworks already proposed earlier [10][7][9][6] as it was discovered that a many steps or phases coincided with each another and the differed primarily in the terminology used. So similar tasks were grouped together and three stages were formed "preparation, investigation and presentation". Here the point to be noted is that knowledge of the relevant legal base was essential prior to setting up of the framework. The advantage of this framework is that it can be easily expanded to include any number of additional phases required in the future.

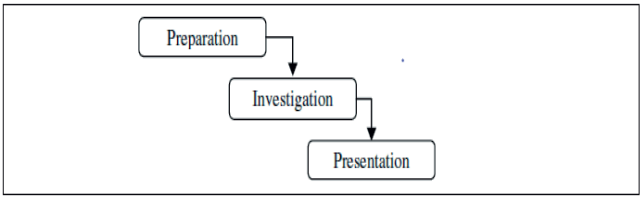

Figure 10: Framework for a Digital Forensic Investigation

The Common Process Model for Incident and Computer Forensics[18] proposed by Freiling and Schwittay has introduced a new framework in overall process of

investigation is improved by combining the two conceptions of Incident Response and Computer Forensics. This model fixated significantly on analysis and it comprises of "Pre- Incident Preparation, Pre-Analysis, Analysis and Post- Analysis". All phases and actions that are completed before the actual analysis starts are combined in the Pre-Analysis Phase and Post-Analysis Phase deals with the documentation of the all actions undertaken during the course of an investigation. Computer Forensics can be applied during the analysis phase. Thus a proper technique to conduct incident response and integrating forensic analysis into Incident Response is suggested by this framework.

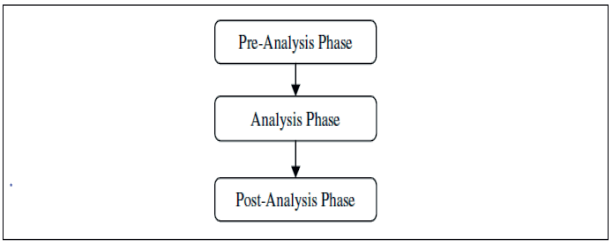

Figure 11:Common Process Model for Incident and Computer Forensics

2.3 Phase 3: 2008-2014

Perumal [19] proposed a model based on Malaysian Investigation Process in which more emphasis was given on "live data acquisition and static data acquisition" to focus on fragile evidence. It included steps of "Planning, Identification, Reconnaissance, Transport and Storage, Analysis, Proof and Defence and Archive Storage."

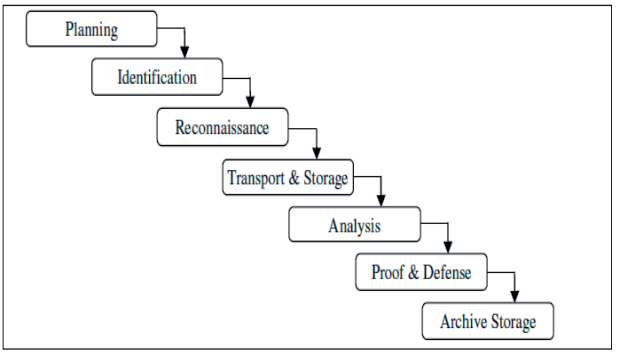

Figure 12: Digital Forensic Model based on Malaysian Investigation Process

The Digital Forensic Process Model proposed by Cohen [20] consists of seven listed processes or phases as "Identification, Collection, Transportation, Storage, Examination and Traces, Presentation and Destruction." Thus as we can see the focus of given model is on the examination of digital evidence.There is no need to include page numbers or running heads; this will be done at our end. If your paper title is too long to serve as a running head, it will be shortened. Your suggestion as to how to shorten it would be most welcome.

Agawal [21] established a systematic model for assisting forensic practitioners and organizations in making suitable strategies and processes .The proposed model suggests eleven stages and the diverse methods involved in the investigation of cyber fraud and cyber-crime -"Preparation, Securing the scene, Survey and Recognition, Documenting the scene, Communication Shielding, Evidence Collection, Preservation, Examination, Analysis, Presentation, Result and Review". The model emphasizes on study cases of cyber-crimes and computer frauds. The drawback of the model is that application of the model is limited to computer frauds and cyber-crimes only.

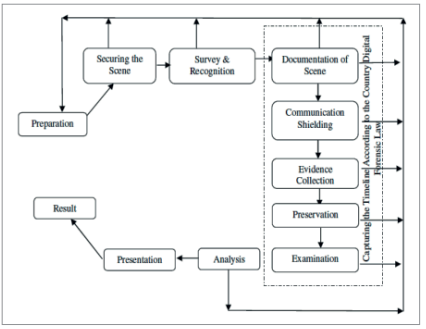

Figure 13: Systematic Digital Forensic Investigation Model

A new approach [22] was proposed by Ademu, Chris and David in which they the digital forensic investigation process was generalized into 4 tier iterative approach. The first tier will have 4 rules for digital forensic investigation which involves "preparation, identification, authorization and communication". The second tier has rules such as "collection, preservation and documentation", the third tier has rules consisting "examination, exploratory testing, and analysis" and the 4th tier which is the presentation phase has rules such as "result, review and report". The advantages of this model are that it identifies the need for interaction as well as exploratory testing but this model is ambiguous has not been tested, thus it is hypothesis only at present. It also does not mention clearly how the proposed model should be integrated with the forensic investigation process.

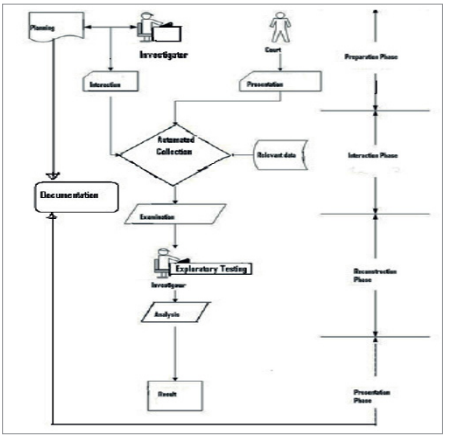

Figure 14:A New Approach of Digital Forensic Model for Digital Forensic Investigation

Valjarevic and Venter [23] defined a digital forensic investigation process model intended at harmonizing existing models. The model is quite similar to other models propsed by different authors as it is inclusive, but it differs from the others as it offers different placement of the phases and presents a new method for executing some of digital forensic principles through actionable items calls “parallel actions”. The proposed model comprises the following twelve phases: “incident detection, first response, planning, preparation, incident scene documentation, potential evidence identification, potential evidence collection, potential evidence transportation, potential evidence storage, potential evidence analysis, presentation and conclusion”. They propose a multi-tiered model which was built by accumulating a set of sub-phases. The drawback is that this model is yet to be verified for its accuracy and efficiency.

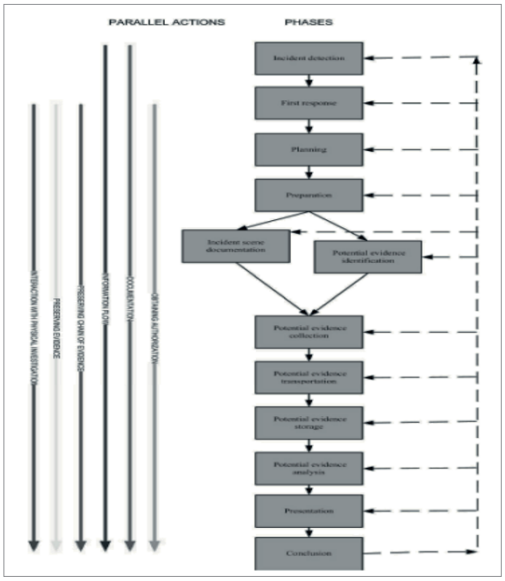

Figure 15:Harmonized Digital Forensic Investigation Process Model

The Integrated Digital Forensic Process Model [24] consists of the following processes: “preparation, incident, incident response, physical investigation, digital forensic investigation and presentation”. Numerous complications were recognized in the present models, such the same processes or steps being written by dissimilar names, or altered explanations of a phase. “Therefore, the IDFPM is not just a merging of existing DFPMs, but an integration of the discussed DFPMs and a purification of the terminology used, resulting in an all-encompassing standardized IDFPM” [24]. The disadvantage is that this model is not applicable everywhere as it was made by considering only a few of the forensic models.

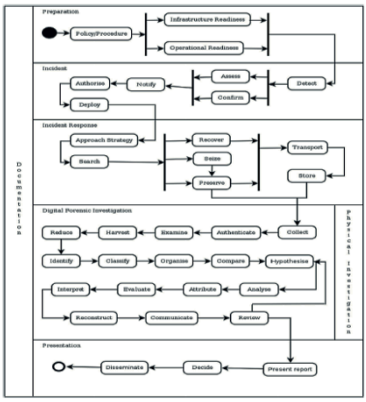

Figure 16: Integrated Digital Forensic Process Model

3 Conclusion

It has been over two decades since the first paper was published but we can see that much needs to be done in this field. This paper predicts an imminent predicament in digital forensics given the tremendous changes in technology. Other papers propose precise calculated capabilities that need to be developed looking at the future of forensics, this paper discusses the need to make digital forensics research more effective through the creation of new forensic models.

References

[1] Mark M. Pollitt. “Computer Forensics : An approach to Evidence in Cyberspace”. National Information System Security Conference.1995

[2] Farmer D.,Venema W. :” Computer Forensics Analysis Class Handouts.”1999

[3] Mandia K., Prosisse C. Incident Response. Osbourne/McGraw-Hill.2001

[4] Technical Working Group for Electrical Crime Scene Investigation. ”Electronic Crime Scene Investigation:A Guide for First Responders.”2001

[5] Digital Forensics Research Workshop. “A Road Map for Digital Forensics Research” 2001.

[6] Reith,M.,Carr,C., Gunsch,G., “An Examination of Digital Forensic Models”. International Journal of Digital Evidence, 2002.

[7] Carrier,B., Spafford,E. “Getting Physical with the Investigative Process”. International journal of Digital Evidence, 2003.

[8] Stephenson P. “A Comprehesive Approach to Digital Incident Investigation”. Elsevier Information Security Technical Report.2003.

[9] Ciardhuain,SO. “An Extended Model of Cybercrime Investigations”, International Journal of Digital Evidence.2004

[10] Baryamureeba V., Tushabe F. “The Enhanced Digital investigation Process Model”. DFRWS 2004.

[11] Beebe N., Clark J. “ A Hierarchical Objectives Based Framework for the Digital Investigations Process” DFRWS 2004.

[12] Carrier,B. , Spafford, E. “An Event based Digital Forensic Investigation Framework”. DFRWS 2004.

[13] Rubin,G.,Yun C., Gaertner,M. “Case-Relevance Information Investigation : Binding Computer Intelligence to the Current Computer Forensic Framework” International Journal of Digital Evidence. 2005.

[14] Erbacher Robert F., Christensen Kim, Sunderberg Amanda."Visual Forensic Techniques and Processes"2006.
[15] Kohn M., Eloff JHP., Olivier MS., "Framework for a Digital Forensic Investigation". Proceedings of Information Security South Africa(ISSA) 2006.
[16] Kent K., Chevalier S.,Grance T., Dang H. "Guide to Integrating Forensics into Incident Response"NIST Special Publication 800-86.2006.
[17] K.Rogers M., Goldman J., Mislan R., Wedge T. and Debrota S. "Computer Forensics Field Triage Process Model" Conference on Digital Forensics Security and Law.2006.
[18] Freiling F., Schwittay B. "A Common Process Model for Incident Response and Computer Forensics".Conference on IT Incident Management and IT Forensics.2007
[19] Perumal S. "Digital Forensic Model based on Malaysian Investigative Process" International Journal of Computer Science and Network Security .2009
[20] Cohen F. "Towards a science of Digital Forensic Evidence Examination".Advances in Digital Forensics VI,IFIP Advances in Information and Communication Technology,Springer.2010
[21] Agarwal A., Gupta M., Gupta S., Gupta C. "Systematic Digital Forensic Investigation Model"International Journal of Computer Science and Security.2011
[22] Ademu O., Chris O., David S. " A New Approach of Digital Forensic Model for Digital Forensic Investigation." International Journal of Advanced Computer Science and Application.2011
[23] Valjarevic A., Venter H. "Harmonized Digital Forensic Investigation Process Model.IEEE.2012
[24] Kohn M., Eloff M., Eloff JHP. "Integrated Digital Forensic Process Model" International Journal of Computer and Security 2013
[25] Daryabar F., Dehghantanha A., Nur Izura Udzir, Nor Fazlida binti Mohd Sani, Solahuddin bin Shamsuddin, Farhood Norouzizadeh F.,"A Survey about Impact of Cloud Computing on Digital Forensics" International Journal of Cyber-Security and Digital Forensics 2013.