Survey of Digital Forensic Models and Proposed Thematic Scheme

K. O. Peasah, Ebenezer Quayson, Osei Agyei, Ed. Danso Ansong
Kwame Nkrumah University of Science & Technology, Kumasi
Department of Computer Science

ABSTRACT
The internet and advanced technologies has been used as tools by criminals these days to perpetrate all forms of crime and the digital world is exploited to facilitate crimes which are mostly technology driven. The evidence of such crimes which are technologically driven are in digital form hence the need to employ techniques, procedures, and methodologies that are technology inclined to reconstruct events and uncover evidence that are admissible in court. Digital forensics therefore provides the investigative techniques, scientifically derived and proven methods for preserving, collecting, validating, identifying, analyzing, interpreting and presenting admissible digital evidence derived from digital source(s). Methods use to undertake forensic investigation is paramount since inappropriate model choice may result in incomplete or missing evidence. In this paper, we look at some commonly used models, their strength and weakness to inform investigators where to appropriately use those forensic investigation model(s) as well as a proposed scheme to aid the selection of the appropriate investigative model.

Keywords
Digital Forensic Models

1. INTRODUCTION
Advancement in technology and digital systems has to a large extent affected the modus operando of executing activities and task as well as the human computer interactivity. This advancement in technologies and tools has brought about pervasive and ubiquitous forms of computing allowing individuals to interact and communicate from anywhere and everywhere. Reith et al (2002) asserted that, the adept penetrative prowess of technological tools affecting the execution of activities in every human endeavor such as commercial, educational, governmental, healthcare and delivery. This emerging technologies though useful is also being employed as weapons to perpetrate diverse forms of crimes ranging from identity theft, credit card theft, fraud, denial of service attack, child pornography, etc.

Digital forensics however emerged in response to the escalation of crimes committed under the umbrella of anonymity provided by the technological environment. Digital forensic is a step – wise application of scientific methodologies or well – defined techniques to investigate crime(s) perpetuated with the aid of a digital devices or targeted at a digital device to retrieve evidence admissible at the court of law. In digital forensic investigation, the sanctity and integrity of the evidence herein referred to as digital evidence is very paramount thereby driving home the need to give a critical attention to the process or procedure used in the acquisition of the evidence. This notion is buttressed by Yusoff et al (2011) that, the results or outcome of the investigation varies directly with the processes or procedures adopted in the performance of a computer forensic investigation. When an inappropriate investigative processes are chosen or selected, it may result in producing incomplete or missing evidence. Moreover, trespassing a phase or switching any of the steps may lead to inconclusive results; thereby resulting in an invalid conclusions which threatens the admissibility of the evidence in the court of law.

This paper begins with a review of some notable existing digital forensics investigative models, analyze those existing model to identify the strength and some weakness inherent in those investigative models, formulate a schematic framework to guide the selection of an investigative model.

2. LITERATURE REVIEW
In this section, notable digital forensic investigative models and frameworks were strategically selected to cover some reasonable time period and good appreciation of developments carried out in the digital forensic discipline.

2.1 Kruse and Heiser Model
Also known as the Lucent Model, this model was developed by Kruse et al (2001) and popularly christened the "3As". Thus, the model has three phases which are Acquisition, Authenticating and Analysis phases. Pivotal to this model is the need to ensure data integrity and validity, hence the following guidelines were enumerated;

i. Acquire evidence without alteration or damage to the original evidence

ii. Authentication of the recovered evidence to ensure consistency with the data originally seized.

iii. Analyze the data without modification ensuring integrity

This model therefore calls for full and proper documentation of the investigation process as a way of attaining integrity of the data and also to correctly reverse the process in case of any eventually.

Advantages

1. It aims at retrieving data of evidential value whilst ensuring its integrity and validity
2. It is a simple model with few number of phases

Disadvantages
The phases within the model appear to be silence on the presentation and admissibility of the evidence in the court of law.

2.2 US Department of Justice (USDOJ) model
Is a four step – wise model comprising of the collection, examination, analysis and reporting phases. The collection phase deals with the acquisition of diverse forms of evidence, the examination phase performs retrieval of digital evidence

of probative value from the collected evidence. The interpretation of the results derived from the examination phase with the aid of appropriate techniques and methodologies is performed at the analysis phase. The fourth and final stage include activities such as presentation of evidence, tools and procedures used as well as formulation of guidelines and recommendation for improvements if any.

Advantages

1. Inculcates a phase which deals with the presentation of results at the court of law
2. Phases analogous to the Kruse and Weiser model thereby reducing the level of difficulty in usage

Disadvantages

The model is not exhaustive with respect to other forms of digital technologies. Eg: Cyber computing, Internet of Things (IoTs), etc.

2.3 DFRWS model

The Digital Forensics Research Workshop (DFRWS) in 2001 was the first large – scale consortium spear – headed by the academia encompassing, Digital Forensics researchers, practitioners, security institutions as well as civilians. The (DFRWS, 2001) developed a forensics investigation framework or model consisting of six (6) phases, namely: Identifying, presenting, collecting, examining, analyzing and presenting. The model is presented in a tabular form with each column consisting of cells depicting the various activities undertaken at that stage or phase.

Advantages

1. It provides a standard and consistent forensic framework
2. Serve as a framework on which other forensic models are developed
3. Ease of use and easily comprehensible by both technical and non – technical users

Disadvantages

Due to its general nature, it becomes relatively difficult to test and implement. Moreover, it appear to be a bit rigid.

2.4 Abstract Digital Forensics Model (ADFM, 2002)

Reith et al (2002) prosposed the Abstract Digital Forensics Model (ADFM) which was both an inspiration from and enhancement of the Digital Forensic Research Workshop (DFRW) model. The ADFM model introduced three new phases (Preparation, Approach Strategy and Returning Evidence) to six (6) phases in the DFRW model making the ADFM a model with nine(9) phases which are; Identification, Preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation and Returning Evidence.

This model starts with the **Identification** phase where the type of incident is determined based on the indicators recognized from the incident. The **Preparation** phase deals with tools and technique preparation, search warrants, and monitoring authorizations and management support to further investigation. Then is the **Approach Strategy** phase with the aim of maximizing the collection of untainted evidence while minimizing impact to the victim. Next is the **Preservation** phase where activities such as isolation, securing and preserving the state of physical and digital evidence are undertaken. With the **Collection** phase, the physical scene and duplicate digital evidence is recorded using standard and acceptable procedures. In – depth procedural search of evidence relating to the suspected crime is undertaken at the **Examination** phase to prepare detailed documentation for analysis. Following the Examination phase is the **Analysis** phase which determine significance, reconstruct fragments of data and draw conclusions based on evidence found and also to support a crime theory. In the **Presentation** phase, findings are collated to provide explanation of conclusions which is mostly done in such a way that a layperson can comprehend and finally the **Returning Evidence** phase which ensure physical and digital property is returned to proper owner and determining what criminal evidence must be removed.

Advantages

1. Diverse methodology suitable for array of digital devices
2. This methodology can easily be appreciated by non – technical observers
3. Potential for incorporating non-digital, electronic technologies within the abstraction

Disadvantages

1. The generality of the model may pose some practical challenge.
2. There is no easy or obvious methodology for testing the model

2.5 Integrated Digital Investigation Process (IDIP)

This model proposed by Brain et al (2003) perceived a crime scene as both physical and digital integrated together to identify person(s) responsible for the digital activity. The authors of the paper undoubtedly admitted that while digital investigations have recently become prevalent, clues and experiences from physical investigations which has existed thousands of years ago could be co – opted to augment digital investigations.

According to the paper, a digital environment is created by the software and hardware as oppose to the school of thought which considers every crime scene with a computer or other digital device as a computer crime scene.

This process model encompasses seventeen (17) phases organized into five (5) groups which are the readiness phase, deployment phase, physical crime scene investigation phase, digital crime scene investigation phase and the review phase.

Discussion

It is an out and out model which considers the dual investigative nature of the digital forensic investigation by including the digital and the physical crime scene investigation phases. The model envisaged that although the crime was perpetrated using a digital device as a means or target, the forensic investigation encompass both physical and digital crime scenes hence the need to include them in the investigations.

Replication in digital environment is relatively easier, making it easier to create a complete forensically sound image backup for analysis in the lab. Unlike many process models that focus primarily on the digital evidence, the interaction existing between the digital and physical environment is vividly highlighted in this model.

2.6 The Enhanced Digital Investigation Process Model (EDIP)

EDIP, developed by Venansius et al (2004) is an investigative model hinged on the expansion of the deployment phase in the Brian et al (2003) IDIP model. The EDIP model has two categories of crime scenes which is the suspect's or the primary crime scene and the victim's or the secondary crime scene.

This model has five major phases namely, readiness, deployment, trace back, dynamite and review. The model starts with the readiness phase which deals with operations and infrastructure readiness, the needed human capacity is properly trained and equipped to deal with the situation. The **deployment** phase provides mechanism for the detection and confirmation of an incident. This phase has five sub – phases which includes detection and notification, physical crime scene, digital crime scene, confirmation and the submission sub – phases. The **traceback** phase tracks down the operations of the suspect's physical crime scene and has two sub – phases; digital crime scene investigation and authorization phase. Succeeding the traceback phase is the **Dynamite** phase which conducts investigation at the primary crime scene with the aim of collecting and analyzing items that were discovered at the scene to enhance the apprehension of potential culprits. The entire investigative process is reviewed and possible areas of improvement is identified in the **Review** phase.

Advantages

1. The model provides a wide spectrum to include electronic and non – digital technologies.
2. Create consistent and standardized framework for digital forensic development
3. This investigative model framework is suitably applicable to future digital technologies.

Disadvantages

1. Additional sub – phases introduces some ambiguity with respect to the activities performed.
2. There seems to be duplication of activities. E.g. Digital crime scene investigation activity appears under the Deployment phase, Traceback phase, as well as Dynamite phase.

2.7 Computer Forensics Field Triage Process Model (CFFTPM)

Rogers et al (2006) proposed this model as a technique targeted at on the site or field investigation for identifying, analyzing and interpreting digital evidence in a short time frame.

The three basic components of forensic investigation by Kruse II et al (2002) also called the "3As" of computer forensics investigation guided the formulation of CFFTPM foci which is; immediately finding relevant evidence, identifying victims at minimal risk, providing guidance for an ongoing investigation, in order to identify potential charges and accurately assessing the danger of the danger and the perpetrator(s) to society while at the same instance protecting the integrity of the evidence. The CFFTPM has six (6) main phases with two (2) of the phases having three (3) sub – phases each and these are, Planning, Triage, User Usage Profile (Home, File Properties, Registry), Chronology Timeline, Internet (Browser, Email, IM) and Case Specific.

This model begins with the **planning** phase where formulation of some indicators and directions highly probable to result in successful investigation. After the Planning phase is the **Triage** phase where priority based activities are executed. Hence items, pieces of evidence or potential containers of evidence that are highly important or the most transient are first dealt with. In the **User Usage Profile** phase, actual examination and analysis is performed on evidence found on digital media in order to link the evidence to a specific, identifiable suspect. **Chronology Timeline** phase deals with the reconstruction of events in a chronological manner to sequence the probable crime activities mostly by using some timing model such as the MAC (Modification, Access and Creation) times. With the **Internet** phase, examination of artifacts related to internet activity such as Instant Messaging (IM), e – mail and web browsing is performed. The final phase is the **Case Specific Evidence** phase whose success largely depends on the competence of the investigator as well as the application of the appropriate model to the investigation. Also, adjustments are made to the focus of the examination and possible reconciliation of conflicting requirements are done in a manner to suit each specific set of circumstances.

Advantages

1. This model is much concerned about time, hence help to undertake quick information and investigation in a time critical situations.
2. This model is used to conduct investigation on scene which provides additional benefit of having feedback loop with the investigator(s).
3. It also affords computer forensics analyst to modify their searches right on the scene based on input from the primary investigator(s) as well as those in direct contact with the suspect.

Disadvantages

1. This model is only appropriate for investigation conducted at the scene
2. It may be seen as an incomplete investigative model should the case under investigation require additional work to be done off the scene.
3. There is a likelihood of compromising evidence in the usage of this model, due to its time critical nature.

2.8 Generic Computer Forensics Investigation Process Model (GCFIPM)

Yusoff et al (2011) proposed a five (5) generic grouped phase forensic investigation model known as the Generic Computer Forensics Investigation Process Model after reviewing existing forensics investigation models.

The Pre – process phase deals with activities that are carried out prior to the actual investigation and official collection of data such as getting the necessary approval from relevant authority, etc. Under the Acquisition & Preservation phase, tasks related to identifying, collecting, transporting, storing and preservation are performed. Next is the Analysis phase which is considered as the core of the forensic investigation processes and various types of analysis are performed on the acquired data to identify the crime source and possibly the perpetrator of the crime. The Presentation phase is were various outcomes of the Analysis phase are documented and presented to authority in a format which is easily understood and mostly backed by sufficient and acceptable evidence.

Finally is the Post – Process phase where proper closing of the investigation exercise is done, rightfully owners are given the needed digital and physical evidence and review of the investigation process is done for lessons to learnt and improvement be done for future investigations.

Advantages
This model puts phases of several models into groups making the model suitable or applicable to diverse types of forensics investigations. The model serves as a broad or generic framework which can provide a good starting point for the development of new digital forensics investigation model.

Disadvantages
The phases within this model was formed by grouping phases of other models which eventually introduces duplicate activities in the grouped phases. Due to the generalized nature of this model, it is considered more of a guideline framework than a model.

3. COMPARATIVE ANALYSIS

This section makes a comparative analysis of the some existing digital forensic models. Forensic process models defined by different researchers consisted of multiple steps with some process models having limited number of steps while others have elaborative number of steps. However, the number of steps or phases within a forensic model is not an indication of the usefulness or otherwise of the process model.

Kruse& Heiser	**USDOJ**	**DFRWS**	**ADFM**	**IDIP**	**EDIP**	**CFFTPM**	**GCFIPM**
2001	2001	2001	2002	2003	2004	2006	2011
3 Phases	4 Phases	6 Phases	9 Phases	5 Phases	5 Phases	6 Phases	5 Phases
Acquiring Evidence	Collection	Identification	Identification	Readiness	Readiness	Planning	Pre – process
Authenticating Evidence	Examination	Preservation	Preparation	Deployment	Deployment	Triage	Acquisition & Preservation
Analyzing Evidence	Analysis	Collection	Approach Strategy	Physical Crime Scene Investigation	Trace back	User usage Profile	Analysis
	Reporting	Examination	Preservation	Digital Crime Investigation Scene	Dynamite	Chronology Timeline	Presentation
		Analysis	Collection	Presentation	Review	Internet	Post – process
		Presentation	Examination			Case specific	
			Analysis				
			Presentation				
			Returning evidence				

4. PROPOSED SCHEMATIC MEASURE

As earlier stated, the relevance of a forensic model is not dependent of the number of steps or phases. Hence, to select a suitable digital forensic investigation model we recommend the following guidelines;

i. The nature of digital evidence is complex, delicate and mostly volatile in nature.

ii. The relevant of the digital evidence is mostly time bound

iii. The aim of the digital evidence is to be admissible in a court of law, hence the need to preserve its integrity before, during and even after the forensic investigation.

In line with these guidelines, an ideal or suitable digital forensic model should meet the proposed schematic measure which consist of the following phases;

1. Detection and Notification phase which deals with the determination or detection of possible digital crime and triggering the right alert.
2. Pre – Analysis phase encompass activities such as selection of appropriate tools, methodologies and personnel, securing search warrants as well as the securing crime scene and preservation of the integrity of the evidence.
3. Acquisition phase deals with the collection and retrieval of forensically sound digital evidence while maintaining its integrity
4. Analysis & Interpretation phase deals with the examination of the evidence retrieved and reporting or presenting it in a suitable manner comprehensible to both technical and non – technical users.
5. Securing Evidence phase deals with post investigation activities aimed at properly and securing storing the evidence, maintaining its integrity to augment and direct future investigations.

5. CONCLUSION

The development of several forensics investigation models is

to provide a well-tailored, accurate and efficient means of acquiring, authenticating and analyzing digital evidence while ensuring the integrity and sanctity of the evidence to make it admissible in court of law. However, these models are not without some inherent shortfalls. This paper reviewed and analyzed some common forensics investigation models, enumerated some advantages and disadvantages associated with those models to serve as a guide to investigators in choosing the appropriate model(s) which will yield maximum result with respect to the case under investigation.

6. REFERENCES

[1] Brian, C. and Eugene, H. S. (2003). Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, Fall 2003, Volume 2, Issue 2.

[2] Gary, L. P. (2001). A Road Map for Digital Forensic Research. Technical Report DTR – T0010-01, DFRWS. Report for the First Digital Forensic Science Communications, Vol. 2 No. 4

[3] Kruse II, W. and Jay, G. H. (2002). Computer Forensics: Incident Response Essentials. Addison – Wesley.

[4] Lee, H., Palmbach, T., Miller, M. (2001). Henry Lee's Crime scene Handbook. London: Academic Press

[5] Marcus, K. R., James, G., Rick, M., Timothy, W. and Steve, D. (2006). Computer Forensics Field Triage Process Model. Journal of Digital Forensics, Security and Law, Vol. 1 No. 2

[6] Mark, R., Clint, C. and Gregg, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, Fall 2002, Volume 1, Issue 3.

[7] Michael, N., Mark, M. P. and Lawrence, P. (2000). Recovering and Examining Computer Forensic Evidence, Forensics Science Communications, Vol. 2, No. 4

[8] Technical Working Group Electronic Crime Scene Investigation – A Guide for First Responders, USDOJ, July 2001

[9] Venansius, B., and Florence, T. (2004). The Enhanced Investigation Process Model, in proceeding of Digital Forensic Research Workshop, Baltimore, MD.

[10] Yunus, Y., Roslan, I. and Zainuddin, H. (2011). Common Phases of Computer Forensics Investigative Models. International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No. 3.