Asian Journal of Information Technology 5(7): 790-794, 2006

The Enhanced Digital Investigation Process Model

Venansius Baryamureeba and Florence Tushabe
Institute of Computer Science, Makerere University P.O.Box 7062, Kampala Uganda

Abstract: Computer crimes are on the rise and unfortunately less than two percent of the reported cases result in conviction. The process (methodology and approach) one adopts in conducting a digital forensics investigation is immensely crucial to the outcome of such an investigation. Overlooking one step or interchanging any of the steps may lead to incom-plete or inconclusive results hence wrong interpretations and conclusions. A computer crime culprit may walk Scot-free or an innocent suspect may suffer negative consequences (both monetary and otherwise) simply on account of a forensics investigation that was inadequate or improperly conducted. In this study, we present a brief overview of forensic models and propose a new model based on the Integrated Digital Investigation Model.

Key words: Computer forensics, crime scene investigation, forensic process model, Abstract digital forensic model, integrated digital investigation model

INTRODUCTION

Computer forensics emerged in response to the escalation of crimes committed by the use of computer systems either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime. Computer forensics can be traced back to as early as 1984 when the FBI laboratory and other law enforcement agencies begun developing programs to examine computer evidence. Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE) and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a 1discipline including the need for a standardized approach to examinations[1].

Digital forensics has been defined as 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 anticipate the unauthorized actions shown to be disruptive to planned operations[2]. One important element of digital forensics is the credibility of the digital evidence. Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines etc. The legal settings desire evidence to have integrity, authenticity, reproductivity, non-interference and minimization.

Since computer forensics is a relatively new field compared to other forensic disciplines, which can be traced back to the early 1920s, there are ongoing efforts to develop examination standards and to provide structure to computer forensic examinations. This paper attempts to address the methodology of a computer forensic investigation.

PREVIOUS WORK

Computer and network forensics methodologies consist of three basic components that Kruse and Heiser[3] refer to as the three As of computer forensics investigations. These are: acquir-ing the evidence while ensuring that the integrity is preserved; authenticating the validity of the extracted data, which involves making sure that it is as valid as the original and analyz-ing the data while keeping its integrity. Some process models that put the three factors into consideration include the Forensics Process Model[4], the Abstract Digital Forensics Model[5] and the Integrated Digital Investigation Model[6].

The forensics process model: The U.S. Department of Justice published a process model in the Electronic Crime Scene Investigation: A guide to first responders[4] that consists of four phases:

- **Collection:** Which involves the evidence search, evidence recognition, evidence collection and documentation.
- **Examination:** This is designed to facilitate the visibility of evidence, while explaining its origin and significance. It involves revealing hidden and obscured information and the relevant documentation.

Corresponding Author: Venansius Baryamureeba, Institute of Computer Science, Makerere University P.O. Box 7062, Kampala Uganda

- **Analysis:** This looks at at the product of the examination for its significance and pro-bative value to the case.
- **Reporting:** This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation.

The analysis phase of this model is improperly defined and ambiguous. It for instance emerges as an interpretation of the results from the examination phase and in the process confuses analysis with interpretation despite these being two distinct processes.

The abstract digital forensics model: The Abstract Digital Forensics model[5] proposes a standardized digital forensics process that consists of nine components:

- **Identification:** Which recognizes an incident from indicators and determines its type.
- **Preparation:** Which entails the preparation of tools, techniques, search warrants and monitoring authorizations and management support.
- **Approach strategy:** That develops a procedure to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim.
- **Preservation:** Which involves the isolation, securing and preservation of the state of physical and digital evidence.
- **Collection:** That entails the recording of the physical scene and duplicate digital evi-dence using standardized and accepted procedures.
- **Examination:** Which involves an in-depth systematic search of evidence relating to the suspected crime.
- **Analysis:** Which involves determination of the significance, reconstructing fragments of data and drawing conclusions based on evidence found.
- **Presentation**: That involves the summary and explanation of conclusions.
- **Returning evidence:** That ensures physical and digital property is returned to proper owner.

Although this model is generally a good re ection of the forensic process, it is open to at least one criticism. Its third phase (the approach strategy) is to an extent a duplication of its second phase (the preparation phase). This is because at the time of responding to a notification of the incident, the identification of the appropriate procedure will likely entail the determination of techniques to be used.

The Integrated Digital Investigation Model(IDIP): Brian Carrier and Eugene Spafford[6] proposed yet another model that organizes the process into five groups consisting all in all 17 phases.

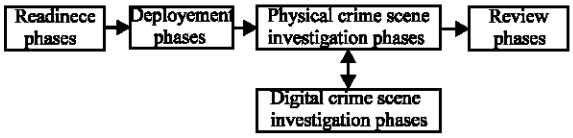

Fig. 1: Phases of the IDIP model

Readiness phases: The goal of this phase is to ensure that the operations and infrastructure are able to fully support an investigation. It includes two phases:

- **Operations Readiness phase:** Which ensures that human capacity is fully trained and equipped to deal with an incident when it occurs.
- **Infrastructure readiness phase:** That ensures that the underlying infrastructure is suf-ficient enough to deal with incidents that come. For example equipment like video cameras and card readers being there and in good working condition.

Deployment phases: The purpose is to provide a mechanism for an incident to be detected and confirmed. It includes two phases:

- **Detection and Notification phase:** Where the incident is detected and then appropriate people notified.
- **Confirmation and Authorization phase:** Which confirms the incident and obtains au-thorization for legal approval to carry out a search warrant.

Physical crime scene investigation phases: The goal of these phases is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident. It includes six phases:

- **Preservation phase:** Which seeks to preserve the crime scene so that evidence can be later identified and collected by personnel trained in digital evidence identification.
- **Survey phase:** That requires an investigator to walk through the physical crime scene and identify pieces of physical evidence.
- **Documentation phase:** Which involves taking photographs, sketches and videos of the crime scene and the physical evidence. The goal is to capture as much information as possible so that the layout and important details of the crime scene are preserved and recorded.
- **Search and collection phase:** That entails an in-depth search and collection of the scene is performed so that additional physical evidence is identified and hence paving way for a digital crime investigation to begin.

- **Reconstruction phase:** Which involves organizing the results from the analysis done and using them to develop a theory for the incident.
- **Presentation phase:** That presents the physical and digital evidence to a court or cor-porate management.

Digital crime scene investigation phases: The goal is to collect and analyze the digital evidence that was obtained from the physical investigation phase and through any other future means. It includes similar phases as the Physical Investigation phases, although the primary focus is on the digital evidence. The six phases are:

- **Preservation phase:** Which preserves the digital crime scene so that evidence can later be synchronized and analysed for further evidence.
- **Survey phase:** Whereby the investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location.
- **Documentation phase:** Which involves properly documenting the digital evidence when it is found. This information is helpful in the presentation phase.
- **Search and collection phase:** Whereby an in-depth analysis of the digital evidence is performed. Software tools are used to reveal hidden, deleted, swapped and corrupted files that were used including the dates, duration, log file etc. Low-level timelining is performed to trace a user's activities and identity.
- **Reconstruction phase:** Which includes putting the pieces of a digital puzzle together and developing investigative hypotheses.
- **Presentation phase:** That involves presenting the digital evidence that was found to the physical investigative team.

Review phase: This entails a review of the whole investigation and identifies areas of improvement.

The IDIP model does well at illustrating the forensic process and also conforms to the cyber terrorism capabilities[7] which require a digital investigation to address issues of data protection, data acquisition, imaging, extraction, interrogation, ingestion/normalisation, analysis and reporting. It also highlights the reconstruction of the events that led to the incident and emphasizes reviewing the whole task, hence ultimately building a mechanism for quicker forensic examinations.

However, the IDIP model is open to some criticisms. First, despite encompassing all the earlier models, there is reason to question the IDIP model's practicality. It for instance depicts the deployment phase which consists of confirmation of the incident as being indepen-dent of the physical and digital investigation phase. In practice however, it seems impossible to confirm a digital or computer crime unless and until some preliminary physical and digital investigation is carried out. Secondly, it does not offer sufficient specificity and does not, for instance, draw a clear distinction between investigations at the victim's (secondary crime) scene and those at the suspect's (primary crime) scene. Neither does it re ect the process of arriving at the latter. Since a computer can be used both as a tool and as a victim[8] , it is common for investigations to be carried out at both ends so that accurate re ections are made. Henry Lee[9] defines the primary crime scene as the place where the first criminal act occurred. The process of tracing back to it can be challenging when dealing with larger networks and in particular, the Internet[8].

THE PROPOSED MODEL

Definitions

Physical crime scene investigation: This is the investigation that takes place at the physical crime scene. A physical crime scene is defined as the physical environment where physical evidence of a crime or incident exists[6]. Building from[6,10] discussions, we propose that the physical crime scene investigation includes five phases:

- **Preservation phase:** Which preserves the crime scene so that evidence can be later identified and collected by personnel trained in digital evidence identification. It would consist of securing and protecting the crime scene while identifying, removing and separating the witnesses from the scene.
- **Survey phase:** Whereby an investigator walks through the physical crime scene, iden-tifies the pieces of physical evidence, determines the extent of the search, develops a preliminary theory, identifies potential evidence and documents a narrative.
- **Documentation phase:** Which would involve taking photographs, sketches and videos of the crime scene and the physical evidence. The goal is to capture as much information as possible so that the layout and important details of the crime scene are preserved and recorded.
- **Search and collection phase:** Is when an in-depth search and collection of the scene is performed so that additional potential physical evidence is identified and hence paving way for a digital crime investigation to begin.

- **Presentation phase:** Where the identified electronic evidence is transported and deliv-ered to the digital investigation team.

Digital crime scene investigation: This is the investigation that will be made to the digital crime scene. The digital crime scene has been defined as the virtual environment created by software and hardware where digital evidence of a crime or incident exists[6]. Building from[6,10] discussions, we propose that the digital crime scene investigation includes four processes:

- **Preservation phase:** Which preserves the digital crime scene so that evidence can be later synchronized and analysed for further evidence. Duplication of evidence (creation of bit-by-bit copies of the seized data) should be performed for use in multiple analysis.
- **Survey phase:** Whereby the investigator identifies and separates potentially useful data from the imaged dataset; forexample the recovery of damaged, hidden, deleted, or manipulated data.
- **Search and collection phase:** Whereby an in-depth analysis of the digital evidence is performed. Software tools are used to reveal hidden, deleted, swapped and corrupted data. Fusion, correlation, graphing, mapping and timelinning of data or files that were used is performed while various investigative hypotheses are developed.
- **Documentation phase:** Involves properly documenting the digital evidence when it is found. This information is helpful in the presentation phase.

Phases of the EIDIP model: The proposed EIDIP model consists of five major phases:

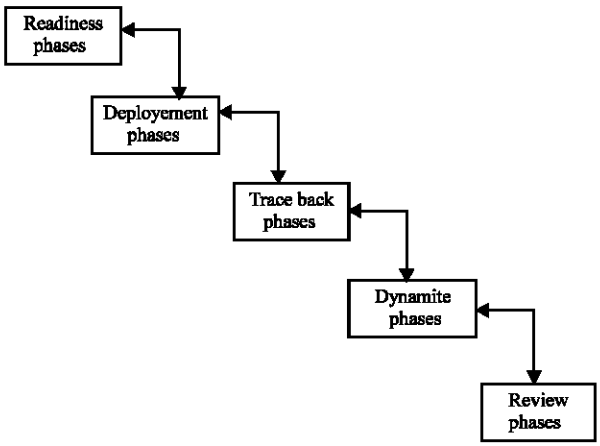

Fig. 2: Phases of the EIDIP model

Readiness phases: These phases are described in Sub-section 2.3.1 on page 3.

Deployment phases: The deployment phases provide a mechanism for an incident to be detected and confirmed. They take place at the place where the crime was detected and consist of five phases:

- **Detection and Notification phase:** When an incident is detected and the appropriate people notified.
- **Physical Crime Scene Investigation:** When a physical examination of the scene is per-formed and potential digital evidence identifified.
- **Digital crime scene investigation phase:** When an electronic examination of the scene is performed and digital evidence obtained with possibly an estimation of the extent of the impact or damage.
- **Confirmation phase:** When the incident is confirmed and authorization given to obtain legal approval to carry out a search warrant and further investigations at suspect premises.
- **Submission phase:** Which involves presenting the physical and digital evidence to legal entities or corporate management.

Traceback phases: Within these phases, the perpetrator's physical crime scene of operation is tracked down leading to identification of the devices that were used to perform the act. They consist of:

- **Digital crime scene investigation:** Whereby primary crime scene is traced from the clues obtained from the previous phases. Forexample acquiring public and private IP addresses and mapping them to the country and instituion will eventually lead to the host computer. IP addresses can be easily obtained by using the following commands: ping, nslookup, dig, tracert from a DNS server[11]. Locating the country and institution is simplified by various tools and websites like ip-to-location.com and whatismyipaddress. net[12,13].
- **Authorization phase:** When authorization from local legal entities is obtained to permit further investigations and access to more information.

Dynamite phases: These phases investigate the primary crime scene.They aim at collecting and analysing the items that were found at the primary crime scene to obtain further evidence that the crime originated from there and they help identify the potential culprits. They would consist of:

- **Physical Crime Scene Investigation phase:** When a physical examination of the scene is carried out to identify potential digital evidence.
- **Digital crime scene investigation phase:** When an electronic examination of the scene is performed to obtain digital evidence of the incident and possibly an estimation of the time and dates when the incident was launched.
- **Reconstruction phase:** That includes putting the pieces of a digital puzzle together and identifying the most likely investigative hypotheses.
- **Communication phase:** Which involves presenting the final interpretations and conclu-sions about the physical and digital evidence that has been investigated to a court or corporate management.

Review phase: The whole investigation is reviewed and areas of improvement identified.

DISCUSSION

The Enhanced Digital Investigation model (EIDIP) separates the investigations at the pri-mary and secondary crime scenes while depicting the phases as iterative instead of linear. It is based on the IDIP model and expands the deployment phase in the IDIP model to include the physical and digital crime investigations while introducing a new phase dedicated to tracing back to the computer(the primary crime scene) that was used as a tool to commit the offense. In this proposed model the reconstruction is only made after all investigations have taken place instead of having two reconstructions which might be inconsistent.

CONCLUSION

The Enhanced Integrated Digital Investigation Process (EIDIP) model is an enhanced version of the Integrated Digital Investigation Process Model and seeks to redefine the forensic process and its progression. It describes the development right from the point when the initial infrastructure is put in place, to investigations when the incident is reported, through the traceback phases that would lead to the point where the crime was committed and finally to the ultimate investigations that would lead to conclusive interpretations of the evidence collected. Thus EIDIP model is suitable for cyber crime investigations.

REFERENCES

1. Noblett, M., M.P. Mark and P. Lawrence, 2000. Recovering and ex-amining computer forensic evidence, Forensic Science Communications, pp: 2.
2. Gary L. And Palmer, 2001. A road map for digital forensic research. Technical Re-port DTR-T0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).
3. Kruse, I.I., Warren and Jay, G. Heiser, 2002. Computer forensics: Incident Re-sponse Essentials. Addison-Wesley.
4. National Institute of Justice, 2001. Electronic crime scene investigation. A Guide for First Responders. http://www.ncjrs.org/pdffiles1/nij/187736.pdf.
5. Reith, M., C. Clint and G. Gregg, 2002. An Examination of digital foren-sic models. Intl. J. Digital Evidence, pp: 1.
6. Carrier, B. and E.H. Spafford, 2003. Getting physical with the investiga-tive process, Intl. J. Digital Evidence, pp: 2.
7. National Institute of Justice, 2002. Results from tools and technology working group, Governors Summit on Cybercrime and Cyberterrorism, Princeton NJ.
8. Kizza, J.M., 2003. Ethical and Social Issues in the Information Age, 2nd Edn., Springer .
9. Lee, H., P. Timothy and M. Marilyn, 2001. Henry Lee's Crime Scene Handbook, Academic Press.
10. Criminal Justice Academy notes available at http://scdps.org/cja/csr-csmgmt.htm.
11. Michael Pastore, 2003. Security, Study Guide,SYBEX Inc
12. http://www.ip-tp-location.com
13. http://whatismyipaddress.net.