A Model for Hybrid Evidence Investigation

K. Vlachopoulos, E. Magkos and V. Chrissikopoulos

Department of Informatics, Ionian University
Plateia Tsirigoti 7, 49100, Corfu, Greece
e-mail: {kostasv, emagos, vchris}@ionio.gr

Abstract

With the advent of Information and Communication Technologies, the means of committing a crime and the crime itself are constantly evolved. In addition, the boundaries between traditional crime and cybercrime are vague: a crime may not have a defined traditional or digital form since digital and physical evidence may coexist in a crime scene. Furthermore, various items found in a crime scene may worth be examined as both physical and digital evidence. In this paper, a model for investigating such crime scenes with hybrid evidence is proposed. Our model unifies the procedures related to digital and physical evidence collection and examination, taking into consideration the unique characteristics of each form of evidence. Our model can also be implemented in cases where only digital or physical evidence exist in a crime scene.

Keywords

Physical forensics, digital forensics, crime investigation models

1. Introduction

Crime is an undisputable part of every society. During the centuries crime has been developed and so did crime investigation techniques. In the 20th century the need for investigating crime in a more accurate way has introduced forensic science, focusing on the collection and examination of evidence connected to a crime. In the 80's-90's the proliferation of computing and Internet technologies has broadened the means of committing a crime. Nowadays, the majority of conventional crime investigations face the need to search for extra evidence that may have been stored in digital form or been produced by digital devices. For example, offenders of the -so called- traditional crimes, like homicides or rapes, may have used the Web, e-mail, or cellular communication services to collect and transfer information related to the crime. Examining this evidence can for example produce valuable information about a crime, the motives of the offenders, the relationship between the offender and the victim, the accomplices of the offender. As a result, digital forensics flourished, becoming the key player in the battle against crime. (Reith *et al.*, 2002; Palmer, 2002; Vlachopoulos, 2007; Beebe, 2009; Garfinkel, 2010; Agarwal *et al.*, 2011).

In this cyber-physical environment it becomes extremely difficult to collect every single scratch of evidence or to find a specific piece of evidence. In the digital investigation field for example, a number of challenges need to be studied and addressed (Sheldon, 2005; Beebe, 2009; Garfield, 2010), including: The decreasing

size of storage devices which makes the creation of a forensic image or the processing of the data they contain, challenging; the expansion of malware stored in RAM that demands the development of specialized RAM forensics tools; the proliferation of smartphones and pervasive computing technologies that extend the need to search for evidence in a variety of new digital devices or physical items with embedded systems-on-chip (SOC), *e.g.*, clothes; the use of cloud computing technologies so that evidence cannot be found in a single computer or network and may be stored and/or processed outside the legal jurisdiction; legal issues related to security and privacy that influence both physical and digital investigation and the admissibility of collected evidence.

The growing role of digital evidence to support conventional criminal evidence also illustrates the need for law enforcement agencies to adopt new investigation methods. Up to now, most investigation models deal with only physical or only digital evidence, thus imposing a clear separation. For example U.S. National Institute of Justice (2000) manual about the crime scene investigation and Lee's *et al.* (2001) Scientific Crime Scene Investigation Model do not include specifications about digital evidence and their role in the documentation of a case. Even the U.S. National Institute of Justice Special Report for electronic crime scene investigation (2008), focuses mainly on procedures concerning digital devices and not on the interpretation of the data they contain. On the other hand, state-of-the-art digital forensic models do not sufficiently pay much attention to physical evidence which is also very important for a case. (Palmer, 2001; Carrier and Spafford, 2003; Ciardjuain, 2004; Rogers *et al.*, 2006; Agarwal *et al.*, 2011; Yusoff *et al.*, 2011).

We believe there is often a constant interaction between digital and physical evidence in a crime scene and novel investigation strategies should be pursued, aiming to avoid the loss of crucial evidence, physical or digital. For example, if an operating computer is used only as a source of physical evidence (for example fingerprints), there is the danger of losing volatile data or terminating a running process by an accidental move of the mouse or a keystroke. On the other hand if a computer is faced only as a source of digital evidence it is possible to miss physical evidence like fingerprints and DNA which could be collected from the surface or the internal of a computer or peripheral device. Furthermore, various items found in a crime scene may worth be examined as both physical and digital evidence *e.g.*, a printed paper which can be related to a specific printer, personal computer, flash memory etc, or a piece of clothes with an embedded system-on-chip (SOC) which may contain important data about the case under investigation. Clearly, dealing with hybrid evidence in a crime scene requires law-enforcement agencies to use a combination of physical and digital forensics methods and techniques.

Our Contribution. In this paper we propose a model for hybrid evidence investigation where both digital and physical evidence may co-exist in a crime scene. The novelty of the proposed model is that we do not discriminate between physical and digital evidence investigation, but instead we consider all evidence types potentially present in most crime investigations. Our model extends the traditional physical crime scene investigation models which law enforcement agencies use for

decades to incorporate the digital environment. An important feature of the model is that it can also be used in crime scenes where only digital or physical evidence exist.

2. Related work

Crime investigation theory remains an open field of research as offenders find new ways to commit crimes. In law enforcement investigations, commonly accepted procedures are implemented by most agencies around the world. For instance a typical investigation includes the following basic steps (Vlachopoulos, 2007): Police are notified about a crime; after the necessary preparation an investigation takes place at the crime scene; the scene is secured, a thorough search for evidence is contacted and items considered as evidence are documented, bagged, labeled, collected and transported to the lab for further examination; finally a police report refers to the results of the investigation.

The majority of models that have been presented so far for physical crime scene investigations include a number of common steps. For example, the U.S. National Institute of Justice report on Crime Scene Investigation (2008) includes nine top level steps: a. Preparation, b. Preservation, c. Preliminary Documentation and Evaluation of the scene, d. Documentation, e. Collection, f. Preservation, g. Package, h. Transport, i. Report. These steps are met in most investigation models.

Lee *et al*. (2001) presented the *Scientific Crime Scene Investigation Model*, which focuses on a systematic and methodical way of investigating a physical crime scene. Although the model refers only to physical crime scene investigation, it became a point of reference as many of its aspects can be used to search for digital evidence in an electronic crime scene investigation. The model refers only to the forensic part of an investigation, while issues such as preparation and exchange of information with other investigators are not addressed.

In the *Digital Forensic Research Workshop* (Palmer, 2001), a digital forensic investigation model was suggested which includes a set of seven steps derived from a number of actions that have to be performed in each step. The aim of the model was to set the basis for future work which would define a full model. It became a point of reference in the coming years as its steps are included in most of the recent models. The model cannot be used directly in a real investigation as it does not include a comprehensive explanation of the actions that have to be performed in each step but only a list of overlapping techniques.

Carrier and Spafford (2003) suggested a digital investigation process, which includes both physical and digital evidence investigation in one integrated process. The model consists of seventeen phases organized into five groups. The basic characteristic of the model is the separation of the investigation process to physical and digital crime scene investigation. Firstly, items found in the crime scene are handled as physical evidence using traditional investigation methods (*e.g.*, fingerprints). If these items are source of digital evidence (*e.g.*, computers, cellphones, peripherals) they are examined again according to digital crime scene investigation sub-phases and the

results are added to the primary physical scene. The main disadvantage of this approach is that the time needed to collect physical evidence could lead to loss of volatile data or other digital evidence related to the crime.

Ciardjuain (2004) evaluated and combined the existed models to propose the *Extended Model of Cybercrime Investigations* which consists of thirteen steps. Unlike previous models, it includes steps and processes before and after the crime scene investigation. The sequence of steps in the model is not absolute. Some steps can be omitted, their sequence can be modified and the results from a step can influence not only the next step but the previous one as well. The sequence of the activities described in the model could contribute to the development of new tools for digital evidence examination. The model only refers to digital evidence.

The *Computer Forensics Field Triage Process Model* (Rogers *et al.*, 2006) aims to identify, examine and interpret digital evidence as soon as the investigation begins, without the need to take the evidence to the lab for further examination. The model focuses on the need to collect as much evidence as possible, immediately after the investigation begins as in many cases immediate action is required to resolve the crime. The model also focuses on the specifics of each case *e.g.,* investigating child pornography is different than investigating drug activities or financial crimes. This feature limits the model's value since it can be used only in a limited number of cases. Furthermore, the format of the model resembles to a computer-based or network-based forensic model, where physical evidence is totally ignored.

The *Systematic Digital Forensic Investigation Model* (Agarwal *et al.*, 2011) includes eleven stages which are similar to the ones that had been suggested in previous models, except the evidence collection stage which is divided into Volatile Evidence and Non-Volatile Evidence Collection sub-phases. It is a comprehensive model, targeting computer frauds and cyber crimes investigations. Basically, the model ignores the physical nature of evidence. Only the Non-volatile evidence collection sub-phase considers evidence of non-digital nature such as written passwords, hardware and software manuals, related documents and computer printouts. Critical physical evidence like fingerprints or DNA which could be found on the surface or the internal of the devices placed at the crime scene, are ignored.

Recently, Yusoff *et al.* (2011) presented an assessment on digital investigations models, from 1985 to 2011. They examined the existed models and determined their common phases. These common phases were used to make the *Generic Computer Investigation Model* which consists of five generic phases. The five generic phases which are included in the model represent the main phases of each investigation in a physical or digital crime scene. Their model seems more like a framework than a model, since its phases are too general to be implemented ad hoc in a real world investigation process.

Table 1, presents the top level phases of a selection of state-of-the-art investigation models and the target evidence of each model (physical or digital) is highlighted.

NAME OF MODEL - AUTHOR	TOP LEVEL PHASES		TARGET EVIDENCE	
			PHYSICAL	*DIGITAL*
Scientific Crime Scene Investigation Model (Lee *et al.* 2001)	**1.** Recognition **2.** Identification	**3.** Individualization **4.** Reconstruction	X	
The Digital Forensic Research Workshop Investigative Model (Palmer, 2001).	**1.** Identification **2.** Preservation **3.** Collection	**4.** Examination **5.** Analysis **6.** Presentation		X
An Intergraded digital investigation process (Carrier and Spafford, 2003)	**1.** Readiness Phases **2.** Deployment Phases **3.** Physical Crime Scene Investigation Phases	**4.** Digital Crime Scene Investigation Phases **5.** Review	X	X
Extended Model of Cybercrime Investigations (Ciardjuain, 2004)	**1.** Awareness **2.** Authorization **3.** Planning **4.** Notification **5.** Search for and identify evidence **6.** Collection	**7.** Transport **8.** Storage **9.** Examination **10.** Hypothesis **11.** Presentation **12.** Proof / defense **13.** Dissemination		X
Computer Forensics Field Triage Process Model (Rogers *et al.*, 2006)	**1.** Planning **2.** Triage **3.** User Usage Profile	**4.** Chronology Timeline **5.** Internet **6.** Case Specific		X
Systematic Digital Forensic Investigation Model (Agarwal *et al.*, 2011)	**1.** Preparation **2.** Securing the Scene **3.** Survey and Recognition **4.** Documenting the Scene **5.** Communication Shielding	**6.** Evidence Collection **7.** Preservation **8.** Examination **9.** Analysis **10.** Presentation **11.** Result		X
Generic Computer Investigation Model (Yusoff *et al*, 2011)	**1.** Pre-Process **2.** Acquisition and **3.** Preservation	**4.** Analysis **5.** Presentation **6.** Post-Process	X	X

Table 1: Top level phases of crime investigation models

3. A model for hybrid evidence investigation

The proposed model can be implemented in investigating crime scenes with hybrid evidence, but also in investigations where only digital or only physical evidence exists. The model consists of four major phases and twelve secondary sub-phases (Fig. 1).

3.1 Phase A: Preparation

(A1) Notification. This first step includes: (a) Notification that a crime has been committed. For example using European Emergency Number (112) to report a crime, sending an email, going to a police station etc. (b) Notification to the proper law enforcement agency responsible to conduct the investigation. The responsible agency can be determined by geographical criteria (location of crime scene) or the nature of the crime-incident (robbery, suicide etc.). Notification is very important, because the information collected here is crucial for the next steps of the investigation.

(A2) Authorization. Authorization is obtained from the agency assigned to conduct an investigation. The form and details of the authorization depend on the type of crime and the procedural law of the country where it is committed. Typically, immediately after a crime has been discovered, assigned officers can conduct an investigation at once and inform the attorney on duty as soon as possible.

(A3) Preparation. Preparation includes availability of the necessary tools, equipment and personnel able to conduct the investigation. Preparation is important not only after the notification for a crime or incident but also before, including education and training, response, availability and functionality of tools and equipment. In this sub-phase the person responsible for the investigation is determined.

3.2 Phase B: Crime scene investigation

(B1) Preservation. The Lead first respondent at the crime scene is responsible for organizing a number of things: first aid, search for witnesses and securing the scene from people who are not authorized to approach. Additionally, possible source of physical and digital evidence should also be recognized and secured.

(B2) Identification. This is a specialized task that is preferably conducted by crime investigation experts. Their task is to identify possible evidence, physical or digital related to items set in the crime scene. In serious crimes, the investigation could be conducted by a number of technicians specialized in different fields. Their level of cooperation and understanding is a major factor for a successful investigation. This phase also includes documentation which refers to photographing, sketching and mapping the crime scene, taking notes about items or people present at the crime scene etc.

(B3) Collection – Examination. This is one of the most important sub-phases of the model. The investigator has to collect fingerprints, items related to the crime, biological material and other physical evidence. In case there is digital evidence at the crime scene the investigator should firstly search for volatile data. In this stage the cooperation between the digital and physical crime scene experts is highly important because collection of physical evidence can destroy digital evidence and vice versa. This stage also contains examination. This is not the thorough examination procedure that is conducted in a laboratory environment. However sometimes it is important for the investigation to get as much information as soon as possible. For example in a serious crime investigation it is extremely urgent for the investigator to search the victim's mobile phone for *e.g.*, last calls or messages or a personal computer for e-mails or recent posts on social networks.

(B4) Transportation. Although transportation of evidence is usually perceived as a secondary procedure, we consider it as important as collection. During transportation special measures should be taken to avoid any damage to the evidence. Careful packaging, humidity and temperature, should be considered to avoid any destruction of physical and/or digital evidence.

3.3 Phase C: Laboratory examination

(C1) Examination. The examination of evidence in a laboratory environment is essential to any investigation because it can provide the investigator with crucial evidence related to the case. While at the crime scene only a part of the collected

evidence can be examined, in this phase all evidence is thoroughly examined and analyzed according to the nature of evidence and the specifics of each case.

(C2) Storage. After examination, evidence should be stored properly in a locked evidence room with stringent access controls. The evidence should be labeled and segregated to avoid any cross contamination, to avoid destruction and to enable re-examination if such need occurs in a court or any other step of the investigation.

(C3) Report. The Report determines the outcome of the laboratory examination phase. The report of the lab is one of the most important documents for the investigator and all parties involved in a case (prosecution and defence).

3.4 Phase D: Conclusion

(D1) Reconstruction. Crime reconstruction is the main responsibility of the investigator who evaluates the collected and examined evidence and represents the facts as defined by the evidence analysis. This step is only of value if the previous steps have been followed forensically such that anyone following the same method would arrive at the same results.

(D2) Dissemination. Dissemination is the last step of the model. A thorough review of the investigation is conducted in this step to preserve gained knowledge and identify areas of improvement. Lessons learned should be carefully recorded and disseminated to other parties which conduct similar investigations.

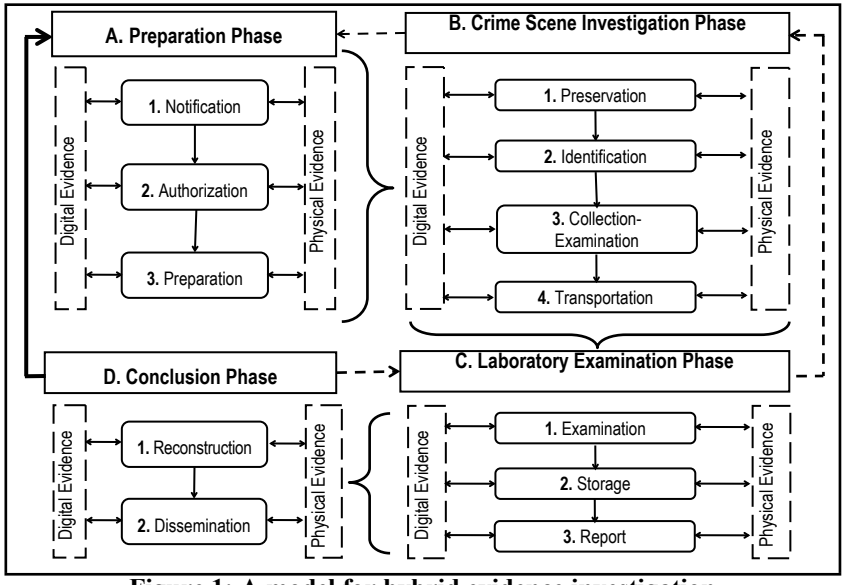

Figure 1: A model for hybrid evidence investigation

4. Model Analysis

The proposed model for hybrid evidence investigation holds the majority of the benefits of the existing models adding an extra advantage: It can be implemented to every crime scene investigation whether digital evidence is present or not. The format of the model resembles a traditional law enforcement investigation model, but it has been adjusted to also face the challenges of digital evidence. The model can be easily interpreted, because it is divided into specified phases and a number of sub-phases. This is very important for the investigators who are called to practice it but also for the trainers who teach crime investigation methods and techniques.

The model examines the whole process of crime investigation, starting from the notification that a crime has been committed, ending to the findings of the research. Digital and physical evidence are equally important and influence every sub-phase of the model (double arrows in Fig. 1). Phase B targets the search and collection of physical and digital evidence, which are in constant interrelation. In this phase, the collection-examination sub-phase is highly important. In the collection sub-phase, there is not a defined order in evidence collection. The investigator is responsible to take a critical decision and determine if volatile and other digital data should have priority over collection of physical evidence such as fingerprints or biological material. The examination sub-phase at the crime scene does not intend to replace the laboratory examination but to help the investigator to collect important evidence crucial for the next steps as soon as the investigation begins. Digital evidence seems to mostly affect this phase; however its role is highly important to all phases of the model. For example, in Phase A, the existence of digital evidence affects the type of authorization needed and the personnel who will conduct the investigation. Unlike previous models, laboratory examination of the collected evidence from the crime scene is a separate and very important phase.

Although there is a defined order in the phases of the model, iteration at each phase or returning to a previous phase is also an option. Inarguably an investigation is a process where a number of unpredictable factors can occur. Returning to a previous phase (marked in Fig. 1 with dotted arrows) could help the investigator to fill in the gaps and ensure that all evidence is adequately collected and analyzed. After the investigation ends, the knowledge gained may be used as feedback to improve the investigation process (straight bold line in Fig. 1) so that lessons learned can be considered in future investigations.

As in every model for law enforcement investigations the responsibility of the investigation belongs to the assigned investigator. He/she is in charge of all the aspects of the investigation, guides experts of other fields who participate in the investigation process and in Phase D he/she draws conclusions about the investigation. Despite the key role of the investigator other people are also involved in the investigation process. For example in Phase A emergency call first responders should collect all the necessary information and report to the proper agency as soon as possible. In Phase B first responders have to secure the crime scene while forensic experts of different fields have to collect and examine primary evidence, possibly of

different types, and, finally, in Phase C collected and transported evidence is examined in a laboratory environment by specialized personnel.

5. Conclusions

In this paper, we considered crime scene investigation where digital and physical evidence may co-exist, and presented the key challenges of law enforcement investigation in the new environment. Additionally, we reviewed a selection of investigation models for physical/digital evidence and proposed a model for hybrid evidence investigation. Our model unifies the procedures related to digital and physical evidence collection and examination, taking into consideration the unique characteristics of each form of evidence. Inarguably, the proposed model is still in its infancy. It should be tested and evaluated in real investigation environments and get feedback which would define the necessary modifications. Additionally, a more detailed description of each phase of the model is needed, also supported by a manual for investigators which should include further technical instructions related to an investigation. These are left for future work.

6. References

Agarwal, A., Gupta, M., Gupta, S. and Gupta S.C. (2011), "Systematic Digital Forensic Investigation Model", *International Journal of Computer Science and Security*, Vol. 5, No. 1, pp 118-131.

Beebe, N. (2009), "Digital Forensic Research: The Good, The Bad, and The Unaddressed," in Advances in Digital Forensics V, Peterson G. and Shenoi S. (eds.), Boston, Springer, pp 17-33. ISBN 978-3-642-04154-9.

Carrier, B. and Spafford, E. (2003), "Getting Physical with the Digital Investigation Process, *International Journal of Digital Evidence*, Vol. 2, No. 2.

Ciardhuain, S. (2004), "An Extended Model of Cybercrime Investigations", *International Journal of Digital Evidence*, Vol. 3, No. 1.

Garfinkel, S. (2010), "Digital Forensics Research: The next 10 years", *Digital Investigation*, Vol. 7, pp S64-S73.

Hunton, P. (2010), "Cyber Crime and Security: A New Model of Law Enforcement Investigation", *Policing,* Vol. 4, No. 4, pp. 385-395.

Hunton, P. (2011), "The stages of Cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation", *Computer law and Security Review*, Vol. 27, No. 1, pp. 61-67.

Lee, H., Palmbach, T., and Miller, M. (2001), *Henry Lee's Crime Scene Handbook*, Academic Press, San Diego, ISBN: 0-12-440830-3.

National Institute of Justice (2000), "Crime Scene Investigation, A guide for law enforcement", Research Report, *U.S. Department of Justice,* https://www.ncjrs.gov/pdffiles1/nij/178280.pdf, (Accessed 27 January 2012).

National Institute of Justice (2004), "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", Special Report, *U.S. Department of Justice, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf,* (Accessed 27 January 2012).

National Institute of Justice (2008), "Electronic Crime Scene Investigation. A Guide for first Respondents", Special Report, Second Edition, *U.S. Department of Justice* https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, (Accessed 27 January 2012).

Palmer, G. (ed.), (2001), "A Road Map for Digital Forensic Research", Digital Forensic Research Workshop (DFRWS) Technical Report DTR-T001-01, Utica, New York, http://www.dfrws.org/2001/dfrws-rm-final.pdf, (Accessed 27 January 2012).

Palmer, G. (2002), "Forensic Analysis in the Digital World", *International Journal of Digital Evidence*, Vol. 1, No. 1.

Reith, M., Car, C., and Gunsch, G. (2002), "An Examination of Digital Forensic Models", *International Journal of Digital Evidence*, Vol. 1, No. 3.

Rogers M., Goldman J., Mislan R., Wedge T. and Debrota S. (2006), "Computer Forensic Field Triage Process Model", *Journal of Digital Forensics, Security and Law*, Vol. 1, No. 2, pp 19-38.

Sheldon, A. (2005), "The future of forensic computing", *Digital Investigation*, Vol. 2, pp 31-35.

Vlachopoulos, K. (2007). *Electronic Crime*, Nomiki Vivliothiki, Athens, ISBN: 978-960-272-458-3.

Yussof, Y., Ismail, R., and Hassan Z. (2011), "Common Phases of Computer Forensics Investigation Models", *International Journal of Computer Science & Information Technology*, Vol. 3, No. 3, pp 17-31.