The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review

Soltan Alharbi[1, 1], Jens Weber-Jahnke[2], Issa Traore[1]

[1]*Electrical and Computer Engineering, University of Victoria*
[1,1] *Email: salharbi@ece.uvic.ca*
[1]*Email: itraore@ece.uvic.ca*
[2]*Computer Science Department, University of Victoria*
Email: jens@cs.uvic.ca

Abstract

Recent papers have urged the need for new forensic techniques and tools able to investigate anti-forensics methods, and have promoted automation of live investigation. Such techniques and tools are called proactive forensic approaches, i.e., approaches that can deal with digitally investigating an incident while it occurs. To come up with such an approach, a Systematic Literature Review (SLR) was undertaken to identify and map the processes in digital forensics investigation that exist in literature. According to the review, there is only one process that explicitly supports proactive forensics, the multi-component process [1]. However, this is a very high-level process and cannot be used to introduce automation and to build a proactive forensics system. As a result of our SLR, a derived functional process that can support the implementation of a proactive forensics system is proposed.

Keywords: *Proactive Forensics Investigation, Reactive Forensics Investigation, Anti-forensics, Systematic Literature Review and Automation.*

1. Introduction

Computer crimes have increased in frequency, and their degree of sophistication has also advanced. An example of such sophistication is the use of anti-forensics methods as in Zeus Botnet Crimeware toolkit that can sometimes counter-act digital forensic investigations through its obfuscation levels. Moreover, volatility and dynamicity of the information flow in such a toolkit require some type of a proactive investigation method or system. The term *anti-forensics* refers to methods that prevent forensic tools, investigations, and investigators from achieving their goals [2]. Two examples of anti-forensics methods are *data overwriting* and *data hiding*. From a digital investigation perspective, anti-forensics can do the following [2]:

- Prevent evidence collection.
- Increase the investigation time.
- Provide misleading evidence that can jeopardize the whole investigation.
- Prevent detection of digital crime.

To investigate crimes that rely on anti-forensics methods, more digital forensics investigation techniques and tools need to be developed, tested, and automated. Such techniques and tools are called proactive forensics processes. Proactive forensics has been

suggested in [1-4]. To date, however, the definition and the process of proactive forensics have not been explicated [1].

In order to develop an operational definition for proactive forensics process and related phases, we have conducted a systematic literature review (SLR) to analyze and synthesize results published in literature concerning digital forensics investigation processes. This SLR has ten steps, described in sections 3.1 to 5.2, grouped under three main phases: planning, conducting, and documenting the SLR [5]. As result of this SLR, a proactive forensics process has been derived.

The SLR approach was selected for a couple of reasons. Firstly, SLR results are reproducible. Secondly, since all resources (databases) will be queried systematically there is less chance of missing an important reference.

The rest of the paper is organized as follows. Section 2 outlines the related work and the motivation behind the proactive investigation process. Section 3 lays out the plan of the systematic literature review prior to implementation. Section 4 describes the implementation of the review and the extraction of the primary studies from the selected resources. Section 5 generates the report of the review after synthesizing the data collected in the previous section. Section 6 presents the review findings, results, and the proposed process. Section 7 contains the conclusion and suggestions for future work.

2. Related Work and Motivation for the Proactive Investigation Process

According to the literature, only a few papers have proposed a proactive digital forensics investigation process. Some of these papers have mentioned the proactive process explicitly, while in others the process is implicit, but all have indicated the need for such a process.

In [6], Rowlingson stated that in many organizations , incident response team already performs some activities of evidence collection. But he added, that the need for collecting those evidence and preserving it in a systematic proactive approach still an open issue.

In [2], Garfinkel implicitly suggested that in order to investigate anti-forensics, organizations need to decide early what information to collect and preserve in a forensically sound manner.

In [1], Grobler *et al*. noted that live (proactive) forensic investigations are hindered by lack of definitions of live forensics and standard procedures in live investigations. In addition, the authors suggested the automation and activation of evidence-collection tools in live investigations. This automation should involve minimal user intervention to improve the integrity of the evidence. Thus, a multi-component view of the digital forensics investigation process has been proposed. However, it is a high-level view of the investigation and, as such, cannot directly be operationalized to create automated tools. Additionally, the process described in [2] contains phases, such as service restoration, that lie outside the scope of the investigation.

In [3], Garfinkel summarized digital forensics investigation processes that have been published in literature. In his summary, he stated that it would be unwise to depend upon "audit trails and internal logs" in digital forensics investigation. In addition, he noted that a future digital forensics investigation process will only be possible if future tools and techniques make a proactive effort at evidence collection and preservation.

In [4], Orebaugh emphasized that the quality and availability of the evidence collected in the reactive stage of the investigation is more time consuming to investigate. Conversely, the proactive stage collects only potential evidence, which is less time consuming to investigate. In addition, a high-level proactive forensics system is proposed as ideal. As future work, the

author suggested that in order to address anti-forensics crimes, methods should be identified to handle evidence collection and proactive forensics investigation.

In summary, previous papers have shown the importance of a proactive digital forensics investigation process. The proposed notion of proactiveness is, however, still insufficient and imprecise, and more work needs to be done. To this end, we will follow a systematic literature review and derive the missing components.

3. Planning the Systematic Literature Review (SLR)

The planning stage of the systematic literature review consists of the following steps:

3.1 Specify Research Questions:

This step defines the goal of the SLR by selecting the research question that has to be answered by the review. The research question is: "What are all the processes in digital forensics investigation?"

Processes include the phases of any digital forensics investigation. According to [7], the six phases of digital forensics investigation are: identification, preservation, collection, examination, analysis, and presentation. The reader can refer to [7] for elaboration of these phases.

3.2 Develop Review Protocol:

The review protocol is outlined in steps 4.1 through 5.2 below. These steps show how data for the review is selected and summarized.

3.3 Validate Review Protocol:

The review protocol was validated by querying the selected databases and looking at the search results. Those results were meaningful and showed the feasibility of the developed protocol.

4. Conducting the Systematic Literature Review

The review was conducted by extracting data from the selected sources using the following steps:

4.1 Identify Relevant Research Sources:

Six database sources were selected as being most relevant to the fields of computer science, software engineering, and computer engineering. The expert engineering librarian at the University of Victoria corroborated the relevance of those databases, and also recommended another indexed database that is considered to contain reliable sources: *Inspec*. Two extra public indexed databases were used for sanity check: *CiteSeer* and *Google Scholar*. The *International Journal of Computer Science and Network Security* (IJCSNS) was located while conducting a sanity check in Google Scholar using "digital forensic investigation process" as keywords.

All of the searches were limited in date from 2001 to 2010.

4.1.1 IEEE Xplore: http://ieeexplore.ieee.org/Xplore/dynhome.jsp

4.1.2 ACM Digital Library: http://portal.acm.org/dl.cfm

4.1.3 Inspec: http://www.engineeringvillage2.org/

4.1.4 SpringerLink: http://www.springerlink.com

4.1.5 ELSEVIER: http://www.sciencedirect.com

4.1.6 IJCSNS: http://ijcsns.org/index.htm

4.1.7 CiteSeer: http://citeseerx.ist.psu.edu *(indexed database)*

4.1.8 Google Scholar: http://scholar.google.ca *(indexed database)*

The queries used to search the databases above, except for IJCSNS, were as follows:

(Computer OR Digital) AND (Forensic OR Crime) AND (Investigation OR Process OR Framework OR Model OR Analysis OR Examination)

For IEEE Xplore, the basic search screen window was used to search only within title and abstract (metadata, not a full text).

In ACM Digital Library, the basic search screen window was used to search for the queries within the database.

In the case of SpringerLink, the advanced search screen window was used to search within title and abstract. Furthermore, in SpringerLink the search field for queries could not take all of the queries so last two keywords, "Analysis" and "Examination," had to be excluded.

In the case of ELSEVIER, the advanced search screen window was used to search within abstract, title, and keywords.

Running the above queries against the databases gave the following numbers of papers:

- IEEE Xplore: 42 (on Nov 1, 2010)
- ACM Digital Library: 27 (on Nov 3, 2010)
- SpringerLink: 158 (on Nov 3, 2010)
- ELSEVIER: 346 (on Nov 4, 2010)

For IJCSNS, as an exception, the keywords "Digital Forensic Investigation" were used in the search screen window. The search returned this number of papers:

- IJCSNS: 86 (on Nov 24, 2010)

Since using the above queries for Inspec and CiteSeer would result in a considerable number of irrelevant Primary Studies (PS), Control Terms (CT) were used instead. In addition, CT were run against previous databases as well, to be able to capture more relevant PS. The CT recommended by the Inspec database as well as the subject librarian are:

(Computer Crime) OR (Computer Forensics) OR (Forensic Science)

The first two CT (computer crime OR computer forensics) were used to search IEEE Xplore, ACM, SpringerLink, and ELSEVIER. "Forensic Science" was excluded since it returns PS out of the scope of this study. For IEEE Xplore, the advanced search screen window was used in searching the metadata only. In the ACM digital library, the advanced search screen window was used to fetch the database within the keywords field. In SpringerLink, the advanced search screen window was used to search within title and

abstract. For ELSEVIER, the advanced search screen window was used to search within the keywords.

In the case of Inspec, using the CT above, the database was searched in three categories. In the first category, all of the CT (including "forensic science") were used with an AND Boolean operator between them in the quick search screen window for searching within CT fields in the database. In the second category, only "computer forensics" was used in the quick search screen window to search within the CT field. In the third category, "forensic science" was used in the quick search screen window to search within CT.

For CiteSeer, the advanced search screen window was used. In addition, since CiteSeer does not have the option to search within CT, it was necessary to search its database using keywords. These keywords were "Computer Crime" OR "Computer Forensics" OR "Digital Forensic." The search was conducted in two categories. First, an OR operator was used between all the keywords in the abstract field. Second, only the first two keywords were used, with an OR operator between them, in the keywords field.

When the above CT and keywords were run on different dates, the following numbers of papers were returned from the databases listed above:

- IEEE Xplore: 1,053 (on Nov 6, 2010)
- ACM Digital Library: 134 (on Nov 8, 2010)
- SpringerLink: 128 (On Nov 10, 2010)
- ELSEVIER: 69 (on Nov 14, 2010)
- Inspec: 459 (on Nov 5, 2010). The PS were distributed as follows:
  - Category 1: 13
  - Category 2: 290
  - Category 3: 156
- CiteSeer: 162 (on Nov 15, 2010)
  - Category 1: 143
  - Category 2: 19

Finally, the primary studies that were collected from running all the above queries are [1], [8-26]. Additional primary studies were collected by examining the previous primary studies [7, 27-31].

4.2 Select Primary Studies:

4.2.1 Selection Language

Publications in the English language only were selected from the above database resources.

4.2.2 Selection Criteria

Primary studies were selected and irrelevant ones were excluded using three filters. The criteria for those filters are as follows:

- The first filter excludes any papers whose titles bear no relation to the question in section 3.1. According to this filter, the total number of papers is 32.
- The second filter excludes any papers that do not target processes of the digital forensics investigation in their abstract or title. After this filter, the total number of papers is 26.
- The third filter excludes any papers that do not discuss processes of the digital forensics investigation in more detail in their full text. This leaves only the primary studies that need to be included in the systematic review. With this filter, the total number of PS remaining is 20 [1], [8-26] . Six additional primary studies were found by investigating the 20 PS. Out of these 26 primary studies only 18 papers dealt with the processes of digital forensics investigation.

4.3 Assess Study Quality

The quality of the primary studies was assessed according to the following categorizations, starting from the highest level to the lowest:

1. Peer-reviewed journals: Level 5 (Highest).
2. Peer-refereed book chapters: Level 4.
3. Peer-reviewed conference papers: Level 3.
4. Peer-reviewed workshop papers: Level 2.
5. Non-peer refereed papers: Level 1 (Lowest).

Table 1 shows the summary of the primary studies genre. Nine of the 18 primary studies were journals; these reveal the maturity of the processes listed in this paper and its patterns.

4.4 Extract Required Data:

The processes of digital forensics investigation that were extracted from the total 26 primary studies are grouped in Table 2.

4.5 Synthesize Data:

The processes of digital forensics investigation were mapped to the proposed investigation process (see Table 3).

Table 1. Paper genre and the number of primary studies

Genre	*Number of Primary Studies*
Peer-reviewed journals	9
Peer-refereed book chapters	1
Peer-reviewed conference papers	7
Peer-reviewed workshop papers	1
Non-peer-refereed papers	0

5. Documenting the Systematic Literature Review

This stage is about generating the systematic literature review report.

5.1 Write Review Report

The review report is contained in the current paper.

5.2 Validate Report

The same review protocol was used to validate the systematic literature review twice during execution of the review.

6. Research Findings

All the processes of digital forensics investigation in Table 3 shows that they all share the reactive component, but only one [1] includes the proactive component. (In [1], this proactive component has been named the active component.) The reactive component of all processes was inspired by [7]. Recent papers such as [2], [1], [3], and [4] have suggested that there is a need for advancement in the area of proactive forensic systems.

In [1], a multi-component view of digital forensics process is proposed. This process is at a high level and consists of three components: proactive, active, and reactive. The term "proactive" as it is used in [1] deals with the digital forensics readiness of the organization as well as the responsible use of digital forensics tools. The active component, termed the proactive component in the current study, deals with the collection of live evidence in real time while an event or incident is happening. The active component of the investigation is not considered to be a full investigation since it lacks case-specific investigation tools and techniques. The reactive component is the traditional approach to digital forensics investigation.

The process proposed in this study is derived from [1], but has only two components, proactive and reactive (see Figure 1). Even though Figure 1 shows that the investigation process is a waterfall process, in real-life it has some iteration. The proposed proactive component is similar to the active component in [1].

Table 2. Processes of Digital Forensics Investigation

Process No.	Authors, Reference # & Genre	Digital Forensic Investigation Process Name	Number of Phases
1	Palmer [7] & Conference	Investigative Process for Digital Forensic Science	6 Phases
2	Reith, Carr, and Gunsch [8] & Journal	An Abstract Digital Forensics Model	9 Phases
3	Carrier and Spafford [27] & Journal	An Integrated Digital Investigation Process	17 phases organized into 5 major phases
4	Stephenson [12] & Journal	End-to-End Digital Investigation Process	9 phases
5	Baryamureeba and Tushabe [10] & Journal	The Enhanced Digital Investigation Process	5 major phases including sub-phases
6	Ciardhuain [28] & Journal	The Extended Model of Cybercrime Investigations	13 phases
7	Carrier and Spafford [9] & Conference	An Event-Based Digital Forensic Investigation Framework	5 major phases including sub-phases

8	Harrison [14] & Journal	The Lifecycle Model	7 phases
9	Beebe and Clark [15] & Journal	The Hierarchical, Objective-Based Framework	6 phases
10	Kohn, Eloff, and Olivier [11] & Conference	The Investigation Framework	3 phases
11	Kent, Chevalier, Grance, and Dang [31] & Journal	The Forensic Process	4 phases
12	Rogers, Goldman, Mislan, Wedge, and Debrota [29] & Conference	The Computer Forensics Field Triage Process Model	6 major phases including sub-phases
13	Ieong [16] & Journal	FORZA – Digital Forensics Investigation Framework Incorporating Legal Issues	8 phases
14	Freiling and Schwittay [30] & Conference	The Common Process Model for Incident Response and Computer Forensics	3 major phases including sub-phases
15	Khatir, Hejazi, and Sneiders [17] & Workshop	Two-Dimensional Evidence Reliability Amplification Process Model	5 major phases including sub-phases
16	Shin [19] & Conference	Digital Forensics Investigation Procedure Model	10 phases including sub-phases
17	Billard [20] & Book Chapter	An Extended Model for E-Discovery Operations	10 phases
18	Grobler, Louwrens, and Solms [1] & Conference	A Multi-component View of Digital Forensics	3 major phases including sub-phases

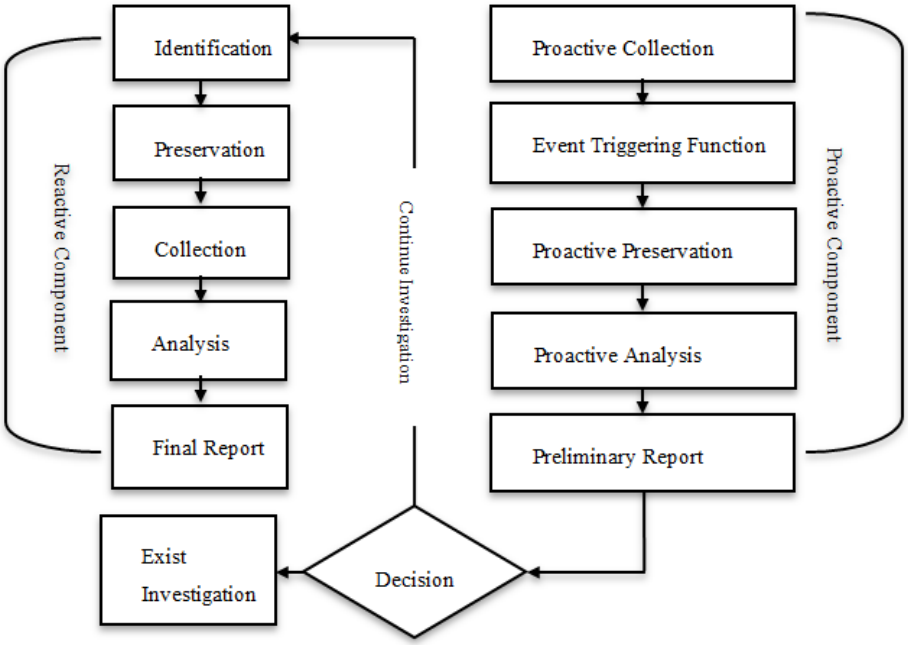

Fig. 1. Functional process for proactive and reactive digital forensics investigation system

Both the proposed process and the multi-component process share the reactive component. Table 3 maps phases of the proposed proactive and reactive digital forensics investigation process to phases of the existing processes.

Description of the two components in the proposed process is as follows:

1) Proactive Digital Forensics Component: is the ability to proactively collect, trigger an event, and preserve and analyze evidence to identify an incident as it occurs. In addition, an automated preliminary report is generated for a later investigation by the reactive component. The evidence that will be gathered in this component is the proactive evidence that relates to a specific event or incident as it occurs [4]. As opposed to the reactive component, the collection phase in this component comes before preservation since no incident has been identified yet.

Phases under the proactive component are defined as follows:

- Proactive Collection: automated live collection of a pre-defined data in the order of volatility and priority, and related to a specific requirement of an organization.
- Event Triggering Function: suspicious event that can be triggered from the collected data.
- Proactive Preservation: automated preservation of the evidence related to the suspicious event, via hashing.
- Proactive Analysis: automated live analysis of the evidence, which might use forensics techniques such as data mining to support and construct the initial hypothesis of the incident.
- Preliminary Report: automated report for the proactive component.

This proactive component differs from common Intrusion Detection Systems (IDS) by ensuring the integrity of evidence and preserving it in a forensically sound manner. In addition, the analysis of the evidence will be done in such a way as to enable prosecution of the suspect and admission to court of law.

2) Reactive Digital Forensics Component: is the traditional (or post-mortem) approach of investigating a digital crime after an incident has occurred [7]. This involves identifying, preserving, collecting, analyzing, and generating the final report. Two types of evidence are gathered under this component: active and reactive. Active evidence refers to collecting all live (dynamic) evidence that exists after an incident. An example of such evidence is processes running in memory. The other type, reactive evidence, refers to collecting all the static evidence remaining, such as an image of a hard drive.

Phases under the reactive component are defined by [7]. It is worth mentioning that the examination and analysis phases in [7] are combined in the proposed process under a single phase called analysis.

In order to see how the two components work together, let us take the scenario that electronic health records with an elevated risk will be proactively collected all the time for any read access of such records. This live collection is automated and is conducted without the involvement of the investigator. When a suspicious event is triggered during collection, consequently all evidence related to that event will be preserved by calculating MD5 hashing algorithm. Thereafter, a forensic image will be made from the preserved evidence, and this image must produce the same MD5 number. Next, a preliminary analysis will be conducted

on the forensic image and maybe some data mining techniques will be applied to reconstruct the event. Such analysis will help in identifying if the event has occurred or not. Finally, an automated report will be generated and given to the person in charge to decide if the reactive component needs to take over or not.

Next, if needed, the reactive component will conduct a more comprehensive approach investigation. This initial event will be used as identification for the occurrence of the incident, and additional clues can be gathered from the scene. Since this is a post-mortem of an incident or an event, the evidence will be preserved first by calculating the MD5 hashing algorithm. Then a forensic image will be made from the original source of evidence. This forensic image must produce the same MD5 number to preserve the integrity of the original evidence. Thereafter, a deeper analysis will be conducted using forensic tools and techniques to enable the investigator to reach a conclusion. Finally, a report will be generated.

Goals to be achieved by the addition of the proactive component are as follows:

- Develop new proactive tools and techniques to investigate anti-forensics methods.
- Capture more accurate and reliable evidence in real time while an incident is happening live [1], [3], [4].
- Promote automation without user intervention in the following phases in the proactive component of the digital forensics investigation: proactive collection, event triggering function, proactive preservation, proactive analysis, and preliminary report.
- Provide reliable leads for the reactive component to take place.
- Save time and money by reducing the resources needed for an investigation.

Table 3. Mapping phases of the proposed proactive and reactive digital forensics investigation process to phases of the existing processes

Digital Forensic Investigation Process Name & Reference	***Proactive Investigation***					***Reactive Investigation***				
	Proactive Collection	Event Trigging Function	Proactive Preservation	Proactive Analysis	Preliminary Report	Identification	Preservation	Collection	Analysis	Report
Investigative Process for Digital Forensic Science (2001) [7]						✓	✓	✓	✓	✓
An Abstract Digital Forensics Model (2002) [8]						✓	✓	✓	✓	✓
An Integrated Digital Investigation Process (2003) [27]						✓	✓	✓	✓	✓
End-to-End Digital Investigation Process (2003) [12]								✓	✓	
The Enhanced Digital Investigation Process (2004) [10]						✓	✓	✓	✓	✓

The Extended Model of Cybercrime Investigations (2004) [28]						✓	✓	✓	✓	✓
An Event-Based Digital Forensic Investigation Framework (2004) [9]						✓	✓	✓	✓	✓
The Lifecycle Model (2004) [14]						✓	✓	✓	✓	✓
The Hierarchical, Objective-Based Framework (2005) [15]						✓	✓	✓	✓	✓
The Investigation Framework (2006) [11]						✓	✓	✓	✓	✓
The Forensic Process (2006) [31]							✓	✓	✓	✓
The Computer Forensics Field Triage Process Model (2006) [29]						✓	✓	✓	✓	
FORZA – Digital Forensics Investigation Framework Incorporating Legal Issues (2006) [16]						✓	✓	✓	✓	✓
The Common Process Model for Incident Response and Computer Forensics (2007) [30]						✓	✓	✓	✓	✓
Two-Dimensional Evidence Reliability Amplification Process Model (2008) [17]						✓	✓	✓	✓	✓
Digital Forensics Investigation Procedure Model (2008) [19]						✓	✓	✓	✓	✓
An Extended Model for E-Discovery Operations (2009) [20]						✓	✓	✓	✓	✓
A Multi-component View of Digital Forensics (2010) [1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

The advantages of the proposed process over the multi-component process are as follows:

- It is a functional process compared to the high-level multi-component process.
- It will be used to develop techniques and automated tools to investigate anti-forensics methods.
- It will automate all phases of the proactive component.
- It combines both digital forensics readiness, as in proactive collection phase, and live investigation, in the other phases, under the same component.

The disadvantages of the proposed process are as follows:

- Not yet fully implemented and may be adapted to implementation requirements.
- The investigator will have to decide whether to move from the proactive to the reactive component or to exit the whole investigation. This decision is not automated yet.
- It will not be able yet to address all techniques used by anti-forensics methods.

7. Conclusion

In order to investigate anti-forensics methods and to promote automation of the live investigation, a proactive and reactive functional process has been proposed. The proposed process came as result of SLR of all the processes that exist in literature. The phases of the proposed proactive and reactive digital forensics investigation process have been mapped to existing investigation processes. The proactive component in the proposed process has been compared to the active component in the multi-component process. All phases in the proactive component of the new process are meant to be automated.

For future work, the proposed process will be used to develop and implement the proactive and reactive systems using domain-specific modeling language and automated code generation. This new method will help in creating the skeleton of the new digital investigation tools and techniques. Two major issues will be addressed in the implementation of the new process: 1) the ability to predict an event (an attack) proactively, and 2) optimizing the proactive component by providing a feedback loop whenever the proactive or the reactive component is concluded.

References

[1] C. P. Grobler, C. P. Louwrens, and S. H. von Solms, "A Multi-component View of Digital Forensics," in *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, 2010, pp. 647-652.

[2] S. Garfinkel, "Anti-forensics: Techniques, detection and countermeasures," in *2nd International Conference on i-Warfare and Security*, 2007, p. 77.

[3] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation,* vol. 7, pp. S64-S73, 2010.

[4] A. Orebaugh, "Proactive forensics," *Journal of Digital Forensic Practice,* vol. 1, p. 37, 2006.

[5] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software,* vol. 80, pp. 571-583, 2007.

[6] R. Rowlingson, "A ten step process for forensic readiness," *International Journal of Digital Evidence,* vol. 2, pp. 1-28, 2004.

[7] G. Palmer, "A road map for digital forensics research-report from the first Digital Forensics Research Workshop (DFRWS)," *Utica, New York,* 2001.

[8] R. Mark, C. Clint, and G. Gregg, "An Examination of Digital Forensic Models," *International Journal of Digital Evidence,* vol. 1, pp. 1-12, 2002.

[9] B. Carrier and E. Spafford, "An event-based digital forensic investigation framework," in *In Proceeding of the 4th Digital Forensic Research Workshop*, 2004, pp. 11-13.

[10] V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process Model," *Asian Journal of Information Technology,* vol. 5, pp. 790-794, 2006.

[11] M. Kohn, J. Eloff, and M. Olivier, "Framework for a digital forensic investigation," in *Proceedings of Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference,* 2006.

[12] P. Stephenson, "A comprehensive approach to digital incident investigation," *Information Security Technical Report,* vol. 8, pp. 42-54, 2003.

[13] P. Stephenson, "Completing the Post Mortem Investigation," *Computer Fraud & Security,* vol. 2003, pp. 17-20, 2003.

[14] W. Harrison, "The digital detective: An introduction to digital forensics," in *Advances in Computers, Vol. 60*. vol. 60, ed, 2004, pp. 75-119.

[15] N. L. Beebe and J. G. Clark, "A hierarchical, objectives-based framework for the digital investigations process," *Digital Investigation,* vol. 2, pp. 147-167, 2005.

[16] R. S. C. Ieong, "FORZA - Digital forensics investigation framework that incorporate legal issues," *Digital Investigation,* vol. 3, pp. 29-36, 2006.

[17] M. Khatir, S. M. Hejazi, and E. Sneiders, "Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics," in *Digital Forensics and Incident Analysis, 2008. WDFIA '08. Third International Annual Workshop on*, 2008, pp. 21-29.

[18] M. M. Pollitt, "An Ad Hoc Review of Digital Forensic Models," in *Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on*, 2007, pp. 43-54.

[19] S. Yong-Dal, "New Digital Forensics Investigation Procedure Model," in *Networked Computing and Advanced Information Management, 2008. NCM '08. Fourth International Conference on*, 2008, pp. 528-531.

[20] D. Billard, "An Extended Model for E-Discovery Operations," in *Advances in Digital Forensics V*. vol. 306, G. Peterson and S. Shenoi, Eds., ed: Springer Boston, 2009, pp. 277-287.

[21] A. Tanner and D. Dampier, "Concept Mapping for Digital Forensic Investigations," in *Advances in Digital Forensics V*. vol. 306, G. Peterson and S. Shenoi, Eds., ed: Springer Boston, 2009, pp. 291-300.

[22] C. Ruan and E. Huebner, "Formalizing Computer Forensics Process with UML," in *Information Systems: Modeling, Development, and Integration*. vol. 20, J. Yang, A. Ginige, H. C. Mayr, and R.-D. Kutsche, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 184-189.

[23] J. Slay, Y.-C. Lin, B. Turnbull, J. Beckett, and P. Lin, "Towards a Formalization of Digital Forensics," in *Advances in Digital Forensics V*. vol. 306, G. Peterson and S. Shenoi, Eds., ed: Springer Boston, 2009, pp. 37-47.

[24] J. Kizza, "Computer Crime Investigations-Computer Forensics," in *Ethical and Social Issues in the Information Age*, ed: Springer London, 2007, pp. 343-358.

[25] S. Selamat, R. Yusof, and S. Sahib, "Mapping process of digital forensic investigation framework," *IJCSNS*, vol. 8, p. 163, 2008.

[26] S. Perumal, "Digital forensic model based on Malaysian investigation process," *IJCSNS*, vol. 9, p. 38, 2009.

[27] B. Carrier and E. Spafford, "Getting physical with the digital investigation process," *International Journal of Digital Evidence*, vol. 2, pp. 1-20, 2003.

[28] S. Ciardhu·in, "An extended model of cybercrime investigations," *International Journal of Digital Evidence*, vol. 3, pp. 1-22, 2004.

[29] M. Rogers, J. Goldman, R. Mislan, T. Wedge, and S. Debrota, "Computer forensics field triage process model," *Journal of Digital Forensics, Security and Law*, vol. 1, pp. 27-40, 2006.

[30] F. Freiling and B. Schwittay, "A common process model for incident response and computer forensics," in *3rd International Conference on IT-Incident Management and IT- Forensic*, 2007.

[31] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *NIST Special Publication 800-86*, 2006.