International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 2– No.2, June 2012 – www.ijais.org

Multi-Perspective Cybercrime Investigation Process Modeling

ATSA ETOUNDI Roger
University of Yaounde I
Faculty of Sciences
Cameroon

MBOUPDA MOYO Achille
University of Yaounde I
Faculty of Sciences
Cameroon

ABSTRACT
Several works have been carried out in the domain of cybercrime investigation. Each of the resulting models is based on a set of activities that should be performed in order to obtain the required evidences that are needed in the court for prosecution. In the literature, three processes have been highlighted for the digital forensic investigation based on a current situation; they include proactive, active and reactive processes. However, none of the defined approaches for investigation has taken into consideration the three perspectives despite the fact that they are linked together in the management of cybercrime within an organization. Moreover, there is no agreement in the definition of different tasks to be performed for each process in the achievement of the associated investigation goal. Each researcher comes with a specific set of activities based on the case under studies. In the same manner, the ordering of activities for a given process is not clearly specified; therefore, in different cases using the same process with the same activities, the associated executions are sometimes very different. There is a lack of standards in the cybercrime investigation processes. As the cybercrime increases in the modern society based on the use and the growth of ICTs (Information and Communication Technologies), there is an urgent need to set up a standard which takes into account the above issues. This paper proposes a multi-perspective cybercrime investigation process modeling that can be considered as a basis for standardization. The proposed model is constructed by extending and unifying the existing approaches.

Keywords
Computer forensics, Cybercrime investigation, Forensic process models, Proactive forensic investigation, Active and Reactive forensic investigation.

1. INTRODUCTION
The use of computer systems todays either as an object of crime, an instrument used to commit a crime or a storehouse of evidence related to a crime has led to the emergence of computer forensics [1]. When an infraction implies an information technology support, a fast and methodical intervention must be committed to bound and protect the crime scene. These procedures are indispensable, before any analysis, to guarantee the control and the admissibility of the evidence collected and treated in case of legal proceedings. The development of many forensic investigation models by countries and organizations is the obvious consequence of the spread of digital crime and its rising rate of improvement all over the world. The technological aspect of investigation is the goal of the ones, and data analysis part for the others [3]. Very few of the existing models take into account a proactive or active digital investigation process. Whenever conducting a computer investigation for potential criminal violations of the law, the legal process only depends on local cyber law. Anyway, the investigation is made after a complaint and the prosecution follows. The increasing rate of computer crimes is a fact. For example: the use of anti-forensic methods as the "Zeus Botnet Crime-ware toolkit" that has the ability to counteract digital forensic investigations with its obfuscation levels. Thus, some specific types of proactive investigation methods or systems are required viewing the volatility and the dynamicity of the information flow in such a toolkit. In this paper, we present a brief overview of previous forensic models and propose a model which explores the different processes involved in the investigation of cybercrime in case of proactive, active and reactive forensic approaches. Furthermore, the model can be used in a proactive way to identify opportunities for the development and deployment of technology to support the work of investigators, and to provide a framework to capture and analyze the requirements for investigative tools, particularly for advanced automated analytical tools. At present, there is a lack of general models specifically directed at cybercrime investigations. The current models focus on part of the investigative process (that concerns gathering, analyzing and presenting evidence) but a fully general model must integrate other important aspects to be comprehensive.
The rest of the paper is organized as follows. Section 2 outlines the previous works. Section 3 describes the proposed model. Section 4 lays out a mapping between the proposed model and the previous ones. Section 4 deals with the conclusion and highlighting some perspectives as future works.

2. PREVIOUS WORKS
Although several models exist within the digital forensic industries, there are essentially limited to reactive digital forensics. The investigation of the crime scene and the evidence are the main targets of most of the existing models; as such, their sphere of action is very tight [4]. Other models have tended to concentrate on the middle part of the process of investigation, i.e. the collection and examination of the evidence. However, the earlier and later stages must be taken into account if a comprehensive model is to be achieved, and in particular if all the relevant information flowing through an investigation is to be identified.
In accordance with the documentation, very few writings have considered a proactive digital forensic investigation process. Some of these writings have mentioned very clearly the proactive process, while the others did not. However, all have

revealed that such a process is essential. In [10], CP *Grobler and al.* proposed a high-level framework that consider three components, Proactive DF (the proactive reorganization and describing of processes, procedures and technologies in order to generate, accumulate, preserve and manage exploitable digital evidence so as to facilitate a successful, cost effective investigation, with minimal interruption of business activities), Active DF or "live forensics" (the skill of an organization to easily identify, collect, and preserve exploitable digital evidence in a live environment so as to enable a prosperous investigation) and Reactive DF or "dead forensics" (the methodical and exploratory practices used for the identification, extraction, preservation, documentation, analysis, and interpretation of digital media stored or encoded for evidence issue).

In [11], *Soltan Alharbi and al.* proposes a digital forensic model with two components : Proactive and Reactive Digital forensic investigation. The proactive component deals with the collection of live evidence in real time while an event or incident is happening. The reactive component is the traditional approach to digital forensic investigation.

A multi-component view of the digital forensic investigation process proposed in [10] is a high-level view of the investigation and, as such, cannot directly be operationalized to create automated tools. Additionally, the process described in this model contains phases, such as service restoration, that lie outside the scope of the investigation. So doing, the investigator roles and those of the incident response team of an organization are completely confused. Furthermore, the proactive digital forensic aspect of the multicomponent view proposed by *Grobler and al.* only focuses on the readiness.

Proactive and Reactive Digital forensic investigation process proposed in [11] do not take into account the eventuality of an attack during the investigations. This model entirely ignores the readiness in its reactive component in the case that an organization is not able to set up proactive or anti-forensic measures. Furthermore, there is a misplacement of the *event triggering function* which involves abusive storage in proactive collection step.

All these breaches lead us to set up a multiperspective model of investigation which automation (future works) would lead to an efficient conditioning of the digital evidence ready to be received in a court of law.

3. THE PROPOSED MODEL

The proposed model holds on proactive, active and reactive components. A detailed description of each one follows.

3.1 Proactive digital forensics (ProDF) component

Proactive Digital Forensics is the proactive reorganization and describing of processes, procedures and technologies in order to generate, accumulate, preserve and manage exploitable digital evidence so as to facilitate a successful, cost effective investigation, with minimal interruption of business activities. That forensics disposition must be establish so as to involve negligible business activity interruption. It will ensure that admissible evidence and sound processes are in place and available when needed for an investigation or as required during the normal flow of business. Requirements for admissible evidence are specific to the country, the jurisdiction and the industry. The success of any investigation is determined by the credibility of the evidence [10]. Therefore, Proactive Digital Forensic Component is the ability to proactively identify, collect, gather an event, preserve and analyze evidence to detect an incident as it eventually occurs. Furthermore, a programmed documentation is produced for a later investigation by the active and reactive components [11]. The evidence contained within this component is proactive evidence that leads to a specific event or incident as it happens [12].

This proactive component differs from common Intrusion Detection Systems (IDS) by safeguarding the integrity of evidence and preserving it in a forensically sound manner, while IDS only detects an intrusion as it happens and be able to respond to it. In addition, the analysis of the evidence will be done so as to be admitted in a court and enable prosecution of the suspect.

Phases under the proactive component are defined as follows:

1. **Alert**: According to the local cyber law, the incidence response team of any organization should display an alert system considering a set of cataloged incident.
2. **Identification**: Identified data in the order of volatility and priority, and related to a specific requirement of an organization. Hostile and outstanding behaviors are also selected and cataloged.
3. **Collection**: Programmed live collection of identified data and unusual behaviors. This can be done by a trigger event that will start live data collection as soon as certain types of incident alerts are detected.
4. **Preservation**: Automated preservation of the evidence related to the suspicious event, via hashing methods.
5. **Analysis**: Automated live analysis of the evidence, which might use forensic techniques such as data mining to support and construct the initial hypothesis of the incident.
6. **Documentation**: Automated report for the proactive component.

3.2 Reactive digital forensics (ReaDF) component

None of existing organizations are fully prepared for incidents. Reactive Digital Forensics as defined by this paper focuses on the traditional DF investigation that will take place after an incident had been detected and confirmed. This includes physical investigation (eventually), identifying, preserving, collecting, analyzing, and generating the final report. Should an incident happen, there should be an acceptable proven DF investigation protocol in place as detailed by ProDF on how to conduct the investigation [10]. Reactive evidence refers to collecting all the static evidence remaining, such as an image of a hard drive. The goals of ReaDF are to [11]:

- Successfully investigate an incident (offences);
- Collecting evidence;
- Determine the root-cause of the incident;
- Identify and link the perpetrator and accomplices to the incident.

As result of various DF methodologies or investigation protocols studied from literature, many authors have proposed the inclusion of the following phases with steps [1-9].

1. **Complaint/Alert/Individual detection**: Detect an incident, activity or offences; report the incident; check Readiness [6]; determine the assessment of worth, incident confirmation; obtain an authorization; obtain search warrant; determine a containment strategy; formulate an investigation plan; coordinate the resources; accelerate the investigation; notification of the investigation.

2. **Physical Investigation**: It is absolutely necessary to take in account the physical crime scene to gather as much evidence as possible so as to ensure successful investigation, even if it is a DF investigation. Steps involve the security of the physical crime scene; survey of crime scene for potential evidence; examine witness, search and collect; documentation (label and seal all evidence); acquire; analyze; identify possible digital evidence; reconstruct the event; make a finding; transport and store the evidence.
3. **Digital Investigation**: The success of the investigation is determined by the essential steps followed during this phase. The steps are:

Evidence acquisition: This step consist of identification and seizure, preservation and collection of evidence; acquirement of the relevant evidence if live evidence is required, activation of the ActDF component; ensure integrity; authentication; transportation of the evidence; storage of the evidence; and documentation of the acquisition process.

Identification: The investigator is mostly interested by the process of identifying all the electronic equipment used by the suspect. Additional imperative sub-procedure will be identifying fragile or volatile evidence. Live acquisition process can be set up to retrieve the file time stamp, registry key, swap files, and memory details. All what is mentioned above falls under the fragile evidence category as most probably will change or will be lost upon the plugging of the power cable. The investigators must try to obtain the maximum information from the various people present in the scene, without violating the jurisdictional laws and corporate policies. Everything surrounding the incident (those who reported it at first, the date and the time) has to be taken in account. It is important to make a list of those present at the scene, those who came after, and those who left, etc., at the same time with the summary of their activities while at the scene. It is very important to put people per group (victims, suspects, bystanders, witnesses, other assisting personnel etc..) and store their location by the time they entered.

Preservation: All the evidence collected has to be located in a safe place as it is important that the evidence is safe from tempering and need to preserve the integrity of the evidence. Thus, cybercrime investigators establish "police line" to protect evidence of damaged cybercrime scene. They set cybercrime evidences collection equipment such as Encase, imaging devices in the victim scenes. Evidences in the victim scenes can also be obtain through photo evidences by digital or video camera. Thus, all the electronic devices at the scene must be photographed along with the power adaptors, cables, cradles and other accessories. What is appearing on the screen should also be documented if the digital or mobile device is unpowered. A record of all visible data must be created, which helps in recreating the scene and reviewing it any time. This is mainly important when the investigator has to do a testimony in a court, which could be several months after the investigation.

Collection: The investigating organization takes possession of the evidence in a form which can be preserved and analyzed in the collection step. So doing, some activity of the investigator can consist of imaging hard disks or seizure of entire computers.

- ***Collect Volatile Evidence***: Most of the evidence concerning mobile devices are volatile, because they are present in Random Access Memory. Because the device state and memory contents can be changed, the collection of volatile evidence presents a serious problem. The choice of collecting evidence at the crime scene or after in a secure forensics workshop will lie on the specific situation, taking in account the ongoing power state. If the device is running out of battery power, the entire information will be lost soon. In that case, adequate power needs to be maintained if possible by using the power adaptor or replacing batteries. In case the battery power is not sure, the memory contents should be copied using suitable tools as fast as possible. To obtain better results, it is suitable to combine tools. A suitable power supply ought to be maintained through recharging or replacing the battery. In case sufficient power is not possible to be provided, the device must be switched off to save battery and the content of the memory. At this stage, the presence of any malicious software installed by the user has to be checked too.
- ***Obtain the evidences of storage media***: This stage deals with collecting evidence from external storage media lying on devices like MMC cards, compact flash (CF) cards, memory sticks, secure digital (SD) cards, USB memory sticks etc. Evidence from computers, which are synchronized with these devices, must be collected. Appropriate forensic tools must be used for collecting evidence to ensure its admissibility in a court of law. The integrity and authenticity of the evidence collected should be ensured through techniques like hashing, write protection etc. It is important to collect all power cables, adaptors, cradle and other accessories. Care should also be taken to look for evidence of non-electronic nature, like written passwords, hardware and software manuals and related documents, computer printouts etc.
- ***Obtain the evidences of network [10][15]***: This consist of capturing, recording, analyzing network audit trails in order to discover the source of security breaches or other information assurance problems. Not all the information captured or recorded will be useful for analysis. Network forensic systems are mainly classified as "Catch it as you can" and "Stop, look and listen" systems. Most network forensic systems are based on audit trails. Network forensic products are sometimes known as Network Forensic Analysis Tools (NFATs). For example, nstreams, slogdump, tcpflow, chaosreader, dhcpdump, etc. This stage involves proper documentation of the crime scene along with photographing, sketching and crime-scene mapping.

Analysis: The investigative team will revisit the investigation plan; review the relevance of tools and expertise available; develop the hypothesis; analyze the evidence; test the hypothesis; make a finding; validate the results of analysis; document the case; and secure the documentation.

4. **Reconstitution**: The physical investigation phase (1) and digital investigation phase (2) findings will be strengthened by the investigation team in this stage. In the case of lack of evidence to support the hypothesis, repeat phase (1) and (2). A well documented report in approving the hypothesis is the main aim of this phase.
5. **Present findings to management or authorities**: Legal jurisdiction location requirements are taken in account by the investigation team while preparing the case; the timeline of the whole case is to be incorporated; the target audience has to be determined; expert witness should be prepared; exhibits have to be prepared; suitable presentation aids should be used; and the chain of custody

and the evidence should be preserved while presenting the case. The protocol must also involve an appeal process.

6. **Dissemination of results of investigations**: It is very important to review the result of the identified case an apply lessons learned from it. All evidence ought to be preserved, returned or disposed, in accordance with the policies.
7. **Incident closure**: A waterfall framework seems to characterize all identified phases for ReaDF with some eventual repetition (whenever needed) between the different phases. ReaDF as discussed meets the need to investigate incidents to reveal the root-cause of an incident and successfully prosecute a perpetrator.
8. **Final report**: Documentation is a permanent loop back needed in all the stages of investigation and required to maintain proper chain of custody. A final report is produced at the end of investigations.

3.3 Active digital forensics (ActDF) component

ActDF is the skill of an organization to easily identify, collect, and preserve exploitable digital evidence in a live environment so as to enable a prosperous investigation. Eventually based on the documentation powered by the Proactive Digital Forensic, the goals for ActDF are [10]:

- Reduce the effect and impact of an ongoing incident;
- Collect relevant live receivable digital evidence (including volatile evidence) on a live system or production environment by using appropriate tools and technologies;
- Provide a meaningful starting point for a reactive investigation within the parameters of the risk control framework of the organization.

We have identified the following phases for Active Digital Forensics from the literature [13-16] and have formulated the following phases independent of any tool or technology.

1. **Complaint / Alert / Individual detection**: Once the investigators are on the scene, they have to rapidly identify volatile or live evidence and determining which of them have to be preserved to successfully investigate the incident or to acquire potential missing evidence for a new or unknown incident; From this point, an investigation plan is supposed to be set up. The management plan of the organization is to be taken into consideration. Therefore, Reactive DF must be activated whenever the risk management policies of the organization did not allow the continuity of the current Active DF evidence acquisition. It important for an organization to have a trigger event because a predefined one is supposed to be activated to release monitoring or other procedures as soon as an incident alert is activated. At the end, a containment strategy must be deployed. This is very important as ActDF deals with ongoing or real time incidents.
2. **Active investigation**:

Evidence acquisition: (Part 3 of ReaDF applies). All the remaining evidence that can be exploited or used as proof of any type of dis-functioning should be collected with the use of appropriate tools. In fact, some specific technologies or applications are required to profile the attacker, gather volatile evidence or to determine the source of the attack. Those applications can also serve to collect additional live evidence lacking from, or required by the exploitable digital evidence map. The next act is to secure and authenticate all the extracted data. This is easily done by hashing immediately after the collecting process to preserve before analysis. To ensure that chain of custody of the evidence acquired was maintained, all performed actions must be documented. There exists several applications capable of collecting digital evidences. A good technology is to be chosen in order to automatically collect such information. Some authors like *Ieong and Leung* [15] hold that human intervention in the collection of evidence should be reduced to the lowest rate. They affirm that all what is necessary is to be done by human intervention be reduced at all course. The static digital evidence is to be recorded without any modifications. In all, according to these authors, data acquisition should follow the order of volatility and priority of digital evidence collection; the other evidence which is not priority can be acquired using traditional evidence collection methods. The extraction of the data obtained can only be done when the original data has not been altered or corrupted. [4].

Analysis: (Part 3 of ReaDF applies). The primary acquires evidences are to be analyzed in order to determine whether it constitutes sufficient information for the reconstruction of the incident or it is in line with the initial hypothesis. It is of great importance to document progressively all the activities that are being carried out. That is the different task realized, actions that are undertaken with the aim assuring that the evidences are acquired completely. The regularity and the reliability of the results are to be assured. The computer on which the operating system is still running should be totally examined by using custom forensic technics or existing system administrator tools for the extraction of evidences. This practice is suitable when we have to do with encrypting file systems for example, where the encryption keys has to be collected and, in some instances, an image of the logical hard drive volume should be realized before turning off the computer.

Reconstitution: Here, results from the analysis should be exploited and one can proceed to a brief reconstruction of the incident. The prime objective of this phase is to establish whether sufficient evidence have been assembled so as to put an end to ActDF. However, ActDF can be repeated if the amount of evidence needed is not yet attained.

Incident closure: If on the other hand sufficient evidence has been accumulated, the investigation team now documented case files with exploitable digital evidence for the reactive investigation team to complete investigation. As soon as the ActDF investigation ends, the Reactive DF component has to continue its analyzes and reconstruct the incident basing on all the other evidences (comprising physical evidence and static exploitable digital evidence) which will serve in drawing conclusions of the investigation. In fact, during ongoing attacks, the ActDF component meets the need to gather live evidence.

3.4 Interactions between suggested components

In this subsection, we discuss the relationship between the different components of digital forensic to demonstrate the dependency between these components.

A complaint about an incident, an alert or an individual/automatic detection of an incident is the starting point of an investigation; a trigger event is known to be set-up by organizations to permanently perform live data acquisitions as soon as certain types of incident alerts are detected in proactive investigation purposes. The established

rules about any suspicious activity or event detection determine whether to run an investigation or not. If an investigation is needed, the investigator must consult the exploitable digital evidence map of the organization delivered at the ProDF component as well as the risk profiles and risk profile case scenarios mentioned in the incident guide books. If there is not sufficient evidence or the need for live evidence, ActDF must start, otherwise the ReaDF component will be activated. Once the investigator is satisfied that sufficient evidence exist, the ActDF component is terminated and the ReaDF component is then activated.

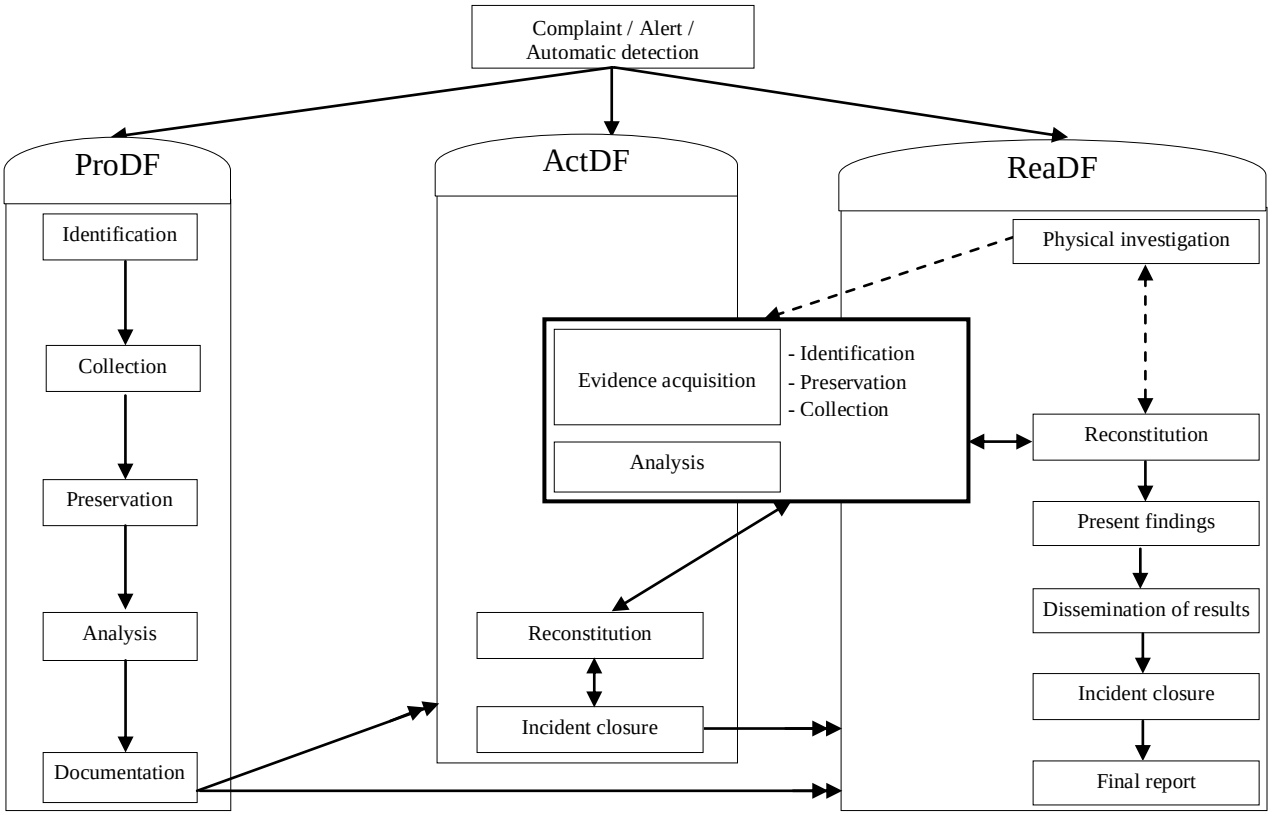

Fig 1: Process for ProDF, ActDF and ReaDF investigation system and interactions

4. MODELS MAPPING

CP Grobler and al. in 2010 [10] have defined a mapping between their model and the existing ones. They argue that their model is more appropriate than the previous models. Their argument was based on the advantages of their model compared to previous existing models. However, their proposed model does not cover the entire digital forensic investigation process. It does not deal with the proactive investigation integrating identification, collection, preservation, and analysis of salient data to prevent attacks. Dealing with this perspective, *Soltan Alharbi and al* in 2011 [11] have proposed a proactive-reactive digital forensic approach. However, this approach does not take into consideration the attacks detection. Furthermore, the ActDF process is quite ignored. This lies to insufficient actions to be undertaken to efficiently address reactive issue of digital

Digital forensic model	Proactive investigation						Active investigation					Reactive investigation								
	Alert	Identification	Collection	Preservation	Analysis	Documentation	Complaint / Alaert / Individual detection	Evidence acquisition	Analysis	Reconstitution	Incident closure	Complaint / Alaert / Individual detection	Physical Investigation	Evidence acquisition	Analysis	Reconstitution	Present findings	Dissemination of results	Incident closure	Final report
A multi-component view of Digital Forensics, 2010							√	√	√	√	√	√	√	√	√	√	√	√	√	√
The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review, 2011		√	√	√	√	√								√	√					√
Multi-perpective cybercrime investigation process modeling, 2012,	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

Table 1: Models mapping

investigation. Based on the different activities that need to be carried out in the digital forensic investigation process, the following table gives the mapping between the *CP Grobler and al.* model, the *Soltan Alharbi and al.* model and our proposed model. In this defined table, the symbol √ specifies the fact that the approach supports the associated activity. Moreover, the absence of this symbol denotes the fact that the approach does not address a given activity. By comparing the different rows representing each model, the row representing our proposed model support all the activities that should be taken into consideration in dealing with digital investigation within an organization. These activities are regrouped into reactive, active and proactive process and should be conducted within an organization that needs to efficiently face the cyber crime problem. The main problem in this domain is the definition of a complete investigation process of cybercrime. Our model gives the base for this process that needs to be validated by its application in various cybercrime situations within organizations. When this process will be validated, the next step will be the concrete implementation of the associated activities. In this phase, the Service Oriented Architecture (SOA) can be used since each main activity, i.e proactive, active and reactive, can be seen as a service. This is one of our future focuses.

5. CONCLUSION AND SUGGESTIONS FOR FUTURE WORKS

A detailed digital forensic procedure provides important assistance to forensic investigators in gathering evidence admissible in a court of law. From the digital forensic investigation process model proposed, it has been clearly stated that the investigation process will lead into a better prosecution as the very most important stages such as live data acquisition and static data acquisition are being implanted to focus on fragile evidence. Several models have already been established in the digital forensic field. However, none of this models take into consideration the overall investigation process characterize by three main interrelated activities: (a) Proactive digital forensics; (b) Active digital forensics; (c) Reactive digital forensics. In this paper, a multi-perspective cybercrime investigation process model has been defined by considering the three mains activities defined above. The defined model has been compared with the proposed models in [10, 11]. This comparison shows that the proposed digital forensic model takes into consideration the different properties of the three activities which is not the case for the previous models. The digital forensics community needs a structured framework for the rapid development of standard operational procedures that can be peer-reviewed, tested effectively and validated quickly. Digital forensics practitioners can benefit from the iterative structure proposed in this research paper to build forensically sound cases. The proposed model aims to develop a consistent and simplified forensics guides on digital forensic investigations that can be a guideline for standard operational procedure and a model for developing future technologies in digital forensic investigations.

This work does not consider the detection of an attack for which the inherent alert is the condition for beginning a digital investigation; In perspective, investigation are required to be done in order to extend the defined model by taking into consideration the detection of an attack in order to trigger the investigation process. Moreover, some case studies need to be done in order to validate the model.

6. REFERENCES

[1] Yong-Dal Shin. "New Model for Cyber Crime Investigation Procedure". Journal of Next Generation Information Technology, Volume 2, Number 2, May 2011.

[2] Inikpi O. Ademu, Dr Chris O. Imafidon, Dr David S. Preston: "A New Approach of Digital Forensic Model for Digital Forensic Investigation". (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.12, 2011.

[3] Sundresan Perumal: "Digital Forensic Model Based On Malaysian Investigation Process". IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[4] Séamus Ó Ciardhuáin: "An Extended Model of Cybercrime Investigations". International Journal of Digital Evidence Summer 2004, Volume 3, Issue 1.

[5] Ankit Agarwal, Megha Gupta, Saurabh Gupta \& Prof. (Dr.) S.C. Gupta: "Systematic Digital Forensic Investigation Model". International Journal of Computer Science and Security (IJCSS), Volume(5): Issue(1): 2011, 118-131.

[6] Baryamureeba and Florence Tushabe: "The Enhanced Digital Investigation Process Model". Institute of Computer Science, Makerere University P.O.Box 7062, Kampala Uganda www.makerere.ac.ug/ics.

[7] Brian Carrier Eugene H. Spafford: "Getting Physical with the Digital Investigation Process". International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2.

[8] W. Thomas: Automata on Infinite Objects". Handbook on Theoretical Computer Science, J. Van Leeuwen, ed, pp. 133-187, Elsevier Science, 1990.

[9] G. Berry, P. Couronne and G. Gonthier:} "\texttt{Synchronous Programming of Reactive Systems: An introduction to ESTEREL". Proc. 1st Franco-Japanese Symp. on programming of Future Generation Computers, 1986, Tokyo. pp.35-56.S. Garfinkel, "Anti-forensics: Techniques, detection and countermeasures," in 2nd International Conference on i-Warfare and Security, 2007, p. 77.

[10] CP Grobler, CP Louwrens, SH von Solms "A multi-component view of Digital Forensics}". International Conference on Availability, Reliability and Security, 2010.

[11] Soltan Alharbi, Jens Weber-Jahnke, Issa Traore: "The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review". International Journal of Security and Its Applications Vol. 5 No. 4, October, 2011.

[12] A. Orebaugh: "Proactive forensics". Journal of digital forensic Practice, vol. 1, p. 37, 2006.

[13] Ieong, R. and H. Leung: "Deriving Cse-specific Live Forensics Investigation Procedures from FORZA". In Symposium on Applied Computing archive Proceedings of the 2007 ACM symposium on Applied computing 2007. Seoul, Korea: ACM Press New York, NY, USA.

[14] Ren, W. and H. Jin: "Honeynet Based Distributed Adaptive Network Forensics and Active Real Time Investigation". In 2005 ACM Symposium on Applied Computing. 2005. Santa Fe, New Mexico, USA.

[15] Foster M, W.J: "Process Forensics: A pilot study on the use of checkpointing technology in computer forensics". International Journal of Digital Evidence, 2004. 3(1).