A NEW APPROACH FOR RESOLVING CYBER CRIME IN NETWORK FORENSICS BASED ON GENERIC PROCESS MODEL

Mohammad Rasmi[1], Aman Jantan[2], Hani Al-Mimi[3]

[1, 2]School of Computer Sciences, Universiti Sains Malaysia
[3]Faculty of Science & Information Technology, Al-Zaytoonah University
[1, 2]Penang /Malaysia, [3]Amman /Jordan
[1]mr77mr@hotmail.com, [2]aman@cs.usm.my, [3]hani_mimi@yahoo.com

Abstract

Current network forensics approaches are costly and time consuming. In addition, these approaches normally use active and reactive processes to resolve cyber crimes, and such processes start after the cyber crime has been identified, which makes identifying useful evidence difficult. Moreover, the information required to understand and resolve cyber crime are limited. This paper proposes a new approach to resolve cyber crime in network forensics. The proposed approach aims to use cyber crime evidence to help investigators to resolve cyber crime efficiently. The paper presents the current network forensics approaches and various existing digital forensics models in order to determine the suitable process to be used in the proposed approach. Thus, the proposed approach based on the generic and modern process model for network forensics.

Keywords - Network Security, Cyber crime, Network forensics.

1 INTRODUCTION

Network forensics extends from network security and computer forensics [1]; it works with the laws and guiding principles indicated in the judicial system, as shown in Fig.1. Traditionally, forensic specialists work hand in hand with law enforcement officers. The former utilizes scientific techniques to collect, examine, analyze, and document digital evidence from digital sources and network security programs. These techniques are incorporated into firewalls, intrusion detection systems, or network devices such as routers and switches to uncover facts related to cyber crime [2, 3].

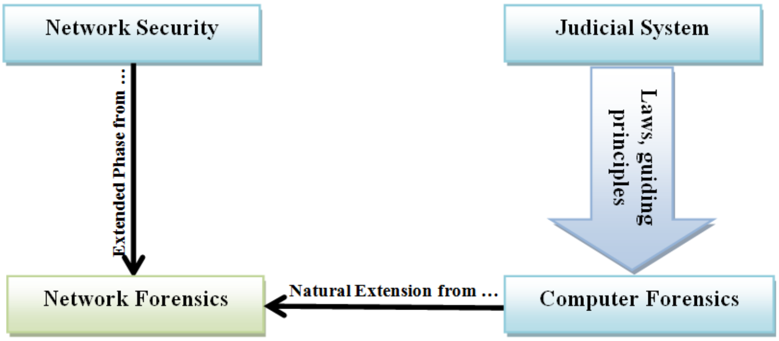

Fig. 1. Network Forensics Locations

In early 2001, the first Digital Forensics Research Workshop (DFRWS) [4] defined network forensics as “the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, or compromise system components as well as providing information to assist in response to or recovery from these activities.” This definition indicates that the main phases of network forensics are collection, fusion, identification, examination, correlation, analysis, and documentation of digital evidence. These phases guide other researchers in proposing new approaches for network forensics. The identification of the deliberate intent behind cyber crimes is the main goal of network forensics.

Network forensic systems as reported by Pilli et al. [5, 6] can be classified depending on the three characteristics indicated in Fig. 2. The group also proposed two approaches in network forensics: proactive and reactive. Proactive network forensics is a new approach in live investigation that deals with the phases of network forensics during an attack. In contrast, reactive network forensics is a traditional approach that deals with cyber crime cases after a period of time, which consumes a considerable amount of time during the investigation phase. As reported by [7-10], proactive forensic approaches reduce the time and cost of investigation by identifying potential evidence and reducing the resources needed in the investigation phase. These approaches are utilized in the preliminary analysis of a cyber crime and help improve and accelerate the decision making process.

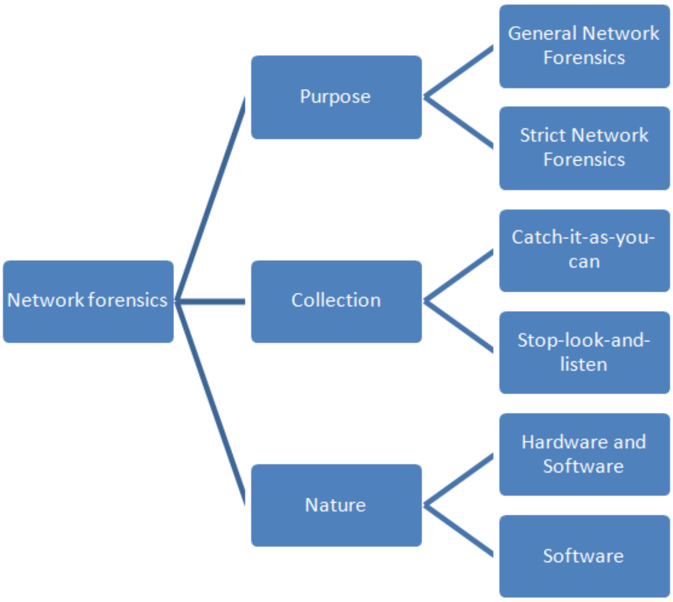

Fig. 2. Network Forensics System Classifications

This paper is proposing a new approach to resolve cyber crime for network forensics.. The approach based on the generic process model for network forensics as mentioned in [5], which will be described in section 3. The proposed approach is described in section 4, where the process will be illustrated. The next section will present a related work of network forensics approaches.

2 CURRENT NETWORK FORENSICS APPROACHES

This section reviews literature on network forensic approaches and their processes. The section shows how other approaches dealt with network forensic processes to resolve cyber crimes. The main goal of this section is incorporated with the related studies that deal with the analysis phase of network forensics. The section also aims to discover the limitation of the analysis phase in network forensic approaches as well as to show the relationship between the analysis phase and other phases.

In August 2001, the first Digital Forensics Research Workshop (DFRWS) [4] defined the first network forensic reactive approach as a generic investigation framework that can be applied to network environments and to most investigations. The framework includes six classes of tasks, i.e., identification, preservation, collection, examination, analysis, presentation, and decision making. Reith M. refined the DFRWS framework in 2002 and proposed a new model called Abstract Digital Forensics (ADF) [11]. This model consists of nine phases, i.e., identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence. The model creates a standardized framework for network forensics. The drawback of this model is that it provides a general definition of phases without providing any details on practical methods to test and implement the model.

Network forensic approaches are generally categorized into three sections. The first section reviews the approaches based on the Integrated Digital Investigation Process (IDIP) framework [12]. The second section reviews the general proposed approaches. The last section reviews the approaches that work proactively.

2.1 IDIP-based Network Forensics Approaches

In 2003, the IDIP framework proposed by [12], which is based on the investigation process of a physical crime scene. This framework has seventeen phases which are organized into five groups, as shown in Fig. 3. The groups are readiness (operations and infrastructure) phases, deployment (detection and notification and confirmation and authorization) phases, physical crime scene investigation (preservation, survey, documentation, search and collection, reconstruction, and presentation) phases, digital crime scene investigation (preservation, survey, documentation, search and collection, reconstruction, and presentation) phases, and review phase. The reconstruction phases are similar to the analysis phase in the ADF model in which the processes of the analysis phase are conducted by the search and collection phase of the digital crime scene investigation group. This framework is used as a guideline in law enforcement to resolve cyber crimes because the framework utilizes physical crime scene investigation.

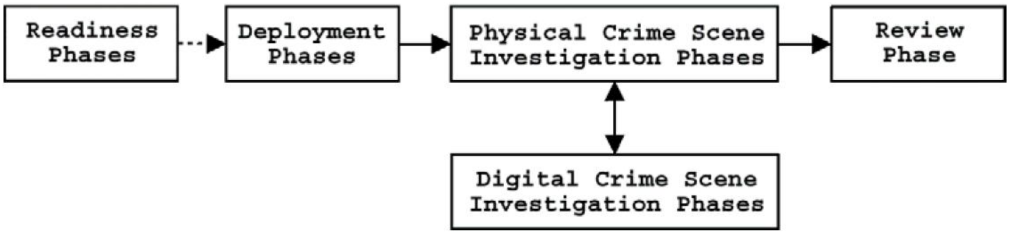
Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

Fig. 3. The five groups of phases in the Digital Investigation Process (IDIP), [12]

Another approach was suggested by [13]. The approach, which is called End-to-End Digital Investigation (EEDI), combines the tools of the traditional investigative methods. The approach was developed based on the DFRWS framework. EEDI consists of nine processes: evidence collection, analysis of individual events, preliminary correlation, event normalizing, event deconfliction (uncountable), second-level correlation, timeline analysis, chain of evidence construction, and corroboration. The researcher developed a formal representation through the Digital Investigation Process Language (DIPL), which is a formal process language utilized to represent the investigation of a cyber crime incident, to present the aforementioned processes. DIPL is derived from the List Processing (LISP) programming language. The EEDI approach facilitated the development of new case-modeling techniques for cyber crime investigation. Unfortunately, DIPL, which adopts the EEDI approach, does not provide solutions for all cyber crime cases because it is designed to solve only specific cases [14].

A new methodology for incident response was developed by FBI special agents Mandia and Prosise (2003) [15] to help organizations investigate cyber crimes in a simple manner. This methodology has seven components: pre-incident preparation, detection of incidents, initial response, formulation of response strategy, investigation of the incident, reporting, and resolution. The analysis phase is included in the investigation component, which begins after collecting data from the same components.

In 2004, a new model called the Enhanced Integrated Digital Investigation Process (EIDIP) proposed by [16], which based on an IDIP framework [12]. This model consists of five major phases that include subphases: readiness (operation and infrastructure readiness), deployment (detection and notification, physical crime scene investigation, digital crime scene investigation, confirmation, and submission), traceback (digital crime scene investigation and authorization), dynamite (physical crime scene investigation, digital crime scene investigation, reconstruction, and communication), and review phase. The model classifies the investigation processes into two phases, namely, traceback and dynamite. These phases separate the investigations conducted at the primary and physical crime scenes and depicts the other phases as iterative instead of linear.

Another framework based on the IDIP framework proposed by [17] called the event-based digital forensic investigation framework. The framework is based on the physical crime scene and is organized into five phases that include the subphases, i.e., readiness (operation and infrastructure readiness), development (detection and notification and confirmation and authorization), physical crime scene investigation (search and reconstruction), presentation, and digital crime scene investigation phase. Each phase in this model has a clear goal and requirements to achieve the expected results. However, [18] reported that the integrated phases, when combined, are insufficient to investigate real cyber crime cases because these phases have not mention the completeness of each phases.

A new model derived from the IDIP framework by [19] called the Computer Forensic Field Triage Process Model (CFFTPM). The CFFTPM has six phases, i.e., planning, triage, usage or user profiles, chronology or timeline, Internet activity, and case-specific evidence phases. The CFFTPM provides the identification, analysis, and interpretation of cyber crime evidence within a short time frame without the need to generate a complete forensic image of the lab. However, these features do not make the model suitable for investigating all types of cyber crimes because evidence is very difficult to distinguish and collect.

An extended model of investigation was presented by [20]. The model combines the above mentioned previous models of network forensics. The model consists of thirteen activities, namely, awareness, authorization, planning, notification, search and identification of evidence, collection, transport, storage, examination, hypotheses, presentation, proof or defence, and dissemination activity. This model is more comprehensive than the previous models because it encompasses almost all the investigation activities. However, the model needs more evaluation in terms of scalability to ensure that it analyzes evidence efficiently.

The framework as above mentioned, which is based on single-tier processes, focuses on the abstract layer in each phase. The advantage of single-tier processes is that they produce unambiguous outputs. The main limitation of single-tier processes, as reported by [21], is that they reduce the scalability and flexibility of the investigation when more details are required from the user. Beebe and Clark [21] addressed this limitation by proposing a multi-tier, hierarchical framework to guide digital investigations. The first tier shown in Fig. 4 has six phases, namely, preparation, incident response, data collection, data analysis, presentation, and incident closure. The framework introduces objective-based phases and subphases to each layer in the first tier with the ability to add more details in advance to guide digital investigations, especially in data analysis. The main limitation of this framework, as stated by the researchers, is that it is incomplete and requires a more methodical approach to identify the objectives of each layer.

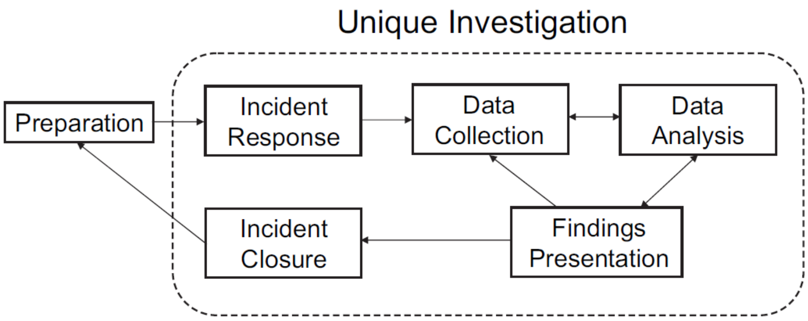

Fig. 4. The First-tier phases of a Hierarchical Framework for Digital Investigations, [21]

2.2 General Network Forensics Approaches

The first general process model for network forensics was proposed by [22]. The model performs standardization processes to cover the fundamentals of network forensics. The model, shown in Fig. 5, includes six steps, i.e., capture, copy, transfer, analysis, investigation, and presentation. These steps are divided into three process stages. The first stage identifies the basic techniques to preserve the security process. The second stage describes the status of the transformation process. The final stage provides the architecture of the proposed network forensic system to indicate the integrity of the system components. The analysis step is the most comprehensive and sophisticated step, as mentioned by [22]. However, the proposed model does not include the analysis of network traffic, which remains an open issue.

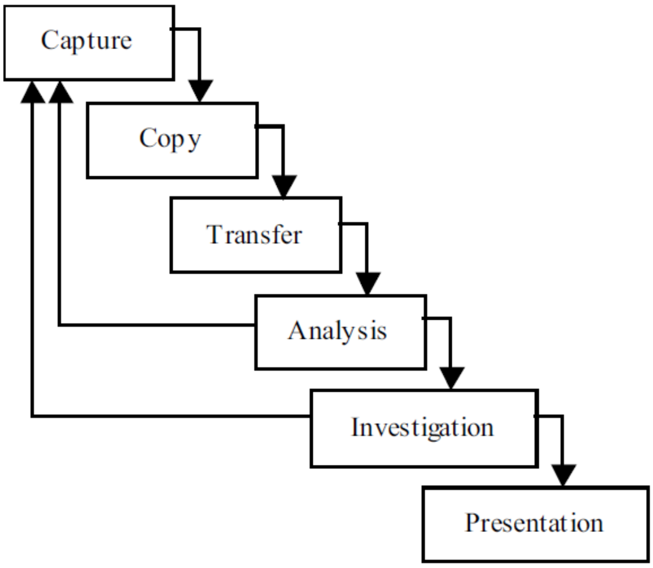

Fig. 5. The General Process Status Transfer, [22]

A new framework called the step-by-step framework was proposed by [23] to clarify the definition of network forensics. The framework studies previous research to establish a step-by-step framework, which groups all the existing processes into three stages, namely, preparation, investigation, and presentation, which are implemented as guidelines in network forensics. The proponents of the framework claim that the framework offers scalability to allow the addition of more required stages in the future. However, understanding how the framework addresses all phases of network forensics in the main stages is difficult. For example, the framework includes the analysis phase in the investigation stage without clarifying the procedures and outcomes. [24] proposed another guideline based on existing frameworks to integrate forensic techniques into incident response through a set of processes that contains four stages: collection, examination, analysis, and reporting. The proposed guideline is useful because it utilizes forensic tools to identify the rules governing the network forensic phases, especially the analysis phase.

A digital forensic investigation framework was proposed by [25] called Forensics Zachman (FORZA). The proposed framework focuses on the legal rules and participants in the organization rather than the technical procedures. The rules of FORZA depend on the Zachman framework [26]. The Zachman framework solves complex problems by integrating the answers with the questions what, how, when, who, where, and why. The FORZA framework includes eight rules: case leader, system or business owner, legal advisor, security or system architect or auditor, digital forensic specialist, digital forensic investigator or system administrator or operator, digital forensic analyst, and legal prosecutor. The FORZA framework addresses the questions of the Zachman framework for each rule, i.e., what (the data attributes), why (the motivation), how (the procedures), who (the people involved), where (the location), and when (the time) questions. The main drawback of this framework is that it is human dependent. It requires more tools to conduct a network forensic analysis and to provide accurate results in the investigation phase.

A new digital forensic model process called two-dimensional evidence reliability amplification process model was proposed by [27]. The model includes sixteen subphases and grouped into five main phases, namely, initialized, evidence collection, evidence examination or analysis, presentation, and case termination. The phases of the model are described in detail by identifying the roles of the inspector and manager for each phase. The model aims to provide answers to cyber crime questions, such as what happened, when did it happen, and who perpetrated the action, without considering the cyber crime intention and strategy analysis (why and how questions).

According to [28], a similarity exists between incident response and computer forensics. The two present a common process model for both incident response and computer forensics to improve the investigation phase. The model includes a set of steps grouped into three main phases, i.e., pre-analysis (detection of incidents, initial response, and formulation of response strategy), analysis (live response, forensic duplication, data recovery, harvesting, reduction, and organization), and post-analysis (report and resolution). Incident response is conducted in the model during the actual analysis. However, the procedures and methods of incident response are unclear in terms of the type of evidence that is utilized to analyze the incident. No standard method of detecting and collecting evidence exists, which produces insignificant evidence and affects the accuracy of the incident response.

A new digital forensics investigation procedure model was presented by [29]. The model consists of ten phases: investigation preparation, classifying cyber crime and deciding investigation priority, investigating damaged (victim) digital crime scene, criminal profiling consultant and analysis, tracking suspects, investigating injurer digital crime scene, summoning suspect, additional investigation, writing criminal profiling, and writing report. The author just proposed the block diagram without any technical details or methods to manipulate with these phases. This indicates that the author focusing on the number and the type of the network forensics phases rather than how it works and how they conduct the outcomes.

The study in [18] reviewed the existing frameworks until 2007 to construct the mapping process between the phases of digital forensics frameworks. It summarizes the mapping of processes into five appropriate phases as the following, preparation, collection and preservation, examination and analysis, presentation and reporting, and disseminating the case. The result of this study simplified the overall processes of existing frameworks in order to identify the critical and important phases for any digital forensics framework as the collection and preservation phase, examination and analysis phase, and presentation and reporting phase. In general, this mapping aims to clarify the output for each phase. However, the output of the examination and analysis phase doesn’t mention about the methods and techniques which could be used to conduct the output from this phase.

The oldest models that were proposed before 2009 have disadvantage that the categories that may be extremely general defined for practical use which is difficult for testing, and more cumbersome to use. The modern process proposed by [3, 5, 6] conducted through designing a generic process model for network forensic analysis based on various existing digital forensics models. The framework includes the following phases: preparation, detection, incident response, collection, preservation, examination, analysis, investigation, and presentation. In this research we determine the phases of this model as a baseline phases for proposing new approach in analyzing evidence in order to integrate the analysis phase with other phases. The process of the generic process model will be discussed in Section 3.

2.3 Proactive Process Approaches in Network Forensics

The approaches that utilized the proactive process are reviewed in this section. The proactive process determines the activities in advance for those processes that occur subsequently. Thus, the activities of the network forensic process begin without waiting for a response right after a cyber crime happens.

The multi-component view of digital forensics was proposed by [9]. The view includes three components, i.e., proactive digital forensics (ProDF), active digital forensics (ActDF), and reactive digital forensics (ReDF), as illustrated in Fig. 6. ReDF includes six subphases, which are incident response and confirmation, physical investigation, digital investigation, incident reconstruction, presentation of findings to the management or authorities, dissemination of the result of the investigation, and incident closure. ActDF includes four subphases: incident response and confirmation, ActDF investigation, event reconstruction, and ActDF termination. The ProDF component defines and manages the processes and procedures of the comprehensive digital evidence. The same authors proposed a theoretical framework [10] to guide the implementation of proactive digital forensics and to ensure the forensic readiness of the evidence available for the investigation process. This framework helps organizations reduce the cost of the investigation process because it provides manageable components and live analysis. However, the components proposed in the high-level view make the implementation and automation of the framework more difficult to create automated tools, as stated by [7].

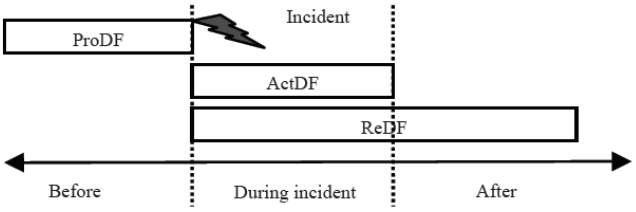

Fig. 6. The Multi-Component View of Digital Forensics, [9]

The reactive and proactive digital forensic investigation process approaches was studied by [7] and generated the Systematic Literature Review (SLR). SLR reports the gap and limitations of the digital forensic investigation process approaches. The researchers mentioned that from 2001 to 2010, 18 research studies that deal with digital forensic phases were conducted. One of these studies focused on the proactive digital forensic approach [9], and the others focused on the reactive approach. This fact indicates the need for more focus on proactive forensics. The research studies in SLR propose a model or framework for digital forensic investigation without discussing the evolution and implementation techniques needed to resolve cyber crimes. Furthermore, the studies in SLR do not consider the analysis phase process to determine the attack intention and strategy.

A functional process model was proposed by [7] to map the digital investigation process. The proposed model is derived from the multi-component view of digital forensics [9]. The model, as shown in Fig. 7, has two components. The first one is the proactive digital forensic component, which includes five phases: proactive collection, event triggering function, proactive preservation, proactive analysis, and preliminary report. The second component is a reactive digital forensic component that also has five phases: identification, preservation, collection, analysis, and final report. The proposed proactive component is similar to the active component of the multi-component process such that they share the same reactive component process. According to the proponents, the disadvantage of this model is that it fails to identify the implantation requirements. Furthermore, the model has limited capabilities because it does not include all the anti-forensic techniques, which could affect the ability of the components to resolve the cyber crime in an efficient manner.

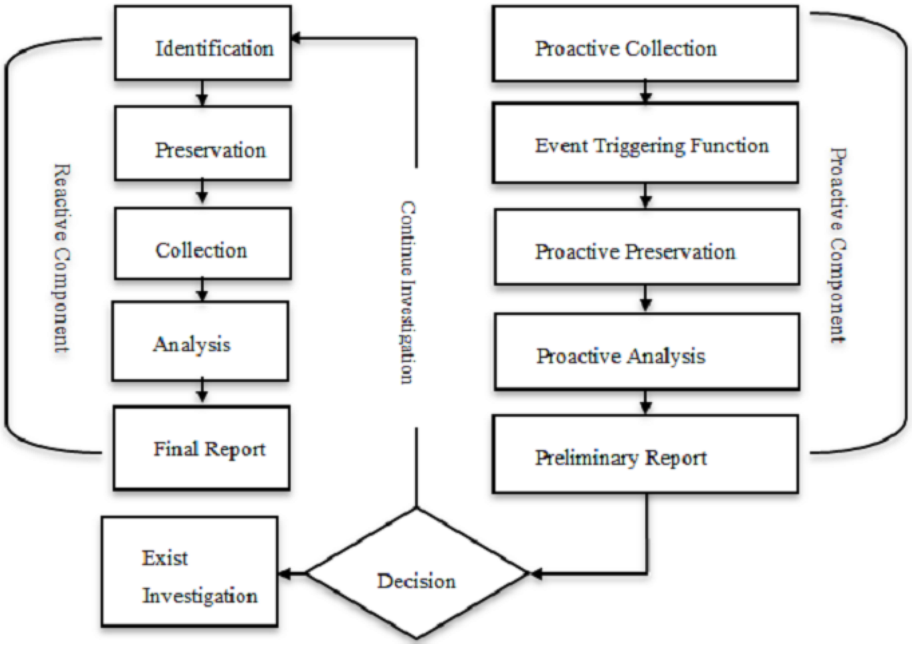

Fig. 7. The Functional Process Model for Proactive and Reactive Digital Forensics Investigation System, [7]

Table 1 summarizes the previous approaches in the network forensic process. We conclude from the table that no standard processes exist in network forensics. The network forensic process models proposed from 2001 onwards handle only networked environments. Most of these models include the same main phases of network forensics, i.e., evidence collection, analysis, investigation, and presentation. These phases are utilized explicitly in several of the approaches; whereas in the other approaches, these phases are embedded within other phases, as mentioned above. The approaches have a different number and order of processes as well as different procedures of performing these processes to deal with cyber crime. The study of the above approaches shows that most of the approaches utilize the active and reactive process to resolve cyber crime. Furthermore, it proves that more focus should be given to the proactive process in network forensic approaches [7].

Table 1. The Main Network Forensics Process Approaches

Approach	Process/Activity/Phases	Type
Generic Investigation Framework, [4]	Identification, Preservation, Collection, Examination, Analysis, Presentation and Decision	Reactive
Abstract Digital Forensics, [11]	Identification, Preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation, and Returning Evidence	Reactive
Integrated Digital Investigation Process (IDIP), [12]	Readiness (Operations, and Infrastructure), Deployment (Detection and Notification , and Confirmation and Authorization), Physical Crime Scene Investigation (Preservation, Survey, Documentation, Search and Collection, Reconstruction, and Presentation), Digital Crime Scene Investigation (Preservation, Survey, Documentation, Search and Collection, Reconstruction, and Presentation) and Review	Reactive
End-to-End Digital Investigation (EEDI), [13]	Collecting Evidence, Analysis of Individual Events, Preliminary Correlation, Event Normalizing, Event Deconfliction , Second Level Correlation, Timeline Analysis, Chain of Evidence Construction, and Corroboration	Reactive
Incident Response Methodology, [15]	Pre-Incident Preparation, Detection of Incidents, Initial Response, Formulate Response Strategy, Investigate the Incident, Reporting, and Resolution	Reactive
Enhanced Integrated Digital Investigation Process (EIDIP), [16]	Readiness (Operations Readiness, and Infrastructure Readiness), Deployment (Detection and Notification, Physical Crime Scene Investigation, Digital Crime Scene Investigation, Confirmation, and Submission), Trace Back (Digital Crime Scene Investigation, and Authorization), Dynamite (Physical Crime Scene Investigation, Digital Crime Scene Investigation, and Reconstruction, Communication), and Review	Reactive
Event-Based Digital Forensic Investigation, [17]	Readiness (Operations Readiness, Infrastructure Readiness), Development (Detection And Notification, Confirmation And Authorization), Physical Crime Scene Investigation (Search, And Reconstruction), Presentation, And Digital Crime Scene Investigation	Reactive
Computer Forensic Field Triage Process Model (CFFTPM), [19]	Planning, Triage, Usage/User Profiles, Chronology/Timeline, Internet Activity, and Case Specific Evidence	Reactive
Extended model of Cyber Crime Investigations, [20]	Awareness, Authorization, Planning, Notification, Search and Identify Evidence, Collection, Transport, Storage, Examination, Hypotheses, Presentation, Proof/Defense, and Dissemination	Reactive
Hierarchical Framework for Digital Investigations (First-Tire), [21]	Preparation, Incident Response, Data Collection, Data Analysis, Presentation, and Incident Closure	Reactive
The General Process Status Transfer, [22]	Capture, Copy, Transfer, Analysis, Investigation, and Presentation	Reactive
Step-By-Step Investigation Framework, [23]	Preparation, Investigation, and Presentation	Reactive
Guideline Forensics Process, [24]	Collection, Examination, Analysis, and Reporting	Reactive
Forensics Zachman (FORZA) Digital Forensics Investigation Framework, [25]	Case Leader, System/Business Owner, Legal Advisor, Security/System Architect/Auditor, Digital Forensics Specialist, Digital Forensics Investigator/System Administrator/Operator, Digital Forensics Analyst, and Legal Prosecutor	Reactive
Two-Dimensional Evidence Reliability Amplification Process Diagram, [27]	Initialization, Evidence Collection, Evidence Examination and Analysis, Presentation and Case Termination	Reactive
Common Process Model for Incident Response and Computer Forensics, [28]	Pre-Analysis (Detection Of Incidents, Initial Response, and Formulation Of Response Strategy), Analysis (Live Response, Forensic Duplication, Data Recovery, Harvesting, Reduction and Organization), and Post-Analysis (Report and Resolution)	Hybrid (Reactive / Proactive)
Digital Forensics Investigation Procedure Model, [29]	Investigation Preparation, Classifying Cyber Crime and Deciding Investigation Priority, Investigating Damaged (Victim) Digital Crime Scene, Criminal Profiling Consultant and Analysis, Tracking Suspects, Investigating Injurer Digital Crime Scene, Summoning Suspect, Additional Investigation, Writing Criminal Profiling, and Writing Report	Reactive
Digital Forensic Investigation Framework Map, [18]	Preparation, Collection and Preservation, Examination and Analysis, Presentation and Reporting, and Disseminating the Case	Reactive
Generic Process Model for Network Forensics, [5]	Preparation, Detection, Incident Response, Collection, Preservation, Examination, Analysis, Investigation, and Presentation	Hybrid (Reactive /

Approach	Process/Activity/Phases	Type
		Proactive)
Multi-Component View of Digital Forensics, [9]	Proactive Digital Forensics- PrDF, Active Digital Forensics- ActDF (Incident Response and Confirmation, ActDF Investigation, Event Reconstruction, and ActDF Termination), and Reactive Digital Forensics- ReDF (Incident Response and Confirmation, Physical Investigation, Digital Investigation, Incident Reconstruction, Present Findings to Management or Authorities, and Dissemination of Result of Investigation, and Incident Closure)	Hybrid (Reactive / Proactive)
Functional Process Model for Proactive and Reactive Digital Forensics Investigation System, [7]	Proactive Digital Forensics Component (Proactive Collection, Event Triggering Function, Proactive Preservation, Proactive Analysis, and Preliminary Report) and Reactive Digital Forensics Component (Identification, Preservation, Collection, Analysis, and Final Report)	Hybrid (Reactive / Proactive)

3 GENERIC PROCESS MODEL FOR NETWORK FORENSICS

The generic process model for network forensic analysis proposed by [5] is based on various existing digital forensic models. The framework, as shown in Fig. 8, divides the phases into two groups. The first group relies on actual time and includes five phases: preparation, detection, incident response, collection, and preservation. The four phases in the second group act as post-investigation phases, which include the examination, analysis, investigation, and presentation phase.

According to proactive network forensic concepts as mentioned by [9], the first five phases work proactively because they work during the occurrence of the cyber crime. The first five phases save time and cost during the investigation process. The first phase prepares the network forensic software and legal environments, such as the IDS firewalls, packet analyzer, and authorization privilege. The second phase detects the nature of the attack by generating a set of alerts through the security tools. The third phase extends from the detection phase; it initializes the incident response based on the type of the attack and organizational policy. This phase also groups similar incident responses after the investigation phase. The fourth phase, which also extends from the detection phase, collects network traffic through suitable hardware and software programs to guarantee the maximum collection of useful evidence. The fifth phase backs up the original data, preserves the hash of all trace data, and prepares a copy of the data for utilization in the analysis phase and other phases.

The other four phases of this model work after the investigation phase and act as a reactive process. The phases begin with the examination phase to integrate the trace data and identify the attack indicators; the indicators are then prepared for the analysis phase. The seventh phase is the analysis phase, which reconstructs the attack indicators by soft computing or through statistical or data mining techniques to classify and correlate the attack patterns. The phase aims to clarify the attack intentions and methodology through the attack patterns and provides feedback on how to improve the security tools. The eighth phase is the investigation phase, which aims to identify the path of the attack and the suitable incident response based on the results of the analysis phase. The final phase presents and documents the results, conclusions, and observations about the cyber crime. Given that all the activities of network forensics are included in this model, the present research adopts the phases of this model as a baseline to show how the analysis phase integrates with the other phases.

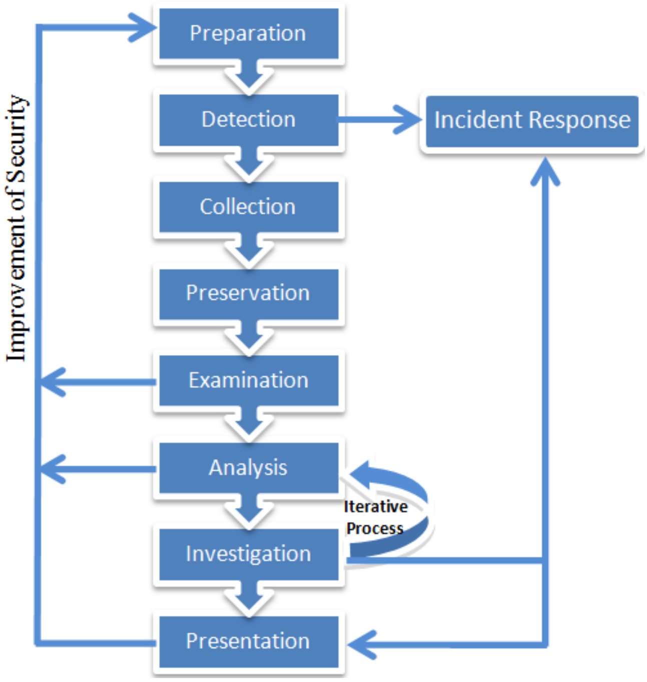

Fig. 8. Generic Process Model for Network Forensics, [5]

The phases of the generic process model are studied in this research to understand how the model works and to present the data flow and the procedures in the phases. Based on the fundamentals of proactive approach, we conclude, that each phase in the first five phases requires a certain amount of time to accomplish its processes. However, each phase works in real time; thus, the phases require the same amount of time and processing cost to accomplish their processes. Given that the other four phases work reactively, we assume that they require more time and processing cost compared with the first five phases. The reason for this assumption is that reactive phases work after the cyber crime happens; therefore, the required amount of time and cost increases during the investigation process.

4 CYBER CRIME RESOLVING APPROACH

We propose a new approach to resolve cyber crime in network forensics as shown in Fig. 9. The proposed approach is characterized as proactive because it retrieves and preserves evidence before and after analyzing the cyber crime. The proposed approach includes five phases, i.e., preservation, capture, classification, analysis, and investigation. These phases are distributed in two modules and linked with the proactive depository.

The two modules implement the preservation phase. The first module gathers evidence and includes the capture and classification phases. The second module analyzes the evidence and improves the investigation process by accurately identifying similar cyber crime cases. It includes the analysis phase, which intermixes with the investigation phase by accurately identifying similar cyber crime cases for the investigators. This approach focuses on the analysis phase and utilizes the other phases to reveal the integrity and flow of cyber crime evidence.

The analysis phase is the main phase in network forensics. It provides sufficient evidence to investigators, which reduces the time and cost of the investigation process. The modules of the proposed approach will discussed and implemented in detail in future research due to limitation of pages in this paper.

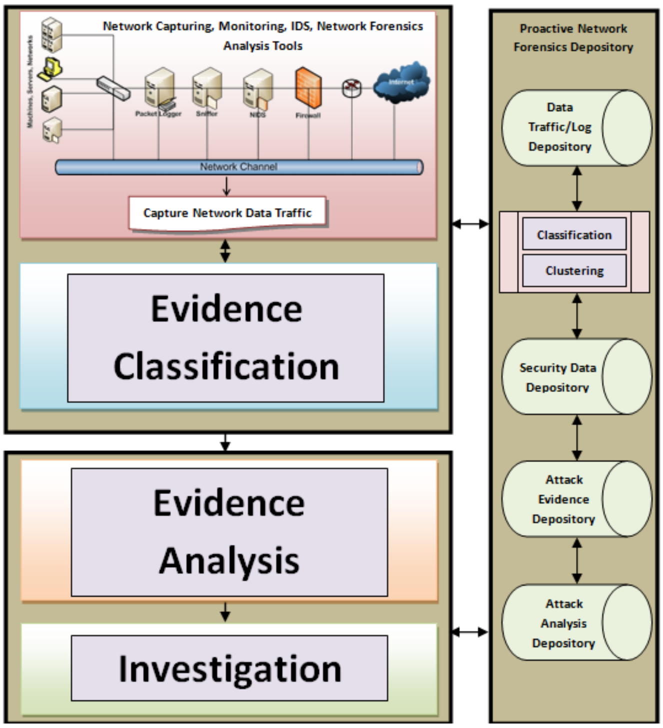
Network Capturing, Monitoring, IDS, Network Forensics Analysis Tools
Machines, Servers, Networks
Packet Logger
Sniffer
NIDS
Firewall
Internet
Network Channel
Capture Network Data Traffic
Evidence Classification
Evidence Analysis
Investigation
Proactive Network Forensics Depository
Data Traffic/Log Depository
Classification
Clustering
Security Data Depository
Attack Evidence Depository
Attack Analysis Depository

Fig. 9. An Approach to Resolve Cyber Crime Evidence in Network Forensics

5 CONCLUSION AND FUTURE WORK

In this paper we proposed a new approach to resolve cyber crime for network forensics with focusing on the analysis process. This paper reviews literature on network forensic approaches and their processes. The paper shows how other approaches dealt with network forensic processes to resolve cyber crimes. The main goal of this paper is incorporated with the related studies that deal with the analysis phase of network forensics. The paper also aims to discover the limitation of the analysis phase in network forensic approaches as well as to show the relationship between the analysis phase and other phases. These approaches are also compared to justify the proposed approach. Based on the generic and modern process model we identified suitable processes of the proposed approach.

The proposed approach can be used as an efficient processes to analyze the cyber crime and to increase the possibility value of evidence in order to reduce the time and processing cost in network forensics. Moreover, the accuracy of resolving the cyber crime could be increased when the Case-Based Reasoning technique is used to implement the proposed approach.

6 ACKNOWLEDGMENTS

This work was supported by RU Grant No.1001/PKOMP/817048, School of Computer Science, Universiti Sains Malaysia, Penang, Malaysia.

7 REFERENCES

[1] Almulhem, A. Network forensics: Notions and challenges. in Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium on. 2009.

[2] Patel, B., Sanjay.M.Shah, and S.S. Chauhan, Comparative Analysis of Network Forensic Systems. Special issues on IP Multimedia Communications, 2011(1): p. 80-83.

[3] Pilli, E.S., et al., A Framework for Network Forensic Analysis, Information and Communication Technologies, 2010, Springer Berlin Heidelberg. p. 142-147.

[4] Palmer, G., A Road Map for Digital Forensic Research, in Report from DFRWS 2001, F.D.F.R. Workshop, Editor 2001: Utica, New York. p. 27–30.

[5] Pilli, E.S., R.C. Joshi, and R. Niyogi, Network forensic frameworks: Survey and research challenges. Digital Investigation, 2010. 7(1-2): p. 14-27.

[6] Pilli, E.S., R.C. Joshi, and R. Niyogi, A Generic Framework for Network Forensics. International Journal of Computer Applications, 2010. 1(11): p. 1-6.

[7] Alharbi, S., et al., The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review Information Security and Assurance, 2011, Springer Berlin Heidelberg. p. 87-100.

[8] Garfinkel, S.L., Digital forensics research: The next 10 years. Digital Investigation, 2010. 7, Supplement(0): p. S64-S73.

[9] Grobler, C.P., 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.

[10] Grobler, C.P., C.P. Louwrens, and S.H. von Solms. A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations. in Availability, Reliability, and Security, 2010. ARES '10 International Conference on. 2010.

[11] Reith M, C.C., Gunsch G An Examination of Digital Forensic Models. International Journal of Digital Evidence, 2002. 1(3): p. 12.

[12] Carrier, B. and E.H. Spafford, Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, 2003. 2(2): p. 20.

[13] Stephenson, P., A COMPREHENSIVE APPROACH TO DIGITAL INCIDENT INVESTIGATION, in Information Security Technical Report, E.A. Technology, Editor 2003. p. 42-54.

[14] Rekhis, S., Theoretical Aspects of Digital Investigation of Security Incidents in Engineering School of Communications, SUP'COM2007, University of 7th of November at Carthage: Tunisia. p. 191.

[15] Mandia, K. and C. Prosise, Incident response and computer forensics. 2 ed2003, New York: McGraw-Hill/Osborne. 507.

[16] Baryamureeba, V. and F. Tushabe. The Enhanced Digital Investigation Process Model. in Proceeding of Digital Forensic Research Workshop. 2004. Baltimore, MD.

[17] Carrier, B.D. and E.H. Spafford, An event-based digital forensic investigation framework, in Proceeding of the 4th Digital Forensic Research Workshop DFRWS20042004. p. 11-13.

[18] Siti Rahayu Selamat, R.Y., Shahrin Sahib, Mapping Process of Digital Forensic Investigation Framework. IJCSNS International Journal of Computer Science and Network Security 2008. Vol. 8(No. 10): p. 163-169.

[19] Rogers, M.K., et al., Computer Forensics Field Triage Process Model. Journal of Digital Forensics, Security and Law, Vol. 1(2), 2006. 1(2): p. 19-37.

[20] Ciardhuáin, S.Ó., An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 2004. 3(1): p. 1-22.

[21] Beebe, N.L. and J.G. Clark, A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2005. 2(2): p. 147-167.

[22] Wei, R. and J. Hai. Modeling the network forensics behaviors. in Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on. 2005.

[23] Kohn, M., J. Eloff, and M. Olivier, Framework for a digital forensic investigation, in Proceedings of Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference2006.

[24] Kent, K., et al., Guide to Integrating Forensic Techniques into Incident Response, 2006: . p. 1-121.

[25] Ricci S.C, I., FORZA - Digital forensics investigation framework that incorporate legal issues. Digital Investigation, 2006. 3, Supplement(0): p. 29-36.

[26] Zachman, J.A. John Zachman's Concise Definition of The Zachman Framework,The New Zachman Framework 3.0. 2008 [cited 2012; Available from: http://www.zachman.com/component/content/category/16-the-zachman-framework.

[27] Khatir, M., 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.

[28] Freiling, F.C. and B. Schwittay. A Common Process Model for Incident Response and Computer Forensics. in Proceedings of Conference on IT Incident Management and IT Forensics. 2007. Germany.

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