International Journal of Computer Applications Technology and Research
Volume 5– Issue 5, 304 - 311, 2016, ISSN:- 2319–8656

A Proactive Approach in Network Forensic Investigation Process

Joseph MbuguaChahira
GarissaUniversityCollege,
Garissa- Kenya

Jane KinanuKiruki,Chuka University,
Chuka- Kenya

Peter KipronoKemei
Egerton University,
Nakuru- Kenya

Abstract

Information Assurance and Security (IAS) is a crucial component in the corporate environment to ensure that the secrecy of sensitive data is protected, the integrity of important data is not violated, and the availability of critical systems is guaranteed. The advancement of Information communication and technology into a new era and domain such as mobility and Internet of Things, its ever growing user's base and sophisticated cyber-attacks forces the organizations to deploy automated and robust defense mechanism to manage resultant digital security incidences in real time. Digital forensic is a scientific process that facilitates detection of illegal activities and in-appropriate behaviors using scientific tools, techniques and investigation frameworks. This research aims at identifying processes that facilitate and improves digital forensic investigation process. Existing digital forensic framework will be reviewed and the analysis will be compiled toderive a network forensic investigation framework that include evidence collection, preservation and analysis at a sensor level and in real time. It is aimed to discover complete relationship with optimal performance among known and unseen/new alerts generated by multiple network sensors in order to improve the quality of alert and recognize attack strategy

Key words: Digital forensic, cybercrimes, proactive network forensic, attack prediction, attack Strategy.

1.0 Introduction

The modern enterprise relies heavily on electronicinformation systemsto improve productivity and speed up processes, allowing new service, product development and new business models. As a result, large amount of information is generated, processed, distributed and stored electronically via digital devices and computer networks. However, their vulnerabilities creates opportunities for hostile users to perform malicious activities exposing the underlying critical informationto cyber threats and attacks (Healy at el, 2008; Alharbi at el, 2011).

Currently, finding the most effective way to secure information systems, networks and sensitive data is a challenging task experienced by many organization.The number of potential attackers targeting a given system has increased drastically and the effect of successful attacks have become more serious. For instance loss of fund, lack of confidence from their clients, legal implications and denial of services (Healy at el, 2008; panda Labs 2011). Skilled attackers frequently changes their attacking strategies and devise new methodologiesto negatively affect their existence, amount and quality of evidence generated for analysisin order to defeat the implementedsecurity mechanisms (Garfinkel at el 2007; will at el, 2011). Information Assurance and Security is a crucial component in the corporate environment to ensure that the secrecy of sensitive data is protected, the integrity of important data is not violated, and the availability of critical systems is guaranteed.It plays a key role on nation health, economy and public security and hence continues to be a research area in the pursuit of an efficient, scalable and intelligent system to provide comprehensive security management domain.

Digital forensic is a scientificprocess that facilitates detection of illegal activities and in-appropriate behaviors using scientific tools, techniques and investigation Frameworks which involves diverse digital devices such as computer system, network, mobile and storage devices (Pilli et al., 2010; Rahayu at el 2008). It comprises of a series of steps followed by security experts to obtain accurate and complete evidence which is forensically sound and acceptable in a court of law. The advancement of Internet into a new era and domain such as mobility and Internet of Things, its ever growing user's base and sophisticated cyber-attacks demonstrate the need to deploy advanced IT security infrastructure to handle the current demands in network security (Wang at el, 2010; Maheyzah at el, 2015; Rahayu at el, 2009). Therefore, it is essential to develop a framework that provides tools,techniques and procedures forcollecting, preserving and analyzing large heterogeneous datasets and system's information in a structured way and for supplying detailed and complete information to IT security management in real time.

This work proposes anetwork forensic investigation framework for detecting, predicting and managing cyber-security incidents in a real time multiple sensor environment. The objective will be achieved through a series of steps first by examining existing digital forensic investigation framework. This study allowed us to identify the missing part and the drawback of those systems. The next section will provide the proposed design for an effectiveframework to improve the whole forensic investigation process. Lastly, we conclude the paper and present potential future work

2.0Existing Digital Forensic Investigation Frameworks

Digital forensic approaches are generally categorized into three sections: Integrated Digital Investigation Process (IDIP) Framework, General Network Forensics Approaches and proactive approaches. (Carrier at el, 2003).

2.1 Integrated Digital Investigation Process (IDIP) Framework

IDIP by (Carrier at el, 2003), .is based on the investigation process of a physical crime scene. The framework has seventeen phases which 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 main limitations of IDIP based framework depicts the deployment phase which consists of confirmation of the incident as being independent of the physical and digital investigation phase. In practice, this seems impossible to confirm a digital or computer crime unless and until some preliminary physical and digital investigation is carried out. Also it does not offer sufficient specificity and does not draw a clear distinction between investigations at the victim's (secondary crime) scene and those at the scene where the first criminal act occurred (primary source). Neither does it reflect the process of arriving at the latter. Since a computer can be used both as a tool and as a victim .It is common for investigations to be carried out at both ends so that accurate reflections are made. The process of tracing back the suspects seems very challenging when dealing with larger networks.

End-to-End Digital Investigation Process (Carrier at el, 2004), contains nine phases consisting of evidence collection, analysis of individual events, preliminary correlation, event normalizing, event deconfliction (uncountable), second-level correlation, timeline analysis, chain of evidence construction, and corroboration,. It combines the tools of the traditional investigative methods. The focus of the model is on the analysis process, particularly correlation, normalization, and deconfliction of events that are reported from different locations. While the model differs from the other models by the interest it gives to analysis, it does not give enough consideration to evidence searching and finding which a complex and time consuming process is. This model was an advancement as it permits formal verification unlike the preceding models. Any state changes that occurred during the course of the event were clearly represented without providing technical details of the incident.

Incident response to help organizations investigate cybercrimes in a simple manner was developed by (Mandia at el, 2003). The framework consists of seven components: pre-incident preparation, detection of incidents, initial response, and formulation of response strategy, investigation of the incident, 3dczxreporting, and resolution. The analysis phase is included in the investigation component. The framework has limitation since investigation component begins after collecting data from the same components.

Enhanced Integrated Digital Investigation Process framework by (Baryamureeba at el, 2006), consists of five major phases that include sub-phases: readiness (operation 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, reconstruction, and communication), and review phase. The approach of the framework classifies the investigation processes into two phases; trace back 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.

Event-based digital forensic investigation framework (Carrier at el, 2003)), is based on the physical crime scene. The framework consists of 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 framework has a clear goal and requirements to achieve the expected results. The integrated phases, when combined, are insufficient to investigate real cybercrime cases because these phases have not mention the completeness of each phases (Rahayuat el, 2008).

Computer Forensic Field Triage Process framework, (Yong-Dal at el, 2008). It has six phases which include planning, triage, usage or user profiles, chronology or timeline, Internet activity, and case-specific evidence phases. The framework provides the identification, analysis, and interpretation of cybercrime evidence within a short time frame without the need to generate a complete forensic image of the lab. The main limitation experienced by the model is suitability for investigating all types of cybercrimes because evidence is very difficult to distinguish and collect.

Extended model of cybercrime investigation, (Ciardhuáin at el, 2003). Consists of thirteen phases that includes awareness, authorization, planning, notification, search and identification of evidence, collection, transport, storage, examination, hypotheses, presentation, proof or defense, and dissemination activity. This model is more comprehensive than the other IDIP framework because it encompasses almost all the investigation activities but the model needs more evaluation in terms of scalability to ensure that it analyzes evidence efficiently. The model also 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 is that they reduce the scalability and flexibility of the investigation when more details are required from the user (Wei at el, 2005).

Hierarchical Framework for Digital Investigations (Beebe at el, 2005), is a multi-tier, hierarchical framework to guide digital investigations. The framework 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 is that it is incomplete and requires a more methodical approach to identify the objectives of each layer.

2.2 General Network Forensics Approaches

Evidence Graphs for Network Forensics Analysis (Wei at el, 2010), is a technique for network forensics analysis mechanism that includes effective evidence presentation, manipulation and automated reasoning. The model includes an evidence graph which facilitates the presentation and manipulation of intrusion evidence. For automated evidence analysis, the model has a hierarchical reasoning framework that includes local reasoning and global reasoning. Local reasoning aims to infer the roles of suspicious hosts from local observations. Global Reasoning aims to identify group of strongly correlated hosts in the attack and derive their relationships. The analysis step is the most comprehensive and sophisticated step. There is a need to refine the model in local and global reasoning process with more realistic experiments and also investigate methods to automate the process for hypothesizing missing evidence and validating hypotheses as mentioned by the authors.

Step-by-step framework (Kohn at el, 2006)), Merges the previous frameworks to compile a reasonably complete framework which groups all the existing processes into three stages, namely, preparation, investigation, and presentation, which are implemented as guidelines in network forensics. The aim of the framework is to establish a clear guideline of what steps should be followed in a forensic process. However, understanding how the framework addresses all phases of network forensics in the main stages is very difficult in clarification.

Forensics Zachman (FORZA) (Stephenson at el, 2003) is a framework that focuses on the legal rules and participants in the organization rather than the technical procedures. The framework solves complex problems by integrating the answers with the questions what (the data attributes), why (the motivation), how (the procedures), who (the people involved), where (the location), and when (the time) questions. 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 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.

Two-dimensional evidence reliability amplification process model (Khatir at el, 2008), consists of 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 cybercrime questions, such as what happened, when did it happen, and who perpetrated the action, without considering the cybercrime intention and strategy analysis (why and how questions). A similarity exists between incident response and computer forensics (Freiling at el, 2000). 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, consisting of 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. 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.

Digital forensics investigation procedure model (Yong-Dal at el, 2008), consists of ten phases: investigation preparation, classifying cybercrime 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 model presented the block diagram without any technical details or methods to manipulate with these phases. This indicates that the main focuswas on the number and the type of the network forensics phases rather than how it works and how they conduct the outcomes.

A categorization of investigation process was done (Rahayu at el, 2008) to group and merge the similar activities or processes in five phases that provide the same output. The phases are: Phase 1 (Preparation), Phase 2 (Collection and Preservation), Phase 3 (Examination and Analysis), and Phase 4 (Presentation and Reporting), and Phase 5 (Disseminating the case). The researcher also proposed a mapping process of digital forensic investigation process model to eliminate the redundancy of the process involved in the model and standardize the terms used in achieving the investigation goal.

2.3Proactive Process framework in Network Forensics

Multi-Component View of Digital Forensics (Grobler at el, 2010), includes three components, consisting of ProDF, ActDF), and ReDF. The ProDF component defines and manages the processes and procedures of the comprehensive digital evidence. ActDF includes four subphases: incident response and confirmation, ActDF investigation, event reconstruction, and ActDF termination. ReDF includes six sub phases, 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.

A theoretical framework to guide the implementation of proactive digital forensics and to ensure the forensic readiness of the evidence available for the investigation process. The framework helps organizations reduce the cost of the investigation process because it provides manageable components and live analysis. The

components proposed in the high-level view make the implementation and automation of the framework more difficult to create automated tools, as stated. Additionally, the process contains phases, such as service restoration, that lie outside the scope of the investigation Alharbi (2011).

Functional Process Model for Proactive and Reactive Digital Forensics, (Alharbi at el, 2011),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. The examination and analysis phases are combined in the proposed process under a single phase called analysis. The limitation of this framework, it has not yet fully implemented and may be adapted to implementation requirements and it does not address all techniques used by anti-forensics methods, which could affect the ability of the components to resolve the cybercrime in an efficient manner.

2.4 Generic Process Model for Network Forensics

The generic process model for network forensic analysis (Grobler at el, 2010), 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. The first five phases work proactively because they work during the occurrence of the cybercrime saving 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. 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 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 cybercrime. 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.

In generic framework each phase in the first five phases requires a certain amount of time to accomplish its processes. 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, it is 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 cybercrime happens; therefore, the required amount of time and cost increases during the \investigation process.

3.0 Discussion and Analysis of Digital Forensic Frameworks

3.1 Summary of existing digital forensics framework

All the discussed techniques have their advantages and disadvantageous as summarized in Table 1 below

Table 1: Summary of existing digital forensics framework

Approach	Type	Limitations
event-based digital forensic investigation framework (Carrier at el 2003)	Reactive	the integrated phases, when combined, are insufficient to investigate real cybercrime cases because these phases have not mention the completeness of each phases
Computer Forensic Field Triage Process framework (Yong-Dal at el 2008)	Reactive	evidence is very difficult to distinguish and collect
Hierarchical Framework for Digital Investigations(Beebe at el,2005)	Reactive	It is incomplete and requires a more methodical approach to identify the objectives of each layer.
Step-by-step framework (Kohn at el 2006)	Reactive	Understanding how the framework addresses all phases of network forensics in the main stages is very difficult need clarification.
Forensics ZachmanDigital forensics Investigation Framework (Stephenson at el, 2008)	Reactive	It requires more tools to conduct a network forensic analysis and to provide accurate results in the investigation phase.

Two-Dimensional Evidence Reliability Amplification Process Diagram (Khatir at el 2008)	Reactive	Does not consider the cybercrime intention and strategy analysis (why and how questions)
Common Process Model for Incident Response and Computer Forensics (Freiling at el 2008)	Reactive	No standard method of detecting and collecting evidence exists, which produces insignificant evidence and affects the accuracy of the incident response.
Digital forensics investigation procedure model [31]	Reactive	The model presented the block diagram without any technical details or methods to manipulate with these phases
Mapping process in digital forensic (Rahayu at el 2008)	Hybrid	They did not implement the model
Generic Process Model for Network Forensics (Ricci at el, 2006)	Hybrid	The output of the examination and analysis phase which doesn't mention the methods and techniques which could be used to conduct the output from this phase.
Multi-Component View of Digital Forensics, (Grobler at el 2010)	Hybrid	The components proposed in the high-level view make the implementation and automation of the framework more difficult to create automated tools(Alharbi at el, 2008)
Functional Process Model for Proactive and Reactive Digital Forensics (Alharbi at el, 2008)	Hybrid)	has limited capabilities because it does not include all the anti-forensic techniques,
Cyber Crime Resolving Approach (Mohammad at el 2013)	Hybrid	The modules of the proposed approach were neither discussed nor implemented

From the existing frameworks discussed in the literature review, it is clearly indicated that the digital forensic investigation is a process consisting of several activities although they may be different in terms used and the order followed but they are all designed to achieve similar objective. Also the proposed frameworks are built on the underlying experience to improve the existing ones.

3.2 Design Consideration in Developing Network Forensic Investigation Frameworks

The challenges in current networkforensic Frameworks includes

- The organization tends to develop its own procedures focusing on the technology aspects such as data acquisition or data analysis and hence a change in the underlying technology forces new procedures to be developed hence investigation should be incorporated with the basic procedures in forensic investigation which are preparation, investigation and presentation (Satpathy at el, 2010; Kohn at el 2006).
- The digital evidence is in a disorganized form and as such it can be very difficult to handle and not all of them is obviously readable by human.
- During collection process, the evidence is related to the aspect on how the evidence is searched, collected, analyzed, presented and documented without tampering the evidence and preserving the chain of evidence.
- During the analysis process, the analysis tools used must be legally accepted, performed by experts or qualified person, and the evidence should not be tampered with or lost.
- The huge amount of collected data from heterogeneous devises needs automated techniques to reduce redundancy, and consequently reduce the analysis time and storage requirement of the evidence (Noor at el 2015; Rahayu at el 2008)
- A proactive approach to help response systems react before the network is compromised, and to have the opportunities to overcome the advantages of attacker by predicting the next attacker action as a proactive step (Noor at el. 2015; Grobler at el, 2010),
- The investigation process should discover complete relationship with optimal performance among known and unknown attacks (Maheyzah at el, 2015).
- The approach of presenting and documenting the evidence should be understandable to non-technical person such as jury and judge for example applications of graph, tree diagrams other than text.

4.0 Proposed Network Forensic Investigation Framework

The proposed theoretical framework can be categorized as proactive and reactive as it predict future attacker actions before damage, and automatically respond to attacks in a timely manner The proposed approach includestwo major modules which are linked together with a proactive depository.

i. Online alert collection and preprocessing
ii. Online and offline alert correlationand optimization

The proposed model processes include evidence collection, evidence identification and classification, analysis and investigation. The final phase presents and documents the results, conclusions, and observations about the

cybercrimethese phases are distributed in two modules and linked with the proactive depository.

4.1 Online alert Collection And Preprocessing

The first module gathers alerts from heterogeneous sources in real time, preprocess by normalization and aggregation of alerts based on given feature such as time, IP source, destination address, etc. the intrusion according to level of evidence accuracy so that forensic professionals will have smaller scope of evidence to investigate and analyze. The result will be stored in the evidence depository. The module includes the preparation, evidence collection, and normalization and aggregation phases. This phase improves the investigation process by accurately identifying similar cybercrime cases for investigation.

4.2 Online and Offline Alert Correlation and Optimization

The second module provides an analysis mechanism that includes effective alert correlation to improve the quality of alerts and integrate them with isolated alerts and also construct all possible attack scenarios. This can be done either online and offline mode. It wills also prioritizing intrusion alerts. Evidence graph will be generated to facilitate the presentation and manipulation of intrusion evidence. Based on the evidence graph an automated reasoning mechanism can be developed with the help of soft computing and advanced analytics for automated evidence analysis. The phase aims to identify the attack group, reconstruct attack strategy predict incoming attacks together with their intentions and provides feedback on how to improve the security system.

Table 2: Summary of Processes in the Proposed Framework

Module	Phase name	Activities / processes
Evidence collection and pre process	Preparation	•Attacker Goal Identification and hypothesis formulation •Network Configuration •Privilege Profile and Trust Setting •Vulnerability and Exploit Permission
	Evidence collection and preservation	• Data aggregation from different data sources • Formatting and standardizing intrusion alerts • Improve the quality of alerts through Filtering redundant and invalid alerts. • dimensional reduction
Online and offline alert correlation and optimization	Analysis and examination	Alert analysis through structural, causal and statistical based correlation techniques • Filtering low-interest and false positive intrusion alerts. • Discovering attack scenario. • Verification and prioritizing intrusion alerts. • Forecasting attacker next action. • Forecasting forthcoming attacks
Evidence presentation and dissemination	Presenting and reporting	Preparing and presenting the information resulting from the analysis phase • Determine the issues relevance of the information, its reliability and who can testify to it • Interpret the statistical from analysis phase • Clarify the evidence, and Document the findings • Summarize and provide explanation of conclusions\ • Presenting the physical and digital evidence to a court or corporate management • Attempt to confirm each piece of evidence and each event in the chain each other, independently, evidence or events • Prove the validity of the hypothesis and defend it against criticism and challenge • Communicate relevance findings to a variety of audiences (management, technical personnel, law enforcement)
	Disseminating and documenting	Ensuring physical and digital property is returned to proper owner • Determine how and what criminal evidence must be removed • Reviewing the investigation to identify areas of improvement • Disseminate the information from the investigation • Close out the investigation and preserve knowledge gained

5.0 Conclusion

Digital forensic is a scientific process that facilitates detection of illegal activities and in-appropriate behaviors using scientific proven tools, techniques and investigation frameworks. Existing practices in digital forensic are not scalable and efficient to handle advanced and modern attacks exploiting emerging services resulting from advancement in Information Communication Technology. This research proposed proactive approach in network forensic investigation process that will address the issue of evidence collection and evidence analysis in a real time multiple sensor environment. It is aimed to discover complete relationship with optimal performance among known and unseen/new alerts generated by multiple network sensors in order to improve the quality of alert and recognize attack strategy.

For future work, a prototype will be developed in order to prove the effectiveness of the proposed framework.Various issues will be addressed in the implementation of the new process: the ability to collect and preserve alerts online, predict an attack strategy, optimizing the proactive component throughfiltering false negatives and prioritizing intrusions and predict attack next cause of action andprovide feedbackproactively

.

REFERENCES

1. Healy, L. (2008) Increasing the Likelihood of admissible electronic evidence: Digital log
2. Handling excellence and a forensically aware corporate culture
3. PandaLabs, Annual Report Panda Security's Anti Malware Laboratory 2009. 2010, Panda Security
4. Will, J. P. (2011). 7 - Cyber X: Criminal Syndicates, Nation States, Subnational Entities, and Beyond. In *Cybercrime and Espionage* (Vol. ISBN 9781597496131, pp. 115-133). Syngress, Boston.
5. S. Garfinkel, "Anti-forensics: Techniques, detection and countermeasures," in 2nd International Conference on i-Warfare and Security, 2007, p. 77.
6. Alharbi, S. e. (2011). The Proactive and Reactive Digital Forensics Investigation Process International Journal of Security and Its Applications Vol. 5 No. 4, October, 2011
7. Orebaugh, "Proactive forensics," Journal of Digital Forensic Practice, vol. 1, p. 37, 2006.
8. Palmer, G. (2001, a). A Road Map for Digital Forensic Research. Utica, New York,: Report From the First Digital Forensic Research Workshop (DFRWS).
9. Palmer. G. (2001, b). *A Road Map for Digital Forensic Research.* Utica, New York: DFRWS TECHNICAL REPORT.
10. Mukkamala, S. S. (2003). Identifying significant features fornetwork forensic analysis using artificial intelligent techniques. *International Journal of Digital Evidence*, 1-10.
11. Nikkel. (2005). Generalizing sources of live network evidence. *Digital Investigation (The International Journal of Digital Forensics & Incident Response*, 193–200.
12. Ren. (2004). on a network forensics model for information security. *In Proceedings of the third international conference on information systems technology and its applications (ISTA 2004)*, 29–34.
13. Wei, R. a. (2005). Modeling the network forensics behaviors. In Security and Privacy for Emerging Areas in Communication Networks.*Workshop of the 1st International Conference on. 2005*.
14. SitiRahayuSelamat, R. S. (2008). Mapping Process of Digital Forensic Investigation Framework. *IJCSNS International Journal of Computer Science and Network Security*, Vol. 8(No. 10): p. 163-169.
15. Will, J. P. (2011). 7 - Cyber X: Criminal Syndicates, Nation States, Subnational Entities, and Beyond. In *Cybercrime and Espionage* (Vol. ISBN 9781597496131, pp. 115-133). Syngress, Boston.
16. Siebert, E. (2010). *The Case for Security Information and Event Management (SIEM) in Proactive Network Defense.*SolarWinds.
17. Khurana H, B. J. (2009). A framework for collaborative incident response and investigation. *In: Proceedings of the eighth symposium on identity and trust on the Internet,Maryland;* , 38–51.
18. Reith M, C. G. (2002.). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, 1(3): p. 12.
19. Mohammad Rasmi, AmanJantan, Hani Al-Mimi A New Approach For Resolving Cyber Crime In Network Forensics Based On Generic Process Model ICIT 2013 The 6th International Conference on Information Technology
20. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process Model," sAsian Journal of Information Technology, vol. 5, pp. 790-794, 2006.
21. Beebe, N. a. (2005). A hierarchical, objectives-based framework for the digital investigations process. *International Journal of Digital Investigation*, 2(2): p. 147-167.
22. Carrier, B. a. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, 2(2): p. 20.
23. Ciardhuáin, S. (2003). An Extended Model of Cybercrime Investigations. *fxInternational Journal of Digital Evidence* , 3(1): p. 1-22.
24. Freiling, F. a. (2007). A Common Process Model for Incident Response and Computer Forensics. *IT Incident Management and IT Forensics.* Germany.
25. Grobler, C. C. (2010). A Multi-component View of Digital Forensics. In Availability, Reliability, and Security,.*ARES '10 International Conference.* ARES.
26. Khatir, M. S. (2008). Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics. In Digital Forensics and

Incident Analysis.*WDFIA '08. Third International Annual Workshop on. 2008.*

27. Kohn, M. J. (2006). Framework for a digital forensic investigation,.*Information Security South Africa (ISSA).* South Africa: Insight to Foresight.
28. Louwrens, C., & von Solms, S. (2010). A Multi-component View of Digital Forensics. *IEEE Xplore* , 647 - 652 .
29. Mandia, K. a. (2003). Incident response and computer forensics. *McGraw-Hill/Osborne.* , 507.
30. Pilli, E. R. (2010). Network forensic frameworks: Survey and research challenges. *Journal of Elsevier Ltd. 2010.*
31. Ricci S.C, I. F. (2006). Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, 29-36.
32. Rogers, M. e. (2006). Computer Forensics Field Triage Process Model. *Journal of Digital Forensics, Security and Law,* Vol. 1(2), 9-37.
33. Stephenson, P. (2003). *A Comprehensive Approach To Digital Incident* .

Investigation,Information Security Technical Report,E.A. Technology, Editor p. 42-54.

34. Yong-Dal, S. (2008). New Digital Forensics Investigation Procedure Model. In Networked Computing and Advanced Information Management,.*NCM '08.*
35. Noora Al Khater , Richard E Overill (2015), Forensic Network Traffic Analysis, Proceedings of The Second International Conference on Digital Security and Forensics, Cape Town, South Africa
36. S. Satpathy, S. K. Pradhan and B. B. Ray, 2010 "A Digital Investigation Tool based on Data Fusion in Management of Cyber Security Systems," International Journal of In- formation Technology and Knowledge Management
37. MaheyzahMdSiraj, Hashim Hussein TahaAlbasheer and Mazura Mat Din,2015,Towards Predictive Real-time Multi-sensors Intrusion Alert Correlation Framework Indian Journal of Science and Technology, Vol 8(12)