Network Forensics Framework Development using Interactive Planning Approach

Missi Hikmatyar
Department of Informatics
Universitas Islam Indonesia
Yogyakarta, Indonesia

Yudi Prayudi
Department of Informatics
Universitas Islam Indonesia
Yogyakarta, Indonesia

Imam Riadi
Department of Information System
Ahmad Dahlan University
Yogyakarta, Indonesia

ABSTRACT
Utilization of the network become a trend present with the development of technology, especially the Internet, but the trend of web use is directly proportional to the usage of the crime, or that is better known as cyber crime. Cyber crime is the duty of law enforcement in combating it.In the disclosure of a case on the network needed a method of handling.

Integrated Digital Forensics Investigation Framework (IDFIF) is a method of investigation of a general nature. IDFIF evolved into IDFIF version 2 that is a method of treatment focuses on smartphones. IDFIF v2 can not be applied to network investigation it is necessary to develop a version 3 IDFIF focused on network forensics. This research is the development of network forensics framework using interactive planning.

General Terms
Digital Forensics

Keywords
IDFIF, Network Forensics Framework, Interactive Planning.

1. INTRODUCTION
Investigations carried out on the network is very complicated, because the crimes committed by the system can be manipulated and used by criminals who exploit the network have expertise in knowledge about computers. So there must be a method of investigation can uncover the crime. A method which would use must Be Having support in the Network investigation with the handling techniques appropriate to the circumstances in the investigation process.

IDFIF version 2 is a methodology of an investigation but can not be used for network investigation then need to develop methods IDFIF version 2 to IDFIF version 3 that can utilize for network investigation that could handle the case on the system with the better handling. To design of the method for the network, investigation needs The process of developing this approach. The interactive planning approach system is a method of thinking to solve unstructured problems. This study aims to develop IDFIF version 2 to be a network forensics framework that can use for cybercrime.

2. BASIC THEORY
2.1 Network Forensics
Network Forensics is part of the Digital Forensics branch of science dealing with the monitoring and analysis of network traffic to the collection of information, evidence gathering and detect attacks. The process of investigation occurred in the network with handling the traffic and activity. Differ from the other method, the network forensics related to dynamic information that easily to is lost.

Network Forensics has two functions, the first relating to security, including traffic monitoring network which aims to get the evidence given is the lack of evidence in the network so that the investigation could not walk. Second, law enforcement-related, in this case, analysis on the capture of network traffic may include sending a file, searching for keywords, and breakdown in communications made as in email and chat.

2.2 Type of Network Forensics
1) A Distributed System
Distributed system is a mechanism in the investigation process by distributing the network connection with platforms for monitoring of each connection. In 2015 [1] suggested research related to the concept of distributed system on network forensics. The concept was designed based on a distribution technique which is used to provide integrated platforms on evidence gathering automatically. The concept is a concept intended to support the method of attack graph depicting seizure activity.

2) Soft Computing
Soft computing is a method of investigation of the network by using artificial intelligence to assist in the process of grouping the evidence in the can. In 2013 [2] suggest uses fuzzy logic to perform clustering system. In research conducted at the stage of development of the activity of identification to identify and categorize the evidence obtained by the impact.

3) Honeypot
A honeypot is a technique of trapping by adding agents to monitor computers that occur on network traffic. This technique is also a method of security on the network. In 2013 [3] conducted related research honeypot by applying the principle of a honeypot on a wireless network. In architecture, there are computer agents that monitor every network activity.

4) Attack Graph
The attack graph is processing the evidence obtained from a graph that generates hypotheses. In this method produced analysis attacks, mode, and motive in a case of an attack. In 2010[4] stated that the method of attack graph is a model graph on the evidence for automation and motives do and as an effective method to testify at the trial.

5) Formal Method
A formal method is a method that is based on the traditional habit of conducting an investigation. In 1999 [5] apply formal methods on the test system by examining the transition to the system.

6) Aggregation
Aggregation method is a method of collecting evidence as well as associated with the crawling of an IP address by

capturing the activity then performed a comparative analysis of the evidence related to possible attacks. In 2008 [6] conducted research based on the method of aggregation with three stages, namely marking or tagging/labeling, capture logging activity and storage of evidence by the classification.

3. RELATED WORK

Development of network forensics framework is based on reviews of research that focus on ten research related to Network forensics as shown in Table 1.

Table 1. Research of Network Forensics

Year	Framework's Name
2004	An Extended Model of Cybercrime Investigation
2004	A Hierarchical Objective-Based Framework for the Digital Investigations Process
2004	The Enhanced Digital Investigation Process Model
2006	Computer Forensic Field Triage Process Model
2010	Generic Framework of Network Investigation
2011	Proactive and Reactive Digital Forensics Investigation
2012	Basic Framework of Network Investigation
2013	Internet Forensics Framework Based on Clustering
2014	Critical Phases in Network Forensics
2015	Proactive Network Forensic Evidence Analysis (PNFEA)

There are several studies related to network forensics as Early In 2004 [7] suggested a model for dealing investigation, in the research, designed an extended investigation of cybercrime (EMCI) with thirteen phases; awareness, authorization, planning, notification, search and identify, collection, transport, storage, examination, hypotheses, presentation, proof / defense and dissemination. This model focused on hypotheses on digital evidence. This model focused on the hypothesis of the digital evidence and proofed of this hypothesis.

In addition to earlier research, other studies were designing a framework that can be used by all communities and have suitable measures in an investigation [8]. That studies suggested other frameworks for dealing investigation that hierarchical objective-based framework with six processes; preparation, incident response, the data collection, the data analysis, presentation, and incident closure. In another research at the same year, [9] evolved a model of the development of the integrated digital investigation process (IDIP) called enhanced Digital Investigation Process Framework (EDIP) by introducing the stages of traceback and dynamite that includes real, digital crime investigation and crime investigation.

Other studies related to network framework is In 2006, designed a framework that is performed directly without having to carry the electronic evidence to the lab and focuses on the effectiveness of time [10]. This framework has six phases and six sub-phases, the processes that defined at the time are planning, triage, user profiles with sub-phase home usage, file properties and registry. Then their chronology timeline, with a sub-phases internet browser, email, IM. And the last stage is the particular case.

In another research, some studies focus on problem-solving related attack patterns, log analysis, and data fusion techniques in understanding the relationship of any data [11]. This study is a combination of other studies that specifically examined the associated network framework.Suggested a generic framework of network investigation with nine phases are preparation and authorization, detection of incident/crime, incident response, the collection of network traces, preservation late protection, examination, analysis, investigation and attribution, and presentation and review. In 2011, There is the study that designed proactive and reactive for digital forensics as a general model for the investigation [12]. Two components are proactive, an action directly against the evidence at the crime scene and Reactive, further investigative measures for the assessment process. This study designed aims to predict events that will occur and optimize the handling of a case.

On the other hand, some researchers argue that the design of a model is not useful, In 2012 [13] Suggested that there is always a gap between theoretical research with what is happening on the ground in the investigation. This study is a combination of academic research with the actual process of investigation in the field. Thi study suggested that Network investigation has found three primary stages are a proactive investigation that includes prepare for and detect the incident, the investigation includes real-time monitoring and preservation, a retroactive investigation which includes the collection and reassembles the data. In 2013, there is a study that conducted on internet forensics framework based on clustering [2]. In this study designed a framework that focuses on the identification stage, with the initial stages of log files, evidence file data, clustering module, extracted information, result, testing, and final reporting.

Other studies that discussed network forensics is [14] that conducted research on critical phase with the developing stages of examination and analysis stages. At this stage of examination, there are sub-stage conversion, identification, extraction, and classification. While at this stage of analysis are sub-stages of validation statistical analysis and visualization. And the other study, [15] suggested An investigation model of the network by focusing on proactive stage. There are five stages of preservation, capturing, classification, analysis, and investigation.

4. RESEARCH METHOD

4.1 Formulating the Mess

Phase analysis conducted formulated the mess of the system. There are four steps according to formulated the mess:

1) System analysis

Phase analysis performed on IDFIF version 2 and its stakeholders. Systems analysis phase in IDFIF version 2 do with an assessment of each stage that exists in the framework to determine the gaps that exist in IDFIF version 2. And a stakeholder analysis conducted for the assessment of the stakeholders who play a role in each stage of IDFIF version 2. The purpose of the assessment of the process and stakeholders is to determine the direction of development will be carried out on IDFIF version 2. While stakeholders are analyzed include several roles, there are:

- Law enforcement consists of investigators as the officer conducting the investigation. And storage of evidence officer in charge of maintaining the integrity of the evidence.

- First responder in a leading role in investigating and processing evidence
- Witness as witnesses who supported the investigation.
- Suspect perpetrators
- The victim as victims who are disadvantaged over the scene of the attack.
- Public as a supporting role in the investigation process.

2) An Obstruction Analysis

This step, analyzed the weaknesses in IDFIF version 2, there are some weaknesses in IDFIF versions two are:

- The process of the IDFIF version 2 can not use for the investigation of network forensics.
- Study of the IDFIF version 2 is not real-time in the capture of network activity.
- The process of the IDFIF version 2 there are stages of protection against network attacks and objects.
- Investigation of the IDFIF version 2 is semi-dynamic and interactive.

3) Reference Projection

To evaluate the IDFIF version 2 with the proposal stages that exist in previous research. The research that is used for the project stages is a research about the network forensics. There is ten related research stage where ten research proposals have described in the title of related work. The study proposed an article describing a framework related to network development and as support in covering the weaknesses found in IDFIF version 2.

4) Reference Scenario

From a research proposal, there are several stages as the basis for the development of network forensics. Stages were resulting from previous studies and then normalized against the names of the steps. Normalization process aims to eliminate the double steps by simplifying each stage.

To establish the phases that serve the purpose of model design then using the flowchart as figure 1.

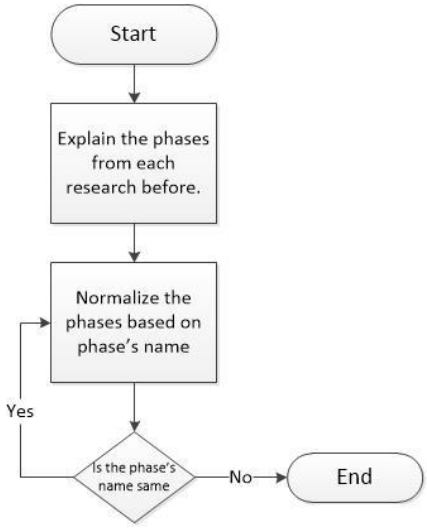

Figure 1. Normalization Flowchart

4.2 Ends Planning

This stage is an ideal concept design stage as an evaluation of IDFIF version 2. The design ideal concept came from previous research proposal. In the last scene has resulted in normalization steps. The stage is then carried out again with normalization based on the terminology stages against IDFIF version 2 using an algorithm as:

If Tn=Ti Then Written =Ti

Else if Tn ≠ Ti then written = Tn

Explain :

Tn = Terminology of Phases

Ti = Terminology of IDFIF's phases

From the normalization based on terminology generated stages that need to be added as a supporter and to cover up weaknesses

In IDFIF version 2. Additional stages of normalizing the results described in Table 2.

Table 2. Normalization based on the Terminology

No	Phases	Description
1	Identification	The introduction of the evidence obtained.
2	Monitoring	Monitored of network activity.
3	Protection	Protected against the object of attack.
4	Capturing	Catching activity on the network.
5	Classification	Grouped of evidence for analysis.
6	Logging	Storage of evidence with labeling for analysis to generate hypotheses.

4.3 Means Planning

After designed the phases, then adjusted to theories that have been studied and following network investigation. Two theories support to complete the design

- Research [1] which states that the network investigation has several methods in the implementation that is a distributed system, soft computing [16], honeypot, attack graph [17], formal methods and techniques aggregation.
- Research [18] states that a first responder should have the ability to four things: resistance, recognition, recovery, and Redress.

The theory produced two things are the addition of **Strategy approach** for the study represent stored in the proactive phase of analysis and additional **protection** terminology on the phase corresponding to the study.

4.4 Resource Planning

This step is a description of resources related to the framework. The funds in question are human resources and tools. The tool itself is divided into hardware and software. For example hardware screwdriver, Faraday bag, power supply, etc. For software which is used for the investigation of networks like Wireshark, Tcdump, etc.

4.5 Design of Implementation

This step is implementing the results of the final design of network forensics framework. The phases from the previous step proposed a model for network investigation called IDFIF version 3. This model would test on case study to know its application on the crime.

4.6 Design of Control

This step is the stage of the role of the human object on the stage IDFIF version 3. Describe the process, the resource and the stakeholder on IDFIF version 3. This stage is the stage of the adjustment phase with the resources; it helps in the preparation before the investigation and the arrangement of each stage.

5. PROPOSED MODEL

Proposed model for network forensics include four primary processes, and there are Preparation, Proactive Process, Reactive Process, and Presentation as figure 2. Each process had some phases with subphases. The model proposed is the result of an explanation model design by interactive planning methods in analyzing, evaluating previous models.

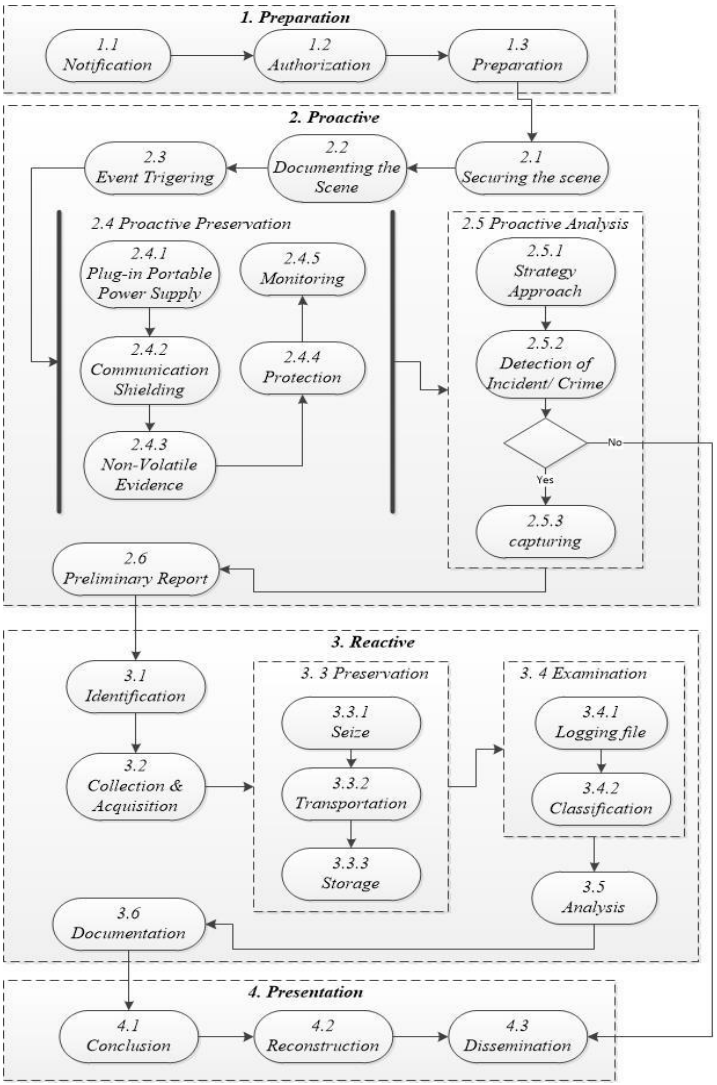

Figure 2. Illustration of IDFIF version 3

5.1 Preparation

An initial phase was covering preparations to conduct an investigation of start doing evidence handling process to making the report. There are several stages to the main stage of preparation, notification, authorization, and preparation.

1) Notification

Notified of violations of law to law enforcement. This stage is the process of receipt a report related to the occurrence of a case.

2) Authorization

The step for the right of access to evidence and the legal status of the investigation process

3) Preparation

Prepared the availability of tools and personnel Equipment that was brought to the investigative process is hardware tools and software tools. Preparing a first responder who will do if the crime scene.

5.2 Proactive Process

A prompt action against a crime scene so that evidence is not contaminated and manipulated digitally. Six stages exist in

proactive main stages, securing the scene, documenting the scene, event triggering, proactive preservation, proactive analysis and preliminary report.

1) Securing the scene
Did a mechanism to ensure the crime scene (the scene). And protect from contamination so that the integrity is maintained.

2) Documenting the Scene
Processing a crime scene, looking for the source of the trigger events looking for connections and network communications and document the crime scene by taking a picture every detail of the scene.

3) Event Triggering
An initial analysis of the process of events that happened looked at the potential evidence at the scene.

4) Proactive Preservation
Direct action against the evidence to maintain its integrity. There five subphases in this phase are:

- Plugin Portable Power Supply, a resource in the process of securing electronic evidence that is being alive.
- Communication Shielding, Protection against electronic evidence to avoid contamination.
- Non-volatile Evidence, securing digital evidence that is non-volatile.
- Protection, protection of the data phase includes the resistance that attacks containment, and recovery is the return of such systems.
- Monitoring, the stage for a real investigation to investigate the network by performing a search for traces on the network and seeking potential data used as evidence

5) Proactive analysis
Analysis of direct action to get the initial hypothesis on the investigation. There three subphases in this phase are:

- Strategy Approach, Strategy or method in the collection. Determine the strategy or technique that according to the case
- Detection of Incident/Crime that detects and confirm a violation of law
- Capturing, capturing of data contained in the network and capture activity happening on the network

6) Preliminary report
Manufacturer of the initial report on the investigation at this stage of proactive

5.3 Reactive Process

The main stage is that continued action on the investigation. In This reactive stages, the investigation process traditionally. The reactive process is a continuation of proactive measures to optimize the process of investigation There six phases in the reactive process are identification, acquisition, preservation, examination, analysis and documentation.

1) Identification
Is to identify the evidence, the search for potential evidence. Digital evidence that identified is a result of capturing the data activity on the network.

2) Collection & Acquisition
A collection stage and the stage of acquisition of electronic evidence. Collecting electronic evidence and acquire digital evidence

3) Preservation
Keep the integrity of the artifacts using a chain of custody and hashing functions. There three subphases in this phase are:

- Seize, is foreclosing on the artifacts as well as the labeling of finding items.
- Transportation, transfer of evidence from the crime scene to the laboratory.
- Storage, storage of electronic evidence in the storage of evidence and data capturing results in a database.

4) Examination
Processing of evidence or data to find a connection with the incident. At this stage of consideration of the data obtained from the network. There two subphases in this phase are:

- Logging file, storage and provision of information to the database data.
- Classification, Classification of the data according to criteria such data.

5) Analysis
A technical assessment and arranging linkages between present findings.

6) Documentation
Documented of all activities phase of the investigation from the beginning to the analysis phase.

5.4 Presentation

Presentation process Is the final step in the course of the investigation which is the description of the results of the investigation in a report by the legal provisions and the use of common language.There are several stages in this stage include the conclusion, reconstruction, and dissemination.

1) Conclusion
Stage summing up the results of the investigations that have been carried out.

2) Reconstruction
The whole process of analysis and evaluation of the results of the investigation.

3) Dissemination
The recording process of the investigation and the note can disseminate to the other investigators who conduct investigations on similar cases.

6. RESULT

6.1 Testing Scenario

Testing IDFIF version 3 performed by applying on a Distributed Denial of Service (DDoS) that illustrated in figure 3. DDoS is a type of attack that uses many hosts to attack a target host. There are several stages in IDFIF version 3 that need testing. These steps are protection, monitoring, strategy approach, capturing, identification, logging file, and classification.

1) Protection
A stage of protection of evidence and data contained on a server that does not cause any loss, damage or manipulation of data. Phase protection or blocking prevention against attacks and recovering the harm posed by the DDoS attack. This stage is first aid for the electrical evidence that attacked

by the DDoS attack. That does not happen any further damage that could lead to in greater losses.

2) Monitoring

Is the stage of monitoring the network to perform network traces to look for possibilities that occurred so that it can determine the method to used in the investigation. In this case, investigator monitoring the traffic activity. In a case of DDoS attacks, each incoming IP address to be monitored to determine the strategy that will be used to conduct an investigation.

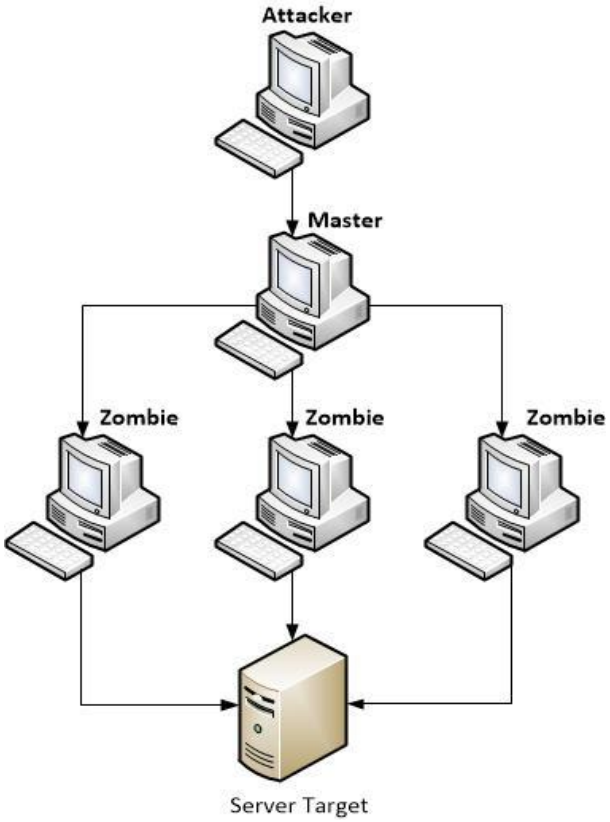

Figure 3. Illustration of DDoS Attack

3) Strategy Approach

Is the selection of the method according to the incident that occurred, testing IDFIF version 3 against DDoS method or a technique Distributed System, which works by analyzing Internet Protocol (IP) Address. Determine a strategy needs to use for the adjustment case with handling techniques. Distributed System method flowchart [6] as figure 4.

4) Capturing

It is the stage of arrest existing trail on the network. In the case of DDoS, all traffic is done Capturing process. Capturing the process of using the software tool is Wireshark. Wireshark is a network packet analyzer program that captures network packets. Captured network packets are information that can be processed, giving rise to the hypothesis. Upon detection of an incident then do the capture using Wireshark.

5) Identification

It is the stage of identification of data packets have captured. At this stage, the determination of the IP Address that has done that has the possibility of capturing process as the source of the attack. This stage Is to identify the evidence, the search for potential evidence.

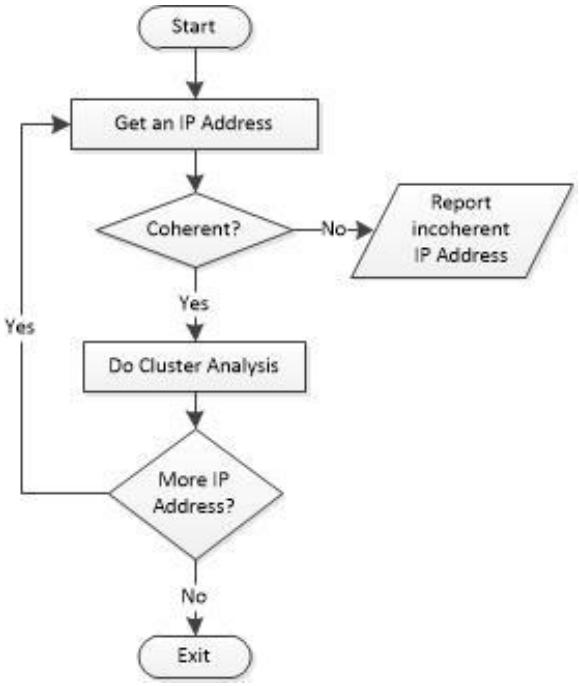

Figure 4. Flowchart Distributed System Method

6) Logging File

It Is the labeling on the packet data is then stored in the database, this stage is to facilitate the analysis phase to generate hypotheses related to the data packet. Ip address that is collect in DDoS attacks then entered into a database and given a label that includes time, place, and intensity of activity.

7) Classification

It is the stage classification of the data packets that have labeled. The classification process to facilitate the analysis process. This classification stage is the stage of database storage of evidence by the type and function.

6.2 Evaluation

IDFIF version 3 evaluation was performed to compare the existing model. It aims to assess the ability IDFIF version 3. According to the assessment of proposed model by comparing IDFIF version 3 with the current model then taken the result from comparing the model. Description of the detailed evaluation as shown in Table 3. Table 3 describes the comparison models IDFIF version 3 with the other models regarding advantages and disadvantages of doing an investigation on the network. From these comparisons, it can be concluded that IDFIF version 3 is a model that has support in the network investigation with the handling techniques appropriate to the circumstances in the investigation process.

Table 3. Result of Evaluation Model

Model's Name	Author	Disadvantages	Advantages
Integrated Digital Forensics Investigation Framework V3 (IDFIF v3)	Hikmatyar, Missi	Can not be used for Cloud Forensics.	Having support in the Network investigation with the handling techniques appropriate to the circumstances in the investigation process.
Integrated Digital Forensics Investigation Framework V2 (IDFIF v2)	Ruuhwan	Not to be used for the network investigation.	Have flexible phrases when used in investigation of computers and smartphones
An Extended Model of Cybercrime Investigation (EMCI)	S. Ciardhuain	Do not have a strategy in Network Investigation techniques and protection of evidence and no monitoring phases.	It can apply in general, especially on Network forensics.
A Hierarchical, Objective-based Framework (HOBF)	N. L. Beebe & J. G. Clark,	The method used is too broad and does not describe in detail at every stage. A related investigate network does not explain in detail.	Simple methods can be developed further and can use in general.
The Enhanced Digital Investigation Process Model (EDIPM)	V. Baryamereeba & F. Tushabe,	do not have any Protection phases for protecting the systems and any strategies in the investigation.	A suitable method for investigating the network by tracking and monitoring of the network.
Computer Forensic Field Triage Process Model (CFFTPM)	M. K. Rogers,	Do not have the protection and engineering phases in the investigation process.	Explain in detail the methods of research related to the investigation on the Internet network.
Generic Framework of Network Investigation (GFNI)	Pilli, Emanuel	No strategy techniques in the investigation.	Having the ability to process Investigation Network in general.

7. CONCLUSION AND FUTURE WORK

IDFIF version 3 is more comprehensive and useful for network investigation than the other existing model. And Having support in the Network investigation with the handling techniques appropriate to the circumstances in the investigation process. IDFIF version 3 have a strategy approach phase for adapting case handling.

This model needs the further development of the Approach Strategy phase or selection techniques in the investigation and handling of evidence and the further development of the examination phase in the processing of evidence.

This model needs further testing of IDFIF version 3 in this test against cybercrime cases that occur.

8. REFERENCES

[1] Chhabra, G.S., 2015. Distributed Network Forensics Framework : A Systematic Review. *International Journal of Computer Applications (IJCA)*, 119(19), pp.31–35

[2] Jazi, I.R. et al., 2013. Internet Forensics Framework Based on Clustering. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 4(12), pp.115–123.

[3] Goel, R., Sardana, A. & Joshi, R.C., 2013. Wireless Honeypot: Framework, architectures, and tools. *International Journal of Network Security*, 15(5), pp.373–383.

[4] Wang, W., 2010. A graph-oriented approach for network forensic analysis. , p.123

[5] Tretmans, J., 1999. Testing Concurrent Systems: A Formal Approach. *Proceedings of the 10th International Conference on Concurrency Theory (CONCUR)*, 1664, pp.46–65.

[6] Almulhem, A. & Traore, I., 2008. Profiling distributed connection chains. *International Journal of Communication Networks and Distributed Systems*, 1(1), pp.4–18.

[7] S. Ciardhuain, 2004. An Extended Model of Cybercrime Investigation. *International Journal of Digital Evidence*, Vol. 3, No. 1, pp. 1-22.

[8] Beebe, N. l., & Clark, J. G., 2004. A Hierarchical, Objectives - Based Framework for the Digital Investigations Process. *Proceedings of Digital Forensics Research Workshop*. Baltimore, MD.

[9] Baryamureeba, V., & Tushabe, F., 2004. The Enhanced Digital Investigation Process Model. *Proceeding of Digital Forensic Research Workshop*. Baltimore, MD.

[10] M. K. Rogers, J. Goldman, R. Mislan, T. Wedge & S. Debrota., 2006. Computer Forensic Field Triage Process Model.*presented at the Conference on Digital Forensics, Security and Law*, pp. 27-40.

[11] Pilli, E.S., Joshi, R.C. & Niyogi, R., 2010. A Generic Framework for Network Forensics. *International Journal of Computer Applications*, 1(11), pp.1–6.

[12] Alharbi, S., Weber-Jahnke, J. & Traore, I., 2011. The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review. *International Journal of …*, 5(4), pp.87–100.

[13] Huang, J.et al., 2012. A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigation. , pp.1–22

[14] Mariza, N.et al., 2014. Critical Phases in Network Forensics - A Review. , pp.68–75.

[15] Al-qerem, A., 2015. PNFEA : A Proposal Approach for Proactive Network Forensics Evidence Analysis to Resolve Cyber Crimes. , (January), pp.25–32.

[16] Kumar, M.V. & Lalitha, T., 2016. Soft Computing : Fuzzy Logic Approach in Wireless Sensors Networks. , (June), pp.1242–1249.

[17] He, J.et al., 2016. Network Forensics Method Based on Evidence Graph and Vulnerability Reasoning. *Future Internet*, 8(4), p.54.

[18] Dhammearatchi, D., 2015. Use of Network Forensic Mechanisms. , 7(4), pp.21–36