Evaluation of Integrated Digital Forensics Investigation Framework for The Investigation of Smartphones Using Soft System Methodology

By Imam Riadi

WORD COUNT 6982

TIME SUBMITTED 16-NOV-2018 08:05AM

PAPER ID 42008858

Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System Methodology

Ruuhwan[1], Imam Riadi[2]*, Yudi Prayudi[3]
[1]Department of Informatics, Perjuangan University, Indonesia
[2]Department of Information Systems, Ahmad Dahlan University, Indonesia
[3]Department of Informatics, Indonesia Islamic University, Indonesia

Article Info

Article history:

Received Oct 17, 2016
Revised Jan 9, 2017
Accepted Apr 11, 2017

Keywords:

Evaluation
IDFIF
Smartphone
SSM

ABSTRACT

The handling of digital evidence can become an evidence of a determination that crimes have been committed or may give links between crime and its victims or crime and the culprit. Soft System Methodology (SSM) is a method of evaluation to compare a conceptual model with a process in the real world, so deficiencies of the conceptual model can be revealed thus it can perform corrective action against the conceptual model, thus there is no difference between the conceptual model and the real activity. Evaluation on the IDFIF stage is only done on a reactive and proactive process stages in the process so that the IDFIF model can be more flexible and can be applied on the investigation process of a smartphone.

Corresponding Author:

Imam Riadi,
Ahmad Dahlan University,
National Chung Cheng University,
Jl. Prof. Dr. Soepomo, Janturan, Yogyakarta 55164, Indonesia
Email: imam.riadi@is.uad.ac.id

1. INTRODUCTION

The effort on making disclosure of cybercrime cases is done through a process known as digital forensics [1]. In this case, the digital forensics is science and methods of finding, collecting, securing, analyzing, interpreting, and presenting digital evidence related to the case in the interests of reconstruction of events as well as the legitimacy of the judicial process [2]. One of the current digital crime is malware with target of computer device and smartphone devices [3].

The way to proof valid evidence is to conduct an investigation using Digital Forensic Examination Procedures approach. A number of stages approach in handling these digital evidence procedures is known as Framework. The stage of investigation must be in accordance with the law and the science that exist by using four different steps in order to investigate the evidence presented in the court, which consists of the acquisition, identification, evaluation and admission [3]. Digital forensics process can be divided into four distinct, they are collection, preservation, analysis and presentation [4].

The implication stages of the Digital Forensic Investigation Framework has too much needs to be done, thus out of the 15 steps, can be simplified into 5 stages of General Digital Forensics Investigation Framework (DFIF) on all cases of incident without destroying evidence and protect the chain of the custody [5-6]. Integrated Digital Forensics Investigation Framework (IDFIF) is expected to become the standard method of investigation for investigator. Taking into account that the previous DFIF so that the DFIF that have been there before can be accommodated by IDFIF [7-8]. The application of IDFIF against the investigation process of the Smartphone needed to perform some evaluations in advance against the IDFIF stages since Smartphones have unique characteristics, so that it cannot be equated with ordinary computers handling [9-10].

Soft systems methodology is a method of evaluation that not only compares a model with the other models but rather compares a conceptual model with a process in the real world, so unknown deficiencies of the conceptual model can be known and directly perform corrective action against a conceptual model so that there is no difference between the conceptual model and the real activity [10-12]. The focus of the SSM is to create an activity system and human relationships within an organization or group in order to achieve common goals [12-13]. Then the SSM can be applied as a solution to the evaluation stage of the IDFIF investigative process for smartphones. Evaluation on the stage of the IDFIF is only done on a reactive and proactive process stages in the process so that the IDFIF v2 model can be more flexible and can be applied to the process of investigation of a smartphone.

2. LITERATURE REVIEW

2.1. Smartphone

In this day, Smartphone devices have the same function with a computer [13]. Yet, even though the functions are similiar, there are some differences in the process of digital forensics handling between computer and smartphones devices [9], [15-14], as shown in Table 1.

Table 1. Comparison of Computer and Smartphone Forensics

Aspect	Computer Forensics	Smartphone Forensics
Connectivity	Limited	Unlimited
Source of Evidence	Hard disk, RAM, External storage	SIM card, RAM, ROM, External Memory, Network Data
Remove Internal Storage	Yes	No
Bypass the Password	Yes	Cannot bypass password during Logical Acquisition
Power and Data Cables	Standard	Wide range of power and data cables
File System	Standard file system	Wide range of file system

2.2. Integrated Digital Forensics Investigation Framework (IDFIF)

The IDFIF method has characteristics, which can record history of input, so it can be assumed that the method can detect the order of the previous DFIF to form a new DFIF. IDFIF (Integrated Digital Forensic Investigation Framework) is a framework that is built by performing the analysis and evaluation of the framework that existed previously. The method used to perform the analysis and evaluation is sequential logic. The final result and framework [7-8] are shown in Figure 1.

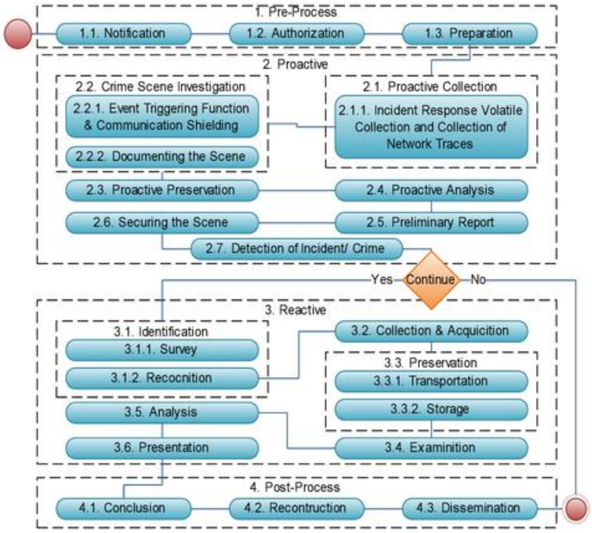


Figure 1. IDFIF model [7-8]

IDFIF stages are divided into 4 main stages which consist of:

1) Pre-Process: Notification, authorization, and preparation.
2) Proactive: Proactive collection, crime scene investigation, proactive preservation, proactive analysis, preliminary report, and securing the scene detection of incident/ crime.
3) Reactive: Identification, collection and acquisition, preservation, examination, analysis and presentation.
4) Post-Process: Conclusion, reconstruction and dissemination.

2.3. Soft System Methodology (SSM)

The system is as a human activity system (HAS). HAS is defined as a set of activities in which men involved in it and the relationship between its activities. SSM recommends that each individual has differences on perception of the situation and differences on interests. This is explicit in the decisions of an acceptable analysis of all people [11-12].

SSM is used to perform the analysis and evaluation of information technology so it produces a framework that is expected can be better than before. SSM can also be used to conduct the evaluation on framework of digital evidence handling so that the existing framework could be better than the previous one [10, 13]. SSM consists of a 7-stage analysis process which uses the concept of human activity in understanding the situation in the surrounding areas to determine the action to be taken in order to develop the existing situation. The seven stages of SSM are:

1) ***Situation Considered Problematic:*** The first stage of SSM is undertaken to determine the process to be explored. A brief understanding about the process in general is attractive and is allowed for later producing a problematic situation of the process. Sources of information is obtained from observations on the course of the process. Overview of the general process is the basis for the making of rich picture to make the groove course of the process to be more visible.
2) ***Problem Situation Expressed:*** The overview presented from the first stage can make a clearer picture called a rich picture. Rich Picture shows the entire details involved in the process and is described in a structured overview of the process.
3) ***Root Definition of Relevant System:*** Defining the entire process that has been described in the problem situation expressed form textual storyline and concise.
4) ***Conceptual Model of System Described and Root Definition:*** Based on the textual definition for each defined element, improvements to the conceptual model is needed to achieve the ideal goal.
5) ***Comparison of Model and Real World:*** Comparing between the conceptual model with the reality in the real world so that adequate level of conceptual model can be revealed to solve a problem.
6) ***Systematically Desirable and Culturally Feasiable Changes:*** Defining the changes that must be made to the existing models. In this step, the specified change is possible.
7) ***Action to Improve the Problem Situation:*** Taking corrective action by means of intervening changes in the implementation model.

3. RESEARCH METHODS

Methodology for conducting evaluation of IDFIF has detail stages and is illustrated in Figure 2.

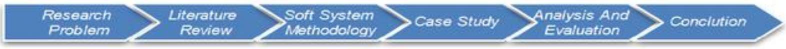


Figure 2. Research methods

1) Identifying a Research Problem by seeing various phenomena, events and information in various ways to tests against IDFIF so that all the shortcomings of that framework can be known.
2) Identifying a Research Problem by seeing various phenomena, events and information in various ways to test against IDFIF so that all the shortcomings of that framework can be known.
3) Reviewing the literature by searching the basics theories related to the IDFIF problems of research and the process of smartphone evidence handling.
4) Soft System Methodology for IDFIF is the stage that must be performed in conducting the IDFIF evaluation. IDFIF stages are evaluated only at the proactive and reactive process stage.
5) Case Study by conducting an evaluation and is undertaken to test both IDFIF models on smartphone investigation handling.
6) Analysis and Evaluation is the evaluation process of comparison on the IDFIF v2 with a DFIF in the process of smartphone investigation.

4. RESULT AND ANALYSIS

The data obtained from the results of literatures are being processed in accordance with the standard digital evidence handling for smartphone. From the results of the evaluation, the framework handling smartphone based on IDFIF can be seen.

4.1. Stage 1 of SSM: Situation Considered Problematic

In General, based on the results in the process of implementation of the Integrated Digital Forensics Investigation Framework (IDFIF), the situational problems include:

1) Step 2.6 securing the scene should be placed in position 2.1 on proactive collection.
2) There is no conditioning if evidence was found in "*on*" or "*off*" mode, especially in the smartphone handling.
3) There is no determination of whether the digital evidence handling process is carried out on the spot or in a computer forensics laboratory.

4.2. Stage 2 of SSM: Problem Situation Expressed

The notion of IDFIF's proactive and reactive phase process does not comply with the conditions in the field and only describes the stages for handling computer as shown in Figure 3.

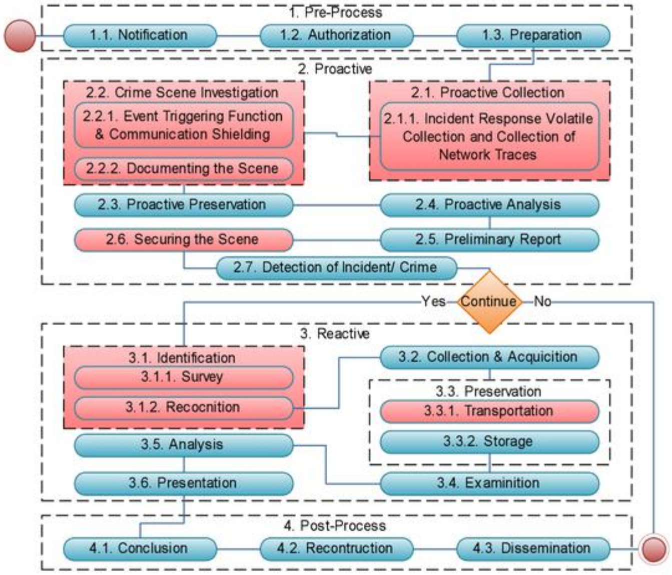


Figure 3. Rich picture IDFIF [7-8]

Evaluation of improvement against the IDFIF is needed, so that the IDFIF can be applied globally on digital evidence handling process.

4.3. Stage 3 of SSM: Root Definition of Relevant System

The step process of the digital evidence handling should be made to overcome the general circumstances that may be encountered by investigator involving digital evidence particularly on electronic media and smartphone devices related in the field [17].

Incident response process is the digital evidence handling at the scene (the crime scene), especially in the smartphone device handling.

1) Securing the Scene is a process to keep the crime scene so that the necessary evidence does not lost, damaged, experience addition or subtraction and there is no different result in difficult or obscure crime scene processing and examination of technical scientific basis [18-20], [25].

2) Documenting the Scene is a documentation process of all locations and digital devices including smartphones devices in the area of the crime scene without touching or polluting the smartphone device and the environment in which it was found [18-22].
3) Event Triggering is the search process that triggers the events at the scene of the matter so that the investigator could conclude on the field while the type of crime has been done [2], [23-24].
4) Plug In Portable Power Supply is a process to keep the smartphone device conditions in a on-state to get to the laboratory for further examination process [18].
5) Communication Shielding is a process of smartphone device isolation from all radio network (e.g. Wi-Fi, Bluetooth) to keep traffic data, such as SMS messaging and others [18-22].
6) Seize is a process of foreclosure against the digital evidence that is mainly on a smartphone device [18].
7) Transportation is at removal process of digital evidence primarily on a smartphone device from scene heading to the lab for further examination process [18], [20-21].

Laboratory process is an examination process of digital evidence in the smartphone device especially those conducted in laboratories wich include several process, i.e.:

1) Acquisition is a process to obtain data or information from the smartphone device or related media [18-23], [25].
2) Storage is the process or result of a doubling of storage acquisitions of digital evidence to maintain the security of the data that has been obtained [18-21].
3) The Examination is an examination process that reveals the digital evidence including those that might be hidden or omitted [18-23].
4) The technical review is an analysis process. It constructs the link among the findings both the perpetrators with evidence, obtained evidence with the victim and the offender with the victim [18-23], [25].
5) Reporting is a process of preparing a detailed summary of all steps taken and conclusions reached in the investigation of the case [18-23], [25].

4.4. Stage 4 of SSM: Conceptual Model of System Described And Root Definition

Digital evidence requires step that has flexibility in handling various types of digital evidence because every crime scene is always different and also uses tools and the investigator have to work based on the handling principles [2], [19]. Figure 4 is a conceptual IDFIF v2.

The principle of IDFIF is to get data that can be used and taken from the computer resources, computer systems, computer networks, communication lines, storage media, computer applications and others [21], [23]. Such data can be processed in accordance with the procedures, so that it can serve as legal and legitimate evidence [22-23].

The main principles to be followed by the investigator in the handling of digital evidence especially smartphones are as follows:

1) May not change the original data that has been obtained.
2) Make a complete record of all activities related to the acquisition and handling the original and copied data. The original data must be preserved.
3) Must not undertake activities that are beyond the ability or knowledge.
4) Must consider all aspects of personal safety and equipment while doing the work.
5) Any time the legal rights of people affected by the action that should be considered.
6) Need to be aware of all the organization's policies and procedures related to activities performed.
7) Communication must be maintained in accordance with the clients, legal practitioners, supervisors and other team members.

IDFIF stages in the process of smartphone digital evidence investigation primarily has four main stages and each stage has a sub-process.

Preparation is a preparation that must be done to perform the process of investigation in handling the digital evidence begins on the sports scene of the matter until making the final report.

1) Notification: The implementation of investigation or crime reported to law enforcement.
2) Authorization: The stage to get the right evidence access and the legal status of the inquiry process.
3) Preparation: The preparation stage that includes the availability of personnel, various tools and all things needed in the investigation.

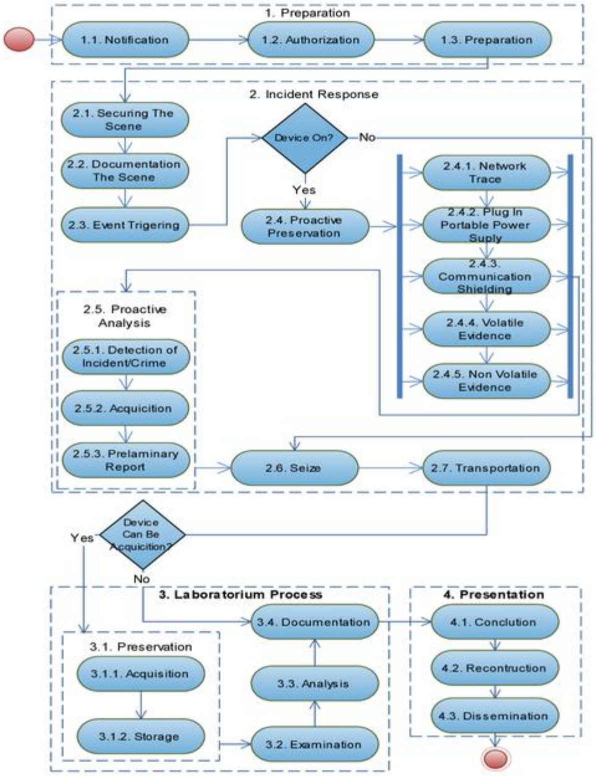


Figure 4. Conceptual IDFIF v2

Incident Response is an activity that is carried out at the scene of the matter with a view to secure the existing digital evidence, so it is not contaminated by other 26gs.

1) Securing the Scene: A mechanism to secure the crime scene and protect the integrity of evidence.
2) Documentation of the Scene: Processing the scene of things, looking for the source of the trigger event, looking for the connection of communication or network and documenting the scene by taking a picture of every detail of the scene.
3) Event Triggering: Initial analysis of the process. In the late stages of the event triggering, there is a decision process.
4) Proactive Preservation: This stage has five sub-phases i.e. network trace, is searching traces through the network that is used by the digital evidence: plug in portable power supply, is the process of safeguarding digital evidence in "on" state so the power contained in the digital evidence can be preserved along the way until in the forensic laboratory; communication shielding, is the isolating data communication on disabling stages exhibits digital so as to prevent data changes from the outside; and volatile and non-volatile evidence, is the process of safeguarding digital evidence.
5) Proactive Analysis: Live analysis stage against the findings and build the first hypothesis of a scene. Detection of incident/crime, at this stage, is a stage to ensure that there has been a violation of the law. Acquisition is the process of data acquisition against the findings to relieve the workload of forensic digital analysis in the laboratory. Preliminary report is the process of making an initial report upon the proactive investigation activities that have been conducted.
6) Seize: The foreclosure process towards the digital evidence that has been found to further be analyzed.
7) Transportation: Represents the removal process of digital evidence from the scene of the matter towards forensic digital laboratory.

The laboratory process is the process of analyzing the data against the previous evidence in the laboratory so that the kind of crimes that have occurred can be found.

1) Preservation: Preserve the integrity of findings using a hashing function and chain custody.
2) Examination: The processing of evidence to find its relationship with genesis.
3) Analysis: Technical studies and string the link among the findings.
4) Documentation: The documentation of all activities that have been done from the beginning of the investigation process until the end of the analysis process in the laboratory.

Presentation is the process of making reports related to the analysis results conducted in the previous stage and to ensure that each process has been conducted in accordance with the rules of the applicable law.
1) Conclusion: Summing up the results of the investigations that have been conducted.
2) Reconstruction: Analysis process and evaluation on the overall investigation results.
3) Dissemination: The recording process of inquiry and notes that can be shared on other investigators who do investigations on similar cases.

4.5. Stage 5 of SSM: Comparation of Model and Real World

The next stage is the process of comparing a conceptual model to suit with the situation of the problem at the moment (the real world). This can be seen in Table 2.

Table 2. Comparison of the conceptual model and real activities

IDFIF Model	Real Activity	Recommendation
Notification	Yes	-
Authorization	Yes	-
Preparation	Yes	The addition of the decision process of the investigation handling to be conducted.
Securing the Scene	Yes	-
Documentation of the Scene	Yes	-
Event Triggering	Yes	-
Proactive Preservation	Yes	The addition of the decision process analysis of evidence that have been discovered.
Proactive Analysis	Yes	-
Seize	Yes	-
Transportation	Yes	The addition of the decision process the handling of digital evidence to the next stage.
Preservation	Yes	The addition of the decision process the handling of evidence type.
Examination	Yes	-
Analysis	Yes	-
Documentation	Yes	-
Conclusion	Yes	-
Reconstruction	Yes	-
Dissemination	Yes	-

4.6. Stage 6 of SSM: Change Systematically Desirable and Culturally Feasible

The next process is to determine the 25ults of improvement based on the recommendations that have been specified in the previous stage and it can be seen in Table 3.

Table 3. The Results of the Recommendation on IDFIF Repairing

IDFIF Model	Recommendation	Repair
Preparation	The addition of the decision process of the investigation handling to be conducted.	The decision process on the investigation handling to be conducted.
Proactive Preservation	The addition of the decision process analysis of the evidence that have been discovered.	The decision process analysis of evidence that have been discovered.
Transportation	The addition of the decision process of the digital evidence handling to the next stage.	The decision process the handling of digital evidence to the next stage.
Preservation	The addition of the decision process of the evidence type handling.	The decision process the handling of digital evidence type.

4.7. Stage 7 of SSM: Action to Improve the Problem Situation

Based on the recommendations of improvements on the previous stage, four decision processes for handling the digital evidence is added on IDFIF v2 stage. It is necessary to make IDFIF v2 to become more flexible when applied on digital evidence handling process in the field based on evidence that has been found. IDFIF v2 in Figure 5.

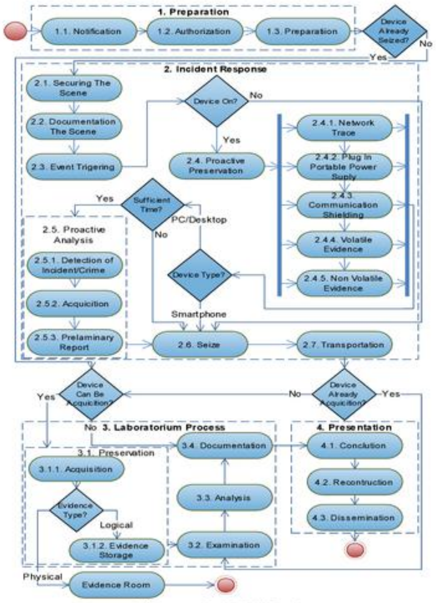


Figure 5. IDFIF v2

5. DISCUSSION

5.1. Case Study

The digital evidence handling process is focused on Smartphone by using IDFIF v1 and IDFIF v2. Case scenarios and simulations in the research are tailored to the fraud cases through short messages service (SMS) and are adopted from the cases that have happened some time ago. The case is a fraud lottery with prizes. The mobile device that is used to send SMS to the victim is Lenovo S860. Perpetrators send SMS to victims with a message that the victims have won a sweepstakes with prizes from PT. X for a single unit car worth 400 million rupiah and the victim was told to contact the number specified by the perpetrator. The victim did what was ordered by the perpetrator without regarding for the sender's SMS number. After the victim contacted the perpetrator, the victim was instructed to send money to the perpetrators' acoount of 10% of the value of the prize for administrative expenses and the cost of delivery of the prizes. Without thinking ahead, the victim do money transfers amounting to 10% of the value of the gifts that was told will be received. However, after the delivery of the amount of money into the account that has already been specified by the perpetrator, the victim feels cheated against the SMS received so that the victim reported the incident to the authorities.

5.2. Digital Evidence Handling Using IDFIF v1

Digital evidence handling process towards smartphones using IDFIF v1 starts from post-process that have three sub-phases i.e. stage of preparation that is investigating the implementation of notices or reported crimes to law enforcement. The next stage is authorization that is the stage to get the right access to evidence and the legal status of the inquiry process. The next stage is the preparation stage that is the process of preparation that includes the availability of personnel and various tools, and all things needed in the investigation.

Proactive process is a process in the scene to get all the evidence related to the crime which has been committed by the perpetrator. The first process that should be done in the sports scene things is securing the scene. Securing the scene is a mechanism to secure the scene of the matter and protect the integrity of evidence.

Smartphone digital evidence handling process by using this model can only be made up to crime scene investigation process due to the smartphone review process that must be done on the digital forensic laboratory, the data security in the smartphone can be assured.

Next, on the IDFIF v1 model, there is no plug in portable power supply process which is a process of exhaustion of Smartphone security from the limitation of battery resources because the Smartphone that is in the scene not always in full condition. As for the handling of the Smartphone, when it is found in an "on" state, then it must remain "on" and if the smartphone is found in an "off" state, it should remain "off". The process of smartphone handling using IDFIF v1 can be seen in Figure 6.

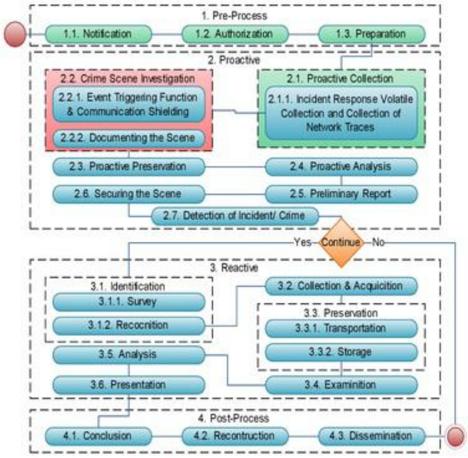


Figure 6. IDFIF v1 for smartphone investigation [7-8]

5.3. Digital Evidence Handling Using IDFIF v2

The process of digital evidence handling process against smartphone use IDFIF v2 can be seen in Figure 7. The preparation process and post process (in the previous IDFIF) or Presentation (in IDFIF that have been evaluated) has the same stages. Different stages of both models are simply being on a proactive process/ incident response and reactive process/ laboratory process.

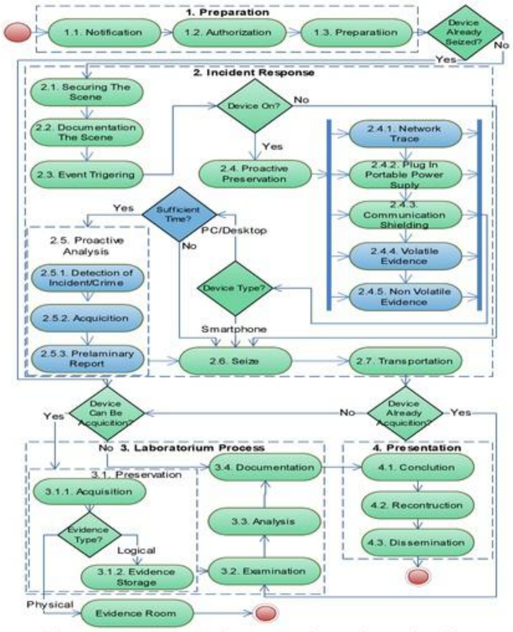


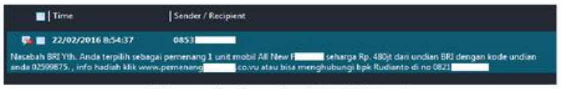
Figure 7. IDFIF v2 for smartphone investigation

Incident response as well as proactive collection is the process trought the scene things to get all the evidence related to the crime which has been committed by the perpetrator. However, there are several stages that must be done in incident response for handling evidence of smartphone are securing the scene, scene documentation, event triggering, proactive preservation, plug in a portable power supply, communication shielding, seize and transportation.

1) Securing the Scene is a step that must be done in the implementation of the supporting scene is keeping the scene from people who do not have any interest in the investigation process so that the integrity of digital evidence can be authentically guaranteed.
2) Documentation of the Scene is the documentation process towards the rounded area and stuff that potentially becomes evidence by photographing the crime scene and evidence in forensic photography (public photos, medium photos and close-up photos) after securing the scene of things.
3) The Event Triggering is the beginning of the analysis process of the events that have occurred on the scene. After securing the scene, investigator conducts an initial analysis of the process against an event that has happened on the scene and searches things that trigger events in the scene so that the investigator can deduce the type of crime that has done to further process analysis in digital forensic laboratories. As for digital evidence found is one unit of Lenovo's smartphone S860 used actors to perform fraud action.
4) Proactive Preservation is the process of securing Smartphone evidence that have been found at the scene of the matter so that the integrity of the data that reside on Smartphone are staying awake until the analysis process in the forensic laboratory.
5) Plug in Portable Power Supply is a charging process against Smartphone evidence using a portable power supply because of the battery power condition on the Smartphone. It is found not always in full condition, so needs a charging process by using at portable power supply to maintain the condition of the smartphone to be in an "on" state until it goes to the digital forensic laboratories.
6) Communication Shielding is a stage of safeguarding Smartphone evidence by isolating it against data communication using a faraday bag so that the exchanging data or control process performed remotely via available networks will not happened.
7) Seize is the foreclosure process of Smartphone's evidence to be examined in the digital forensic laboratory after the battery power security and isolation.
8) Transportation is a process of transferring the evidence that has been found from the scene towards digital forensic laboratories. When in the process of transportation, smartphone's evidence must be completely guarded, so it will not be changed at all and will not reduce the evidence integrity.

The next stage is laboratory process that is the smartphone review process in digital forensics laboratory. The stage of the review process is done in digital forensic laboratory, preservation, acquisition, storage, examination, analysis and documentation.

1) Preservation is the process of securing Smartphone evidence. The Smartphone condition when in the process of acquisition should be in a disconnected state from existing data communications.
2) Acquisition is the first thing that must be done in the laboratory of digital forensic towards Smartphone software that has been found on the scene of things.
3) Evidence Storage is the process of storing Smartphone evidence to a determined place. The form and the content of the digital evidence must be kept in a sterile place to ensure that there is no change. This is very noteworthy because a slight change in the digital evidence could impact the investigation results. Digital evidence is naturally to be temporary (volatile), so if it is not accurate, it will be very easily damaged, lost, altered, or experience an accident.
4) The Examination is the process of processing digital evidence to find the relationship with the crime that has been done by the offender against the victims.
5) Analysis is the process of technical studies in the examination of smartphone evidence and constructing the link among the findings. After getting the expected files or digital data from the review process, the data is then analyzed in detail and comprehensively prove the occurred crime and what to do by the perpetrators of the crime. The analysis results of the digital data known as the digital evidence that should be scientifically justified in the law in the courts. In some cases it is frequently required the collection of physical evidence and logical form of the ekstaksi data. Yet in this case, the required evidence is simply a record of outgoing and incoming calls as well as outgoing and incoming SMS located in the internal storage of a smartphone. The offender notifies the potential victims that were told win a car unit. As for the message sent by the perpetrator can be seen in Figure 8.



Time | Sender / Recipient

22/02/2016 8:54:37 0853[redacted]

Nasabah BRI Yth. Anda terpilih sebagai pemenang 1 unit mobil All New [redacted] seharga Rp. 480jt dari undian BRI dengan kode undian anda 02599875. , info hadiah klik www.pemenang[redacted].co.vu atau bisa menghubungi bpk Rudianto di no 0821[redacted]

Figure 8. Proof of SMS fraud

6) Documentation is the process of making a written report of the investigation activities of the Smartphone evidence which is done from the beginning of the examination until the end of the examination. The report will later serve as consideration by the judge at the Court in the decision making process.

5.4. Analysis and Evaluation

Every digital forensic model has different stages in each handling of the digital evidence found, so in the handling of various evidences, it requires different digital forensic models. The digital forensic model should be applied to all digital evidence found in the field. The difference of each model can be seen in Table 4.

Table 4. Digital Forensic Comparison Model for Handling Smartphone

IDFIF v2	1	2	3	4	5	6	7
Notification			√			√	
Authorization		√	√			√	
Preparation	√		√	√	√	√	√
Securing the Scene	√	√		√			√
Documentation the Scene	√	√	√				√
Event Triggering	√		√			√	√
Proactive Preservation	√	√	√	√		√	√
Proactive Analysis				√		√	
Seize	√	√					
Transportation	√	√	√				
Preservation	√	√	√	√	√	√	
Examination	√	√	√	√	√	√	√
Analysis	√	√	√	√	√	√	√
Documentation	√	√	√	√		√	√
Conclusion				√	√	√	√
Reconstruction							
Dissemination							

Desc.: 1. NIST 4. SFIPM 7. WMDFM
2. ACPO 5. SSFPM
3. ISO 27041 6. HDFIP

Every digital forensic model also has advantages and disadvantages in the digital evidence handling process. The advantages and disadvantages of each of these models can be seen in Table 5.

Table 5. Digital Forensic Difference Model for Handling Smartphone

Author's Name	Process Model Names	Strength	Weakness
Ruuhwan	Integrated Digital Forensic Investigation Framework v2 (IDFIF v2)	Have a flexible stage when used in computers and smartphones investigation	Only for computers and Smartphone
Rahayu	Integrated Digital Forensic Investigation Framework (IDFIF)	Accommodate the whole stages of the existing DFIF	Only for computers
NIST	Smartphone Forensic Investigation Model	It has a fully equipped stage	The whole evidence examined in the laboratory
ACPO	Good Practice Guide For Computer Based Electronic Evidence Internet	4 principles of ACPO can accommodate the entire electronic evidence	3 principles of the ACPO is not applicable to the handling of the smartphone evidence
ISO	Smartphone Forensic Investigation (ISO 27041)	It has a fully equipped stage in general	There is no process of securing the scene
Goel, Tyagi & Agrawal	Smartphone Forensic Investigation Process Model (SFIPM)	It has a fully equipped stage for smartphone handling	Documentation is only done after examination of the smartphone evidence
Mohtasebi & Dehghantanha	Symbian Smartphones Forensic Process Model (SSFP)	It has a fully equipped stage for handling smartphone	All stages are done in place
Raymond & Venter	Harmonized Digital Forensic Investigation Process (HDFIP)	It has a fully equipped stage for digital evidence handling in general	There is no process of securing the scene and the documentation on the scene
Anup Ramabhadran	Windows Mobile Device Forensic Model (WMDFM)	The steps are quite specific to the handling of the Smartphone	All stages are done in place

Based on Table 5, IDFIF v2 has a better flexibility level of the digital evidence handling, especially on investigation process of Smartphone evidence.

6. CONCLUSION

The evaluation stage of the IDFIF using SSM only performed on the stages of the proactive and reactive proces so that the results of the evaluation produce a more flexible IDFIF v2 and can be applied to the process of investigation of a Smartphone.The results of the testing that has been done in the evidence handling shows that IDFIF v2 Smartphone which has been through an evaluation process, flexible than the existing IDFIF v1 because on IDFIF v2, the securing process on behind the scene placed early in the incident response process as well as the presence of an extra plug in portable power supply and removal process as well as seize the transportation process from the laboratory process to the end of the process of incident response. Next research is IDFIF v2 testing should be done on every case is different as in the case of network forensic, cloud forensic etc.

REFERENCES

[1] Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). "A New Approach of Digital Forensics Model for Digital Forensic Investigation." *International Journal of Advance Computer Science and Applications (IJACSA)*, Vol.2, No. 12, pp.175-178.

[2] M. M. Pollitt, (1995) "Computer Forensics: An Approach to Evidence in Cyberspace," in *Proceeding of the National Information Systems Security Conference*, Baltimore, MD, Vol. II, pp. 487-491

[3] Prayudi, Y., &Yusirwan, S. (2015). "The Recognize Of Malware Characteristics Trough Static And Dynamic Analysis Approach As An Effort To Be Prevent Cybercrime Activities." *Journal of Theoretical and Applied Information Technology* (JATIT), Vol. 77, No. 3, pp.438-445.

[4] Widiyasono, N., Riadi, I., & Luthfi, A. (2016). "Investigation on the Services of Private Cloud Computing by Using ADAM Method." *International Journal of Electrical and Computer Engineering* (IJECE), Vol. 6, No. 5, pp. 2387-2395

[5] Selamat, S. R., Yusof, R., & Sahib, S. (2008). "Mapping Process of Digital Forensic Investigation Framework." *International Journal of Computer Science and Network Security*(IJCSNS), Vol. 8, No. 10, pp.163–169.

[6] Yusoff, Y., Ismail, R., & Hassan, Z. (2011). "Common Phases of Computer Forensics." *International Journal of Computer Science & Information Technology* (IJCSIT), Vol. 3, No. 3, pp.17–31.

[7] Rahayu, Y. D. (2014). "The Concept of Integrated Digital Forensics Investigation Framework (IDFIF) As Comparative Framework Standards Investigation. " *Universitas Islam Indonesia*.

[8] Rahayu, Y. D. & Prayudi, Y. (2014). "Build Integrated Digital Forensics Investigation Framework (IDFIF) Using Sequential Logic Method. " *National Seminar on Information and Communication Technology*.

[9] Alharbi, S., Jahnke, J. W., &Traore, I. (2011). "The Proactive and Reactive Digital Forensic Investigation Process." *International Journal of Security and Its Application* (IJSIA), Vol. 5, No. 4, pp.59-71.

[10] PI Santosa, "Cost and benefit of information search using two different strategies., *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 8, no. 3, pp. 195-206, 2010.

[11] Checkland, P.B. (1999). "Systems Thinking, Systems Practice." Chichester: John Wiley & Sons.

[12] Checkland, Peter. (2000), "Soft System Methodology: A Thirty Year Retrospective, System Research and Behavioral Science," pp.11-58.

[13] Creswell, John W., (1998), "Qualitative Inquiry and Research Design: Choosing Among five Traditions," Sage Publication Inc. Thousand Oaks, Calif.

[14] Yan, Y., Xiaohong, H., & Wanjun, Wang. (2015). "Location-Based Services and Privacy Protection under Mobile Cloud Computing." *Bulletin of Electrical Engineering and Informatics,*

[15] Anwar, N., Riadi, I. & Luthfie, A. (2016). "Forensic SIM Card Cloning Using Authentication Algorithm." *International Journal of Electronics and Information Engineering* (IJEIE), Vol. 4, No. 2, pp. 71-81

[16] Alghafli, K. A., Jones, A., & Martin, T. A. (2011). "Guidlines for the Digital Forensic Processing of Smartphone." *Australian Digital Forensics Conference*, pp.1-8.

[17] Al-Azhar, M. N. (2012). "Digital Forensic: A Practical Guide Computer Investigation. Jakarta: Salemba Infotek."

[18] ACPO. (2011). "The ACPO Good Practice Guide for Computer-Based Electronic Evidence." London: 7 Save Information Security.

[19] Goel, A., Tyagi, A., & Agrawal, A. (2012). "Smartphone Forensic Investigation Process Model." *International Journal of Computer Science & Security* (IJCSS), Vol. 6, Issue 5, pp.322-341.

[20] NIST, (2014). Guidelines on Mobile Device Forensics (Draft)

[21] ISO/IEC 27041. (2014). Information technology–Security techniques–Assurance for digital evidence investigation methods (Draft).

[22] Ramabhadran, A. (2007). Forensic Investigation Process Model for Windows Mobile Devices.

[23] Mumba, R. & Venter, H. (2014). "Mobile Forensics using the Harmonised Digital Forensic Investigation Process," *IEEE*.

[24] Agrawal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). "Systematic Digital Forensic Investigation Model." *International Journal of Computer Science and Security* (IJCSS), Vol. 5, Issue 1, pp.118-131

[25] Dehghantanha, A. & Mohtasebi, S. H. (2013). "Towards a Unified Forensic Investigation Framework of Smartphone." *International Journal of Computer Theory and Engineering*, Vol. 5, No. 2, pp.351-355.

Evaluation of Integrated Digital Forensics Investigation Framework for The Investigation of Smartphones Using Soft System Methodology

ORIGINALITY REPORT

7%

SIMILARITY INDEX

PRIMARY SOURCES

1	fti.uajy.ac.id Internet	53 words — 1%
2	journals.plos.org Internet	34 words — < 1%
3	uir.unisa.ac.za Internet	32 words — < 1%
4	Emmanuel Masabo, Kyanda Swaib Kaawaase, Julianne Sansa-Otim, Damien Hanyurwimfura. "Structural Feature Engineering Approach for Detecting Polymorphic Malware", 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2017 Crossref	31 words — < 1%
5	www.airccse.org Internet	30 words — < 1%
6	www.cscan.org Internet	27 words — < 1%
7	uobrep.openrepository.com Internet	27 words — < 1%
8	www.csee.umbc.edu Internet	26 words — < 1%

9	Shrivastava, Gulshan, and B. B. Gupta. "An Encapsulated Approach of Forensic Model for digital investigation", 2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE), 2014. Crossref	23 words —	< 1%
10	onlinelibrary.wiley.com Internet	22 words —	< 1%
11	Hsieh-Tsen Pan, Cchiu-Shu Pan, Shyh-Chang Tsaur, Min-Shiang Hwang. "Cryptanalysis of Efficient Dynamic ID Based Remote User Authentication Scheme in Multi-Server Environment Using Smart Card", 2016 12th International Conference on Computational Intelligence and Security (CIS), 2016 Crossref	21 words —	< 1%
12	pdfs.semanticscholar.org Internet	20 words —	< 1%
13	sibresearch.org Internet	18 words —	< 1%
14	www.energizect.com Internet	17 words —	< 1%
15	doaj.org Internet	16 words —	< 1%
16	proceedings.adfsl.org Internet	15 words —	< 1%
17	destidesternity.blogspot.com Internet	15 words —	< 1%
18	www.virtusinterpress.org Internet	12 words —	< 1%
19	ieeexplore.ieee.org Internet	10 words —	< 1%

20	computerforensics.parsonage.co.uk Internet	10 words — < 1%
21	journal.portalgaruda.org Internet	10 words — < 1%
22	R.C. Joshi, Emmanuel S. Pilli. "Fundamentals of Network Forensics", Springer Nature America, Inc, 2016 Crossref	9 words — < 1%
23	www.jiit.ac.in Internet	8 words — < 1%
24	aksitservices.co.in Internet	8 words — < 1%
25	usir.salford.ac.uk Internet	8 words — < 1%
26	nvlpubs.nist.gov Internet	8 words — < 1%
27	"Advances in Digital Forensics VII", Springer Nature America, Inc, 2011 Crossref	6 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		