International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1): 1-14
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001

ANALYSIS AND EVALUATION DIGITAL FORENSIC INVESTIGATION FRAMEWORK USING ISO 27037:2012

[1]Didik Sudyana, [2]Yudi Prayudi, [3]Bambang Sugiantoro
[1] Department of Information Technology, STMIK Amik Riau, Pekanbaru, Indonesia
[2] Department of Information Technology, Universitas Islam Indonesia, Yogyakarta, Indonesia
[3] Department of Information Technology, UIN Sunan Kalijaga, Yogyakarta, Indonesia
didik.sudyana@stmik-amik-riau.ac.id

ABSTRACT

The important thing that every digital forensic investigator must take into account in carrying out digital forensics activities is the following steps and procedures in digital forensics. These stages are known as frameworks or SOP investigations. Stages of the digital forensic process must be in accordance with the rule of law and also the right mechanism. However, the current investigation framework is still in shortage where there are stages set in the applicable standards such as ISO 27037: 2012, it is not set in the framework. When the stage is missed in the investigation process, it would be a problem and can be sued in court and canceled the results of investigations conducted regarding the existence of procedures that are not implemented. Therefore, a study was conducted to evaluate the previous frameworks with the identification of important processes contained in ISO 27037: 2012 so as to provide an assessment of the extent to which the existing framework meets the requirements of ISO 27037: 2012. Then an improvement on the framework closest to the provisions in ISO 27037: 2012. So as to produce an investigation framework that has been standardized.

KEYWORDS

Digital forensics, investigation framework, ISO 27037:2012, standardized framework, SOP Investigation.

1 INTRODUCTION

The current development of computer crime continues to increase, even based on news published by kompas.com that Indonesia is ranked second in the list of the top five countries with the highest cybercrime. Still based on news published kompas.com also mentioned that in the period of three years, there were recorded 36.6 million cybercrime attacks that occurred in Indonesia, and Cybercrime Crime Police itself has arrested 497 suspects from 2012 to April 2015 The estimated loss reached 33.29 billion [1]. Based on these statistics can be seen in the rapid development of this computer crime.

To be able to uncover cases of computer crime, then used a processed with the scientific method known as digital forensics. According to [2] digital forensics is the science and method used in the conservation, collection, identification, analysis, documentation, and presentation of digital evidence in order to facilitated or made progress in the process of reconstruction of criminal events. From this definition, it can be seen that digital forensics is useful in the process of investigating a criminal offense involving the use of technology.

The important thing that every digital forensic investigator must take into account in carrying out digital forensics activities is the following steps and procedures in digital forensics. These stages are known as frameworks. In this case, according to [3] the stages in digital forensic process must be in accordance with the rule of law and also the right mechanism. It is also supported by [4] that the user of a framework in the investigation of a case can lead to a procedural proof process and keep the process from contamination of evidence and be accountable in the eyes of the law. Because of the importance of guidance that produces this scientific study, The completion of an investigation should be used a well-structured framework.

However, the current investigation framework is still in shortage where there are stages set in the applicable standards such as ISO 27037: 2012, it is not set in the framework. So when there was a provision in the standard that is missed in the investigation processed because the framework or SOP used does not refer to the standard, it will be a problem and can be sued in court and canceled the results of investigations conducted regarding the existence of procedures that are not implemented.

As an example of a framework built by [5], there is no stage or explanation of the stages in securing the crime scene where it is regulated in ISO 27037: 2012. The next example is the framework built by [6], which in the phases of its framework also there is no stage of securing the scene of the case.

However, the current investigation framework is still in shortage where there are stages set in the applicable standards such as ISO 27037: 2012, it is not set in the framework. So when there was a provision in the standard that is missed in the investigation process because the framework or SOP used does not refer to the standard, it will be a problem and can be sued in court and canceled the results of investigations conducted regarding the existence of procedures that are not implemented.

Therefore we needed a studied to evaluate the previous frameworks with the results of identification of the important processes contained in ISO 27037: 2012 so as to provide an assessment of the extent to which the existing framework meets the requirements in ISO 27037: 2012. Then an improvement on the framework closest to the provisions in ISO 27037: 2012. So as to produce an investigation framework that has been standardized.

2 RESEARCH REVIEW

The following will discuss the review of research that has been done previously related to the framework of digital forensic investigation. Beginning with research conducted by [7] which proposed the framework of a digital forensic investigation under the name of framework Systematic Digital Forensic Investigation Model. This framework is based on the development of the DFRWS investigation model and 3 other framework models. Based on these four existing investigative models, they proposed a systematic development of the investigative model and consisted of 11 stages of the investigation.

[8] conducted a study of the investigation framework and proposed a framework with the name Integrated digital forensic process model. This framework builds on the development of previous existing frameworks and accommodates them into new frameworks. There are 6 frameworks used as the foundation for this new framework developed. This framework itself consists of 5 main stages with a total of 36 stages detail.

[4] conducts research related to the investigation framework under the name of the Integrated Digital Forensics Investigation Framework (IDFIF) framework. IDFIF is built using a sequential logic method and uses 6 model of investigation framework as its development base. IDFIF is built by taking into account the six previous frameworks and accommodating them into IDFIF so IDFIF expectations can be a standard comparison of the investigative framework. IDFIF is divided into 4 main stages with 22 stages of detail.

While the problem raised in this study is the framework of the current investigation is still there are deficiencies where there are stages arranged in standards such as ISO 27037: 2012, was not set in the framework. The approach taken to this solution is to evaluate the framework before and then the framework evaluation results become the foundation to make improvements so that it will produce a framework that has met the provisions of international standards.

3 METHODOLOGY

In summary, the method and stages of the research can be described as in Figure 1 below.

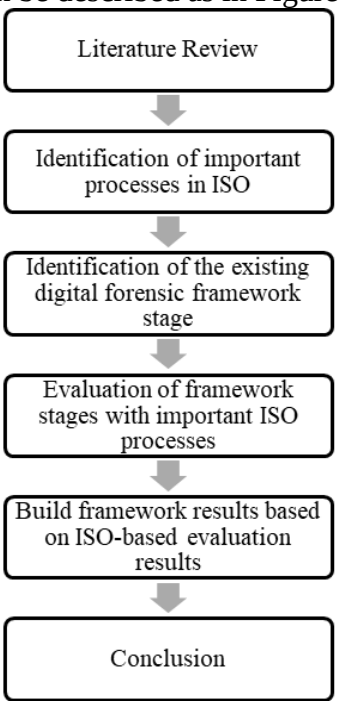

Figure 1 – Methodology

4 RESULTS AND DISCUSSION

4.1 Identification of important processes ISO 27037:2012

This is an international standard that discusses specific guidelines related to digital forensic investigation activities. Which activities include identification, collection, acquisition, and preservation. All of these processes are important processes that must be done carefully to maintain the integrity of the evidence. The methodology used in collecting digital evidence will affect whether or not the evidence is received in court. In addition to discussing digital evidence, ISO also discusses general guidelines on how to collect non-digital evidence [9]. ISO 27037: 2012 consists of 7 chapters or 7 sections consisting of Scope, Normative Reference, Terms and Definitions, Abbreviated Terms, Overview, Key Components of Identification, Collection, Acquisition, and Preservation of Digital Evidence, and Instance of Identification, Collection, acquisition, and preservation. Based on the ISO 27037: 2012 document content structure, the focus on digital forensic investigation is found in sections 6 and 7 and a little explanation in chapter 5 (part of the digital evidence processing). While chapters 1 through 4 contains only the introduction and the terms used. So that the focus to identify the important stages is done in chapters 5, 6, and 7 in ISO 27037: 2012 document.

4.2 Identification of the Previous Framework Stage

In this research, three types of frameworks used to be evaluated are Systematic Digital Forensic Investigation Model [8], Integrated Digital Forensic Process Model [9], and Integrated Digital Forensics Investigation Frameworks [4].

The first framework is SDFIM. In The SDFIM framework, there are 11 stages listed as :

SDFIM = *{Preparation → Securing the scene → Survey & Recognition → Documentation of Scene → Communication Shielding → Evidence Collection → Preservation → Examination, Analysis → Presentation → Result & Review.}*

The second framework is IDFPM. In The IDFPM framework, there are 37 stages which have 6 main stages. The IDFPM listed as :

IDFPM = *{Documentation → Preparation → Incident → Incident Response → DFI → Presentation}*

where

Preparation = {Policy/Procedure → Operational Readiness → Infrastructure Readiness}

Incident = {Detect → Assess → Confirm → Notify → Authorize → Deploy.}

Incident Response = {Approach Strategy → Search → Recover → Seize → Preserve → Transport → Store → Collect}

DFI = {Collect → Authenticate → Examine → Harvest → Reduce → Identify → Classify → Organize → Compare → Hypothesize → Analyze → Attribute → Evaluate → Interpret → Reconstruct → Communicate → Review → Reconstruct → Hypothesize}

Presentation = {Report → Present → Decide → Dissemination}

The last framework is IDFIF. In the IDFIF there are 22 stages which have 4 main stages. The IDFIF listed as:

IDFIF = *{Pre-Process → Proactive → Reactive → Post-Process}*

where

Pre-Process = {Notification → Authorization → Preparation}

Proactive = {Proactive Collection → Incident Response → Crime Scene Investigation (Even Triggering Function & Communication Shielding) → Documenting the Scene → Proactive Preservation → Proactive Analysis → Preliminary Report → Securing the Scene → Detection of Incident / Crime}

Reactive = {Identification (Survey → Recognition) → Collection & Acquisition → Preservation (Transportation → Storage) → Examination → Analysis → Presentation}
Post-Process = {Conclusion → Reconstruction → Dissemination}

4.3 Evaluation of the Framework Phase with ISO 27037: 2012

An evaluation was done by comparing the results of identification of important processes in ISO 27037: 2012 with the stages in the framework that has been described previously. The evaluation table based on [10]. In the evaluation, each stage will be given a code of numbers in accordance with the sequence of stages. The results of the evaluation framework can be seen in table 1 below:

Table 1: Framework Evaluation Results

Important Process ISO 27037: 2012	Contained in the section framework		
	SDF	**IDFP**	**IDFIF**
Identification			
Investigation planning	**1**	**4.1**	
Preparation equipment & team direction	**1**	**2**	**1.3**
Assessment of TKP security risks			
Security of crime scene	**2**	**4**	**2.6**
Evidence search	**3**	**4.2**	**2.2.1**
Identification of evidence	**3**	**4.2**	**2.1**
Determining the priority of evidence			**2.1**
Documentation	**4**	**1**	**2.2.2**
Recording of evidence (Chain of custody)	**4**	**1**	
Collection			
Determining the evidence seized or acquired at the scene	**6**	**4.3**	**2.1**
Conducting seizure of evidence	**6**	**4.3**	**3.2**
• Evidence is on	**6**	**4.3**	**2.1**
- Analyze whether to require volatile data from the device	**6**	**4.3**	**2.1**
- If need to do Live acquisition procedure	**6**	**4.3**	**2.1**
- If you do not need to check the security aspect and data vulnerability to electricity			
- Perform a device shutdown procedure			
• The evidence is not on	**6**	**4.3**	**2.2.1**
- Unplug all connected cables and batteries (if there is a battery)	**6**	**4.3**	**2.2.1**
- Perform the next collection procedure			
Provide evidence labels	**7**		
Backing up the evidence	**7**	**4.4**	**3.2**
Collect verbal information from witnesses	**3**	**4.1**	**3.1.2**
Acquisitions			
Inspection of data security aspects of evidence		**5.1**	
Determination of acquisition model conducted	**6**	**4.3**	**2.1**
• Acquisition of illuminated devices	**6**	**4.3**	**2.1**
- Perform live acquisition procedures to get volatile data	**6**	**4.3**	**2.1**
- If non-volatile data is also needed at that time, do also the acquisition procedure on the non-volatile data		**4.3**	
- If the device can be confiscated, perform evidence collection procedures			
• Acquisition on non-lit devices	**8**	**5.1**	**3.2**
- Perform static acquisition procedures by performing imaging of data storage media	**8**	**5.1**	**3.2**
• Partial Acquisitions			
- Can be done using a combination of live procedures and static acquisition			
Implementation of the acquisition	**6**	**5.1**	**3.2**
Verify the results of the acquisition	**8**	**5.2**	**2.3**
Preservation			
Provide seal of evidence	**7**	**4.4**	
Examination of security aspects of the evacuation of evidence			
Moving evidence	**7**	**4.6**	**3.3.1**
Storage of evidence	**7**	**4.7**	**3.3.2**

The overall evaluation results from the above table can be illustrated by using a bar chart related to which framework sequence most met the requirements set forth in ISO 27037: 2012.

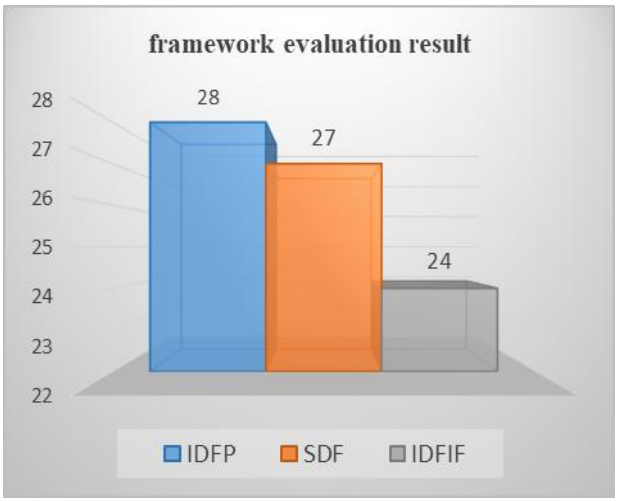

Figure 2: Graph of framework evaluation results

From the graph, it can be seen that the framework of Integrated Digital Forensics Process Model (IDFP) is a framework that the most meet the requirements in ISO 27037: 2012. Where there are 28 provisions in ISO 27037: 2012 set forth in the framework. But there are still some provisions that have not been included in the framework.

Based on the evaluation of the three frameworks, the Integrated Digital Forensics Process Model (IDFP) is chosen to go through the next step of improving the framework so that the framework can refer to the provisions in ISO 27037: 2012 comprehensively.

4.4 Building Framework Based on Evaluation Results Based on ISO 27037: 2012

In accordance with the results of a previous evaluation, then set the framework of Integrated Digital Forensics Process Model (IDFPM) to be repaired. The first improvement will complete all the existing provisions in ISO 27037: 2012 that does not exist into the framework. And from the evaluation results, can be identified there are 10 provisions that do not exist in the framework IDFP.

Fulfillment of these aspects of the provisions of course in addition to increasing the existing stage will be adjusted the sequence of steps back and separation of several stages so that all aspects of the provisions in ISO 27037: 2012 can be comprehensive. Because the current sequence of phases is still separated from one stage to another, it is necessary to adjust the sequence of stages to conform to the provisions of ISO 27037: 2012. The summary of the improvements made are:

4.4.1 Added New Stages

4.4.1.1 Risk Assessment on the scene

In this framework the phases are not yet regulated, whereas ISO 27037: 2012 section 6.2.2 provides an explanation that this stage is important because it involves the security of personnel and evidence at the scene and the stage of the security risk assessment of the crime scene before the personnel goes to the scene. On the basis of this consideration, the stages of Risk Assessment on The Scene are placed at the stage before Deploy. Because the deployment stage is a stage telling the team to get down to the scene and start an investigation. So that the risk assessment stage is done before informing the team to get down to the scene.

4.4.1.2 Securing the scene

In this framework, the security stage of the crime scene is not presented in a separate stage, the security stage of the crime scene is placed only in Incident's explanation in the published journal written by the researcher. While this stage is one of the important stages, ISO 27037: 2012 reveals that the stage of securing the crime scene is done to immediately secure evidence at the scene so as not to be contaminated and maintain its integrity. It also controls the scene of the crime scene, there are some activities such as securing and taking over the scene, isolating the scene so only the licensed personnel who can enter the scene, making sure the devices at the scene no one is disturbed (if in the dead do not turn on, vice versa).

Based on the explanation, the stage of securing the scene needs to be added. For the position of the stage itself, as also described in ISO 27037: 2012, the scene of securing the crime scene is done as soon as it arrives at the scene. Based on these considerations, the stage of securing the scene is placed in the first position in the Incident Response stage which is the stage of activity at the scene.

4.4.1.3 Identify prioritize evidence

This stage is not yet set in the IDFPM framework. So this stage will be added to the framework. The stages of identifying evidence that has priority are more important because some properties of evidence are easily damaged or lost so that if not handled immediately, it will risk losing or the evidence will be damaged. In ISO 27037: 2012 section 5.4.2, it is explained that in identifying, after conducting a search of evidence, it is given priority over the evidence found so that it can be handled early. Based on these considerations and explanations, the phase of identifying prioritize evidence is placed in the position after the Search (the stage of seeking evidence).

4.4.1.4 (Decision Symbol) The device on and Need Volatile Data

Stages with the decision symbol for Device On and Need Volatile Data is then it would be more appropriate if this stage is combined to the assessment because it is known what kind of incident so that it can plan what kind of investigation.

The stage of survey recognition is the stage of conducting a survey of the crime scene and conducting interviews with witnesses around the scene to obtain verbal information from witnesses. This is described in ISO 27037: 2012 section 7.1.1.2 which states that officers should also hold discussions with individuals located at the scene to obtain information relating to potential evidence or evidence to be collected. On this consideration, the stage of the survey will be done after the stage of securing the crime scene and before doing the search for evidence. Because verbal information is used for searching for evidence.

4.4.1.5 Live acquisition

This stage is the next stage of the stage Need volatile data. Where volatile data is required, a live acquisition procedure must be performed to obtain volatile data from the device as soon as described in ISO 27037: 2012 section 6.8.

4.4.1.6 Authenticate

Authentication stages after a live acquisition are mandatory procedures that must be performed after the acquisition to ensure that the data acquired is equal to the original data. This is in accordance with the explanation in ISO 27037: 2012 section 7.1.4.

4.4.1.7 (Decision) The device can be seized, Device can be shut down and Shutdown

This stage is still the stage of continuation of the previous stage. If the device that has been carried out live acquisition can be confiscated, then check whether the device can be shut down, because the procedure should be done checking the security aspects and vulnerabilities of the device against electricity, if no problem then do the procedure shut down by force, and if the device vulnerable to damage if turned off, then perform a normal shutdown procedure. This is regulated ISO 27037: 2012 section 7.1.2. after the shutdown procedure then carried out the next stage is the seizure of evidence that the foreclosure stage has been set in the framework.

4.4.2. Separation of stages

4.4.2.1 Approach Strategy to Survey Recognition and Plan

This stage is divided into 2 stages and separated because in ISO 27037: 2012 section 6.7.2 it is explained that the activity of making the investigation plan is done in the stages of the briefing session. In the framework IDFPM explained that the stages of the briefing session are in the Preparation stage. However, because the stage of assessment of incidents occurring in the assessment stage will be more appropriate if the stage is combined to the assessment because it is known what kind of incident so that it can plan what kind of investigation.

The stage of survey recognition is the stage of conducting a survey of the crime scene and conducting interviews with witnesses around the scene to obtain verbal information from witnesses. This is described in ISO 27037: 2012 section 7.1.1.2 which states that officers should also hold discussions with individuals located at the scene to obtain information relating to potential evidence or evidence to be collected. On this consideration, the stage of the survey will be done after the stage of securing the crime scene and before doing the search for evidence. Because verbal information is used for searching for evidence.

4.4.3 Name change stages

4.4.3.1 Collection to the acquisition

The terms of the collection stages in the framework are described as the stages of doubling the evidence. In the ISO document, the term used is the acquisition. Because the term collection is used to perform the physical collection of evidence. On the basis of this consideration, the collection stage is renamed to the acquisition

After undergoing the process of fulfilling the aspect of the provisions in ISO 27037: 2012 into the Integrated Digital Forensics Process Model (IDFPM) framework by adding stages and re-adjusting the sequence of stages, subsequent improvements are made by eliminating and combining the stages in the Integrated Digital Forensics Process Model (IDFPM). The reason for elimination because there are several stages that should be done in one stage, divided into several stages so that the framework becomes inflexible. Some conditions do the elimination of the stages in the framework are:

4.4.4 Stages performed repeatedly

4.4.4.1 Confirm

Described by [8] is an act of conforming to the team the results of the assessment that an incident has occurred for investigation. While Notify described is an action to notify the team of the incident that occurred. The act of confirming is almost identical to the action of notifying the team. Because essentially both explain the existence of an incident that occurred. So this stage can be combined.

4.4.4.2 Authorize

The Authorize described by [8] is an act to obtain permission to conduct an investigation. This action has been done in the Operational Readiness stage where this stage is described as an action to prepare all operational related administration such as for permit and others. So when it has obtained a license, of course, it can be done to investigate.

4.4.5 Stages are not authority investigators

4.4.5.1 Recover

Recover described by [8] is an action to recover the system as it was. This action is not the authority of the officers who perform the crime scene. So based on the regulation, Recover action is not the authority of the investigation team.

4.4.6 Stages incorporation because it is still one piece with a certain stage

4.4.6.1 Examine, Harvest, and Reduce

Examine described by [8] is an act of examining evidence and ensuring evidence is accessible. Harvest described is an action to map what kind of file system is used in digital evidence and make sure the data can be extracted or opened. And Reduce is the act of knowing the identification of data elements by using unique metadata and identifiers such as MD5 to find out the types and types of files. These three stages are interrelated activities. These three stages can be unified by using the term Examine. As described by [12] in the Forensic Examination of Digital Evidence document: A Guide for Law Enforcement published by U.S. The Department of Justice Office of Justice Programs mentioned that in Examination, several activities were performed such as data extraction, data reduction by using hash value, carving files, deleted file recovery, and some other activities. So that the Harvest and Reduce stages are part of the Examine activity.

4.4.6.2 Organize

The organization described by [8] is the act of organizing data that has been classified so that it can focus on the data. This stage can be combined with classifying stages because The Classify explained that the data is grouped according to the data pattern. Stages of this grouping, of course, will also be arranged data, because it has been grouped. And based on the next stage is Compare mentioned that the data to be compiled is data classify results. Not the result data organize.

4.4.6.3 Attribute

The attribute described by [8] is an act of seeking the linkage of findings to specific individuals regarding the ownership of the data in the digital evidence being analyzed. This stage can be eliminated as it is still part of the process of conducting the analysis. This is supported by [12] in the Forensic Examination of Digital Evidence document: A Guide for Law Enforcement published by U.S. Department of

Justice Office of Justice Programs which states that one of the actions taken in conducting an analysis is to identify ownership of data that creates, modifies, or accesses the suspected data.

4.4.6.4 Evaluate

Evaluate described by [8] is an act of evaluating the findings to ascertain whether the hypothesis is made correct. This stage can be eliminated and incorporated into the Interpret stage. This is supported by [13] explaining that in conducting digital forensic investigations, there will be an interpretation stage, which includes evaluating digital evidence that has been analyzed to find patterns, topics, similarities of people, and so forth. To evaluate is part of the interpretation.

After determining the eight stages are eliminated, then the next is to build a beta framework based on the provisions that have been described previously. The results of the beta framework can be seen in the picture below:

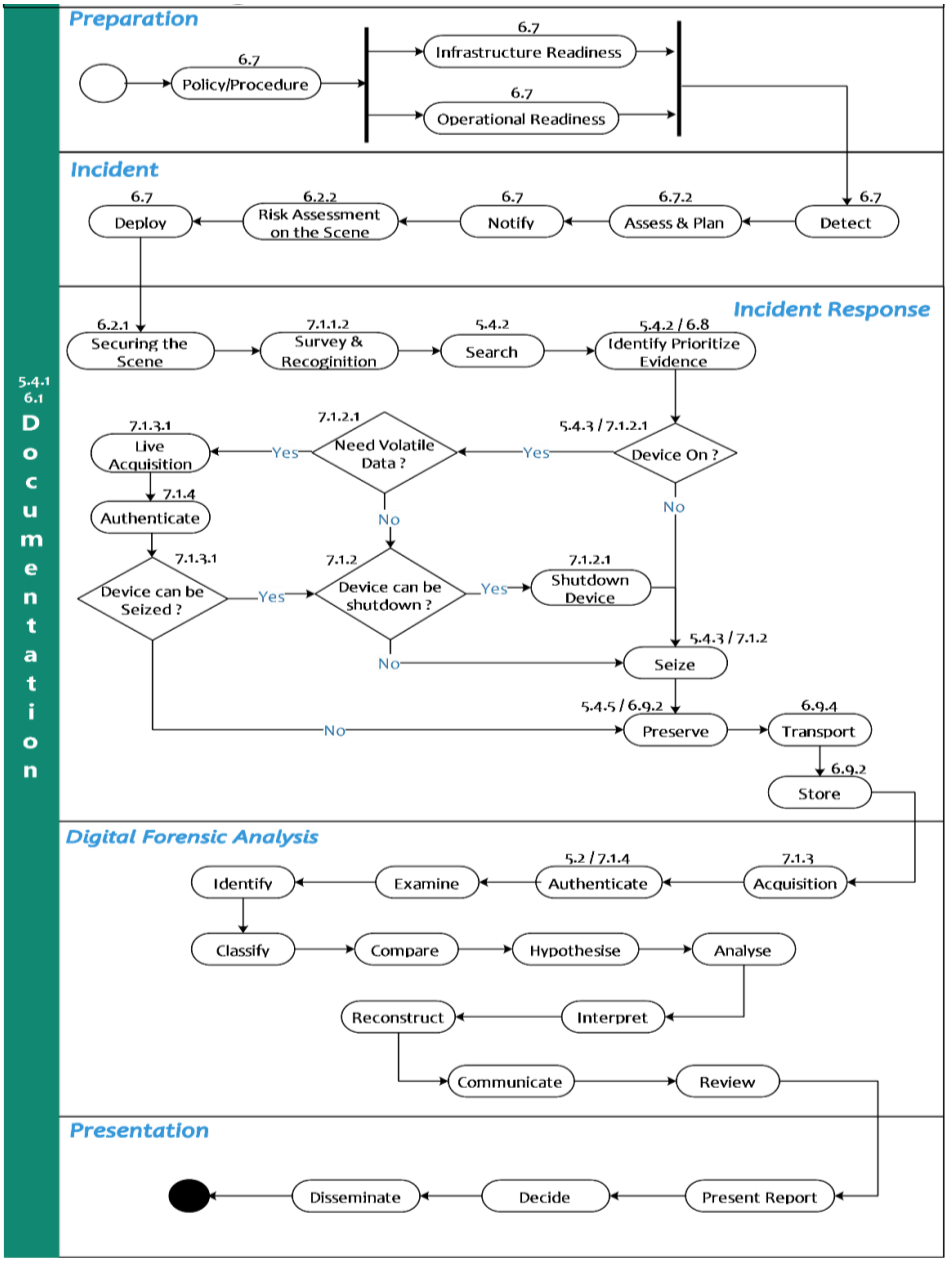

Figure 3: Beta Framework 1.0

4.5 Analysis and User Feasibility Review about The Beta Framework 1.0

After the beta framework of improvement based on SNI 27037: 2014 is completed, the next step is to test the beta framework of this improvement to see if the beta framework 1.0 has fulfilled all the requirements of ISO 27037 and to know whether the stages in this beta framework 1.0

can be implemented in the investigation. The planned trial is to provide a questionnaire on the feasibility of using this framework as to whether each of the steps in the framework is done in conducting investigations and conducting interviews to see their responses and comments about the new framework. The selected respondents were from Forensic Laboratory Center for Computer Forensics of Indonesian Police, Practitioners, and Academics.

4.5.1 Survey Results from Forensic Laboratory Center for Computer Forensics of Indonesian Police

The survey results obtained using a questionnaire that almost all stages of the framework can be done in the investigation process and the framework has met all the provisions of ISO 27037. But there are some stages that are less suitable to be done and there is the use of the term is less and there are stages that have not been covered. From 38 stages of investigation in the framework, there are 7 stages that there are still deficiencies and there are 1 stages that have not been covered in the framework. So that 82% stages in the framework can be done in the investigation. Then do the interview to get more detailed data. The results of these interviews include:

1) In the documentation phase, an explanation is made of forensic photography to perform documentation. There are three types of documentation done in the investigation of documentation using photography, video, and notes. These are not covered in the explanation of the documentation stage.
2) Policy / Procedure step are explained again the letters. In the police, there are warrants of the investigation, search warrant, and permit foreclosure.
3) Infrastructure readiness step is explained that the equipment prepared in conducting such investigation is the preparation of hardware and software for forensic triage purposes.
4) Stages of securing the crime scene should be added explanation that also done the installation of crime scene borderline or commonly called police line. The investigator has the authority to install the Police line.
5) Search step should be changed to Evidence Search to get a clearer terminology.
6) Stages of live acquisition are less suitable. A suitable term for describing the activity is Triage Forensic. Because the triage is a term used in the initial handling to get data quickly at the scene.
7) After the evidence reaches the laboratory, it is not directly acquired. Do first a preliminary hearing. The goal is to equate the perception among digital forensic analysts with investigators. What purpose and instructions will be sought from the evidence.
8) In doing the analysis there is not always a hypothesis. Because the investigation was to investigate the data or look for the data related to the case. Not testing the truth of a statement.

4.5.2 Survey Results from Practitioners

The survey results obtained that almost all stages of the framework can be done in the process of investigation framework and has met all the provisions of ISO 27037. There is only one stage that is considered less suitable. 97% of the stages in the framework can be done in the investigation. Then do the interview to get more detailed data. The results of these interviews include:

1) Unsuitable stages are Decide stages because digital forensic practitioners are requested assistance by the police to conduct an analysis of electronic evidence, whichever party involved has been submitted by the Police in the expert help letter. So the practitioners stay looking for what data wanted by the Police.
2) The main stages of Preparation, Incident, and Incident Response are often the stages that will be carried out by the Police as the investigator. Practitioners are only requested assistance to guide police investigators in obtaining evidence at the scene so as not to drop directly to the scene. However, all of these stages in the Practitioner's view are feasible and indeed carried out in the investigation stage.
3) For the Present Report stage, If the court decides that the written report made is sufficient, then the presence of the

practitioner in court as an expert witness is not required, but if the court is insufficient to submit the report verbally and be an expert witness, the practitioner must come to court and submit the report.

4.5.3 Survey Results from Academics.

The survey results obtained that almost all stages of the framework can be done in the process of investigation framework and has met all the provisions of ISO 27037. There is only one stage that is considered less suitable. 97% stages in the framework can be done in the investigation. Then do the interview to get more detailed data. The results of these interviews include:

1) Examine stages should be more detailed related the explanation stage. The examine stage should include activities to extract the acquisition data. It also extracts files in unallocated space, slack space, extracts file system information such as folder structure, file type, file size, timestamp. So it can be easier to the next stage because all of the data in the evidence have been mapped and structured.

Based on the improvement records in the survey results, the framework improvements are made to complete the deficiency record and the framework can have 100% percent that all stages can be done in the implementation of the investigation. Improvements were divided into four groups. The summary of improvements made such as table 2.

Table 2: Summary of improvements

	Type of Improvements	**Stages are fixed**	**Information**
1	Improvements in the explanation stages	*Documentation*	-
		Policy / Procedure	-
		Infrastructure Readiness	-
		Securing the Scene	-
		Examine	-
2	Change the name stages	*Search*	Replaced to *Evidence Search*
		Live Acquisition	Replaced to *Triage Forensic*
3	Additions new stages	*Analysis Request*	Request for the analysis and purpose correlation between investigators and digital forensic analysts.
4	Improvements stages	*Hypothesis*	Improvements in plot stages.
		Decide	Merger stages to Analysis Request. Because in this stage, will be delivered who has linkages with the evidence.

After Analysis and User Feasibility Review about The Beta Framework 1.0, then the next is to improve the final framework based on the summary table. The results of the final framework can be seen in the picture below.

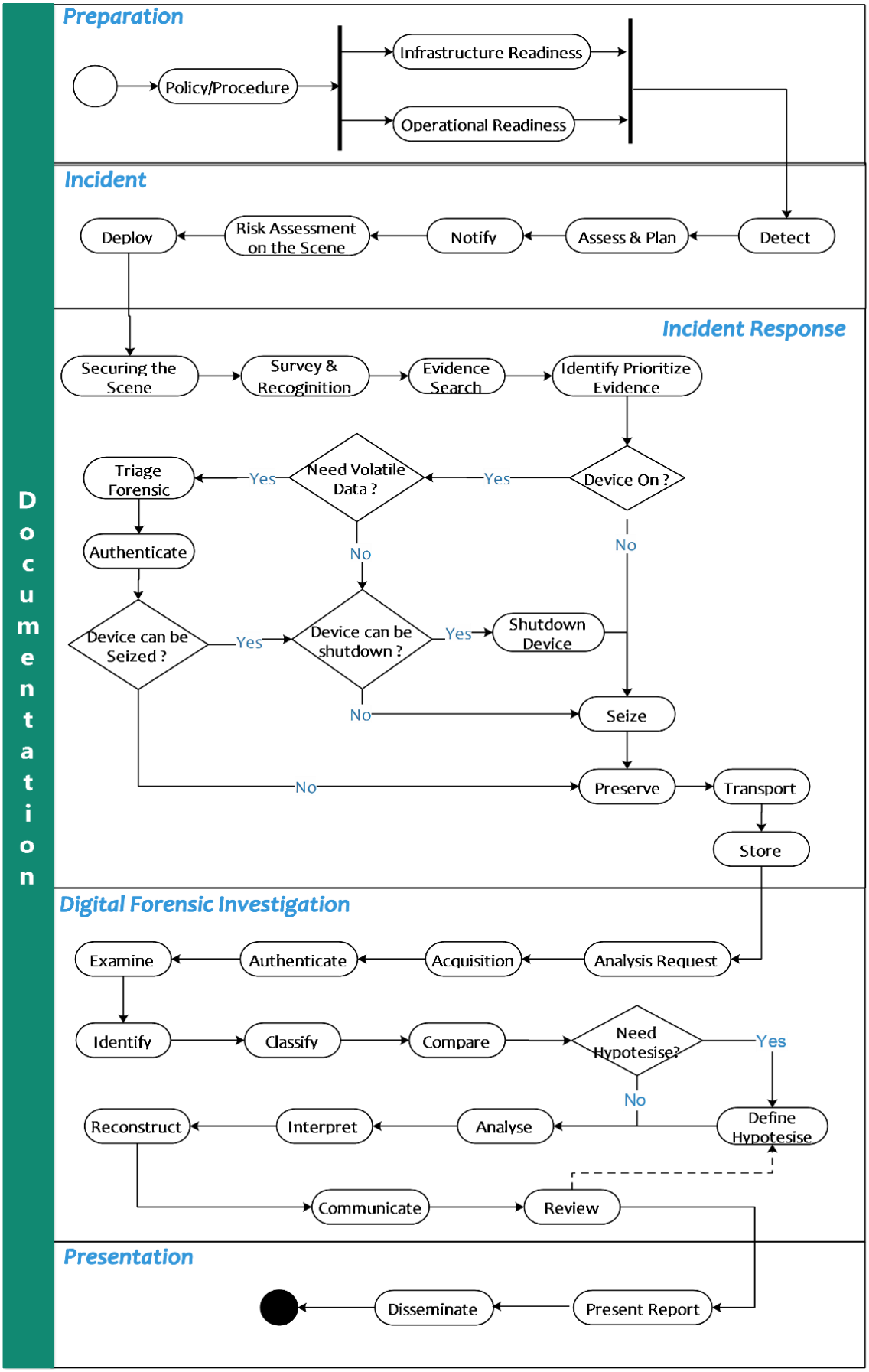

Figure 4: The Final Framework 1.1

4.6 Define the Process about The Improvement Framework Based on Evaluation Results Based on ISO 27037: 2012

There are 6 major stages in the framework of the improvement and retain the number of major stages in the original framework. The explanation of each of the stages in the final framework of the improvement are:

4.6.1 Documentation

The process of documentation at this stage is a continuous process and includes all stages. Documentation in this stage includes activities such as documenting good evidence with photographs, always updating the chain of custody, documenting the scene of the case, and other activities related to the documentation.

4.6.2 Preparation

Is a preparatory activity that must be done to make the process of investigation into the handling of Digital Evidence.

4.6.2.1 Policy / Procedure: Stages of preparing procedures and administration to conduct investigations. There are 3 letters of administration. Its warrants of the investigation, search warrant and permit foreclosure.

4.6.2.2 Infrastructure Readiness: Stages of preparing infrastructure like hardware or software to be used for investigative purposes.

4.6.2.3 Operational Readiness: Stages of personnel preparation to conduct investigations such as training for personnel, and so on.

4.6.3 Incident

Is an activity in analyzing the types of incidents that occurred before the investigative officer to the scene of the Case.

4.6.3.1 Detect Stages of detecting incidents or cases by using prior experience to find out whether there is a common case pattern.

4.6.3.2 Assess & Plan: The stage of assessing the results of the detection of what kind of pattern or type of incidents is occurring.

4.6.3.3 Notify: Stages inform the team of the results of the analysis performed on the Detect stage.

4.6.3.4 Risk Assessment on The Scene: Stages of risk assessment at the crime scene. Risk assessment is conducted to keep the investigation team safe and the evidence.

4.6.3.5 Deploy: Stages tell the team to start the investigation and go to the crime scene.

4.6.4 Incident response

It is an activity carried out at the scene of the case with the aim of securing the existing digital evidence so as not to be contaminated by other matters.

4.6.4.1 Securing the Scene: Stages of a mechanism for securing crime scenes and protecting the integrity of evidence like using the police line.

4.6.4.2 Survey & Recognition: This stage is to conduct a preliminary survey to evaluate the event and identify the surrounding circumstances that have the potential to become evidence. In addition, it also identifies and interviews with people who are around the scene of the case and collect verbal information from the people who are around it.

4.6.4.3 Evidence Search: Stages of searching for evidence.

4.6.4.4 Identify Prioritize Evidence: Stages give priority to evidence found against the vulnerability aspect of the data.

4.6.4.5 The device on or off: Stages of analyzing the evidence found at the scene of the case in a living condition or not. If found alive, do the next procedure, but if found dead, do foreclosure procedures.

4.6.4.6 Need Volatile Data or No? : The stages of analyzing whether the device found in living conditions is required for its volatile data.

4.6.4.7 Triage Forensic: Stages of performing live acquisition of devices found alive to obtain volatile data as well as non-volatile data required as soon as

possible. Perform the data security risk assessment process first to ensure that the acquisition procedure is accurate and does not damage the evidence.

4.6.4.8 Authenticate: Stages of authenticating the results of the acquisition to maintain data integrity and ensure data acquisition results are correct.

4.6.4.9 Can the device be seized? : The stages of analyzing whether the device that has been in the live acquisition earlier can be confiscated or not. For example, if the device is a server in the data center then it is not possible for foreclosure. If it is not possible for foreclosure, perform a preserve procedure.

4.6.4.10 Can the device be shut down? : The stages of analyzing whether the device found in the living circumstances can be turned off or not. For example, smartphone device found, it should not be turned off because it will do the acquisition procedure in the laboratory.

4.6.4.11 Shutdown Device: Stages if the device can be turned off, then the procedure to turn off the device. Perform security aspect and data vulnerability checks against electricity first. If the data is safe and not vulnerable, perform a shutdown procedure by directly unplugging the power cord or battery of the device. But if it turns out vulnerable data will be damaged, perform a normal shutdown procedure.

4.6.4.12 Seize: Stages of loading evidence that has been found at the scene to the labeled evidence bag. Unplug all cables connected to evidence and batteries (if any) and then process the seizure of such evidence for further analysis in the digital forensics laboratory.

4.6.4.13 Preserve: Stages of securing, isolating, and preserving evidence. Including providing seals to the evidence that has been inserted into the bag of evidence. This statement also carried out the examination of security aspects of the evacuation of pieces of evidence.

4.6.4.14 Transport: Stages of the evacuation of evidence from the scene of the case to the storage of evidence.

4.6.4.15 Store: Stages of storing evidence in a special room of evidence storage for later analysis of the evidence.

4.6.5 Digital forensic investigation

It is an act of digital forensic analysis of all the evidence found.

4.6.5.1 Analysis Request : Stages of Request for the analysis and purpose correlation between investigators and digital forensic analysts.

4.6.5.2 Acquisition: Stages of acquisition. This statement also checks the security aspect of evidence before acquisition to ensure that the acquisition process does not damage the evidence. It also determined the acquisition model to be used. Using live, static, or partial acquisition methods.

4.6.5.3 Authenticate: Stages of authentication or verification of acquisition results from one of which can be done with the hash value.

4.6.5.4 Examine: Stages of examining evidence and ensuring evidence of acquisition results can be accessed. it should include activities to extract the acquisition data. It also extracts files in unallocated space, slack space, extracts file system information such as folder structure, file type, file size, timestamp.

4.6.5.5 Identify: Stages of identifying data that can be used as evidence and clues to the case

4.6.5.6 Classify: Stages of grouping data based on identification patterns performed.

4.6.5.7 Compare: The stages of comparing the pattern of identification results with the previous case for whether there are similar patterns.

4.6.5.8 Hypothesis: Stages of making a hypothesis based on similarity patterns of findings with previous cases.

4.6.5.9 Analyze: Stages of doing an overall analysis of digital evidence to find clues related to the case being handled.

4.6.5.10 Interpret: This stage will conduct an evaluation of digital evidence that has been done the analysis to find patterns, topics, people involved, and so forth.

4.6.5.11 Reconstruct: Stages of reconstructing events based on analysis of digital evidence. It is used to describe how an incident can occur.

4.6.5.12 Communicate: Stages of communicating and reporting the results of the analysis to the authorized party.

4.6.5.13 Review: Stages of reviewing the entire analysis process that has been done.

4.6.6 Presentation

Is the final activity of the implementation of digital forensic investigation. Activities in this stage include submitting the completed analysis of the investigation report.

4.6.6.1 Present Report: Stages of reporting of analysis results including detailed investigation process, chain of custody, and all related documents.

4.6.6.2 Disseminate: The final stage in which to review the whole process of the investigation conducted and also the stage of completion of evidence. Evidence can be returned to the owner, stored in the evidence storage room, or destroyed.

5 CONCLUSION

In this paper, have been done evaluated the three previous research frameworks using ISO 27037: 2012. From the evaluation results obtained the result that the framework IDFPM is the most meet the provisions of the framework in ISO but not all are covered. So that improvement of the framework to met all the requirements in the ISO and produced a framework for improvement that has adopted ISO 27037: 2012 and becomes a standards-based framework. So the framework can be used as a standard framework for digital forensic investigation.

REFERENCES

[1] F. A. Permana, "Indonesia Urutan Kedua Terbesar Negara Asal Cyber Crime di Dunia," *kompas.com*, Jakarta, 12-May-2015.

[2] G. Palmer, "A Road Map for Digital Forensic Research," *Proc. 2001 Digit. Forensics Res. Work. (DFRWS 2004)*, pp. 1–42, 2001.

[3] M. Pollitt, "Computer Forenscs: And Approach to Evidence in Cyberspace," *Natl. Inf. Syst. Secur. Conf.*, pp. 487–491, 1995.

[4] Y. D. Rahayu and Y. Prayudi, "Membangun Integrated Digital Forensics Investigation Frameworks (IDFIF) Menggunakan Metode Sequential Logic," *Semin. Nas. SENTIKA*, vol. 2014, no. Sentika, 2014.

[5] Y. Yusoff, R. Ismail, and Z. Hassan, "Common Phases of Computer Forensics Investigation Models," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 17–31, 2011.

[6] S. Saleem, O. Popov, and I. Bagilli, "Extended abstract digital forensics model with preservation and protection as umbrella principles," *Procedia Comput. Sci.*, vol. 35, no. C, pp. 812–821, 2014.

[7] A. Agarwal, M. Gupta, and S. Gupta, "Systematic Digital Forensic Investigation Model," *Int. J. Comput. Sci. Secur.*, vol. 5, no. 1, pp. 118–134, 2011.

[8] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, "Integrated digital forensic process model," *Comput. Secur.*, vol. 38, pp. 103–115, 2013.

[9] International Organization for Standardization (ISO), *ISO/IEC 27037:2012 - Information Technology: Guidelines for Identification Collection Acquisition and Preservation of Digital Evidence*. 2012.

[10] D. Sudyana, B. Sugiantoro, and A. Luthfi, "Instrumen Evaluasi Framework Investigasi Forensika Digital Menggunakan SNI 27037:2014," *J. Inform. Sunan Kalijaga*, vol. 1, no. 2, pp. 75–83, 2016.

[11] Republik Indonesia, *Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 Tentang Manajemen Penyidikan Tindak Pidana*. 2012.

[12] D. J. Daniels and S. V Hart, "Forensic Examination of Digital Evidence : A Guide for Law Enforcement," *U.S. Dep. Justice Off. Justice Programs Natl. Inst. Justice Spec.*, vol. 44, no. 2, pp. 634–111, 2004.

[13] ISO/IEC 27042:2015, *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*. Switzerland, 2015.