The Framework to Support the Digital Evidence Handling:

A Case Study of Procedures for the Management of Evidence in Indonesia

Yudi Prayudi, Universitas Islam, Indonesia & Department of Computer Science and Electronics, Gadjah Mada University, Indonesia

https://orcid.org/0000-0002-2526-8009

Ahmad Ashari, Department of Computer Science and Electronics, Gadjah Mada University, Indonesia

Tri Kuntoro Priyambodo, Department of Computer Science and Electronics, Gadjah Mada University, Indonesia

https://orcid.org/0000-0003-1906-7224

ABSTRACT

Digital evidence has a different meaning from physical evidence, but even though it is different, both are a unity of evidence that supports each other in the investigation process. Unfortunately, laws and regulations generally have not been oriented to the terminology of digital evidence that should be. It becomes a research challenge in how the handling of digital evidence also gets the same treatment as physical evidence. For this reason, technical studies are needed to support the application of law and regulations for digital evidence handling. This article provides a solution in the form of digital evidence cabinets as a framework to support the centralization of digital evidence that following the applicable regulations of procedures for the management of evidence in the territory of Indonesia. This concept can translate the centralization of digital evidence through the analogy of physical cabinet and the interpretation of cabinet, rack, bags, and evidence unit with types of criminals, list of crimes, list of crime scenes and list of digital evidence at one crime scene.

KEYWORDS

Centralization, Cybercrime, Digital Forensics, Evidence Cabinet, Evidence Room, Physical Evidence

INTRODUCTION

In the digital society era as it is today, one of the challenges is the increased cases of cybercrime. This challenge is one of the consequences of the advancement of information technology and the improvement of telecommunication infrastructure that allows each device to connect in an infinite virtual environment. In this case, according to UNODC (2013), the advancement and improvement of information technology have resulted in the emergence of various forms of new crimes committed by

DOI: 10.4018/JCIT.2020070104

individuals or groups known as cybercrime. Surveys and reports made by (Clearsky Cyber Security, 2018; Morgan, 2017; Ponemon Institute and Accenture, 2017) stated that cybercrime is a serious threat to individuals, institutions, and countries with huge losses tend to increase every year.

The mechanism of cybercrime investigation depends on how digital evidence handled by a digital investigator. Currently, in Indonesia, the number of digital investigators and digital forensics laboratories both within law enforcement agencies, government institutions, private companies, and the academic institution is increasing rapidly. This achievement must be supported by improving the quality of resources, especially regarding the proper understanding of regulations relating to digital evidence handling. Every digital investigator must thoroughly understand regulations, laws, and legal process relating to digital evidence (Boddington, Hobbs, & Mann, 2008). For the jurisdiction of Indonesia, digital evidence has been regulated in Law No. 11/2008 and its amendment No. 19/2016 on Information and Electronic Transactions (UU ITE). In the Police of the Republic of Indonesia itself, there is guidance in the form of Head of Police Regulation (Perkap) on Procedures for the Management of Evidence (Kepolisian Negara RI, 2010). While on the broader scope, there are some references commonly used by investigators concerning digital evidence handling, including the UK Police's ACPO (ACPO, 2012), Digital Evidence Handling from NIJ USA (Ashcroft, Daniels, & Hart, 2004), and ISO 27037 (BSN, 2014) as the standard for the acquisition of digital evidence.

However, none of these references describe how the overall mechanisms for digital evidence handling. The references mostly discuss the guidelines to interact with digital evidence, especially concerning an interaction with digital evidence sources or electronic evidence. For example, as a standard, ISO 27037 focuses more on the guideline for First Responder in carrying out its activities for the identification, collection, acquisition, and preservation of digital evidence. This reference does not describe the basic principles for storing digital evidence. Even in some sections, the meaning of digital evidence is still perceived as part of electronic evidence so that the handling of digital evidence is identical to the handling of physical evidence. A relevant guideline is needed in dealing with digital evidence handling because digital evidence has specific properties, so it must be treated differently from physical evidence.

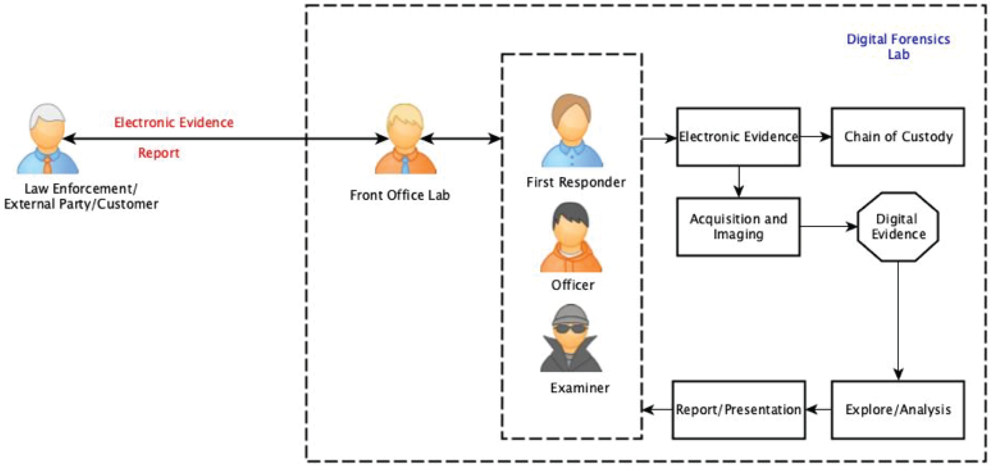
The author has a research focus on how to develop methods of digital evidence handling to be the same as physical evidence and comply with the existing regulations. For that reason, by taking case studies in CDFS (Center for Digital Forensics Studies), preliminary research has been done through the development of relevant business models to support the concept of digital evidence handling (Prayudi, Ashari, & Priyambodo, 2015, 2018). After the existence of the business model, the next step is how to build the basic concept of a framework for digital evidence handling that comply with the regulation. This paper is a follow-up study to detail the technical mechanism of digital evidence handling. The results are expected to be a technical study for improving regulatory aspects to support digital evidence handling.

ORGANIZATIONAL BACKGROUND

Center for Digital Forensics Studies (CDFS) is one of the organizations within Universitas Islam Indonesia, located in Yogyakarta, Indonesia. This center of studies has been established and carrying out its activities since 2014. The main activities are education and research both for undergraduate and master's degree programs. However, CDFS also serves interaction with the community in the form of digital forensics examination services and expert witnesses for the court. These services are not only requested for law enforcement purposes but also the defense of legal counsel or other civil litigation problems. For this reason, one of the divisions available in CDFS is the digital forensic laboratory. Throughout 2016-2018, the digital forensic laboratory at CDFS has handled 25 cases.

The activities that are generally carried out among the examiners in the digital forensic laboratory on CDFS are limited to the following activities: imaging, examination/analysis, and reporting of digital evidence findings. Digital evidence is not stored centrally; digital evidence is controlled and stored directly by the respective examiners. The issue of storage, recording of information, and control of access to evidence are generally applied to electronic evidence as physical evidence, but not to digital evidence. The illustration in Figure 1 provides information about activities that have been carried out by digital forensic examiners at the CDFS digital forensic laboratories.

Figure 1. Current condition of examination process at CDFS



The evidence of a case in the form of both physical and digital evidence will be complementary in an investigation process (Carrier & Spafford, 2003). In this case, the output of the digital evidence analysis must support the overall investigation process, and the digital evidence handling must also be following with applicable regulations. According to our analysis in CDFS, there are gaps in the mechanism of digital evidence handling, mainly if it is associated with the current regulations regarding evidence handling. The existence of the wrong mechanism in digital evidence handling will have an impact on the results of the analysis, so it potentially not be accepted to support the investigation process. Thus, even though physical evidence and digital evidence have different characteristics, however some essential aspects regarding handling mechanism must have the same treatment.

Handling of electronic and digital evidence must be in following the regulations that are generally used as a legal basis for handling evidence. For the territory of the Republic of Indonesia, there are regulations issued by the National Police of Indonesia known as Perkap 10/2010 and 8/2014 concerning Procedures of the Management of Evidence (Kepolisian Negara RI, 2010). The regulation contains five basic principles in handling evidence, that is: (1) the management of evidence, (2) the existence of an officer who has the authority, (3) the place for storing evidence based on its type and characteristics, (4) the principles of admissibility evidence, and (4) the documentation in the register book and stored in the evidence room. This regulation is oriented toward physical evidence. The distinctive characteristics of digital evidence, it is a challenge to implement these principles in digital evidence handling. Therefore, some researchers have attempted to provide solutions to the digital evidence handling such as earlier solution from (Turner, 2006, 2008) (Schatz & Clark, 2006), (Lim & Lee, 2012), (Souza, 2013) until the latest solution from (Bonomi, Casini, & Ciccotelli, 2018). However, the researcher's solution has not yet met the need for a complete solution to the expected overall mechanism of digital evidence handling.

The centralized evidence is a basic concept that becomes the reference for the implementation of the five principles. This is in line with the recommendation given by the Joint Technology Committee (2016) for the improvement of management and control over digital evidence. The recommendation states that for the purpose of management and control over digital evidence, the mechanism of centralization of evidence in the storage is one of the keys. On the physical evidence, after the crime scene is completed, then the evidence will be entered into the bag of evidence and stored in the cabinet/ rack/ storage room of evidence. The physical evidence will be well recorded with a chain of custody. The evidence of a case should be stored in one place, namely the evidence room. If there is a need for borrowing and use of evidence for any purpose, it must be through a particular procedure with the supervision of the authorized person. In this case, the mechanism of centralization of evidence storage in an evidence room becomes one of the main concepts that facilitate the control mechanism of the evidence. With this centralization, control of the evidence will be easy to do so that the authenticity and integrity of the evidence can be maintained well.

However, it is difficult to apply those principles in a digital evidence scheme. A digital evidence bag, storage that serves as a digital evidence-storing cabinet, a mechanism for recording and documentation of digital evidence, and access mechanism for digital evidence cabinet, a secure environment in the process of handling evidence is an ideal set of requirements for realizing the digital evidence handling. Fulfillment of all these requirements becomes one of the challenges of the researchers to make it implemented. Some researchers have attempted to provide solutions to the handling of digital evidence such as from ((Turner, 2006, 2008) and (Souza, 2013), but only in the context of digital evidence storage. The researcher's solution has not yet met the need for a solution to the expected overall mechanism of digital evidence handling. Creating a new regulation that meets the needs of digital evidence handling is a good solution, but this solution needs political will and takes a long time, also needs to be supported by relevant technical studies. Another way is to keep applying the old regulation but must be supported with relevant technical implementation. With such support, the meaning and understanding contained in the old regulation can be adapted to the technical solution provided. This proposed solution is one of the research problems to be discussed in this paper, which is how to provide technical support for the implementation of existing regulations.

LITERATURE REVIEW

Physical Evidence Handling

For the scope of physical evidence, there are many solutions offered for the handling of evidence. Among them is a one-stop solution for infrastructure that includes mechanisms of collecting evidence at the crime of the scene, storage, recording, interaction and security of its room by utilizing the infrastructure and RFID technology of the EPC (Electronic Product Code) (Chen & Huang, 2013). While for digital evidence, one of the research focuses is on the need storage solutions for digital evidence, such as how appropriate network architecture to support the room of digital evidence. In this case (Davis, Manes, & Shenoi, 2015) has proposed the concept of DESL (Digital Evidence Storage Locker), a merging architecture of NAS (Network Access Storage) and SAN (Storage Area Network) designed to be implemented in the Oklahoma State Bureau of Investigation (OSBI) The United States. From the aspect of network architecture, the author has also discussed the potential used of VPN technology to support secure communication for access to digital evidence (Prayudi & Ashari, 2015). In this case, the use of VPN technology, whether its SSL or IPSec, can meet some of the criteria for secure communication for site-to-site or remote access to support mobility of investigators.

The increase in cybercrime indirectly has an impact on the increasing volume of digital evidence handled by investigators/examiners and the increasing of the complexity of management and documentation (Gayed, Lounis, & Bari, 2012). This is in line with the report by Beckett (2013), which states that the increasing number of criminal cases has resulted in the emergence of problems in terms of control and maintenance of evidence. The common constraints faced in handling evidence are in the absence of procedures and protocols on how to handle and transfer evidence between divisions as well as the lack of integrated information system support to carry out evidence management. Although the focus is on the case of physical evidence, the statement put forward by Beckett (2013) also applies to cases involving digital evidence.

Digital Evidence Handling

The handling of digital evidence has been the concern of many digital forensics' researchers. In general, there are two approaches, those based on the information container and the forensics data format. The solutions through an information container approach include XML knowledge representation as well as Digital Evidence Bags (DEB) from (Turner, 2006, 2008), Sealed Digital Evidence Bags from (Schatz & Clark, 2006), then XeBag by (Lim & Lee, 2012). Another solution based on XML is as provided by (Alink, 2005; Alink, Bhoedjang, Boncz, & de Vries, 2006) in the form of XML Information Retrieval Approach to Digital Forensics (XIRAF), which is a solution to automatically perform feature extraction of imaging files stored in a repository and then use an XML approach for the purposes of searching for digital evidence that relevant to the case. Meanwhile, a forensic data format approach as well AFF (Advanced Forensics File Format) from (Garfinkel, 2010; Garfinkel, Malan, Dubec, Stevens, & Pham, 2006). Both approaches will store some important information about digital evidence directly on the digital evidence file itself. Either through metadata representation in XML or space allocation in file format.

Especially for the approach with the forensics data format, there are obstacles with the increasing number of tools available to perform the acquisition process and the demands of dynamic updates of the data file. This happened with the dd extensions generated from dd imaging tools on Linux and several other extensions that are used as a standard in digital evidence, such as EO1 and ExO1 from Encase, AFF / AFF4, LEF (logical evidence file), SMART (Vandepen, 2014). The use of each extension is strongly influenced by the tools used, as well as the type of digital evidence generated from the imaging process. Another constraint to be faced is the interoperability of data formats among digital forensic tools, and this is what underlies (Casey, Back, & Barnum, 2015) to build a new design of XML-based schema named CybOX (Cyber Observable eXpression).

The Digital Evidence Characteristic

According to Matthew Braid in (Richter & Kuntze, 2010), each evidence can be used and supports legal processes if it meets five criteria, that is: admissible, authentic, complete, reliable, and believable. While (Schatz, 2007) states that there are two fundamental aspects for other criteria so that evidence can support legal processes, namely legal aspects with criteria: authentic, accurate, complete, and technical aspects with criteria: chain of evidence, transparent, explainable, accurate. Digital evidence has some uniqueness, namely: easy to duplicate and transmitted, vulnerable to being modified and eliminated, easily contaminated by new data, and time-sensitive. Digital evidence can also be cross-country and jurisdictional. That is why, according to (Schatz, 2007), digital evidence is more difficult than physical evidence handling. Unlike physical evidence, digital evidence will depend on the interpretation of the content. The integrity of the evidence and the ability of the expert in interpreting it will affect the selection of any digital documents as evidence.

Another critical issue is how to maintain the authenticity and integrity of digital evidence. Authenticity, according to (Cohen, 2013) is the ability to maintain initial identity when digital evidence is first obtained and maintains its integrity at every stage of the digital forensics process. While integrity, according to Vanstode (Cosic & Baca, 2010), is a property where digital data is not changed by parties who do not have the authority to make changes. Changes and contacts to digital evidence are only done by those who have authorization. Authenticity and integrity of digital evidence will guarantee that exploration, analysis, and information presented are complete and unchanged from the time it was first discovered until finally used in the court process.

The Digital Evidence Bags

The digital evidence handling through the concept of an analogy of bags has been proposed by Turner with the concept of Digital Evidence Bags (Turner, 2005b). In this case, Turner attempted to apply the Bag concept to the bag of evidence, the Tag for the labeling of evidence and the Seals to the bundle of security of the bag of evidence. The Digital Evidence Bags (DEB) concept is an evidence container approach as an alternative to the existing digital evidence physical formats available at that time, as well as the dd format of Linux and AFF from Garfinkel (2010). The DEB's Turner approach, in addition to providing solutions for information containers, also offers a solution for recording information of chain of custody. The method is much appreciated for providing solutions to the problems faced by digital forensics practitioners, which is how to apply the same procedure in digital evidence handling as procedures in physical evidence.

Therefore, a number of researchers support the concept of Digital Evidence Bags form Turner as well as Roussev (2006) on file systems that can support the implementation of DEB, Schatz (2007) about DEB development through the Sealed DEB concept, then support the implementation of DEB in Banking environment especially to handle cloning magnetic swipe card (Masters & Turner, 2007). Meanwhile, while not referring to the DEB concept of Turner, (Dahiya & Sangwan, 2014) are trying to address some digital evidence handling issues and then provide their conceptual solutions in the form of some requirements that should be available in the handling of digital evidence. In this case, according to (Dahiya & Sangwan, 2014), one of the basic requirements for handling digital evidence is the need for systems that have the ability to record the information and control the access privileges of digital evidence. Through the understanding of the cabinet, this paper proposed a Digital Evidence Cabinet Framework for digital evidence handling. This solution contains basic concepts that meet the physical analogy for the digital evidence bag, the rack, the cabinet, and the room. This concept is expected to be a solution to implement the principles of digital evidence following the law and regulations, as written in Perkap 10/2010 and 8/2014.

SETTING THE STAGE

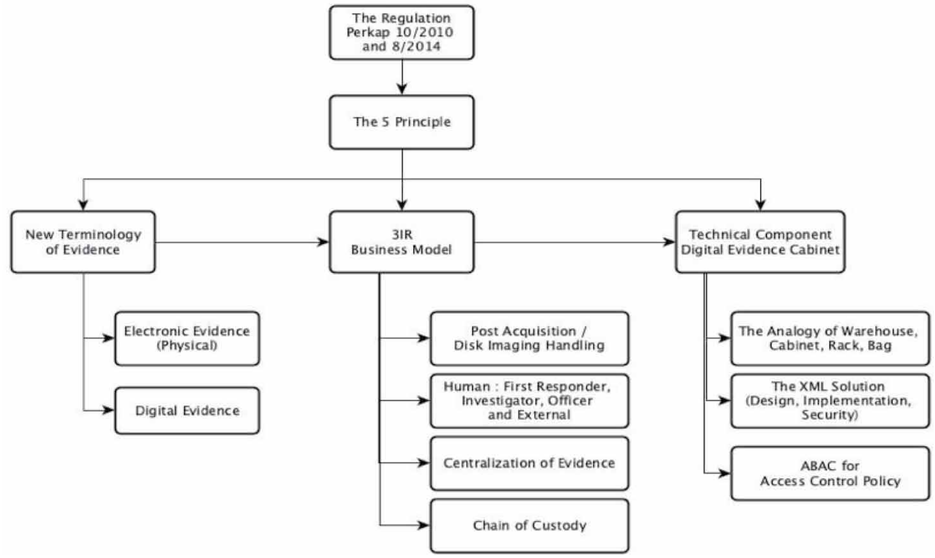
To provide a solution to technical support in implementing Perkap 10/2010 and 8/2014 for the scope of digital evidence, the general solution given is as in Figure 2.

The Terminology of Digital Evidence

The concept of Digital Evidence Cabinet must be supported by a clear terminology between electronic evidence in the form of physical and digital evidence in the form of binary files. In some early literature, as proposed by (Richter & Kuntze, 2010), digital evidence is any valuable information that is stored or transmitted in digital form. Meanwhile, according to (Turner, 2005b), digital evidence is information stored or transmitted in the binary form that can be used in law enforcement and court processes. Therefore, with the increasing complexity of cybercrime problems, according to (Prayudi et al., 2018), it must begin to distinguish between the meaning of electronic evidence and digital evidence.

In this case, two terms are almost identical but have different meanings, between electronic evidence and digital evidence. Electronic evidence is physical, visually identifiable, and can be described physically, e.g., computer, smartphone, camera, hard drive, etc. Electronic evidence is a digital device and selected by first responder officers as evidence because it contains some important information, both non-digital and digital. While digital evidence is evidence in the form of binary files, both are resulting from the disk acquisition and imaging process of electronic evidence or files containing digital information relevant to the investigative activity. So, the future of cybercrime investigation activities will always be faced with two forms of evidence, that is electronic evidence and digital evidence. Electronic evidence will be stored in the evidence room, while digital evidence will be stored in evidence storage.

Figure 2. The methodology for framework development


The Regulation Perkap 10/2010 and 8/2014
The 5 Principle
New Terminology of Evidence
3IR Business Model
Technical Component Digital Evidence Cabinet
Electronic Evidence (Physical)
Digital Evidence
Post Acquisition / Disk Imaging Handling
Human : First Responder, Investigator, Officer and External
Centralization of Evidence
Chain of Custody
The Analogy of Warehouse, Cabinet, Rack, Bag
The XML Solution (Design, Implementation, Security)
ABAC for Access Control Policy

In the real case, electronic and digital evidence is a unified piece of evidence from the crime scene that complements each other and support the investigative process. Electronic and digital evidence will be complementary in an investigative process (Carrier & Spafford, 2003). Likewise, during the court process, between physical and digital evidence is to be a unity of evidence that will be the primary consideration of the judge in believing the truth of the evidence presented by law enforcement against the fault of a defendant.

The Process Business of Digital Evidence Handling

The need to implement the same concept in terms of evidence handling between physical and digital is the main background of the existence of a digital evidence cabinet. The first step is to study the business model that will be the basis for implementing the concept. In this case, the author has developed a business model known as the 3IR Multiview Business Mode (Prayudi et al., 2018). The 3IR business model represents the role of three major components of digital forensics activity; Human, Digital Evidence, and Process at every important stage of investigative activity. Within the 3IR business model, the main stages of the investigation are divided into the Initiative, Investigative, Interactive, and Report. Through the 3IR business model, it can be seen how the flow of electronic and digital evidence handling, also the storage concept of digital evidence as one of the important mechanisms in digital evidence handling. The multiview business model is a detail of the interaction mechanism that occurs as an implementation of the explanation of the difference between electronic evidence and digital evidence. The concept of multiple business models is also explained about the need for storage of physical evidence in the evidence room and digital evidence through evidence storage.

The Basics Concept of Digital Evidence Cabinet

The approach to implementing digital evidence storage by the physical analogy of a cabinet is through a post-acquisition and disk imaging scheme, as discussed earlier by the authors (Prayudi, Ashari, & Priyambodo, 2014; Prayudi et al., 2018). Some of the earlier models of digital evidence solutions by analogy with the handling of physical evidence were Digital Evidence Bags (DEB) of (Turner, 2005b) and Evidence Container submitted by (Souza, 2013). Both of these early models were used as the basis for developing the concept of Evidence Cabinet in a previous study as in (Prayudi et al., 2014).

The basic idea derived from Turner's Digital Evidence Bags concept is how the concept of a bag can be applied to the purpose of storing digital evidence through an XML implementation. While the basic idea taken from Souza's Evidence Container is how to split metadata into a metadata repository to facilitate the management of information that will support the needs of the chain of findings. The output from this research is a design, model, and system that any digital evidence can be inserted into the system and structured into components of bags, racks, and cabinet. This output will be the basic framework of Digital Evidence Cabinet solution.

In this study, a digital cabinet is an imagination solution to apply the concept of bags, racks, and cabinet to digital evidence. So, the question in this research is, from the basic concept of DEB then how to modify and apply the concept of tag, index and bag files built with XML base can be developed to get the concept of bags, racks, and cabinet as a solution for Digital Evidence Cabinet. To provide solutions to the problem of digital evidence cabinet, then given some basic assumptions as follows:

- Warehouse is a room space containing several cabinets;
- Evidence cabinet is a storage unit containing racks, bags and units;
- Evidence rack, contains several evidence bags;
- Evidence bags a bag that can contain multiple evidence units;
- Evidence unit containing direct digital evidence to be managed in digital evidence cabinet system.

The components of bags, racks, and digital evidence cabinet are imaginative solutions based on XML tags that will process each digital evidence file so that it is structured of the above components.

The XML Design of Digital Evidence Cabinet

An XML approach is used to support the evidence room concept through Digital Evidence Cabinet. This approach has also been applied by Turner in DEB (Turner, 2005b) and Souza for Evidence Container (Souza, 2013). The XML design must meet three purposes; the first is for the concept of the cabinet itself; the second is the concept of digital evidence and the third is the concept of chain of custody. The cabinet concept of XML is to translate the analogy of warehouses, cabinet, rack, and bags of evidence, the digital evidence of XML is to recognize the object of digital evidence file, while the XML concept of chain of custody is required for recording and documentation of evidence. One of the basic needs of the centralization of the evidence is to facilitate the control mechanism against evidence through the chain of custody. Figure 3 is an illustration of the design of the main structure of the XML.

The structure of XML elements of digital evidence cabinet will consist of three parts, namely: cabinet elements, rack, and bag. Table 1 shows the XML structure for evidence cabinet.

Figure 3. The XML design of evidence room

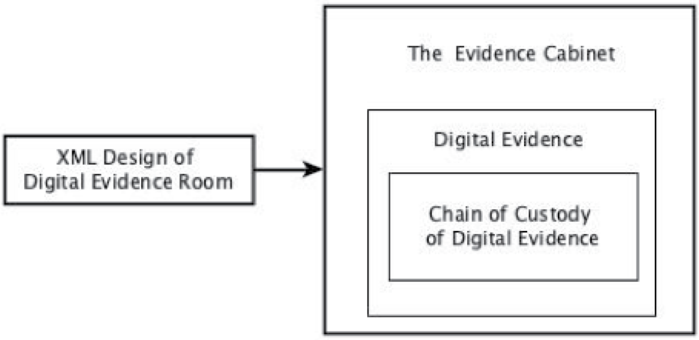


Table 1. XML structure for evidence cabinet

<cabinet cabinet_name=”Name of Cabinet”>	→ Cabinet Name
<rack rack_name=”Name of Rack”>	→ Rack Name
<bag bag_name=”Name of Bag”>	→ Bag Name
<digital_evidence name =”Name of Digital Evidence”> ….. …..	→ Elements where digital evidence information is stored
</bag>	
</rack>	
</cabinet>	

Furthermore, the bag tag will contain information from the evidence unit consisting of the primary information about the digital evidence taken from the file metadata as well as additional information for the chain of custody. Both of this information is stored in an XML structure called *digital_evidence*. The *digital_evidence* element resides on a specific rack and cabinet element. The primary information of digital evidence is any information available on file through its file metadata. The metadata that will be stored as the primary information is; name of digital evidence (file_name), size of digital evidence (size), hashing of digital evidence file using SHA1 and MD5 (hash_key), location of digital evidence uploaded (file_source), cabinet position to store digital evidence (file_position) and date of digital evidence upload (date_uploaded) (see Table 2).

Table 2. Metadata stored as the primary information

<digital_evidence name=”Name of Evidence”>	→ The Highest Structure
<file_name/>	→ Name of Digital Evidence
<size/>	→ The Size of Digital Evidence
<hash_key type=”sha1”/>	→ Hashing of Digital Evidence
<hash_key type=”md5”/>	→ Hashing of Digital Evidence
<file_source/>	→ Location of Digital Evidence
<file_position/>	→ Location of Digital Evidence
<date_uploaded/>	→ The Date of Uploaded File
<digital_evidence>	

There is also other relevant information to record documentation about digital evidence, known as the chain of custody. There is some information that should exist in a chain of custody. The chain of custody will contain basic information about digital evidence and other information relating to interactions with digital evidence. For this purpose, the XML concept applied to documented digital evidence is to divide it into two separate types of XML structures, that is *digital_evidence* and *history*. The elements in the *digital_evidence* will not increase, but the value of each of these elements may change, while the *history* element can be increased if there is a change of data for the chain of custody. The use of the XML approach used will be generated output with a plain-text XML file. With this plain text characteristic, the security aspect becomes one of the most important parts in the XML design of the digital evidence cabinet and the chain of custody of digital evidence. For these purposes, the encryption is one of the techniques that can be implemented to support the security needs of XML plain text documents. To improve the security of the XML file structure that is plain text, then in the Digital Evidence Cabinet system, added the concept of encryption and decryption on XML file output. For this purpose, the RC4 algorithm is applied for encryption and decryption of the XML structure generated by the Digital Evidence Cabinet system.

The Validation Methods Basics

Each research has a distinctive characteristic of how the process of carrying out its research. This characteristic certainly has an impact on the validation model applied in the research (Egonsdotter & Öberg, 2002). The validation issues in the scope of digital forensics and digital evidence are interpreted as an effort to guarantee that all methods and processes that are applied for specific purposes can be accepted and relied upon Forensics Science Regulator (2016). Although the field of digital forensics and digital evidence is a multidisciplinary field, in the context of this research, the field of digital forensics and digital evidence is approached from a computer science perspective.

In this case, according to (Mohammed & Alsanussi, 2017) and (Elio et al., 2011), there are many discussions about the validation model for the field of computer science, one of them is the prototype model. The validation of this model is to show that the hypothesis made in research is feasible to implement. A prototype is an early model that is built to test a concept or to serve as a proof-of-concept and demonstration model for a new solution. In this research, validation is made by making a a list requirements, specifications, and implementation. Based on this requirement, the analysis was made to determine whether the hypothesis in this research had been fulfilled.

CASE DESCRIPTION

Based on the typology of cases handled by digital forensics laboratories on CDFS, the following case scenarios are made. It is assumed that First Responder does his job to crime scenes and upload the digital evidence he gets into the system. In this system, First Responder has the authority to make a cabinet, rack, and bag, then after finished, will be approved by the Officer. Table 3 shows the position of the digital evidence room on the digital evidence cabinet system as centralized storage of digital evidence.

Table 3. Data for the cases scenario

No.	Name of Cabinet	Name of Rack	Nama of Bag	Name of Digital Evidence
1.	cabinet_1	rack_1	bag_1	Evidence1_dd.001
			bag_2	Evidence2_e01.E01
2	cabinet_2	rack_1	bag_1	Evidence_video1.001
				Evidence_video2.E01
3.	cabinet_3	rack_1	bag_1	Evidence101.E01
		rack_2	bag_2	Evidence102.001

The appropriate context to provide an interpretation of the cabinet, rack, bag, and evidence unit is shown in Table 4.

The first responder will enter the data into the system; one of the captured images of data entry is as in Figure 4. There are three cabinet files in the warehouse folder: *cabinet_1, cabinet_2,* and *cabinet_3*. Within each cabinet folder there are two additional files: *cabinet_encrypt.xhtml* and

Table 4. The interpretation of cybercrime cases handling

Yogyakarta police area conducted an investigation of murder cases of Jhonny at two different crime scene locations; the first was in Sleman with digital evidence in the form of the acquisition of a computer hard drive and the second location in Bantul with digital evidence was the result of the acquisition of USB. The structure of the cabinet, as described above, can be interpreted as the centralized storage of the following digital evidence:

Warehouse	**Cabinet**	**Rack**	**Bag**	**Evidence Unit**
Yogyakarta	Murder	Jhonny	Sleman	Evidence1_dd.001
			Bantul	Evidence2_e01.E01

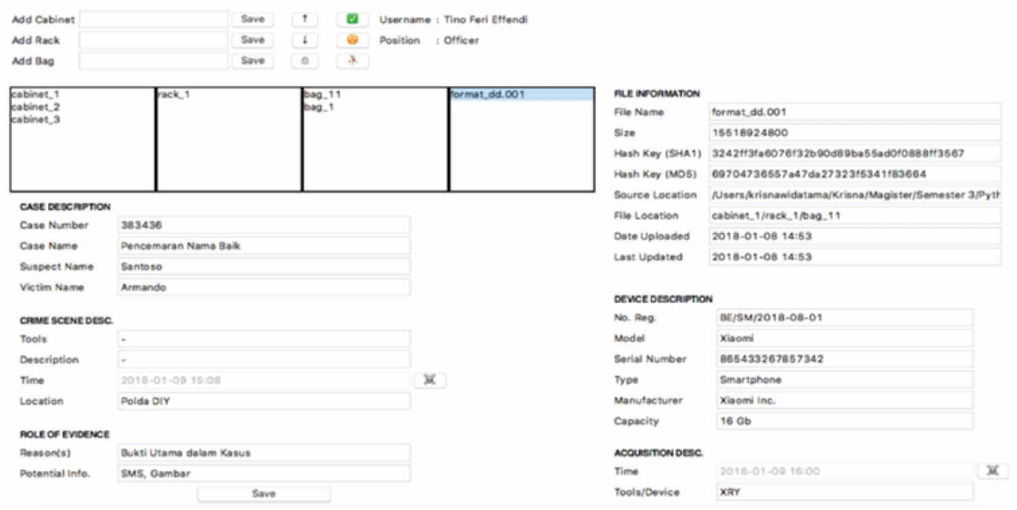
Yogyakarta police area investigated two fraud cases at two different crime scene locations; the first case was Herman's case with a crime scene in Sleman with digital evidence in the form of the acquisition of a computer hard drive and the second case was Ani's case with a crime scene location in Bantul with digital evidence is the result of the acquisition from USB. The structure of the Cabinet, as described above, can be interpreted as the centralized storage of the following digital evidence:

Warehouse	**Cabinet**	**Rack**	**Bag**	**Evidence Unit**
Yogyakarta	Fraud	Herman	Sleman	Evidence101.E01
		Ani	Bantul	Evidence102.001

Yogyakarta police area is investigating corruption and fraud cases. The corruption case is the Rommi case with a crime scene in Berbah with digital evidence in the form of the acquisition of a computer and mobile hard drive, and the second case is the Sundiro fraud case with a crime scene location in Janti with digital evidence is the acquisition of USB.
The structure of the Cabinet, as described above, can be interpreted as the centralized storage of the following digital evidence:

Warehouse	**Cabinet**	**Rack**	**Bag**	**Evidence Unit**
Yogyakarta	Corruption	Rommi	Berbah	Evidence201.E01
			Prambanan	Evidence202.E01
	Fraud	Sundiro	Janti	Evidence302.E01

Figure 4. The captured of digital evidence cabinet system



Username : Tino Feri Effendi
Position : Officer

cabinet_1
cabinet_2
cabinet_3

rack_1

bag_11
bag_1

format_dd.001

CASE DESCRIPTION

Case Number	383436
Case Name	Pencemaran Nama Baik
Suspect Name	Santoso
Victim Name	Armando

CRIME SCENE DESC.

Tools	-
Description	-
Time	2018-01-09 15:08
Location	Polda DIY

ROLE OF EVIDENCE

Reason(s)	Bukti Utama dalam Kasus
Potential Info.	SMS, Gambar

FILE INFORMATION

File Name	format_dd.001
Size	15518924800
Hash Key (SHA1)	3242ff3fa6076f32b90d89ba55ad0f0888ff3567
Hash Key (MD5)	69704736557a47da27323f5341f83664
Source Location	/Users/krisnawidatama/Krisna/Magister/Semester 3/Pyth
File Location	cabinet_1/rack_1/bag_11
Date Uploaded	2018-01-08 14:53
Last Updated	2018-01-08 14:53

DEVICE DESCRIPTION

No. Reg.	BE/SM/2018-08-01
Model	Xiaomi
Serial Number	865433267857342
Type	Smartphone
Manufacturer	Xiaomi Inc.
Capacity	16 Gb

ACQUISITION DESC.

Time	2018-01-09 16:00
Tools/Device	XRY

history_encrypt.xhtml. These two files are formed automatically when a new cabinet is formed, and there is a folder that is also formed when a new cabinet is created, namely the *digitalEvidence* that contains digital evidence uploaded on a particular cabinet.

Current Challenges

The implementation of the Digital Evidence Cabinet is a prototype system that contains all aspects of the framework. Validation of the prototype with an explanation of the results can be seen in Table 5. Based on data in Table 5, it can be seen that the implementation of Digital Evidence Cabinets meets the requirements needed to support the implementation of Perkap No 10/2010 and 8/2014. A prototype system can fulfill some specifications prepared at the beginning. Although it still has some disadvantages, especially concerning storage flexibility and documentation of metadata, however, this framework has fulfilled the necessary requirements to support the implementation of the principles of digital evidence handling as contained in the regulation. The Digital Evidence Cabinet concept can be improved so that in the future, it will be used as a procedure and protocol in managing digital evidence handling in Indonesia. The concept of Digital Evidence Cabinet can also be adopted by more general legal jurisdiction; one of the steps is to take a broader regulatory approach by taking a more global reference. These steps will provide the potential for the resulting framework to be adopted by the legal system in the broader area.

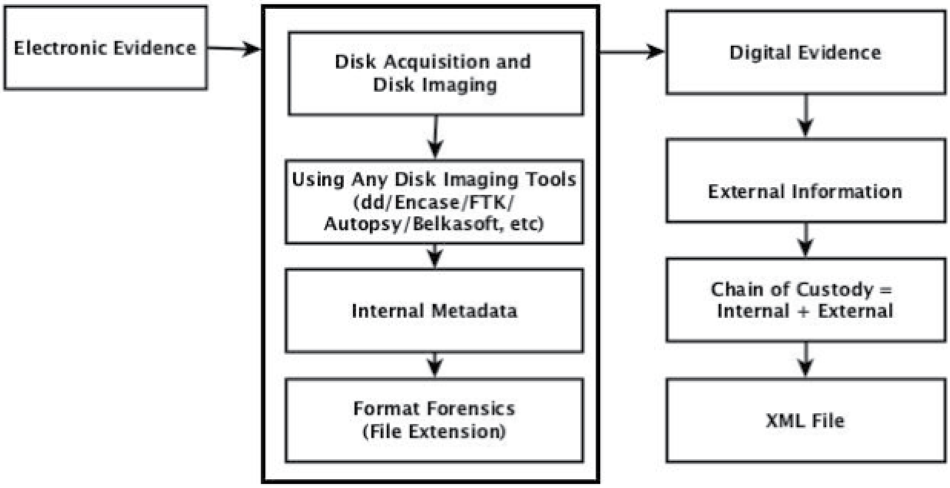
Table 5. The validation of prototype

Project Scope: Framework to Support Digital Evidence Handling in Indonesia		
Specifications	**Requirement**	**Implementation**
Acquisition Process	No interoperability problem for an output of the acquisition process	Post-Acquisition Handling by First Responder Officer
Centralized Concept	The physical approach	Storing all digital evidence in a storage mechanism files in a folder.
	The logical approach	The XML structured for evidence unit, evidence bags, evidence rack, evidence cabinet, and warehouse.
Handling Cases	Evidence room can be grouped into types of criminal cases (cabinet), different types of crimes (racks), different location of crime scenes (bags) and list of digital evidence (evidence units).	Simulation of different evidence and case into cabinets, racks, bags, and evidence units.
Regulatory Aspect	Fulfillment the five principles contained in the regulation of Perkap 10/2010 and 8/2014, namely: The management functions, The existence of an official, A special place for storing evidence, The admissibility of evidence and The documentation.	Checking the suitability and fulfillment of the main aspects of regulation.

Post-Acquisition Handling

The handling of digital evidence is strongly influenced by how the concept of content storage from its digital evidence files. One of the basic problems is how to provide storage of digital evidence content solutions while keeping in mind some important information directly related to digital evidence. The number of formats as a solution to digital evidence containers, according to (Casey et al., 2015), is an ad hoc and partial solution. The interoperability problem between formats is the next problem that arises. Based on the studies that have been done, the general description of the process of storing digital evidence information is done simultaneously with the process of acquisition and disk imaging of electronic evidence. The existence of some problems encountered by such schemes encourages alternative solutions by using different approaches in dealing with digital evidence. In this research, the different approach applied is through the mechanism of handling of digital evidence after the acquisition process and disk imaging is done. Figure 5 provides illustrations of the concept of digital evidence handling that is applied in this research.

Figure 5. The new viewpoint for after acquisition digital evidence handling

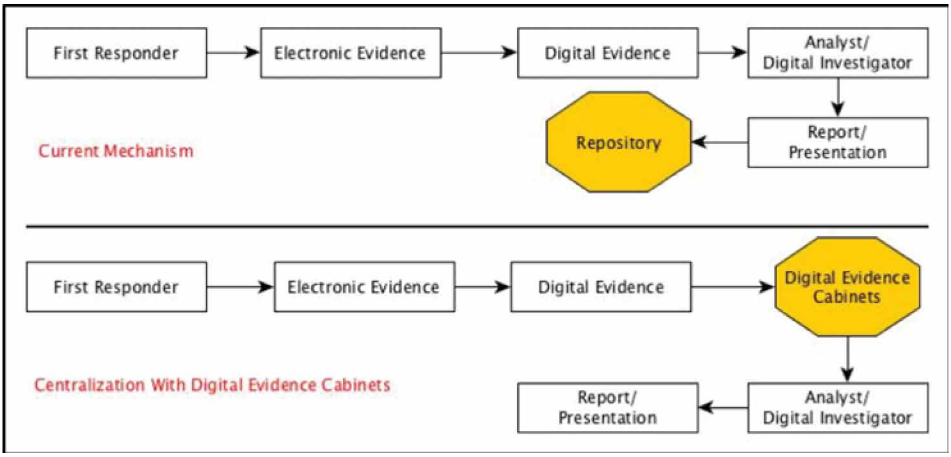

Electronic Evidence
Disk Acquisition and Disk Imaging
Using Any Disk Imaging Tools (dd/Encase/FTK/ Autopsy/Belkasoft, etc)
Internal Metadata
Format Forensics (File Extension)
Digital Evidence
External Information
Chain of Custody = Internal + External
XML File

Through this new approach, the acquisition process will be fully submitted to First Responder Officers, including the selection of tools for its acquisition and the format of the data it chooses. After obtaining digital evidence, then the next process is done for storage and recording the chain of custody. Through this new approach, there will be no interoperability problem because there is no direct interaction between tools and digital evidence. The above method also provides other mechanisms for storing information related to digital evidence. The previous solution from DEB's (Turner, 2005b, 2008), use the information container approach. Through this approach, all information related to digital evidence will be attached directly to the digital evidence file, while the new method proposed by Digital Evidence Cabinet uses the concept of information storage that is separate from its digital evidence. This new approach in the context of applying the rules of digital evidence handling will be more controllable than the previous DEB approach.

The Centralization Concept of Digital Evidence

The control of the interaction and the use of evidence are important elements of the evidence handling. The mechanism for control of evidence will be easily implemented if supported by centralized evidence storage. For this purpose, the concept of centralization in Digital Evidence Cabinet is applied in two approaches, physical and logical. The physical approach leads to storing all digital evidence files in a storage mechanism in such a folder. While logically, digital evidence will be stored in the form of a structure of evidence unit, evidence bags, evidence rack, evidence cabinet, and warehouse. This structure provides a solution to the analogy of evidence storage into an evidence room. Through this centralization, the application of the chain of custody becomes easy to implement. The pseudo metadata concept for the chain of custody of digital evidence through the static and dynamic metadata, as proposed by the authors in (Prayudi et al., 2018), can be integrated as part of this digital evidence centralization system. Through the Digital Evidence Cabinet system, then all the digital evidence as the output of the acquisition process will be stored into the system, and this will make it easier to control the interaction and its use. Figure 6 shows an illustration of the use of Digital Evidence Cabinet as a centralized concept of digital evidence.

Figure 6. The illustration of centralized concept of digital evidence



The centralized approach of digital evidence handling was also discussed by (Bonomi et al., 2018) through the concept of B-CoC (Blockchain-based Chain of Custody). In this concept, centralization is applied only to the storage of digital evidence. The control of the use of digital evidence shared by users in one network is done using the concept of the blockchain. The B-CoC concept, in contrast to the Digital Evidence Cabinet, where centralization applies to the storage of digital evidence along with documentation and control of its use. The B-CoC concept is very relevant for the application of mobile investigators where investigators can carry out an analysis mechanism wherever and whenever they are working. While the concept of the Digital Evidence Cabinet is relatively limited for application to a particular scope of investigators, this concept is under the initial assumption of a digital evidence cabinets solution where this system is an analogy of evidence storage in individual rooms with limited accessibility.

The Regulatory Aspect

The rules concerning the handling of digital evidence, such as ACPO, NIJ, or ISO 27037, do not describe the mechanism of storing digital evidence. The terminology that is still used is the definition of digital evidence in the context of digital devices (physically). The report of the (Joint Technology Committee, 2016) corroborates the statement. In that report mentioned that one of the critical issues currently faced by law enforcement is regarding storing digital evidence. In practice at all law enforcement levels, the mechanism of storing digital evidence is still in the form of physical or digital device/ electronic handling. The understanding of the terminology of digital evidence among law enforcement should be improved to adapt and align with the development of science and technology. The solutions provided through the concept of Digital Evidence Cabinets can give insight to law enforcement on how to get mechanisms for digital evidence handling as well as physical evidence.

For the scope of the territory of the Republic of Indonesia, the documents of Perkap 10/2010 and 8/2014 from National Police Chief of Indonesia (Kepolisian Negara RI, 2010) concerning

Procedures of the Management of Evidence, is a formal guide among law enforcement officers regarding evidence handling. The Digital Evidence Cabinets concept is designed to facilitate the infrastructure requirements that will support the implementation of that regulation, especially for the context of digital evidence handling. The important thing in that regulation is the procedure of evidence management. This procedure includes the mechanism of how to receive and store, how to secure and maintain and how to use and destroy it. All these procedures will be applicable by carrying out the initial mechanism of centralizing the storage of digital evidence in an evidence room. Table 6 shows the evaluation of the main functions of the Perkap regulations contained in DEC.

Table 6. The fulfillment of regulatory aspect

No.	Point	The DEC Framework
1	The management functions	The Framework is based on the 3IR. Process Model where there is a management function in the form of an obligation to follow procedures for handling digital evidence.
2	The existence of an official	There is a function Officer in the system for the purpose of verification and authorization of digital evidence.
3	A special place for storing evidence	Physical storage and logical evidence room with the analysis of warehouse, cabinet, rack, bags and evidence units are implemented with XML structures.
4	The admissibility of evidence	Security aspect of XML and MD5 as a hash function to ensure the security and integrity of digital evidence stored in the system.
5	The documentation	The Chain of Custody of Digital Evidence

According to Table 3, Table 4, and Table 6, the result shows that the prototype developed in this research has supported the implementation of the concept of digital evidence handling. The implementation shows that the interpretation of the bags, rack, cabinet, and warehouses in Digital Evidence Cabinet is relevant to case management in the form of type of crime (cabinet), list of crime/ case (racks), list of crime scenes (bags) and list of evidence in evidence unit. The case management will place all the digital evidence entered into the system into a single folder as well as the cabinet structure into one XML file. This implementation is in line with the initial need to provide digital evidence handling solutions that comply with the regulation.

Based on validation on the prototype, the Digital Evidence Cabinet framework has fulfilled the basic requirement and specifications of digital evidence handling as well as physical evidence. The validation result shown that the framework is feasible to be implemented as a technical aspect of regulations for digital evidence handling in Indonesia. In the context of the legal system in Indonesia, the theoretical concept and their implementation discussed in this paper provide technical support for regulatory improvements in the handling of digital evidence among law enforcement and practitioners. This concept is part of the support for the improvement of some existing regulations to meet the needs of digital evidence handling.

The results of the validation using a number of trial data, the following results are obtained:

- The application of Post-Acquisition Handling to digital evidence for the DEC system shows that there is no interoperability problem for data entry from the acquisition process and disk imaging when inserted into the system;
- The prototype system is capable of storing all digital evidence uploaded on internal storage media with a file storage mechanism in the form of structured tag files: Warehouse / cabinet / rack / bag;

- The prototype system has successfully implemented a relevant XML structure that describes the components of a cabinet in the form of evidence identifier identities, evidence units, evidence bags, evidence racks, and evidence cabinets.

The Comparison of Digital Evidence Handling

Turner has proposed the handling of digital evidence through the concept of analogous digital evidence bags through the concept of DEB (Digital Evidence Bags) (Turner, 2005a, 2008). In this case, Turner tried to apply the concept of Bag for evidence bags, tags for labeling evidence, and seals for binding security of bags of evidence. The concept of Digital Evidence Bags is an approach to evidence container as an alternative to the physical format of digital evidence that was available at that time, as well as the dd format from Linux and AFF (Garfinkel, 2010). The DEB approach from Turner, in addition to providing solutions for information containers, also provides a solution for recording information on the chain of custody. The DEB has much appreciated from the community because it provides a solution to the problems faced by digital forensic actors, which is how to implement the same procedures in handling digital evidence as procedures for handling physical evidence. A number of researchers subsequently supported the concept of Digital Evidence Bags Turner as well as (Roussev, 2006) on file systems that can support the implementation of DEB, (Schatz, 2007)) on DEB development through the Sealed DEB concept, the implementation of DEB in the Banking environment specifically to deal with cloning magnetic swipe card (Masters & Turner, 2007).

However, some researchers provide a review of the shortcomings of the DEB concept that Turner has presented. The feedback from (Richard, Roussev, & Marziale, 2007) provides the shortcomings of the DEB concept and provides a solution in a concept known as the Forensic Discovery Auditing Module (FDAM). Meanwhile, (Richard et al., 2007) gives feedback that there is no trusted log in DEB that will record all operations that have been carried out on digital evidence. A trusted log is needed to find out how far the tools work following the initial concept promised. FDAM was developed as an additional tool from aspects of the operating system module that will provide a “clean room” to run DEB applications. Meanwhile, although it does not refer to the DEB concept of Turner, (Dahiya & Sangwan, 2014) try to discuss some problems of digital evidence and provide conceptual solutions in the form of some requirements that should be present in digital evidence handling. According to (Dahiya & Sangwan, 2014), one of the basic elements in terms of digital evidence handling is the need for a system that has the capability to recording digital evidence and the systems that can control the access of privileges to digital evidence.

Another digital evidence handling issue is also expressed by (Baar, Beek, & Eijk, 2015) through Hansken’s solution as a tool for Digital Forensics as a Service. Hansken is a successor of XIRAF (XML Information Retrieval Approach to Digital Forensics) applications that have been developed previously within the scope of limited research projects. The limited number of experts for handling digital evidence, the efficiency in providing resources to run a series of evidence analysis activities, the integration of the investigative process has led to a solution to the importance of centralized digital forensics activities. This mechanism starts from the acquisition process of electronic evidence, the process of storing digital evidence to the analysis process under the needs of each investigator. Hansken is designed to be used as a standard platform for handling criminal cases by all investigators. In this case, the mechanism developed through Hansken is not only limited to the storage of digital evidence, but also to all processes associated with digital forensics or digital investigation.

The issue of digital evidence handling is also becoming one of the components in the concept of Digital Witness proposed by (Ana Nieto, Roman, & Lopez, 2016; Anna Nieto, Rios, & Lopez, 2017). The concept is an attempt to prepare the environment in such a way that the personal devices can be used actively for the process of acquiring, store, and transmit digital evidence to an authorized entity reliably and securely. It is different from centralization in Digital Evidence Cabinets. The concept of centralization in Digital Evidence Cabinets is more limited in scope than Hansken’s (Baar et al.,

2015) or Digital Witness (Ana Nieto et al., 2016; Anna Nieto et al., 2017). The centralized storage on Digital Evidence Cabinets is a limited focus to centralizing the storage of digital evidence using the initial assumptions for digital evidence resulting from the acquisition and imaging process. While the centralization adopted in Hansken's or Digital Witness is a larger and more complex concept of centralization to support the broader platform of digital forensics solutions.

THE BENEFIT OF SOLUTION

The meaning of evidence room from Digital Evidence Cabinets can be explained from the concept of warehouse, cabinet, rack, bag, and evidence unit. Any digital evidence entered into the system will be able to see its proper placement structure in a physical space. The digital evidence will be placed in the warehouse, cabinet, rack, bag, and evidence unit structure. The concept of warehouses, cabinet, rack, bags, and evidence units as the main elements of the Digital Evidence Cabinet is relevant to the handling of cases in the real world. The evidence room can be grouped into types of criminal cases (cabinet), different types of crimes (racks), different locations of crime scenes (bags), and a list of digital evidence (evidence units). Through this interpretation, a warehouse will contain all the digital evidence of various types of crime, various types of cases, and different locations of a crime scene.

The Digital Evidence Cabinet that was discussed in this paper has fulfilled the initial objective of the research: to obtain the structure of storage as a logical solution for the evidence room and the centralization of digital evidence. However, the solution needs to be integrated with metadata management for the chain of custody and access control for digital evidence stored in the system. The integrated concept will provide digital evidence handling solutions as well as physical evidence. Through these solutions, the integrity of digital evidence can be enhanced because it is supported by a trusted system and access control to digital evidence that has been stored.

The solutions to the problem of handling digital evidence that has not followed the same mechanism as electronic evidence have been extensively studied in this paper. The solution applied through the analogy of a storage cabinet. The solution illustrates that the storage of digital evidence can be structured as well as physical evidence. Through this solution, the mechanism for digital evidence handling in CDFS digital forensics laboratories can be in line with some evidence handling regulations, for example, regulations contained in Perkap 10/2010 and 8/2014. This solution will be increased customer trust in the digital evidence examination process at the CDFS digital forensics laboratory.

CONCLUSION

Physical and digital evidence is a unit of evidence in the process of investigating cybercrime cases. The same regulations should support the handling of both types of evidence. Current rules such as The Procedure of Handling evidence by the Indonesian Police in the form of Perkap 10/2010 and 8/2014 are still referred to the handling of evidence in physical form, so the interpretation of these regulations for the context of digital evidence must also be well prepared. The Digital Evidence Cabinet framework has been extensively studied in this paper as technical support for implementing the regulations of digital evidence as well as physical evidence handling. Although the scope of implementation is only in the CDFS digital forensics laboratory forensics environment, the framework presented in this paper can also be applied to other digital forensics laboratories or legal practitioners and law enforcement agencies.

The solutions discussed in this paper can be further implemented on a broader scope. The steps for implementing it are redefining digital evidence that is more relevant for investigating cybercrime, applying a business model that supports the mechanism of storing physical and digital as well as XML design for the analogy of evidence cabinets. Based on these steps, the digital evidence cabinet framework has fulfilled the requirements and specifications expected as an interpretation of digital evidence handling that following the existing regulations. Thus, the prototype that has been developed is feasible to be applied to support better handling of digital evidence in Indonesia. This framework should be gradually adopted by law enforcement through the adjustment of some regulations to allow for compliance between regulatory and technical aspects for the handling of digital evidence.

For the continuation of the concept of Digital Evidence Cabinet as a solution to the framework for digital evidence handling, some further research can be done. The future research can be focused on integrating the concept of metadata management for the chain of custody to support the documentation of digital evidence and access control policy to support a trusted environment of the Digital Evidence Cabinet system. Both of these aspects will extend the requirements of digital evidence handling and provide a complete study to support the technical aspects of the existing regulatory interpretations.

ACKNOWLEDGMENT

The research was done with the support facilities of the Digital Forensics Laboratory CDFS UII and the Laboratory of Computer Network DIKE UGM.

REFERENCES

ACPO. (2012). ACPO Good Practice Guide for Digital Evidence. England. Retrieved from http://library.npia.police.uk/docs/acpo/digital-evidence-2012.pdf

Alink, W. (2005). *XIRAF: An XML-IR Approach to Digital Forensics. Faculty of Electrical Engineering, Mathematics, and Computer Science*. University of Twente Enschende, The Netherlands. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.7718&rep=rep1&type=pdf

Alink, W., Bhoedjang, R. A., Boncz, P. A., & de Vries, A. P. (2006). XIRAF - XML-based indexing and querying for digital forensics. *Digital Investigation*, *3*, 50–58. doi:10.1016/j.diin.2006.06.016

Ashcroft, J., Daniels, D. J., & Hart, S. V. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Baar, R. (2015). Digital Forensics as a Service: Game on. *Digital Investigation*, *15*, 20–38. doi:10.1016/j.diin.2015.07.004

Boddington, R., Hobbs, V., & Mann, G. (2008). Validating Digital Evidence for Legal Argument. In *Australian Digital Forensics Conference. Pert, Western Australia*. Perth, Western Australia: Edith Cowan University. Retrieved from http://ro.ecu.edu.au/adf/

Bonomi, S., Casini, M., & Ciccotelli, C. (2018). *B-CoC : A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics*. Retrieved from https://arxiv.org/pdf/1807.10359.pdf

BSN. (2014). *Teknologi Informasi - Teknik Keamanan-Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (ISO/IEC 27037:2012)*. Jakarta: Badan Standardisasi Nasional.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*(2), 1–20.

Casey, E., Back, G., & Barnum, S. (2015). Leveraging CybOX??? to standardize representation and exchange of digital forensic information. *Digital Investigation*, *12*(S1), S102–S110. doi:10.1016/j.diin.2015.01.014

Clearsky Cyber Security. (2018). *Cyber Intelligence Report 2017*. Retrieved from http://www.clearskysec.com/wp-content/uploads/2018/01/ClearSky_cyber_intelligence_report_2017.pdf

Cohen, F. (2013). *Digital Forensic Evidence Examination* (5th ed.). Livermore, CA: Fred Cohen & Associates.

Cosic, J., & Baca, M. (2010). (Im) Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. In *MIPRO, Proceedings of the 33rd International Convention International Conference* (hal. 1226–1230). Academic Press. Retrieved from http://czb.foi.hr/upload/datoteke/10_400.pdf

Dahiya, Y., & Sangwan, S. (2014). Developing and Enhancing the Security of Digital Evidence Bag. *International Journal of Research Studies in Computer Science and Engineering*, *1*(2), 14–25. Retrieved from http://www.arcjournals.org/pdfs/ijrscse/v1-i2/3.pdf

De Souza, P. (2013). *A Chain of Findings for Digital Investigations*. University of Pretoria. Retrieved from http://repository.up.ac.za/bitstream/handle/2263/40842/DeSouza_Chain_2013.pdf?sequence=1

Egonsdotter, G., & Öberg, L. (2002). *AMSIDO: Validation and Data Collection*. Palmius. Retrieved from http://www.palmius.com/joel/lic/a2validation.pdf

Elio, R., Hoover, J., Nikolaidis, I., Salavatipour, M., Stewart, L., & Wong, K. (2011). About Computing Science Research Methodology.

Forensics Science Regulator. (2016). *Method validation in digital forensics*. Government of the UK. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/528123/FSR_Method_Validation_in_Digital_Forensics_FSR-G-218_Issue_1.pdf

Garfinkel, S. (2010). AFF and AFF4 : Where We Are, Where We are Going, and Why it Matters to You.

Garfinkel, S., Malan, D. J., Dubec, K.-A., Stevens, C. C., & Pham, C. (2006). Advanced Forensic Format : An Open, Extensible Format for Disk. In M. Olivier & S. Shenoi (Ed.), Advances in Digital Forensics II (pp. 17–31). Springer.

Joint Technology Committee. (2016). *Managing Digital Evidence in Courts* (Vol. 1).

Kepolisian Negara, R. I. (2010). *Perkap 10 2010 Tentang Tata Cara Pengelolaan Barang Bukti di Lingkungan Kepolisian Negara Republik Indonesia*. Jakarta. Retrieved from http://acarapidana.bphn.go.id/peraturan/Peraturan Kepolisian/PERKAP 10 TAHUN 2010.pdf

Lim, K. S., & Lee, C. (2012). Applying Forensic Approach to Live Investigation Using XeBag. In S.-S. Yeo, Y. Pan, Y. S. Lee, & H. B. Chang (Eds.), *Computer Science and its Applications (hal. 389–389)*. London: Springer Dordrecht. doi:10.1007/978-94-007-5699-1_38

Masters, G., & Turner, P. (2007). Forensic data recovery and examination of magnetic swipe card cloning devices. *Digital Investigation*, *4*(Suppl.), 16–22. doi:10.1016/j.diin.2007.06.018

Mohammed, M. A., & Alsanussi, R. A. (2017). Review of Methods Used in Computer Science Research. *Continuous Research Online Library*, *1*(1), 1–8. doi:10.28915/control.0025.1

Morgan, S. (2017). *2017 CyberVentures Cybercrime Report*. Cybersecurity Ventures. Retrieved from https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Nieto, A., Rios, R., & Lopez, J. (2017). Digital Witness and Privacy in IoT: Anonymous Witnessing Approach. In *Proceedings of the 16th IEEE International Conference On Turst, Security And Privacy In Computing And Communications (TrustCom 2017)* (pp. 642–649). IEEE Press. doi:10.1109/Trustcom/BigDataSE/ICESS.2017.295

Nieto, A., Roman, R., & Lopez, J. (2016). Digital Witness: Safeguarding Digital Evidence by Using Secure Architectures in Personal Devices. *IEEE Network*, *30*(6), 34–41. doi:10.1109/MNET.2016.1600087NM

Ponemon Institute and Accenture. (2017). *2017 Cost of Cyber Crime Study*. Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2014). Digital Evidence Cabinets : A Proposed Frameworks for Handling Digital Chain of Custody. *International Journal of Computers and Applications*, *109*(9), 30–36. Retrieved from http://research.ijcaonline.org/volume107/number9/pxc3900106.pdf. doi:10.5120/18781-0106

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. *International Journal of Computer Network and Information Security*, *7*(11), 1–8. doi:10.5815/ijcnis.2015.11.01

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2018). Multiview Business Model for Describing a Mechanism of Handling Physical and Digital Evidence in Digital Forensics. *Journal of Theoretical and Applied Information Technology*, *96*(2). Retrieved from http://www.jatit.org/volumes/Vol96No2/5Vol96No2.pdf

Richard, G. G. III, Roussev, V., & Marziale, L. (2007). Forensic Discovery Auditing of Digital Evidence Containers. *Digital Investigation*, *4*(2), 88–97. doi:10.1016/j.diin.2007.04.002

Richter, J., & Kuntze, N. (2010). Securing Digital Evidence. In *Proceedings of the Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering* (pp. 119–130). Academic Press. Retrieved from http://sit.sit.fraunhofer.de/smv/publications/download/EvidentialIntegrity.pdf

Roussev, V. (2006). File System Support For Digital Evidence Bags. In Advances in Digital Forensics II (Vol. 222, pp. 29–40). Boston: IFIP.

Schatz, B. (2007). *Digital Evidence: Representation and Assurance*. Australia: Queensland University of Technology; Retrieved from http://eprints.qut.edu.au/16507/1/Bradley_Schatz_Thesis.pdf

Schatz, B., & Clark, A. (2006). An Open Architecture for Digital Evidence Integration. In *AusCERT Asia Pacific Information Technology Security Conference* (pp. 15–29). Academic Press. Retrieved from http://eprints.qut.edu.au/21119/

Turner, P. (2005a). Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags). In *Proceedings of the Digital Forensic Research Workshop (DFRWS)* (Vol. 2, pp. 1–8). Academic Press. doi:10.1016/j.diin.2005.07.001

Turner, P. (2005b). Unification of digital evidence from disparate sources (Digital Evidence Bags). *Digital Investigation*, *2*(3), 223–228. doi:10.1016/j.diin.2005.07.001

Turner, P. (2006). Selective and intelligent imaging using digital evidence bags. *Digital Investigation*, *3*(Suppl.), 59–64. doi:10.1016/j.diin.2006.06.003

Turner, P. (2008). *Digital Evidence Bags*. Oxford Brookes University.

UNODC. (2013). *Comprehensive Study on Cybercrime*. Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Vandepen, S. (2014). *Forensic Images: For Your Viewing Pleasure*. Sans. Retrieved from https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447