# Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody

Yudi Prayudi
Department Of Informatics
Universitas Islam Indonesia
Yogyakarta Indonesia

Ahmad Ashari
Department Of Computer
Science and Electronics
Gadjah Mada University

Tri K Priyambodo
Department Of Computer
Science and Electronics
Gadjah Mada University

## ABSTRACT
Chain of custody is the procedure to do a chronological documentation of evidence, and it is an important procedure in the investigation process. Both physical and digital evidence is an important part in the process of investigation and courtroom. However, handling the chain of custody for digital evidence is more difficult than the handling of physical evidence. Nevertheless, the handling of digital evidence should still have the same procedure with the handling of physical evidence. Until now handling the chain of custody for digital evidence is still an open problem with a number of challenges, including the business model of the interaction of the parties that deal with digital evidence, recording of metadata information as well as issues of access control and security for all the handling digital chain of custody. The solution offered in this research is to build a model of Digital Evidence Cabinets as a new approach in implementing the digital evidence handling and chain of custody. The model is constructed through three approaches: Digital Evidence Management Frameworks, Digital Evidence Bags with Tag Cabinets as well as access control and secure communication. The proposed framework is expected to be a solution for the availability of an environment handling of digital evidence and to improve the integrity and credibility of digital evidence.

## General Terms
Digital Forensics, Digital Investigation.

## Keywords
Digital Evidence, Digital Chain Of Custody, Digital Evidence Cabinets, Digital Evidence Bags.

## 1. INTRODUCTION
An increasing number of users for various types of electronic equipment and information technology have resulted in the rise of cybercrime. A report made by PwC [1] and RSA [2] show that cybercrime is a serious threat causing losses that could affect the national income of a country. According to [3],[4],[5], increasing cybercrime impact the increasing volume of digital evidence handled by the investigators; it could also lead to more documentation and complexity of evidence management.

The efforts in the cybercrime disclosure have been devoted through a series of an investigation process known as digital forensics. Generally, digital forensics is the use of science and methods for finding, collecting, securing, analyzing, interpreting and presenting digital evidence related to the case for the benefit of the reconstruction of events as well as the legitimacy of the judicial process [6].

Meanwhile, an important procedure in handling of evidence and investigation is known as a chain of custody (CoC), which is a procedure for documenting the chronological evidence [7]. Based on [6] and [7], a chain of custody is an important part of the investigation process that will ensure an acceptable evidence in the courtroom. Chain of custody will document the case related to where, when, why, who and how the evidence is developed at each stage of the investigation. Evidence must be maintained based on integrity and authenticity according to the condition when firstly discovered until then will be presented in the court.

Although many digital forensic activities are associated with the process of law enforcement, in fact, only a small number of cybercrime cases are handled by law enforcement; most of them are handled by the private investigator. Banking, insurance, multinational corporations are institutions that often become a target of cybercrime activities and internally those institutions have already had a separate unit for handling the cases indicated to lead to cybercrime [10]. Thus, the need for applying the concept of a digital chain of custody is not only for law enforcement environment, but also for all the parties concerned with digital investigation process.

For the jurisdiction of Indonesia, there are references on how management procedures of evidence are implemented, namely the Chief of Police Regulations (Perkap) Number 10/2010 on Procedures for Evidence Management at the Indonesian National Police Environment [11]. These regulations include a set of:

- The Management who is: covering the procedure for receiving, storage, securing, maintenance and destruction of confiscated objects from space for keeping the evidence;
- The Officials who have the authority to receive, store, secure, maintain, issue and destroy the confiscated objects from the space for keeping the evidence;
- The Storage of Evidence based on the nature and type of the evidence;
- The evidence management principles: legality, transparent, accountable and effective;
- The obligation to make records in the register book and store it in the evidence room.

In the actual case, between the physical evidence and digital evidence, there is a part of the investigation that is complementary. Similarly on the judicial process, both evidence becomes an integral part of the investigation process. Thus, the handling of physical and digital evidence should be the same, or at least have a similar mechanism. Figure 1 illustrates that both physical evidence and digital evidence are an entity in the investigation process.

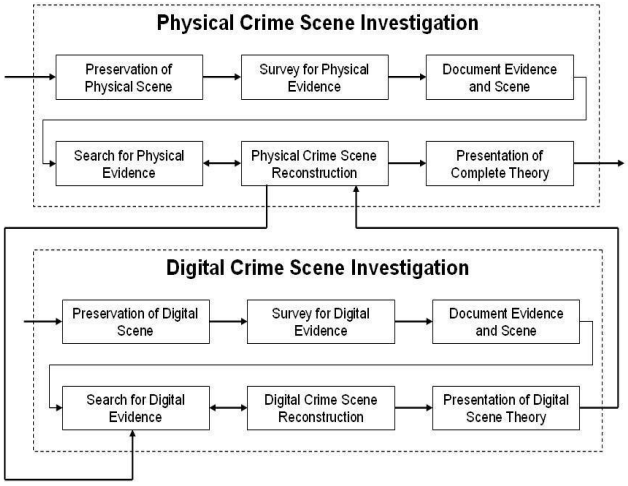


**Figure 1 Relationship of Physical and Digital Evidence**
Source:
http://www.dynotech.com/articles/digitalevidence.shtml

The challenge arises when the evidence is in the form of digital evidence, which is any valuable information that is stored or transmitted in digital form [12]. Digital evidence has a number of characteristics and is easy to duplicate and transmitted, very susceptible to modify and remove, easily contaminated by the new data, as well as time-sensitive. The digital evidence is also very possible to be cross countries and legal jurisdiction. That is why Schatz [13] suggests that the handling of chain of custody of digital evidence is more difficult than physical evidence. Therefore, researches in the field of digital forensics that focus on providing solutions to the digital chain of custody are still a challenge and open more problems [14]. In addition, the rapid growth of cybercrime should always be followed by a new understanding of digital evidence itself along with the handling of its chain of custody.

## 2. DIGITAL CHAIN OF CUSTODY (COC)

The issue of the digital chain of custody, according to [15] and [16] is very broad and complex. However, several indicators that can be identified as difficulties or problems encountered in the handling of the digital chain of custody are:

- The business model involves the complex interactions between the parties related to the digital evidence, namely first responders, forensics investigators, court expert witness, law enforcement, police officers, victim, suspect, and a passerby [17].
- The access control problem of the evidence. On the physical evidence, access to the evidence can be easily controlled. The person who uses, borrows and moves the evidence will be easily recorded and detected. Nonetheless, in the digital evidence, the person who does those actions cannot be easily traced. Being easy to copy activities, duplication, transmission, and access to digital evidence make it difficult to monitor a person's interaction with the digital evidence.
- The integrity issue. On the physical evidence, changes to the evidence can be easily controlled and monitored. However, it is not easy to do that on the digital evidence. The application of the hash key (MD5, SHA1) is the standard method as a solution to control the integrity and credibility of digital evidence. For instance, when a person uses a file, to ensure that the two files are the same, he or she can identify it from the same hash key value between the two files. Almost every imaging or exploration tools for digital evidence will provide the facility to generate and detect the hash key.
- The evidence documentation issue. Recording all interactions with the evidence is easy to do for the handling of physical evidence, but not for the digital evidence. The simplicity of remote access, copy, file transfer, and user mobility trends in performing daily activities allow a digital investigator or another law enforcement to conduct exploration activities and data analysis anywhere and anytime. It will certainly complicate the documentation process of digital evidence. There must be an accurate and complete log of digital evidence, the legal process and the law enforcement agencies that will require much more complete information. Signature of the object, the identity of all parties who interact with the evidence, the location where the evidence is handled, the time of access to the evidence and all the descriptions that contain any transactions and access to evidence is some information that is needed in the process of recording digital evidence [7].
- Handling digital evidence is conducted in particular environment tools. For example, the EnCase Guidance Software tools can start from imaging, extraction, exploration, and reporting phase of digital evidence analysis either in the individual mode or networking mode. Nevertheless, if the same file is then analyzed by using other tools, the recording and documentation process of the file cannot be done in an integrated manner. Garfinkel [14] says that the digital forensic tools that are available today are generally built to help investigators find the specific parts of the digital evidence, but it is not oriented to the concept of the investigation and the legal process in general.
- Handling files as digital evidence in a case is usually only in the form of categorization of different file folders. Only a few applications and a framework that provides a complete solution to the file management of digital evidence.
- Secure/stable storage model concept is to ensure that all the digital evidence data have been stored properly and safely. In other words, the model enables support for storage toughness in the form of the ability to perform data recovery.
- There is no concept of trusted computing is used as a platform to ensure that the infrastructure is implemented completely trust of all interested parties and are protected from system vulnerabilities and attack against the efforts of digital evidence or other confidential information.

## 3. CURRENT STATE

Attempts to conduct research and exploration to get the reliable digital chain of custody concept have been carried out by a number of researchers. In this case according to [3], there are three dimensions of research activity about the digital chain of custody as follows:

a. Research on the topic for improving the quality of the chain of custody. There are at least three research focuses in this dimension. The first is to focus on the

development of a reliable and safe chain of custody through the concept of DEMC (Digital Evidence Management Frameworks). This concept is designed as a framework to be able to answer the questions of who, what, why, when, where and how [18]. The second focus is on the integrity of the chain of custody issue through the adoption of a number of hashing algorithms on digital evidence. The third focus is hardware security approach as developed by the SYPRUS Company through its Hydra PC product. This product is a PC designed to implement cryptographic technology that will ensure a level of confidentiality, integrity and non-repudiation of digital evidence.

b. The second dimension is focused on the efforts for knowledge representation. In this case, Bogen in [3] applies UML and UMML to represent knowledge in the planning, performing and documentation process of digital forensics activity.

c. The third dimension focuses on the forensic format approach. There are many versions of the data format for the benefit of digital forensics. Several formats that have been proposed as summarized by CDEF are as follows: AFF,EWF,DEB,gfzip, Prodiscover and SMART [3]. The forensic format was implemented in 2006 after the forum Digital Forensics Research Workshop (DRWS) established a Common Digital Evidence Storage Format (CDEF) working group as an effort to provide a solution to the storage of digital evidence and its concept of metadata.

Related to the forensic format, according to [19], there are three generations of data imaging techniques that produce forensic format. The first generation is the imaging technique of bit copies of media that will be acquired, and the result is 'raw' or 'dd' image. The second generation is the use of block-based compression to improve the efficiency of the space, and the third generation is the use of multiple image streams integration techniques, expression of information and virtualization storage in forensics format that are known later as the AFF. The format was developed by Garfinkel as a disk image container that supports the storage of metadata in a single archive [3], [20].

To anticipate the trend of increasing information required in the investigation process, in 2009 Cohen [21], [22] proposed an improvement on AFF so its ability to store broader metadata can improve; this improvement is known as AFF4. Furthermore, taking into account on the increasing storage capacity to be acquired, the implementation of hash-based compression scheme is proposed to boost the speed of the image acquisition process.

The other forensic format is a vendor-based, such as EWF (Encase Expert Witness Format). This format was issued by the EnCase vendor that contains checksum data, hash key for integration, verification and information containing bad sectors of the disk imaging process [23].

An evaluation of CDESF as cited by [3] and [4] proves that there are a variety of the existing forensic formats which still contain a number of shortcomings, especially regarding its ability to store the amount of metadata required to support the investigation and judicial process. Therefore, another approach used is through the knowledge representation which is how to map the information required in the chain of custody process via XML, ontology or semantic web. In this case, [3] and [4] himself tried to propose CoC solution through the use of the semantic web to represent the chain of custody using RDF where the forensics information and provenance information are published and used over the web.

Another solution for the digital chain of custody is as proposed by [24] through the XeBag concept. This concept is a combination of the use of PKZIP compression data format with metadata representation through XML. Particularly, the concept was developed to meet the needs of forensic format to handle the cases occurring in South Korea. However, the format of the existing forensics, especially the EWF of Encase, is seen to have a number of limitations to be applied in the jurisdiction of South Korea.

Based on the review, an attempt to provide a solution on the digital chain of custody is divided into three approaches, namely:

- The first approach is through the information container solution that allows storing the amount of metadata in the form of certain forensic format. This approach is as performed by [20] and [21].
- The second approach is through formal knowledge representation of XML, ontology and semantic web solution to store the information of metadata. This approach is as carried out by [8] and [3]. DEB (Digital Evidence Bags) proposed by Turner [25] as a container for storing a number of information such as crime scene artifacts, metadata, information integrity, access; audit records are one of the chain of custody solutions using XML approach. Furthermore, by adding a Tag Integrity File to Turner's DEB concept, then [13] developed a new concept known as Sealed Digital Evidence Bags (SDEB).
- The third approach is a combination of container information and knowledge representation as proposed by [24] in XeBag.

The access control application of the digital evidence has been proposed previously by [26] through the application of cryptographic technique model on the hierarchical access control mechanism. In this case, partial and full supervision mechanisms are developed to describe the rights and functions of the different investigators that directly address the digital evidence and other law enforcement agencies which perform supervisory control on the use of the evidence. The solution provided in this study is more focused on the efforts to perform control and protection against access of digital evidence through the application of cryptography of AES at different security levels.

Related to the access control issue, as far as literature is obtained up to now, there has been no study that specifically leads to the application of the access control concept of the digital chain of custody. However, the importance of the access control concept to the digital chain of custody can take a lesson from the issue of the importance of access control for medical records. In this case, several studies on the access control concept are conducted to protect the integrity of the patient's medical record in a Healthcare Information System. In addition, studies of [27] on the access control model for a collaborative environment can be a valuable input to build the appropriate access control model for the scope of the digital chain of custody.

If the handlings of the chain of custody and the regulations of law enforcement implemented in Indonesia have the same view, then at least there are four key aspects of the chain of custody handling, namely storage, registration and recording,

access control of the evidence and security assurance of the storage and analysis process. Based on this perspective, the previous description of the research in the field of the digital chain of custody can be mapped via the diagram in Figure 2.

## 4. PROPOSED FRAMEWORKS

In the daily practice of the handling of digital evidence, investigators are faced with various types of electronic evidence. Investigators then apply a wide range of acquisition techniques and utilize the availability of various tools to obtain the digital evidence in the form of an image file of the electronic evidence. For the purposes of analysis and management of the case, all the generated image files should have been stored on one place. The simplest illustration is by imagining the handling of physical evidence stored neatly in a shelf in the storage. On the physical evidence, after putting in an evidence bag and stored in shelves, then the borrowing and use of evidence for any purpose must go, through a certain procedure through monitoring performed by the authorized officer. In addition, all activities of physical evidence will be recorded properly in a chain of custody. In this perspective, the most important thing is how to apply the storage and evidence recording principles as well as control access to the evidence.

The proposed solution is in the form of the digital evidence cabinets (DEC). As a cabinet, all the evidence that has been stored in the evidence bag are organized and stored securely. The cabinet will be locked and guarded by an officer. If an investigator requires the evidence, then he/she has to go through the procedure and get a license from the personnel to access the evidence. The officer then opens the cabinet and submits the referred evidence to the investigator. The business model of the digital evidence cabinets is as displayed in Figure 3.

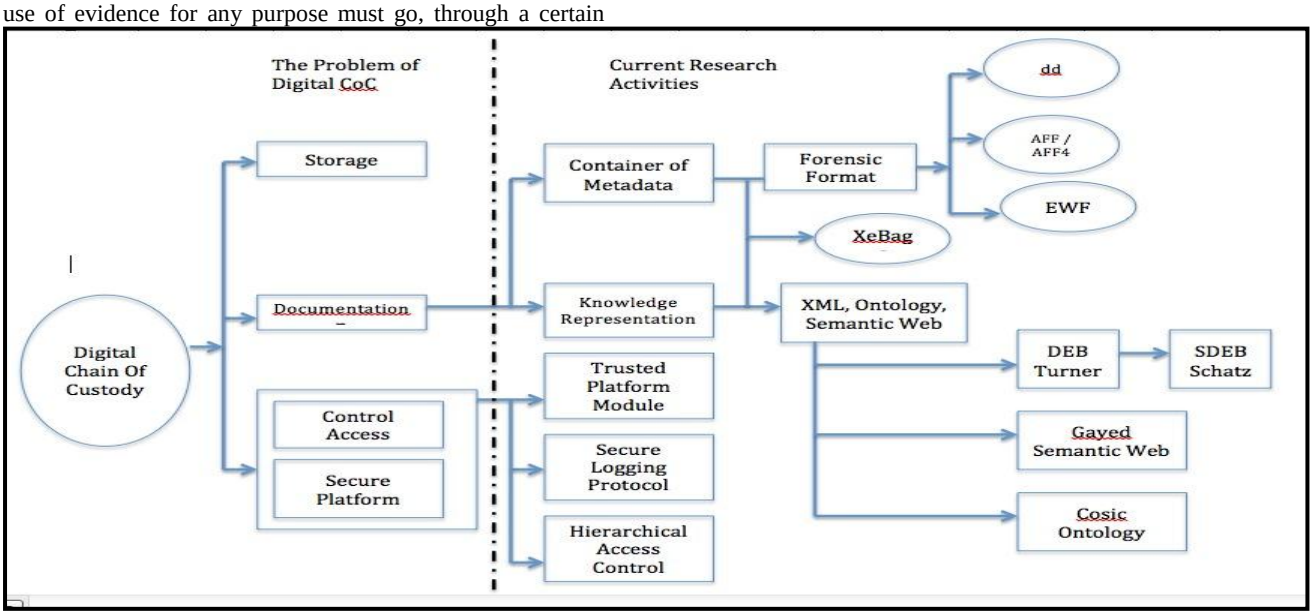


**Fig 2: Problems and Research on Digital Chain of Custody**

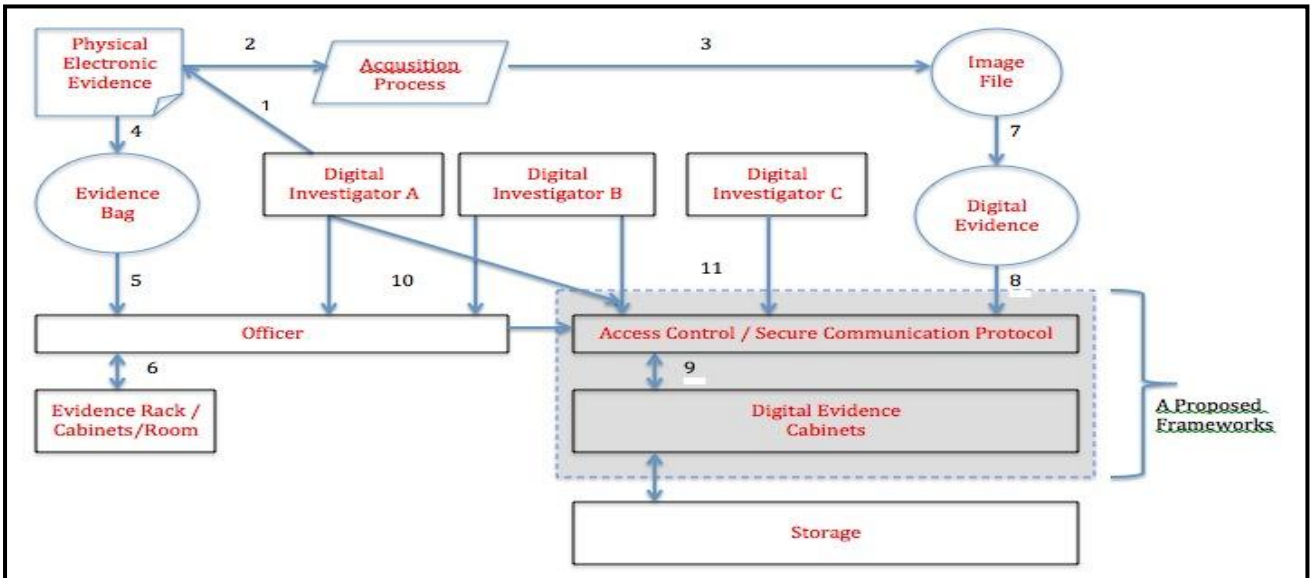


Figure 3 Business Model of Handling the Digital Evidence

A description of the illustration from Figure 3 is as follows:

1. Digital investigator forecloses physical evidence and crime scene investigation.
2. For certain electronic devices, it has been performed the acquisition process to get the image file.
3. The acquisition process can be done online (triage forensics) or offline. The acquisitions could use all the tools and instruments depending on the nature and characteristics of electronic devices found.
4. After the acquisition process is completed, the evidence is put into the evidence bag and then given the label and recording.
5. Physical evidence is then submitted to the officer to register.
6. The officer then stores the physical evidence in a particular place (space, cabinets, shelves).
7. The results of the acquisition process are in the form of image files to a format that suits the equipments and tools used when acquiring electronic evidence.
8. Image file as digital evidence is not stored in a personal computer of the investigator but is stored in a secured storage system.
9. Digital evidence is stored in the digital evidence cabinet, including the interaction records and other forensic records.
10. If the digital investigator requires physical evidence for the benefit of his/her investigation, he or she must go through certain procedures to be able to get access to the physical evidence that has been stored in the evidence room.
11. If another digital investigator is interested to do an analysis of the physical and digital evidence, he/she must go through a specific mechanism

In that business model, digital evidence should be stored properly in a secured system, and the access to it must be through a procedure. This does not happen in the actual practice. Digital evidence will be stored in a computer of the investigator. Then for the sake of analysis, the copy and distribution of digital evidence will be made between the digital investigators without going through a control mechanism. This is not in accordance with evidence handling procedures. The concept of digital evidence cabinet is a new way of handling digital evidence through a mechanism such as the handling of physical evidence.

In that business model, there are three categories of investigators who might interact with digital evidence. Investigator type A, the officer who made the crime scene directly after the initial process of handling digital evidence through acquisition and imaging. Officers of this type are also responsible for storing physical evidence into the evidence room and storing digital evidence in a storage medium. Investigator type B is an officer who is not directly involved in the crime scene and the data acquisition process, but involved in the handling of the case so requires him to interact either directly by physical evidence and digital evidence. Investigator type C is the only officer involved in handling the case through the analysis of digital evidence.

Referring to the business model, the mechanism of handling digital evidence on environmental law enforcement in Indonesia just stop until the seventh step. Mechanism on stage eight to eleven yet to be implemented. Chain of custody is an important procedure in the investigation, the eighth to the eleventh stage of implementation will improve the quality of the handling of digital evidence. Thus, the hypothesis that the handling of physical evidence and digital evidence should have the same procedure can be met. The implementation is then proposed as a framework for digital evidence cabinets (DEC).

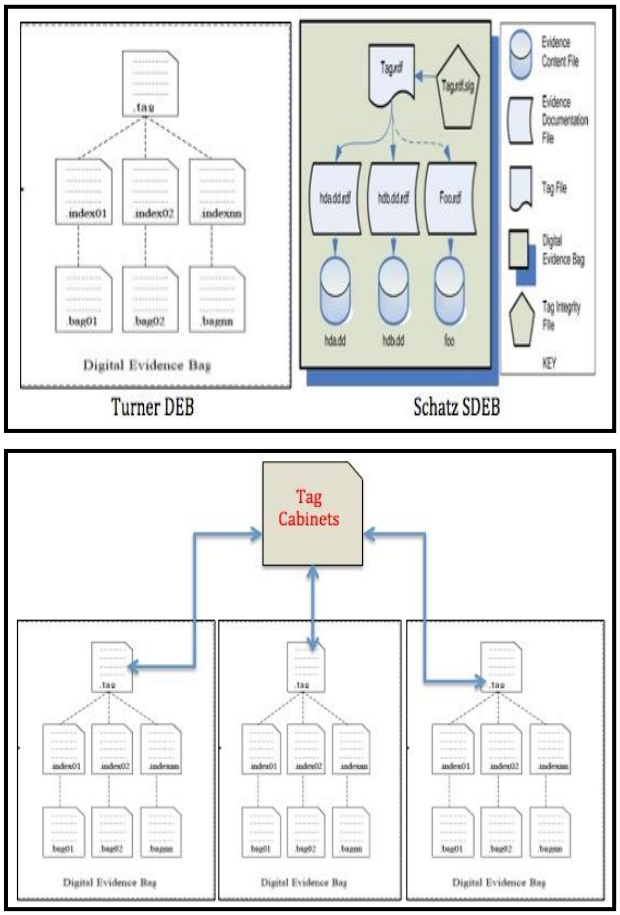


**Figure 4 Basic Concept of the Representation of Digital Evidence Cabinet**

There are several important elements to be able to apply the DEC concept. The following is the identification of the proposed solution:

- The concept of digital evidence management. This concept is necessary as a mechanism to control the role of each digital investigator in various phases of the investigation. Digital investigators can act as a first responder, analyzer, expert witness, or law enforcement or officer. One of the solutions that were ever made is as done by [18] and [8] through the Digital Evidence Management Frameworks (DEMF) concept.
- The concept of recording the information and representations of digital cabinet. This concept is necessary to implement three things: digital evidence bag, digital evidence cabinet concept consisting of several bags for a variety of different cases and control or key concepts of digital evidence cabinet. The approach offered by Turner through the Digital Evidence Bags

(DEB) [25] as well as its development by Schatz though Sealed Digital Evidence Bags (SDEC) [13] can be one of the initial concepts to develop the Digital Evidence Cabinets concept. One step that can be done is to perform reconstruction of the tag integrity concept proposed by Schatz and add tag cabinet concepts as a marker of the unity of digital evidence in a cabinet. One of the development ideas that can be applied is to perform the modification through tag integrity concept as follows.

- The concept of a secure environment to ensure that access to digital evidence in accordance with the provisions. As in the physical concept, access to the evidence set in a secure environment with a particular mechanism. Likewise, the digital concept, there must be a mechanism of control and security that will ensure that access to digital evidence is completely safe.

Digital Evidence Cabinets (DEC) is a modified model of the structure of information storage based models of Turner's Digital Evidence Bags. The modification is through the use of tags Cabinets extension for representing information and documentation from a series of stored digital evidence. Systematically, the DEMC and DEC concepts are unitary frameworks that will handle the overall digital evidence management process.

# 5. CONCLUSION AND FUTURE WORKS

In the conventional model, evidence found at the crime scene will be put into a special place; after the basic information of the evidence is written, it is stored in a particular place. Furthermore, any time the evidence is used by anyone for any purpose would be properly recorded and then confirmed that nothing has changed from the evidence. The challenges arise when evidence is handled in the form of digital evidence. A number of proposals have been submitted by the researchers to help the investigators conduct digital evidence handling along and its chain of custody. However, as far as experience in handling a number of cases and observations that occur in practice among law enforcement, it turns out the digital evidence handling and chain of custody is not in accordance with the actual handling procedures. This happens because of the absence of a frameworks for digital evidence handling and chain of custody are referred by law enforcement.

The Digital Evidence Cabinet (DEC) concept is one of the proposed frameworks to enhance the handling of digital evidence and the recording of its chain of custody. DEC concept in principle consists of three parts, which are the concept of digital evidence management frameworks for handling the interaction of investigator at each different level of investigation, the tag cabinet concept for the representation of digital evidence cabinet through the development of Turner's DEB models as well as the access control concept and secure communication to support trustworthy-based computing.

Overall, DEC concept is constructed to duplicate the handling and storage process of physical evidence. To implement the proposed frameworks then there are at least four stages of research to be done. The first stage is to build a DEC model through the integration of DEMF and Tag Cabinet concept on DEB model; the second is to conduct proof of concept of the model through simulation handling of the case. The third step is to develop an access control mechanism and secure communication concept to support the establishment of a trustworthy-based computing environment for the implementation of DEC. Then, the fourth step is to test the application of the access control and secure communication concept in a simulation of handling a case in one of the law enforcement agencies.

However, frameworks are proposed in this paper is likely to change in accordance with the input and discussions from researchers or practitioners in a digital investigation. This study is the initial stage of the effort to build a framework for digital evidence cabinets. In addition to implementing the proposed frameworks, then there are some other issues that should be explored. There are a number of problems to be solved in future research, such as: how metadata characteristics that meet the needs of the technical and legal information; how to better recording techniques for metadata of digital evidence; how to apply and implement the access control mechanism to integrate the concept of evidence as well as the DEC in a secure environment. These three things are going to be the focus of further research on the issue of digital evidence cabinets.

# 6. REFERENCES

[1] PwC, "US cybercrime: Rising risks, reduced readiness," PricewaterhouseCoopers Report, Available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf, 2014.

[2] RSA, "The Current State Of Cybercrime 2014: An Inside Look at the Changing Threat Landscape," RSA-EMC Report, Available at http://www.emc.com/collateral/white-paper/rsa-cyber-crime-report-0414.pdf, 2014.

[3] T. F. Gayed, H. Lounis, and M. Bari, "Computer Forensics: Toward the Construction of Electronic Chain of Custody on the Semantic Web," in Proc *The 24th International Conference on Software Engineering & Knowledge Engineering*, pp. 406–411, 2012.

[4] T. F. Gayed, H. Lounis, and M. Bari, "Cyber Forensics : Representing and ( Im ) Proving the Chain of Custody Using the Semantic web," in Proc *COGNITIVE 2012 : The Fourth International Conference on Advanced Cognitive Technologies and Applications*,pp. 19–23, 2012.

[5] N. Kshetri, *The Global Cybercrime Industry*. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 267, 2010.

[6] A. Agarwal, M. Gupta, and S. Gupta, "Systematic Digital Forensic Investigation Model," *International Journal of Computer Science and Security*, vol. 5, no. 1, pp. 118–134, 2011.

[7] G. Giova, "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems," *International Journal of Computer Science and Network Security.*, vol. 11, no. 1, pp. 1–9, 2011.

[8] J. Cosic, G. Cosic, and M. Baca, "An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence," *JIOS Journal of Information and Organization Science.*, vol. 35, no. 1, 2011.

[9] J. Cosic and G. Cosic, "Chain of Custody and Life Cycle of Digital Evidence," Journal of *Computer Technology and Aplications*, vol. 3, pp. 126–129, Feb-2012.

[10] C. Easttom and J. Taylor, *Computer Crime, Investigation, and the Law*. Boston, Massachusetts USA: Course Technology, 2011.

[11] Y. Prayudi, "Problema dan Solusi Digital Chain Of Custody," in Proc *Seminar Nasional Aplikasi Teknologi Informasi (Senasti)*, 2014, no. 2011, pp. 197–204.

[12] N. Kuntze, C. Rudolph, and I. Technology, "Secure Digital Chains of Evidence," in Proc S*ixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 1–8, 2011.

[13] B. Schatz, "Digital Evidence: Representation and Assurance," Thesis, Queensland University of Technology, Australia, 2007.

[14] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, pp. S64–S73, Aug. 2010.

[15] P. G. Bradford and D. A. Ray, "Using Digital Chains of Custody on Constrained Devices to Verify Evidence," in *Proc IEEE Intelligence and Security Informatics*, pp. 8–15, 2007.

[16] J. Rajamäki and J. Knuuttila, "Law Enforcement Authorities ' Legal Digital Evidence Gathering," in Proc *European Intelligence and Security Informatics Conference*, pp. 198–203, 2013.

[17] J. Cosic and G. Cosic, "Chain of Custody and Life Cycle of Digital Evidence," *Computer Technology and Aplications*, vol. 3, pp. 126–129, Feb-2012.

[18] J. Ćosić and M. Bača, "A framework to (Im)Prove „Chain of Custody" in Digital Investigation Process," *Proc. 21st Cent. Eur. Conf. Inf. Intell. Syst.*, pp. 435–438, 2010.

[19] M. Cohen and B. Schatz, "Hash based disk imaging using AFF4," *Digital Investigation*, vol. 7, pp. S121–S128, Aug. 2010.

[20] S. L. Garfinkel, "Providing Cryptographic Security and Evidentiary Chain-of-Custody with the Advanced Forensic Format ," *International Journal of Digital Crime Forensics*, vol. 1, no. March, pp. 1–28, 2009.

[21] M. Cohen, S. Garfinkel, and B. Schatz, "Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow," *Digital Investigation*, vol. 6, pp. S57–S68, Sep. 2009.

[22] B. Schatz and M. Cohen, "Refining Evidence Containers for Provenance and Accurate Data Representation," in Proc *IFIP Advanced Information Communication Technology*, vol. 337, pp. 227–242, 2010.

[23] CDESFWG, "Survey of Disk Image Storage Formats," 2006.

[24] K. Lim and D. G. Lee, "A New Proposal for a Digital Evidence Container for Security Convergence," in Proc *IEEE International Conference on Control System, Computing and Engineering*, pp. 171–175, 2011.

[25] P. Turner, "Unification of Digital Evidence from Disparate Sources ( Digital Evidence Bags )," in *Digital Forensic Research Workshop (DFRWS)*, pp. 1–8,2005.

[26] C.-L. Hsu, B.-C. Liu, and Y.-L. Lin, "A Digital Evidence Protection Method with Hierarchical Access Control Mechanisms," in *IEEE Carnahan Conference On Security Technology (ICCST)*, pp. 1–9, 2011.

[27] W. Zhou, "Access Control Model and Policies for Collaborative Environments," PhD Dissertation, Universitaet Potsdam, Potsdam Germany, 2008.