Digital Chain of Custody: State of the Art

Yudi Prayudi
Department of Informatics - Universitas Islam Indonesia Yogyakarta, Indonesia

Azhari SN
Department of Computer Science and Electronics Gadjah Mada University, Yogyakarta, Indonesia

ABSTRACT
Digital forensics starts to show its role and contribution in the society as a solution in disclosure of cybercrime. The essential in digital forensics is chain of custody, which is an attempt to preserve the integrity of digital evidence as well as a procedure for performing documentation chronologically toward evidence. The characteristics of digital evidence have caused the handling chain of custody is becoming more complicated and complex. A number of researchers have contributed to provide solutions for the digital chain custody through a different point of views. This paper gives an overview of the extent to which the problem and challenges are faced in the digital chain of custody issue as well as the scope of researches that can be done to contribute in the issue of the digital chain of custody.

General Terms
Digital Forensics

Keywords
Digital Forensics, Digital Evidence, Chain of Custody, Cybercrime

1. INTRODUCTION
Chain of Custody is a procedure in the handling of evidence in a series of investigations. According to [1], chain of custody is a procedure for performing documentation to the evidence in chronological events. Meanwhile according to [2], chain of custody is an important part of the investigation process that will ensure evidence can be accepted in the court system. In this case, chain of custody will document the terms related to *where, when, why, who, how* in the use of evidence at any stage of the investigative process. The issues of chain of custody become very important, as authenticity of evidence must be maintained in accordance with the condition when it was first discovered until later presented in the court. The scope of chain of custody includes all individuals involved in the process of acquisition, collection, analysis of evidence, time records as well as contextual information, which includes case labeling, and the unit and laboratory that process evidence.

In today's digital society era, the issue of the digital chain of custody becomes important considering the number of cybercrime activities that appear. This is one of the consequences of development in information technology and the telecommunication infrastructure improvement that make it easier to connect every individual in a virtual environment that is without limit. In this case, according to [3] the development and improvement of information technology have impacted on the openness of various forms of crimes recently committed by individuals and groups known as cybercrime. Survey and reports made by [4],[5],[6], shows that cybercrime is a serious threat to individuals, institutions or countries in which the amount of losses globally might equal to national income of a country. In Indonesia, according to the Indonesia Computer Emergency Response Team (IDCERT) cited by Alkazimy (2011) in [7], in the first half of 2011, there have been 78.238 cases of cybercrime and the number increased to 144.284 at the fifth two-month year 2011.

The attempts to disclose cybercrime are done through a process known as digital forensics. According to [8], the digital forensics is the use of science and methods for finding, collecting, securing, analyzing, interpreting and presenting digital evidence related to the case occurring and it is beneficial for event reconstruction as well as the legitimacy of the judicial process. Although digital forensics activities are mostly associated with law enforcement process, in fact, only a small number of cybercrime cases that have been handled by law enforcement. Most of the cases are handled by private investigators. Banking, insurance, and private company are institutions that often become the target of cybercrime, and the institutions have had an internal unit for the handling cases that lead to cybercrime [9].

In Indonesian jurisdiction, the procedure of handling of evidence refers to Regulation of the Chief of National Police No. 10/2010 on the Procedure of Handling of Evidence in The Indonesian National Police [10]. The regulation provides an overview of the business model for handling of evidence by law enforcement officers. It mentions about:

- Management namely: procedure or the process of receiving, storing, securing, maintenance, using and destroying confiscated object to/from the evidence room.
- The officer, who has the authority to receive, store, secure, care, release and destroy the confiscated objects from the evidence room.
- Storage based on the different type of evidence.
- Principles of evidence handling: legality, transparency, accountability and effectiveness.
- The obligation to write and record into the register book of all activities related to the evidence.

The challenges faced by investigators when the evidence handled is digital evidence, i.e. any valuable information that is stored or transmitted in digital form [11] or information stored or transmitted in a binary form that can be used in the law enforcement and judicial process [12]. In this case, there are two terms that are almost the same, i.e. electronic evidence and digital evidence. Electronic evidence has a physical form and can be identified visually (computer, mobile phone, camera, CD, hard disk, etc.), while digital evidence is evidence that is extracted or recovered from electronic evidence (can be a file, email, short message, image, video, log, text).

According to Matthew Braid in [11], in order each evidence can be used to support the judicial process, the evidence must meet five criteria, namely: admissible, authentic, complete, reliable and believable. Meanwhile,[13] mentions the two basic aspects of other criteria so that evidence can support legal proceedings, namely legal aspects, with the criteria: authentic, accurate, complete; and technical aspects, with the criteria: chain of evidence, transparent, explainable, accurate.

Digital evidence has a number of characteristics, such as easy to be duplicated and transmitted, very susceptible to be modified and removed, easily contaminated by new data, and time sensitive. Digital evidence is also very possible to cross

countries and legal jurisdictions. For this reason, according to [13], the handling of chain of custody of digital evidence is much more difficult than the handling of physical evidence, in general. In contrast to physical evidence, digital evidence is very dependent on the interpretation of its content. Therefore, the integrity of the evidence and the ability of the expert to interpret the evidence will be influential in sorting digital documents available to serve as evidence [13].

This paper will provide an overview of the extent to which research with a focus on the digital chain of custody has been performed by a number of previous researchers. The expected output of this paper is to obtain a general overview of the problems and challenges that can become an area of research on the digital chain of custody.

2. AN OVERVIEW OF THE PROBLEMS IN CHAIN OF CUSTODY

In the actual case, physical and digital evidence are part of the investigation process that is complementary to each other. Similarly, when the judicial process, the physical and digital evidence are becoming an integral part of the investigation process. Thereby, the handling of physical or digital evidence is supposed to be the same, or at least has a similar mechanism. Figure 1 illustrates that both physical and digital evidence is a unity in the investigation process.

The problem encountered these days is the gap in the handling between physical and digital evidence. This is certainly going to be an obstacle in the judicial process. That is why it requires the contribution from academician to provide solutions and set the framework for the handling of evidence, both physical and digital evidence that will support the digital forensics activities.

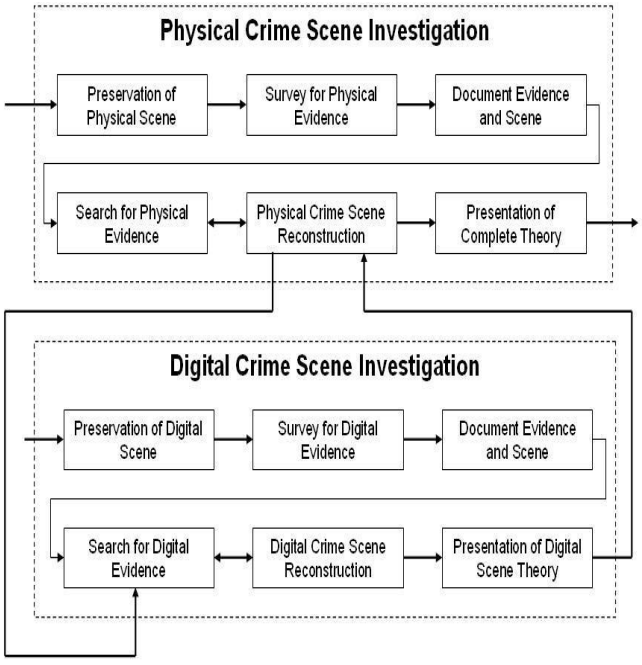

Figure 1. Unity of Physical and Digital Evidence Handling

(Source: http://www.dynotech.com/articles/digitalevidence.shtml)

One of the problems encountered in the handling of digital chain of custody is the various frameworks and business models in the digital forensics activities. The digital forensics frameworks that are varying actually do not have a principle and fundamental difference because in general any framework used by the researchers is different only in terms of the addressing and detail of digital forensics activities [14],[15],[16].

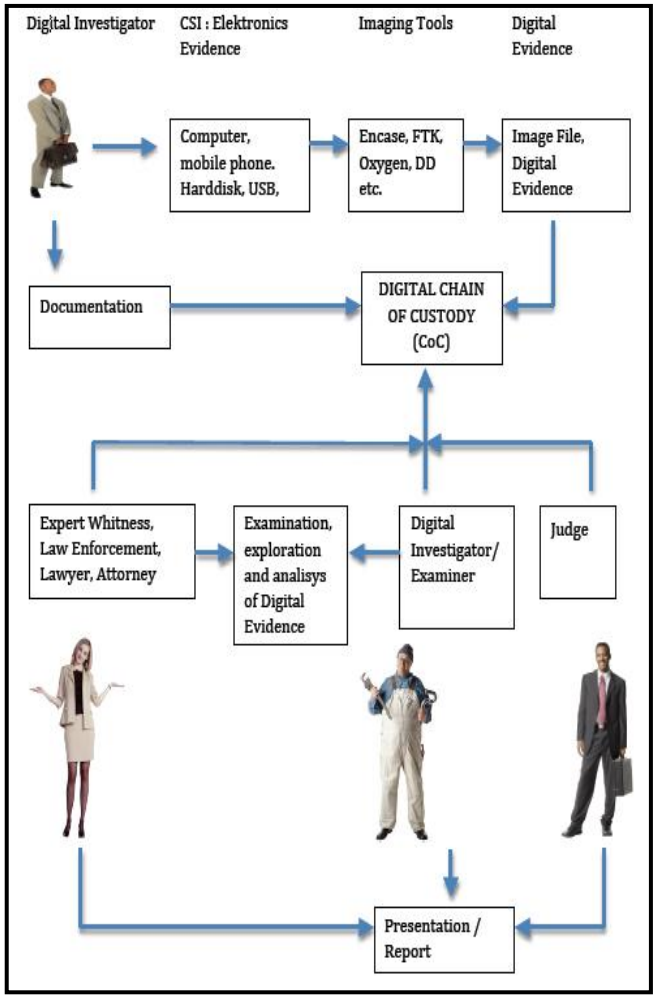

Figure 2. An Illustration of Business Model and Digital Evidence Chain of Custody

Nevertheless, this phenomenon does not apply to digital forensics business model. Business model will provide a description of the relation between parts in every stage of the digital forensics frameworks. The difference in a business model will cause a difference in the overall handling of the digital forensics, including the handling of chain of custody. Unfortunately, up to now there has been no study concerning the issue of business model in digital forensics and the real implementation among digital forensics practitioners. Therefore, the study of business model in digital forensics will be a reference to every institution that conducts digital forensics activities. Figure 2 shows one of the concepts of business models that can be implemented in digital forensics.

Digital chain of custody according to [17], [18] raises a problem that is vast and complex. The main problem in the chain of custody is related to the documentation of evidence. Documenting and recording of all interactions on the physical evidence is extremely easy to do; however, this does not apply to digital evidence. The easiness to do remote access, copy, transfer the file, coupled with and user mobility trend in daily activities allow a digital investigator or other law enforcement agencies to explore and analysis the data anywhere and anytime. This is certainly going to complicate the documentation process of digital evidence. It requires accurate

and complete documentation as well as data logs of the digital evidence.

In the future, court and law enforcement will require much more detailed information to support the investigation process. Signature of the object, identity of all parties who interact with the evidence, location of handling the evidence, time of access and all the descriptions that contain transactions and any access to the evidence would be required [1].

Meanwhile, according to [19], the documents issued by several organizations (such as IOCE, SWGDE, DRWS) are basically only in the form of report or paper about general aspects of the handling of digital evidence and chain of custody, whereas the technical implementation of the handling of the digital chain of custody is still not further explained. To this end, researches in the field of digital forensics that focus on providing solutions to the concept of digital chain of custody still pose a challenge and open problem [20]. In addition, the rapid growth of cybercrime must always be followed by a new understanding of digital evidence along with the handling of chain of custody.

One of the problems in chain of custody is data integrity. In this case, according to Vanstode in [21], digital integrity is a property on which digital data do not experience any change by the party who is not authorized to do any change. Changes and contacts on digital evidence are only done by those who have the authority. The integrity of digital evidence warrants that the information presented is complete and unchanged from the first until used lastly in the court.

Meanwhile, based on the characteristics of digital evidence, the handling of evidence should also consider the order of volatility of digital evidence. In this case, Brezinski & Killalea [22] state that the order of volatility of digital evidence is as follows: register, memory, table, processor, temporary file system, disk, remote logging and data monitoring, physical configuration and network topology, as well as archived data. The improvement capabilities of digital technology allows the emergence of various new characteristics of digital evidence. Therefore, the order of volatility of the digital evidence is very possible to change.

Digital forensics processes applied in disclosure of cybercrime must follow the procedures and mechanisms for the handling of digital evidence. In this regard, proper concepts and tools of digital chain of custody are necessities for a digital investigator. According to Garfinkel (2010), concepts and tools that are available today are still partially able to explore digital evidence and not yet supporting the investigation process as a whole.

Numerous studies have been done in an effort to implement the concept of digital chain of custody. Regarding the handling of chain of custody, according to [23], there are at least four main issues, namely:

- Flexibility and capability of documentation of the chain of custody in line with the increasing data volume generated from various new tools.
- Interoperability between digital evidence and documentation of the chain of custody.
- Security of chain of custody documentation, considering that evidence can move from one party to another.
- Knowledge of the judge and jury in dealing with cases involving digital evidence so he or she can decide cases in the right way. One of them is the way to present information that can be understood by both the judges and other law enforcement agencies. In this case, chain of custody must provide 2 aspects of information, i.e. information that is directly related to the case (includes 5W and 1 H), as well as information related to the source, originality and the process for obtaining such evidence. Gayed called these two aspects as forensics information as and provenance information.

3. CURRENT RESEARCH

According to [24], digital forensics developed as an independent field of study began in early 2000. However, according to [25], the initiation of digital forensics in fact already started since 1976 where the terminology of computer crime was used to refer deletion and modification of data by a person who was not entitled. This is in line with the opinion from [20] that initially digital forensics activities were only necessary for the data recovery.

One case of which required a complex computer analysis and engaged a large investigation team was a crime done by a hacker named Markus Hess and this case was handled by FBI in 1986 [25]. Then, the increasing of technology and the lifestyle of human that often interacts with technology support the growing activities of digital forensics. This is as what [20] mentions, that one factor supporting the rising cases of cybercrime is a growing number of personal computer users as well as easy connection between computers. In these case, [20] mentions; that within 15 years, digital forensics enters the golden age as seen from the number of academics who conduct a research on various aspects of digital forensics, coupled with the increasing interest of vendors to invent a variety of tools and applications for digital forensics.

Also, [20] and [24] suggest and describe an overview of current research as well as challenges in the field of digital forensics. Based on paper mapping on some media publication [25], [26] reveal an overview of the topics and research areas that are mostly examined in digital forensics.

Attempts to do some researches and explorations to get a reliable concept of digital chain of custody have been done by previous researchers. In this case, according to [23], broadly speaking there are three dimensions of research activities regarding digital chain of custody.

- Researches on the topic of improving the quality of chain of custody. There are at least three research focuses on this dimension; the first one is by focusing on the development of chain of custody that is reliable and secure through the concept of DEMC (Digital Evidence Management Framework) and this concept is designed as a framework to answer the questions of *who, what, why, when, where* and *how*. [21]. The second focus is an integrity issue of chain of custody through the adoption of a number of hashing algorithms on digital evidence. The third focus is security approach on hardware as developed by SYPRUS Company through their product called PC Hydra. This product is a PC designed to implement cryptographic technology that will guarantee the level of confidentiality, integrity and non-repudiation of digital evidence.
- The second dimension focuses on an attempt to represent knowledge. In this case, Bogen in [23] applies UML and UMML to represent knowledge in the process of planning, performing and documenting digital forensics activities.
- The third dimension is focused on forensic format approach. There are many versions of data format for digital forensics. Some formats that have ever been proposed are as summarized by the CDEF, such as FF,

EWF, DEB, gfzip, Prodiscover and SMART. [23]. These forensic format approaches started to be used widely in Digital Forensics Research Workshop (DRWS) forum in 2006 formed Common Digital Evidence Storage Format (CDEF) working group as an attempt to give a solution to the concept of digital evidence storage and their metadata.

In the field of forensics in general, the issue revolving around the chain of custody has called the attention of a number of researchers, one of them is [27]. On the research, a system is built named Disciple LTA (Learner, Tutor and Assistant) as a computer-based cognitive assistant that will help analysts to conduct a credible assessment of a number of intelligence evidence so that the assumption of uncertain changes in information on the evidence during some stages of investigation process can be overcome. The study provides a systematic and comprehensive approach to make an assessment so that at any stage of the chain of custody, the integrity of any part of the evidence is really guaranteed and no hesitation or assumption for the possibility of missing information in the handling of evidence.

One issue in the chain of custody is data integrity. The common solution used to overcome this problem is to apply the concept of a hash key to check the integrity of digital evidence. On this issue, one of the early researches was conducted by [17]. The study presents a method to perform validation and authentication of digital chain of custody through the approach of Jacobsson algorithm, which is an algorithm for validating a hash value that is generated by the algorithm via online. In the preliminary research, [28] specifically proposed an algorithm for generating Jakobsson's fractal hash chain, which is an algorithm which can generate, traverse, and store the hash keys in large amounts especially in small and constrained devices. Another study about the integrity of digital evidence was conducted by [29] by doing computational analysis through comparison of several algorithms for hash function on digital evidence.

Given the rapid development of the characteristics of digital evidence, the attempts to find digital evidence and the documentation are becoming increasingly difficult. That is why [2] opines that one of the initial steps is to understand in more details about the characteristics of digital evidence and chain of custody through ontology approach. In the study, through top-down based approach, an ontology model is built that consists of five hierarchies, namely: *Characteristics*, *Dynamics*, *Factors*, *Institutions* and *Integrity.* Those five elements of the hierarchy are named DCoDeOn (*Digital chain of custody Digital Evidence Ontology*) and directed to be able to respond to the aspects of *what, why, who, when, where and how* in the chain of custody.

Furthermore, when the handling of chain of custody has the same point of view with the law enforcement regulations prevailing in Indonesia, then at least there are 6 aspects of key handling of digital chain of custody, namely (a) business model and life cycle; (b) forensic format, (c) information record keeping (d) the storage, (e) security assurance of the storage and (f) access control for the storage of digital evidence.

3.1 Life Cycle

Cosic [2] has modelled interaction process in chain of custody that includes five actors, namely: *first responders, forensics investigator, court expert witness, law enforcement* and *police officer*. Additionally, [1] also has constructed a model of an interaction process of chain of custody that engages five different actors, namely: *first responder, investigator, prosecutor, defense* and *court.* According to Giova (2011), the model of actors in the interaction process of chain of custody will be affected by the provisions of the law in each country. However, the model that is built must be able to explain the activity, relationship, and involvement of the actors in digital evidence.

To understand the relation between digital evidence and chain of custody, the term of life cycle is used. Petri Nets model approach is used to build the life cycle of digital evidence. Previous researchers have been doing a research on the solution of chain of custody but due to the wide and complex issue in this field, it needs a further description of relations and interactions between parties involved in the handling of digital evidence.

3.2 Forensic Format

Other researches about digital chain of custody are conducted through forensic format approach by [30] and [31]. In this case, [30] provides a solution related to the digital chain of custody by proposing an improvement on the concept of AFF version 3 (Advanced Forensic format Library) into AFF version 4. The concept of AFF is an approach to digital signature and other cryptographic protections for digital evidence that allow an investigator to apply the chain of custody system that is reliable from the crime scene until in the trial. Meanwhile, [31] applies AFF4 framework through the implementation of XML to build a chain of custody on the network scheme of Internet Control Message Protocol (ICMP) sweep attack.

Another study has been conducted by [23] that develops a digital chain of custody solution in the form of a modified forensic format and combines it with AFF4 forensics concepts of RDF to bridge the gap between the real condition in juridical proceedings and common practice which takes place in digital forensics community.

In regard to forensic format, according to [32], there are three generations of data imaging techniques that produce forensic format. The first generation is imaging with the technique of bit copies from the media that will be acquired and the result is 'raw' or 'dd' image; the second generation is the use of block-based compression to increase space efficiency; while the third generation is using integration technique of multiple image streams, that is an expression of information and storage virtualization into forensic format later known as AFF. This format is developed by Garfinkel as disk image container that supports storage of metadata in a single archive [23], [30].

Given the trend of increasingly varying information required in the investigation process, then in 2009, Cohen in [33], [34] created a proposal for AFF improvements to enhance its ability in storing metadata more extensively. This upgrade is known as AFF4. Then, considering the greater storage capacity that must be acquired, and then it is suggested to use the application of hash scheme based compression to boost the speed of image acquisition process [32].

Another forensic format is vendor-based in nature, namely the EWF (Encase Expert Witness Format). This format is issued by Encase vendor that contains data checksum, a hash key to verify information and integrations containing bad sectors from the disk imaging process [35].

An evaluation from CDESF as cited by [23] mentions that the various existing forensic formats still contain a number of weaknesses, especially in the ability to keep the number of metadata needed to support the process of investigation and trial. For this reason, the other approach used is through knowledge representation, namely how to map out necessary information in the chain of custody process via XML, ontology

or semantic web. In this case [23], [36] try to propose a CoC solution through the use of semantic web to represent a chain of custody using RDF where forensics information and provenance information is published and utilized through the web.

Another solution for the digital chain of custody is as proposed by [37] through the concept of XeBag. This concept is a combination of the use of PKZip data compression format with representation of metadata via XML format. This concept is developed specifically to meet the needs of forensic format to handle the cases that take place in South Korea. The existing forensic format, particularly EWF from Encase is seen as having a number of limitations to be applied in the juridical area of South Korea.

3.3 Information Record

The most important thing of the chain of custody is the ability to store metadata information [12]. Considering the digital evidence acquisition process through 'dd' tools or other tools does not facilitate the needs for metadata information of digital evidence, then a mechanism is needed for additional record keeping of metadata information through the concept known as Digital Evidence Bags (DEB). The concept of Digital Evidence Bag (DEB) as information container for digital evidence is then implemented with an XML approach through the availability of three main files, namely tag file; .indexnn file; and .bagnn file.

Another approach to chain of custody issue carried out by Schatz (2007) is known as sealed digital evidence bags. This concept is the development of DEB (Digital Evidence Bags) concept proposed earlier by Turner. The approach is to use the concept of RDF/OWL for the representation of necessary knowledge, as well as control of digital evidence. Meanwhile, [37] proposes the concept of XeBag (XML PKZip Based Digital Evidence Bag) as a solution for digital evidence storage technique. In the concept, the evidence file is stored in PKZip format while the information associated with the forensics is saved using XML format.

The same thing is done by [23]. In this matter, [23]provides a digital chain of custody solution through semantic web approach using RDF and provenance vocabularies to ensure the trustworthiness and integrity of the information on digital evidence. The study begins by setting the definition and analysis of all data information related at each stage of digital forensics process. The next stage is linking the information from chain of custody into interlinked RDF, including integrating the forensics and provenance metadata. On the final stage, the web interface is built that allows all parties to access necessary information from chain of custody that has been made.

On the other hand, according to [38], one of the problems encountered in the handling of digital chain of custody is how to present the information that is needed during the judicial process. The information presented in the chain of custody according to [38] should be a combination of a technical area of digital evidence and legislation area from the judicial point of view. Thus, there must be a good interface so that the data generated by digital investigator can be understood by the judges and other law enforcement agencies in accordance with the applicable law. In this case, there is what so-called as supervision data as the depiction of data extracted from the technical aspect that meets the legal aspects.

The similarity obtained from a variety of solutions for digital chain of custody is an approach to integrate a number of essential information as required in the chain of custody directly on each digital evidence file. This is done particularly because of the difficulty in controlling the mobility and accessibility of digital files. In addition, digital chain of custody solution is not included in a framework of digital forensics investigation that is binding. Therefore, the research of Digital Evidence Cabinets tries to perform another approach through digital evidence collection using the information stored in the media storage (evidence cabinets) and not directly on the digital evidence.

Next, [39] sees the necessity for data integrity concept to ensure the handling of digital evidence and chain of custody and then develops the concept of DEMF (Digital Evidence Management Framework) through several criteria to obtain information that meets 5W 1 H. For any information 5W and 1 H is included to ensure the security (Who-fingerprint, Where-GPS, When-timestamp, What-hash).

3.4 Storage Area

The volume of the digital evidence is growing and increasingly varied in terms of the file size. Storage of digital evidence is not just ordinary storage, but it should have technical specifications that comply with the provisions of the law, for example, the ability of data storage, data maintenance as well as data recovery [40]

As any other storage, digital evidence storage should pay attention to a number of criteria, namely: read/write data technology applied in the storage, strength and durability of the storage, as well as its architecture. The solution for storage can refer to the storage technology that has been available, for instance, as developed by Rimage [41]. Besides, the solution for storage can also be through the application of some topology storages as done by [40] through the implementation of NAS (Networked Attached Storage) and SAN (Storage Area Network) in a concept called DECL (Digital Evidence Storage Locker).

A number of studies have been done to optimize the use of NAS and SAN storage solutions, as well as High Performance Storage Network (HPSN) by [42] and High Availability Storage Network (HASN) by [43]. Digital forensics activities and digital chain of custody require storage solution that supports the process of storage and access to digital evidence. As a result, establishing the storage model solution according to the needs of the digital forensics activities and chain of custody is an area of research that can be studied further.

According to [41], almost all crime activities at this time will include digital components. Therefore, it is no wonder that every 18-24 months, digital evidence stored in the storage will double than before. According to [44], depending on the type of institution and company, in general the amount of data stored doubles in 1-2 years. On the other hand, considering investigation process until the end of judicial proceedings requires a very long time, then the storage of digital evidence must also be maintained and retained for a long period.

In practice, the HDD (Hard Disk Drive) is often used as a standard for data storage for a long period. In spite of that, according to [41], the technology on HDD is not intended to serve as a digital data storage solution for a very long period (HDD capacity ranges from 5 to 6 years only). In addition, HDD also still has a number of constraints in terms of the possibility of failure in the process of storage and data reading that will potentially corrupt data. Therefore, a solution offered by Rimage is a storage technology using DVD/BD (Blue-ray Disc) that will guarantee the concept of secure data preservation, reliable data retrieval and readability.

3.5 Infrastructure Security

Meanwhile, for the infrastructure of chain of custody, [11], [45], [46] have offered a solution for the secure infrastructure for digital evidence handling, that is, by establishing the concept of valid evidence based on a hardware-based security using a TPM (trusted platform module).

Secure infrastructure is very important especially for the handling of digital evidence in cases where the digital data are taken directly from the device. One example is the application of Traffic Monitoring System in particular areas that are mostly done in several major cities. Trusted Computing and Trusted Platform Modules serve as trustworthy based computing platforms to the solution. Another approach to infrastructure solution is given by [47] i.e. through secure logging protocols for the benefit of digital evidence handling.

Another attempt to provide a solution to the handling of chain of custody is the application of RFID technology to perform monitoring and data record keeping on physical or electronic evidence. This is as developed by [48] via EPC global approach to Architecture Frameworks.

3.6 Access Control

Integrity and credibility of evidence on digital chain of custody are determined by the concept of access control applied to it. Therefore, there is a necessity for mechanisms to protect digital evidence that supports the integrity, confidentiality and authenticity of the digital evidence. In this case, according to [49], in the policy region, access control indicates whether a subject (e.g. processes, computers, users, tools etc.) is allowed or not to perform an operation (such as read, write, execute, delete, search etc.) on an object (e.g. database, table, file, service, resource etc.). While according to [50], access control is a mechanism that gives authorization only to the legitimate users to be able to use the data and existing resource.

The application of access control on digital evidence has previously been proposed by [51] through the implementation of cryptographic techniques to model the mechanism of hierarchical access control. In this case, partial mechanism and full supervision are developed to describe rights and functions that are different between the investigator who directly handles digital evidence and other law enforcement agencies that perform supervisory control against the use of such evidence. The solution given in the study is focused on the efforts to carry out control and protection toward access to digital evidence through the application of AES cryptography on different security levels.

In terms of computer security, according to research by [52] an attack on the system can be because of inconsistencies the application of access control. Thus, in the research, an algorithm is built to detect any inconsistency in access control on a firewall as part of IDS (Intrusion Detection System) system

In relation to this access control issue, based on the existing literature, there has been no study that specifically refers to the application of access control concept for digital chain of custody. However, to know the importance of access control concept for digital chain of custody can refer to the importance of access control for medical record. In this case, a number of studies have been done on the concept of access control to protect integrity of the medical records of patients in a Healthcare Information System. In addition, a study by [53] about access control model for a collaborative environment can be a valuable input to construct an appropriate model of access control in the scope of digital chain of custody.

4. DISCUSSION

Business model approach, as can be seen in Figure 2, can give an idea of the importance of the chain of custody in a process of digital forensics. In addition, through this approach, to understand the importance of and the position of the chain of custody in the digital forensics also can be done through a modelling approach. In this case, [54] has introduced the general model and the conceptual model of digital forensic. Unfortunately, on both the proposed model is not visible the role and position of the digital chain of custody in digital forensics. For that, refers to the model of the proposed general model and the conceptual model of digital forensics with include the chain of custody as one of the elements of importance. A new proposed model are:

General Model DF = {I, S, D, E, A, R}

I = Identification process, S = Storage for digital evidence, D = Documentation of digital evidence, E = Exploration, A= Analysis data and R = Reporting.

Conceptual Model DF = {Pi[Tj, Lk], DE}

Pi = A series of digital forensics process, Tj = Technique, methods, approach, system, tools. Lk = Legal principle, DE = Digital Evidence.

Both of these models suggests that the chain of custody is an inseparable part of the activity of digital forensics. On the general model of the chain of custody is represented by D while in the conceptual model are represented by Lk and DE.

Based on the review, the attempts to provide solutions to digital chain of custody are divided into two approaches, namely:

- The first approach is using information container as a solution that allows to save a number of metadata in the form of specific forensic format. This approach is as committed by [30], [33].
- The second approach is through formal knowledge representation with XML, ontology and semantic web solution to store information metadata. This approach is as committed by [2], [23]. DEB (Digital Evidence Bags) expressed by Turner [12] as a container for loading some information such as crime scene artifacts, metadata, information integrity, access, and audit records is one of the chain of custody solutions using XML approach. Then with the addition of a Tag Integrity File on the concept of DEB Turner, [13] develops a new concept known as Sealed Digital Evidence Bags (SDEB).
- The third approach is a combination of container information and knowledge representation as expressed by [37] in XeBag.

In addition, if the handling of chain of custody has the same point of view with the law enforcement regulations prevailing in Indonesia, at least there are four key aspects of the handling of chain of custody, namely, storage, registration and record-keeping, control access to the evidence, as well as security guarantee of the storage and analysis process. Based on this perspective, the previous explanation about researches in the field of a digital chain of custody can be mapped through the diagram in Figure 3.

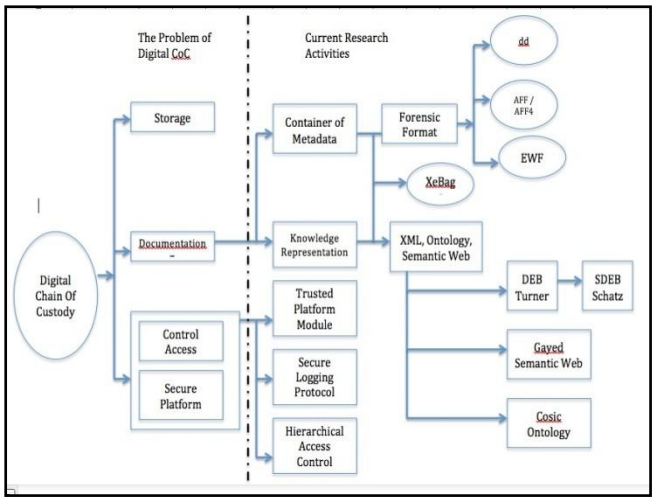

Figure 3. Problem and Chain of Custody Research Area

Based on the review above, in principle there are a few things that still rise a challenge in researches about the chain of custody, namely:

- Business model for handling digital chain of custody. The first step to build the solution is to fix the business model of digital forensics. The business model will give an idea on how the relation and order of interactions process between actors in digital forensics activity. Further researches can be done by referring to input from the practitioners in digital forensics either from the law enforcement agencies or from the private actors.
- Storage of digital evidence. The issue is how to implement and build storage infrastructures to fulfil the needs as well as meet the criteria set by the law. Therefore, things that can be done are identifying the criteria for digital evidence storage and mapping vendor products that meet the criteria or storage model development through the implementation of NAS and SAN concept.
- The concept of metadata information record keeping on chain of custody. One way that can be developed is building a new logging model based on a previously built model namely the concepts of DEB Turner and SDEB from Schatz. The other thing that can be done is to integrate record-keeping concept with DEMC concept from Cosic.
- A secure Infrastructure. Digital forensics and handling chain of custody should be supported by a secure infrastructure. That is why, given the mobility characteristics of the officers, a method that can be applied is implementing SSL VPN concept as a means of access to the server and storage. This can be supported by the application of trusted computing-based and access control concepts as a medium for the secure platform. The incorporation of SSL VPN and Trusted Computing based brings a challenge for research about infrastructure on digital chain of custody.
- Establishing a framework for handling digital chain of custody in a comprehensive manner. The framework will provide an overview of solutions ranging from storing process of digital evidence until interaction process among business actors in a chain of custody along with the record keeping.

In this study, an overview of digital forensics activities requiring digital chain of custody mechanism refers to the legal documents Regulation of the Chief of National Police No. 10/ 2010 and the regulation system prevailing in Indonesia that contains the settings of evidence, such as Law No. 8/ 2008 about Information and Electronic Transaction. Referring to this document, in practice, based on the experience in handling cases and interacting with digital forensics practitioners, the activities generally performed at this time among the digital investigators are limited to imaging, examination/exploration, analysis and reporting the findings of evidence. Activities that support the implementation of the digital chain of custody still have not been taken into account by the digital investigator. Chain of custody is only applied for the sake of physical evidence documentation, but not on digital evidence. Interaction process with digital evidence is not well documented. In addition to the lack of tool and framework that support digital chain of custody, there is also no mutual agreement related to the management of digital evidence.

This is certainly a challenge for researchers to establish a mechanism of the digital chain of custody so that the integrity and credibility of the evidence can still be guaranteed. Then, there is no presumption against digital evidence submitted by investigators because all parties have achieved compliance with the standard handling of evidence, in general. Therefore, one research area for digital chain of custody is to provide a more comprehensive solution through unity in the existing solution and the concept of business model, the concept of record and storing information, as well as security and access control. This is what underlies [55] to propose a solution known as Digital Evidence Cabinets. The solution offered is like a new approach to dealing with digital evidence and documentation of a digital chain of custody. This model is built through the approach of business model concept that corresponds to the legal aspects, development of a reliable storage model, development of record keeping and documentation concept based on the Digital Evidence Bags and Digital Evidence Sealed Bags, as well as support for infrastructure based on trusted computing. Though the proposal is still in the early stages, but in principle the solution offered has enriched the studies about digital chain of custody.

5. CONCLUSION AND FURTHER RESEARCH

Disclosure of cybercrime can be done through a series of digital forensics activities. The important elements in these activities are the integrity and credibility of the digital evidence in a single procedure for handling the chain of custody (or chain of evidence). In this case, the handling of evidences either digitally or conventionally is supposed to use the same concept. However, due to the specific characteristics of digital evidence, the handling of chain of custody for digital evidence is not the same in practice. The difficulties found are the handling of digital evidence turns out to be more difficult than of physical evidence. For this reason, a system environment that supports the implementation of handling digital chain of custody is required by the law-enforcement institution to support the handling and investigation of cybercrime.

This paper discusses the problems faced in the digital chain of custody as well as various points of view the contributions of researchers in providing solutions to these problems. There are still many problems that must be resolved in order for the digital chain of custody solutions can truly serve as an aggregation process of handling evidence that will support the process of investigation by law enforcement.

Based on the description in the paper, the next research step is supposed to do further study by exploring a number of issues that have been identified in particular to the concept of record and information storage as well as security and access control scheme in a digital chain of custody system.

Based on the description that has been conducted in this paper the next research steps that can be done is to do further studies to explore a number of issues that have been identified as particularly about concept of the writing and storage of metadata information as well as security and access control scheme in a digital chain of custody system.

6. REFERENCES

[1] G. Giova, "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems," *Int. J. Comput. Sci. Netw. Secur.*, vol. 11, no. 1, pp. 1–9, 2011.

[2] J. Ćosić, Z. Ćosić, M. Bača, J. Cosic, G. Cosic, and M. Baca, "An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence," *JIOS*, vol. 35, no. 1, pp. 1–13, 2011.

[3] UNODC, "Comprehensive Study on Cybercrime," New York, USA., 2013.

[4] CSIC, "Net Losses : Estimating the Global Cost of Cybercrime," Washington DC, 2014.

[5] PwC, "US cybercrime: Rising risks, reduced readiness," 2014.

[6] RSA, "THE CURRENT STATE OF CYBERCRIME 2014 An Inside Look at the Changing Threat Landscape," 2014.

[7] T. Widodo and Y. Prayudi, "Model Digital Forensic Readiness Index (DiFRI) untuk Mengukur Tingkat Kesiapan Insititusi," in *Seminar Nasional Teknologi Informasi (SNTI)*, 2013.

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

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

[10] Kepolisian Negara RI, "Perkap Tata Cara Pengelolaan Barang Bukti," Jakarta, 2011.

[11] J. Richter and N. Kuntze, "Securing Digital Evidence," in *Fifth International Workshop on Systematic Approaches to Digital Forensic Engeneering*, 2010, pp. 119–130.

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

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

[14] C. P. Grobler, C. P. Louwrens, and S. H. Von Solms, "A framework to guide the implementation of Proactive Digital Forensics in organizations," in *International Conference on Availability, Reliability and Security*, 2010, pp. 677–682.

[15] O. Ademu, C. O. Imafidon, and D. S. Preston, "A New Approach of Digital Forensic Model for Digital Forensic Investigation," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 12, pp. 175–178, 2011.

[16] J. Shah and L. G. Malik, "An Approach Towards Digital Forensic Framework for Cloud," in *IEEE International Advance Computing Conference (IACC)*, 2014, pp. 798–801.

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

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

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

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

[21] J. Cosic and M. Baca, "(Im) Proving Chain of Custody and Digital Evidence Integrity with Time Stamp," in *MIPRO,Proceedings of the 33rd International Convention International Conference*, 2010, no. Im, pp. 1226 – 1230.

[22] S. Dossis, "Semantically-enabled Digital Investigations," Master, Department of Computer and Systems Sciences, Stockholm University, Swedia, 2012.

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

[24] S. Raghavan, "Digital forensic research: current state of the art," *CSI Trans. ICT*, vol. 1, no. 1, pp. 91–114, Nov. 2012.

[25] Damshenas, A. Dehghantanha, and R. Mahmoud, "A Survey on Digital Forensics Trends," *Int. J. Cyber-Security Digit. Forensics*, vol. 3, no. 4, pp. 209–234, 2014.

[26] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, and N. F. Binti, "Digital Forensic Trends and Future," *Int. J. Cyber-Security Digit. Forensics*, vol. 2, no. 2, pp. 48–76, 2013.

[27] D. Schum, G. Tecuci, and M. Boicu, "Analyzing Evidence and its Chain of Custody : A Mixed-Initiative Computational Approach," *Int. J. Intell. Counterintelligence*, vol. 22, no. 2, pp. 298–319, 2009.

[28] P. G. Bradford and D. A. Ray, "An Online Algorithm for Generating Fractal Hash Chains Applied to Digital Chains of Custody," Jul. 2013.

[29] S. Saleem, O. Popov, and R. Dahman, "Evaluation of Security Methods for Ensuring the Integrity of Digital Evidence," in *International Conference on Innovations in Information Technology*, 2011, pp. 220–225.

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

[31] Nandhakumar and U. Agarwal, "Use of AFF4 'Chain of Custody'- Methodology for Foolproof Computer Forensics Operation," *Int. J. Commun. Netw. Syst.*, vol. 1, no. 1, pp. 49–57, 2012.

[32] Cohen and B. Schatz, "Hash based disk imaging using AFF4," *Digit. Investig.*, vol. 7, pp. S121–S128, Aug. 2010.

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

[34] B. Schatz and M. Cohen, "Refining Evidence Containers for Provenance and Accurate Data Representation," *IFIP Adv. Inf. Commun. Technol.*, vol. 337, pp. 227–242, 2010.

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

[36] T. F. Gayed, H. Lounis, and M. Bari, "Cyber Forensics : Representing and (Im) Proving the Chain of Custody Using the Semantic web," in *COGNITIVE 2012 : The Fourth International Conference on Advanced Cognitive Technologies and Applications*, 2012, no. Im, pp. 19–23.

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

[38] W. Yi, "Extraction and Supervison Of Data Of Chain Of Custody in Computer Forensics," *China Communication*, vol. 12, 2010.

[39] 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.

[40] M. Davis, G. Manes, and S. Shenoi, "A Network-Based Architecture For Storing Digital Evidence," in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi, Eds. Springer New York, 2005, pp. 33–42.

[41] Rimage Corporation, "Digital Evidence Preservation and Distribution : Updating the Analog System for the Digital World," 2012.

[42] X.-G. Yu and W.-X. Li, "A New Network Storage Architecture Based on NAS and SAN," in *10 th International Conference on Control, Automation, Robotics and Vision*, 2008, no. December, pp. 2224–2227.

[43] D. Han and F. Feng, "Research on the High Availability Storage Network," in *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, 2008, pp. 1–4.

[44] K. Engelhardt, "Secure Data Storage - An Overview of Storage Technology," 2008.

[45] Kuntze, C. Rudolph, T. Kemmerich, and B. Endicott, "Chapter 1 SCENARIOS FOR RELIABLE AND SECURE DIGITAL EVIDENCE," in *Ninth Annual IFIP WG 11.9 International Conference*, 2013, pp. 1–13.

[46] N. Kuntze, C. Rudolph, and I. Technology, "Secure Digital Chains of Evidence," in *SADFE (Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering)*, 2011, pp. 1–8.

[47] R. Accorsi, "Safekeeping Digital Evidence with Secure Logging Protocols : State of the Art and Challenges," *2009 Fifth Int. Conf. IT Secur. Incid. Manag. IT Forensics*, no. 1, pp. 94–110, 2009.

[48] C. Chen and C. Huang, "Applying EPCglobal Architecture Framework for Criminal Physical Evidence Safety Monitoring System," in *TANET (Taiwan Academics Network Conference)*, 2013, pp. 1–6.

[49] . Thion, "Access Control Models," in *Cyber Warfare and Cyber Terorism*, IGI Global, 2008.

[50] Samarati and S. D. C. di Vimercati, "Access Control: Policies, Models, and Mechanisms," in *Foundation Of Security Analysis*, Springer Berlin Heidelberg, 2001.

[51] C. Hsu and Y. Lin, "A Digital Evidence Protection Method with Hierarchical Access Control Mechanisms," in *IEEE International Carnahan Conference on Security Technology (ICCST)*, 2011, pp. 1–9.

[52] D. Zhang, "The Utility of Inconsistency in Information Security and Digital Forensics," in *IEEE International Conference on Information Reuse and Integration (IRI)*, 2011, pp. 141 – 146.

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

[54] A. Hellany, H. Achi, and M. Nagrial, "An Overview of Digital Security Forensics Approach and Modelling," in *2008 International Conference on Computer Engineering & Systems*, 2008, pp. 257–260.

[55] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "Digital Evidence Cabinets : A Proposed Frameworks for Handling Digital Chain of Custody," *Int. J. Comput. Appl.*, vol. 109, no. 9, pp. 30–36, 2014.