The Management of Physical Evidence and Chain of Custody (CoC) in Digital Forensic Laboratory Storage

Tino Feri Efendi

Universitas Islam Indonesia Yogyakarta, Indonesia
Corresponding email: tinoferit@yahoo.co.id

Abstract:

Computer crime has 2 types of evidence, namely: physical evidence and digital evidence. Storage on physical evidence requires a special space that can hold physical evidence. However, a system that can store and manage physical evidence is needed.The current problem is the absence of a concept of storing physical evidence and its documentation (Chain of Custody). Management of Physical Evidence is proposed as a solution to solve the problem. This concept is in the form of a Physical Evidence Management System and Chain of Custody by taking the analogy of a Data Inventory. Problems with Physical Evidence Management require a Management System for Physical Evidence that is suitable for use in the UII Digital Forensics Laboratory. This research has successfully implemented the concept of Data Inventory. It is expected that with the concept of Physical Evidence Management the control of physical evidence and all activities related to it can be maintained and documented properly.

Keywords:

physical evidence; chain of custody; inventory data

JEL: O30, O33, O38

INTRODUCTION

Investigation and investigation of criminal acts is a major responsibility carried by an investigator. The outcome is proof of a criminal offense in court and obtaining a decision that has permanent legal force. However, the problem arises when the evidence of the crime is not strong, and cannot form the judge's conviction that a criminal act has occurred, which for the Judge will be the basis for the conviction. Electronic evidence itself is tangible evidence or in other words has a tangible form such as: computers, smartphones, tablets, laptops and other storage devices. Electronic evidence found at the crime scene will be confiscated for further investigation by the PPBB (Evidence Management Officer). Handling of digital evidence must be done properly by paying attention to 5 aspects, namely: admissible, authentic, complete, reliable, believable so that digital evidence can be presented in court (Prayudi & Azhari, 2015).

The problem that has arisen so far is that the evidence is not well documented and coordinated according to the case at hand. This can weaken the evidence of a case based on digital evidence in court. Some things that can cause evidence to become unacceptable are the process of extraction or collection of evidence that is unprofessional, there is no match between the case and the evidence presented, or is not well documented between the case being handled with the evidence obtained at the scene.

Based on Ashcroft, Daniels, & Hart, (2004) in the National Institute of Justice report, the Chain of Custody form document contains a history or chronology of the journey of evidence containing complete information such as subjects / objects involved in collection and analysis activities, date / time and place collection and analysis, full names and nicknames of victims and perpetrators, agency names and full description of evidence. There are 4 things that must be considered in handling Chain of Custody (Widatama, et al., 2018), namely: Flexibility and capability in the chain of custody documentation, Interoperability between evidence obtained with the chain of custody, Security in the chain of custody documentation, Chain making of custody must be understood by everyone, especially when the case is brought to court.

One of the solutions is to create a management information system that can store physical evidence data as well as case data for later raised in the form of chain of custody documentation. The stored data will be stored in a DBMS (Database Management System), namely SQLite. The purpose of using this type of DBMS is because SQLite is in the form of files so that it can be transferred to other computers quickly without the need to access the database server (Bhosale, et.al. 2015).

The result of this research is the creation of a management information system that can store case data and physical evidence data obtained from the crime scene. In addition to storing data, this management information system can also display output in the form of a chain of custody document between physical evidence and the case being handled.

LITERATURE REVIEW

Digital Evidence

Digital forensics and digital evidence are related, but both have different definitions. Digital forensics is a method that can be explained scientifically and can be proven. The purpose of this digital forensic activity is to maintain, collect validate, identify analyze, interpret, document and present documented digital evidence in the form of chains of custody to be presented in court (Morioka & Sharbaf, 2016). In digital forensics procedures, there are basic procedures that are often used, namely: collection of evidence (collection), treatment of evidence (preservation), verification, analysis, interpretation, documentation and presentation of results in court (presentation).

Another opinion about digital forensics procedures, that in general there are 4 main processes in digital forensics, namely: collection, examination, analysis and reporting (Dogan & Akbal, 2017). Following is the process of digital forensics.

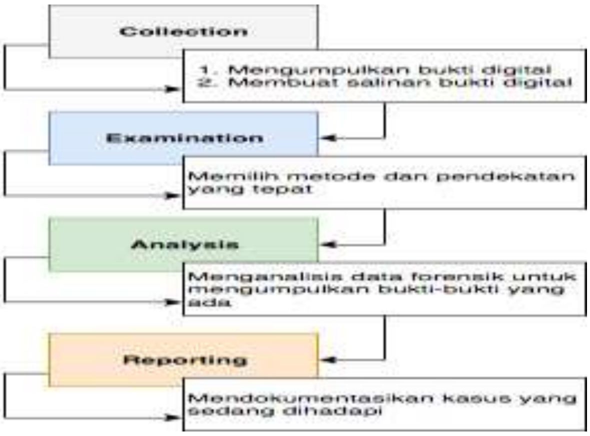

Collection
1. Mengumpulkan bukti digital
2. Membuat salinan bukti digital
Examination
Memilih metode dan pendekatan yang tepat
Analysis
Menganalisis data forensik untuk mengumpulkan bukti-bukti yang ada
Reporting
Mendokumentasikan kasus yang sedang dihadapi

Figure 1 Main Process of Digital Forensics

The following is an explanation of the main processes in digital forensics in Figure 1.

- Collection, digital evidence collected and carried out the imaging process.
- Examination, searching and determining methods that aim to test digital evidence.
- Analysis, a step to analyze which aims to find digital evidence that is compatible with the information needed by judicial or justice authorities.
- Reporting, the preparation phase of documentation to be submitted to court authorities.

While the definition of digital evidence is a trail that is wanted or undesirable originating from changes in digital data on electronic devices (Harbawi & Varol, 2017). Based on the source, digital evidence is divided into 2 categories (Marshall, 2009), namely closed system and open system. Closed system is a system that was once connected to the internet.

The Concept of a Digital Evidence Storage Cabinet

The emergence of the concept of digital evidence storage cabinets is based on problems in handling digital evidence that deals with a number of things, namely: business models of the parts that deal directly with digital evidence, storing digital evidence metadata information as well as access control and security of digital CoC. This concept was introduced by Prayudi et al in his study entitled Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody (Prayudi, et.al., 2014). In his research mentioned that the digital evidence storage cabinet is a system created for handling the CoC of any digital evidence that has been obtained. This concept is built on 3 approaches, namely: Digital Evidence Management Frameworks, digital evidence bags and security.

Digital Evidence Bag

Digital Evidence Bag (DEB) is a storage of digital information from all electronic data sources (Turner, 2006). In this digital evidence bag, 4 tag files will be recorded, namely: header, evidence units, footer and TCB (Tag Continuity Blocks). The header contains information on the officer conducting the investigation, when the DEB was made and a description of what, where, and when the digital evidence was obtained. This header information written, shortened by dividing it into 4 categories: labels (file name, path, origin description, file attributes, commands), timestamps (last modified / completed, accessed, created / started / commenced), numeric (physical sector, logical cluster number, logical file size, physical file size) and integrity (MD5, SHA).

Evidence units are used to store all digital evidence stored on the DEB. Every digital evidence stored on DEB has index files, hash functions and bags. The footer section on the DEB is used to store digital proof numbers that have been stored on the DEB. Next the DEB is sealed with the hash function found on the digital proof.

Information Systems

Information systems can be interpreted as a framework that coordinates human resources or computers to turn input into information, in order to achieve goals. An online inventory management system can do better monitoring. Weak supervision is a bad impact on management so that reporting of receipt or release of goods and supervision of the use of goods is hampered. The purpose of this study is to create an inventory management information system using the EasyUI Framework that can be accessed and monitored online. The system design uses Unified Modeling Language, PHP programming language and MySQL database. This research produces an inventory management information system that provides stock information in real-time and reports on the semester of receipt and release of goods, so that the process of reporting and controlling stock information can be done well (Bari & Kasmawi, 2016).

MySQL

MySQL is a type of database server that uses SQL (Structured Query Language) as the basic language for accessing its database. MySQL is a type of Relational Database Management System (RDBMS), so that terms such as tables, rows and columns are used in MySQL. MySQL is very popular among software developers because MySQL is a free and fast database server. In addition, adequate support from companies and communities makes MySQL a preferred database server and is included in the category of a reliable database (M. Yunus, 2016).

DBMS

Database Management System, namely SQLite. SQLite is an in-process library that implements a standalone transactional SQL database engine, without configuration, without servers. The source code for SQLite is in the public domain and is free for personal and commercial purposes. SQLite has ties to several programming languages such as C, C ++, BASIC, C #, Python, Java and Delphi. The COM (ActiveX) wrapper makes SQLite more accessible to scripted languages on Windows such as VB Script and JavaScript, thus adding the ability to HTML applications. It is also available in embedded operating systems such as iOS, Android, Symbian OS, Maemo, Blackberry and WebOS because of their small size and ease of use.

RESEARCH METHODS

The methodology in this research uses the literacy method in the form of a literature study developed through the creation of a physical evidence management concept, then the system is designed and implemented and then tested to obtain results.

RESULTS AND DISCUSSION

So that the problems encountered can be resolved, the results and difficulties found during the research process can be analyzed. The flow of research can be seen in Figure 2.

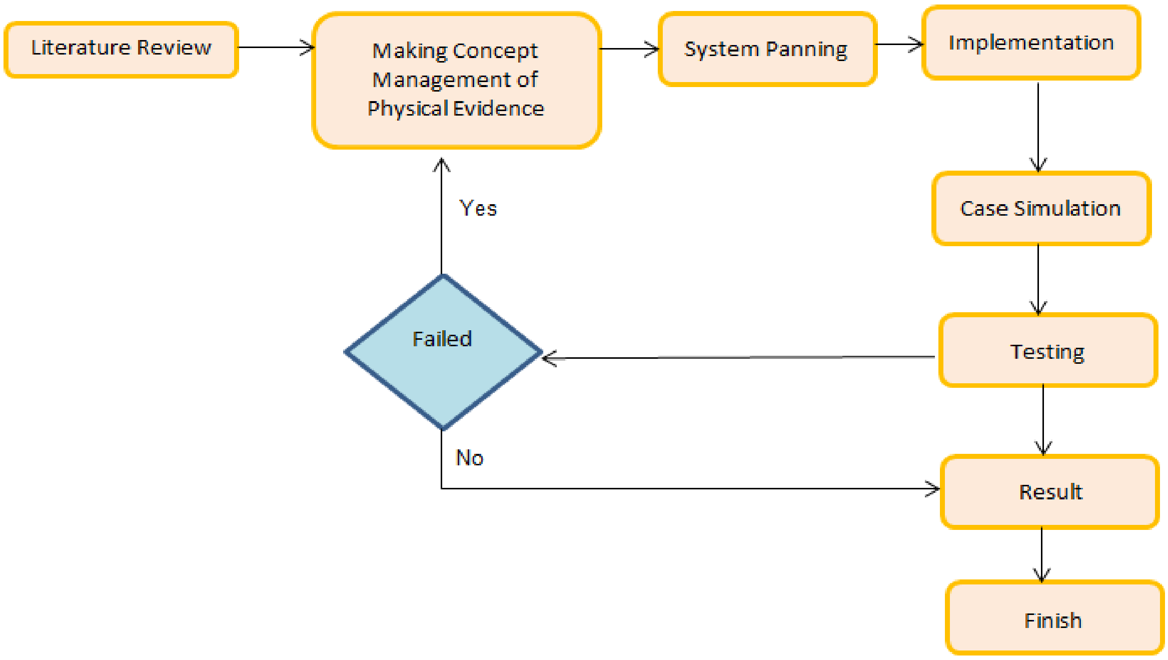


Figure 2. Research Flow

Literature review

Literature study is carried out in the first step to gather information relevant to the topic or problem to be studied. Sources of information in library research can be obtained through physical evidence that has a physical relationship with the problem to be studied, scientific journals and other sources of information that can be obtained through the internet. The information can also be obtained by attending scientific seminars that are often held by several universities.

This research requires library research to get all information about Management and Management of Physical Evidence and Chain of Custody (COC) in the Digital Forensic Laboratory Storage of digital evidence analogous to inventory data. In addition, theories are needed about the chain of custody in digital evidence, theories of handling digital evidence put forward by experts through their journals.

Distribution of Activities Against the System

The stages after the collection of information through the literature study stage are the stages of making the concept of management of physical evidence storage and Chain of Custody (Coc) in the Digital Forensic Laboratory Storage. The design of this concept starts with separating the distribution of authorization rights of people who interact with the control and management of the physical evidence. There are at least 3 actors who interact with the physical evidence management information system. The distribution of the first responder's authorization rights to the physical evidence inventory system related to the handling of evidence is explained through the use case in the picture as follows.

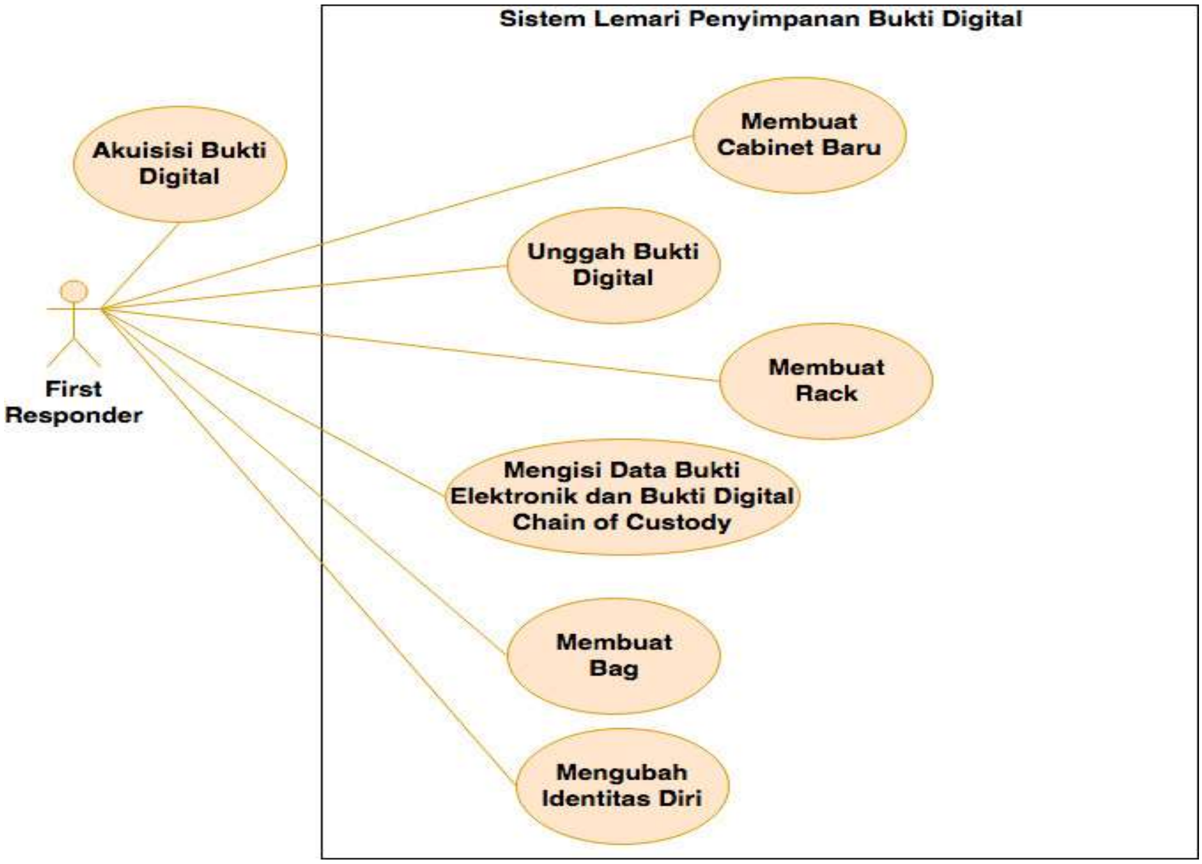


Figure 3. Use Case Authorization on First Responder

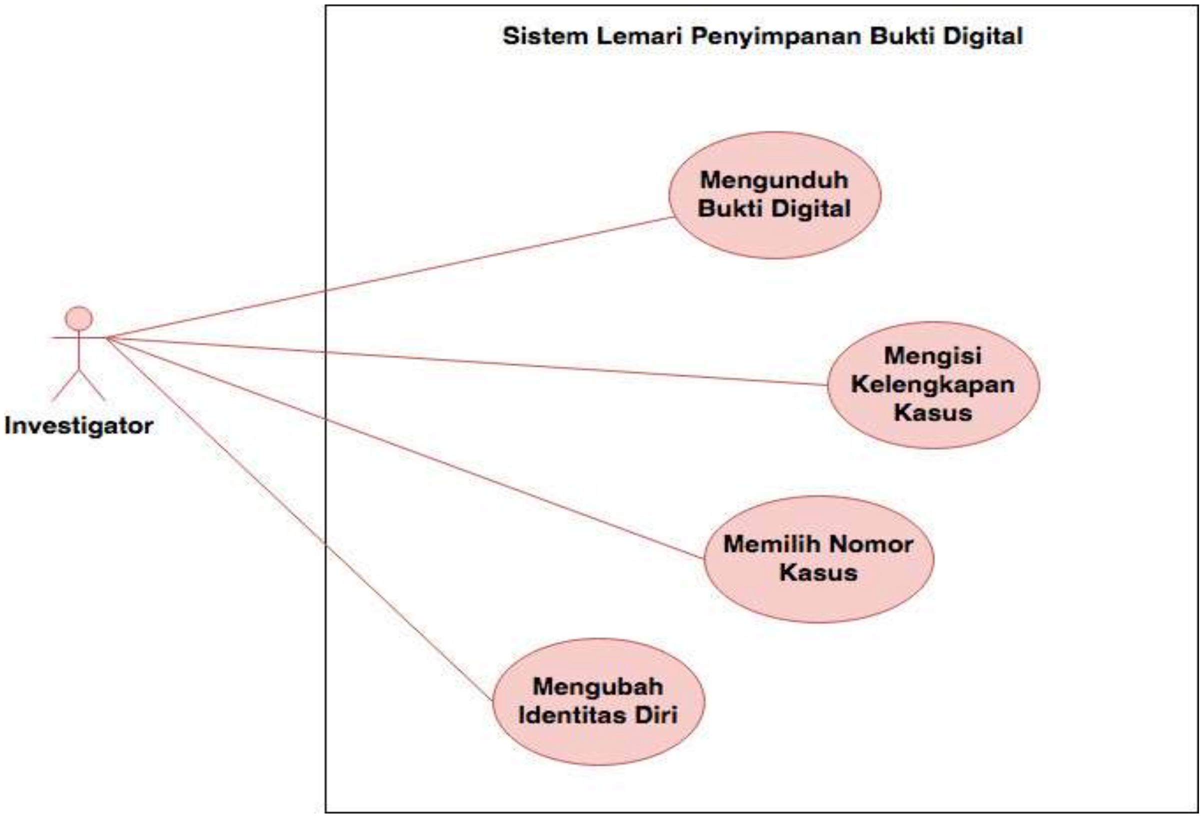


Figure 4. Use Case for Investigator's authorization

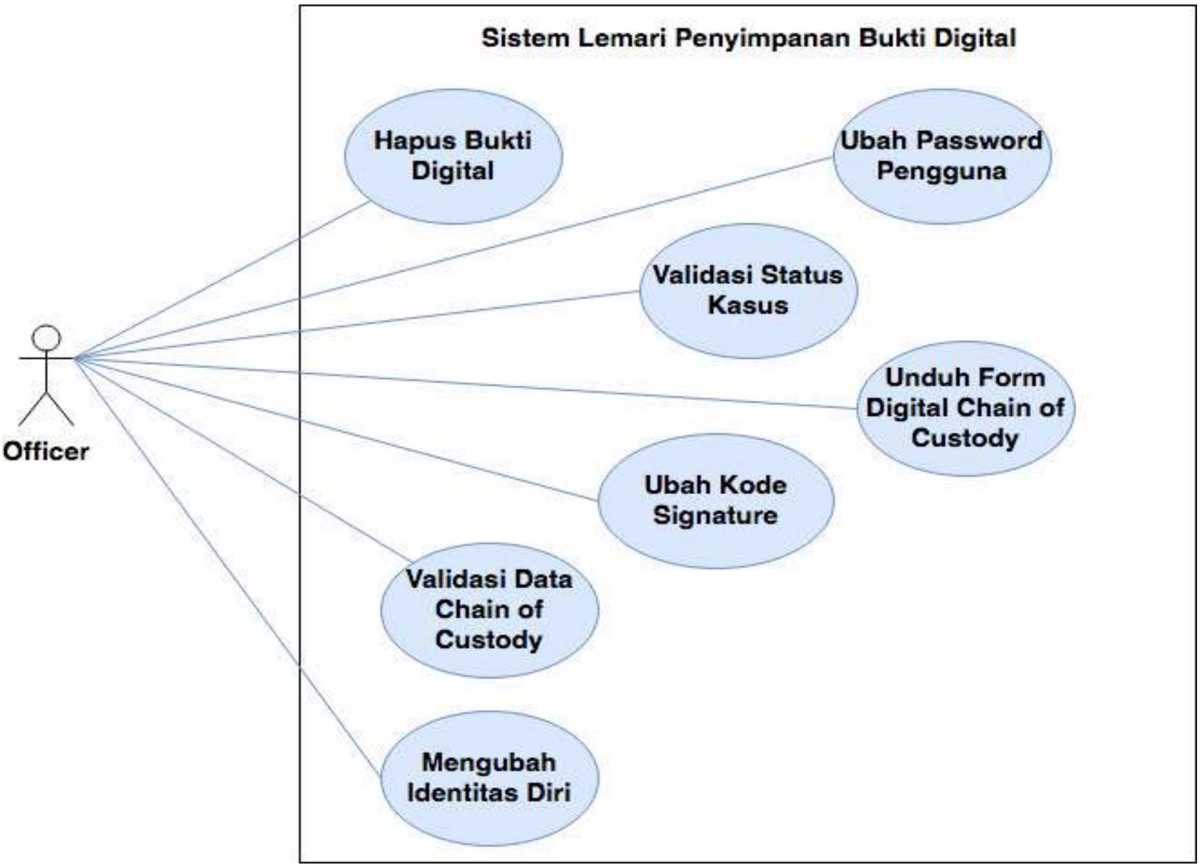


Figure 5. Use Case Authorization to Officer

The Concept of Making Physical Evidence Management

The flow of digital evidence storage in this concept is that when a first responder acquires digital evidence, he will store the digital evidence into a bag labeled with a name. The bag itself is stored in a rack in a particular cabinet. The structure of the concept of a digital proof storage cabinet can be seen in the image below.

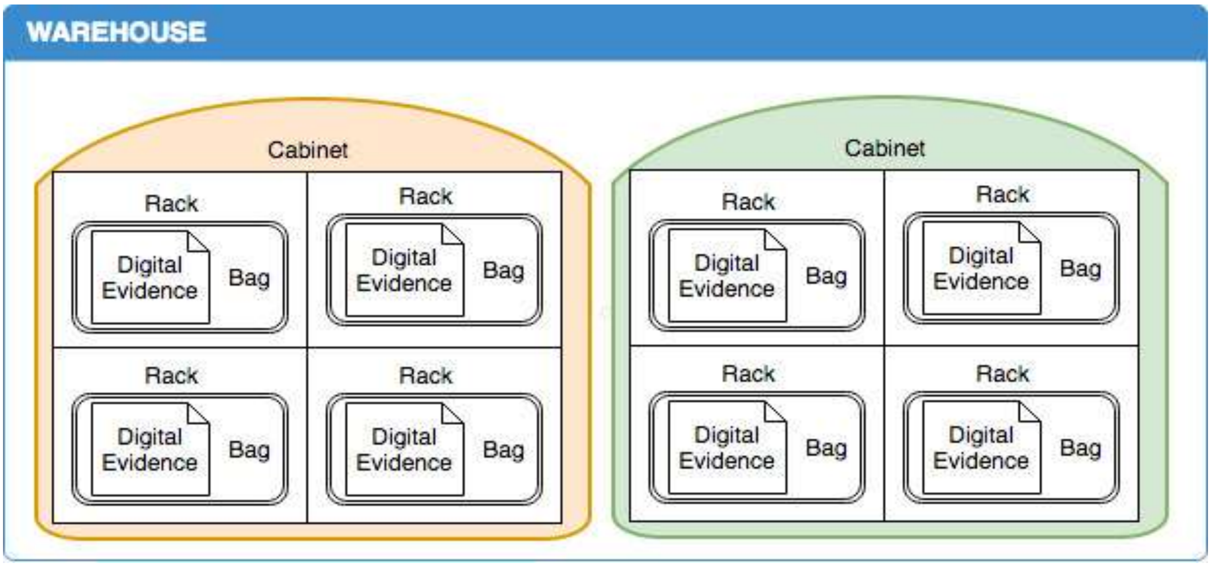


Figure 6. Structure of Physical Evidence Management

The concept of digital evidence storage cabinets is a development of physical evidence storage. The concept of digital proof storage cabinets must be able to store 2 important information, namely digital proof metadata and CoC.

System Planning

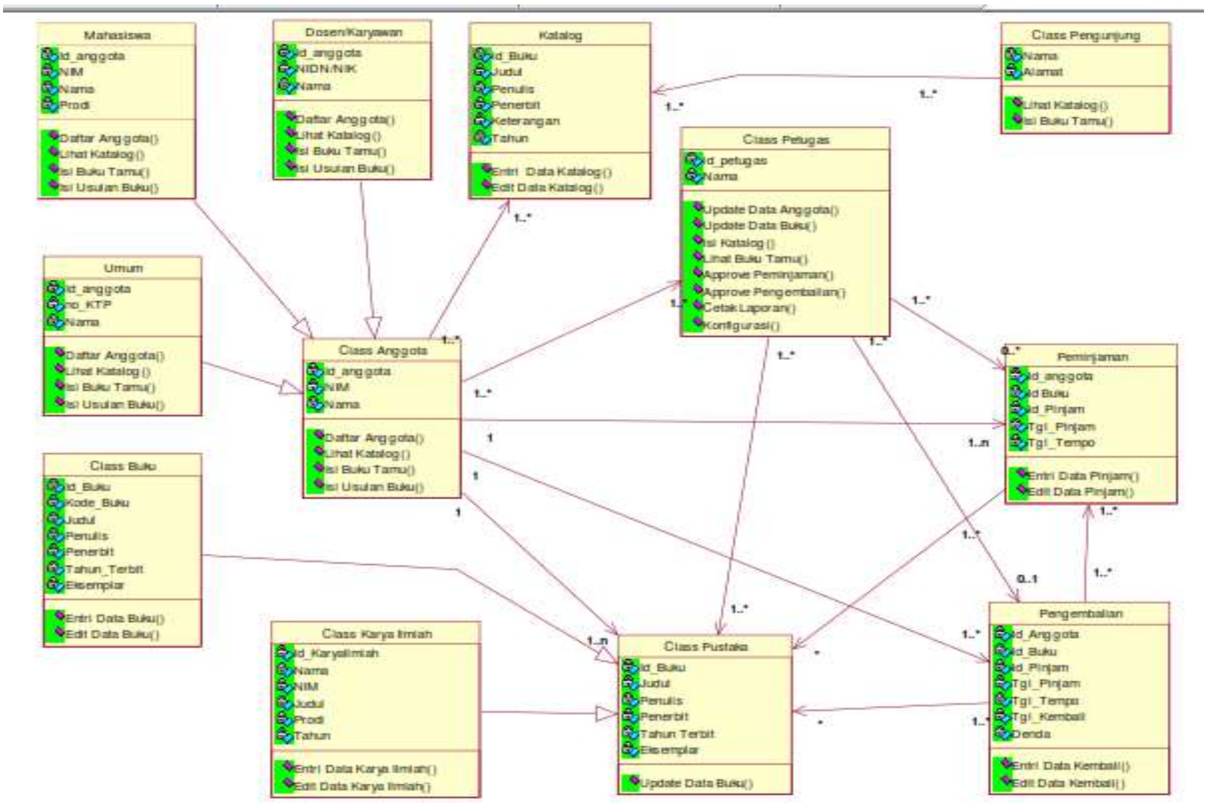
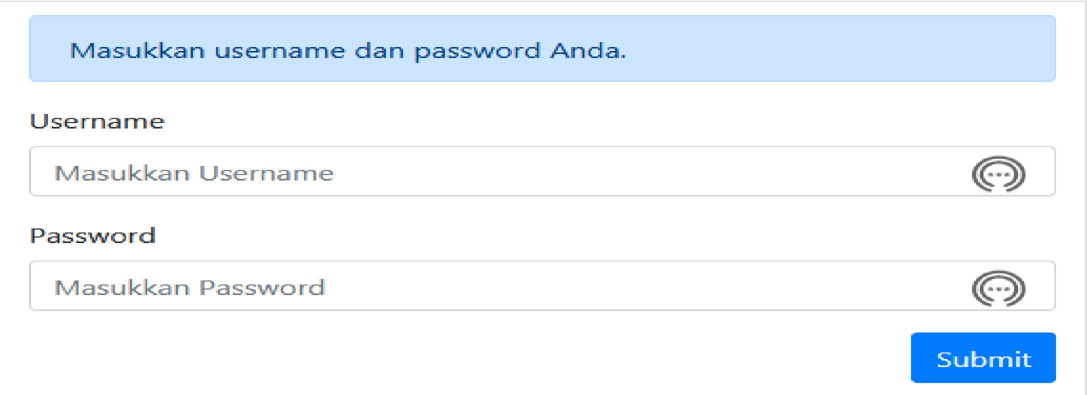


Figure 7. System Design

Implementation

The system is designed with a client server. The application design will be designed using Dreamweaver and the database is created using the Mysql database. An overview of this system will be presented using UML.


Masukkan username dan password Anda.

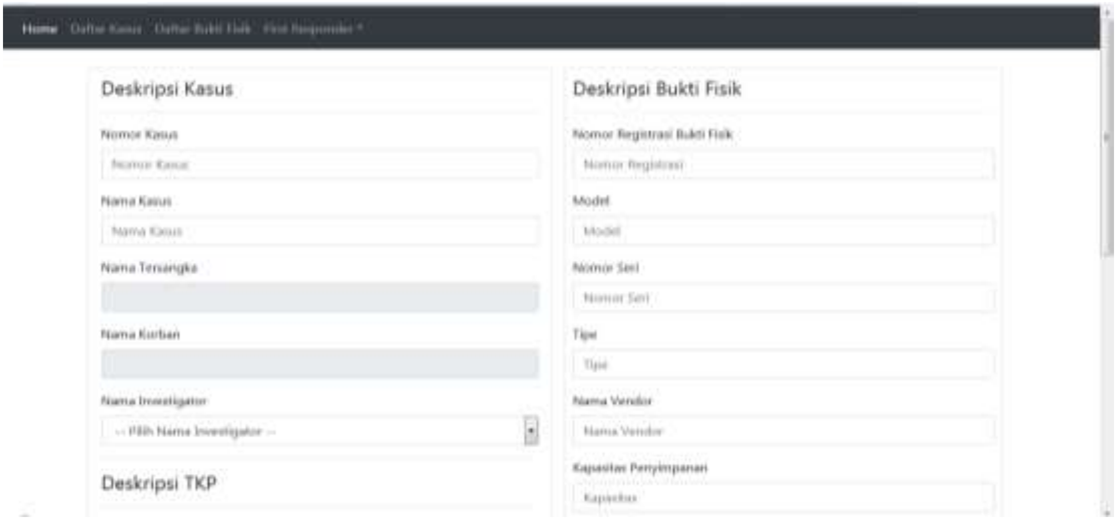
Username

Masukkan Username

Password

Masukkan Password

Figure 8. Home Display



Deskripsi Kasus

Nomor Kasus: Nomor Kasus

Nama Kasus: Nama Kasus

Nama Tersangka

Nama Korban

Nama Investigator: -- Pilih Nama Investigator --

Deskripsi TKP

Deskripsi Bukti Fisik

Nomor Registrasi Bukti Fisik: Nomor Registrasi

Model: Model

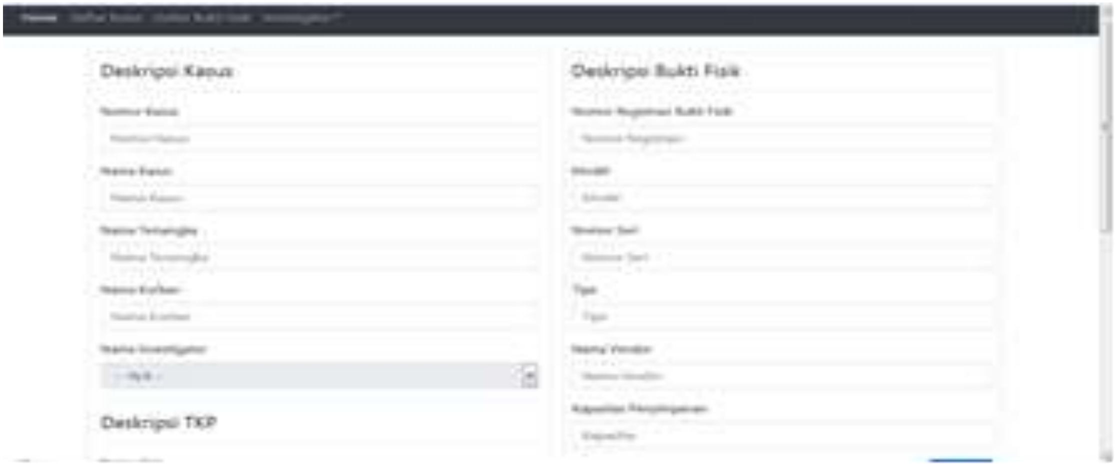
Nomor Seri: Nomor Seri

Tipe: Tipe

Nama Vendor: Nama Vendor

Kapasitas Penyimpanan: Kapasitas

Figure 9. First Responder



Deskripsi Kasus

Nomor Kasus: Nomor Kasus

Nama Kasus: Nama Kasus

Nama Tersangka: Nama Tersangka

Nama Korban: Nama Korban

Nama Investigator: -- N/A --

Deskripsi TKP

Deskripsi Bukti Fisik

Nomor Registrasi Bukti Fisik: Nomor Registrasi

Model: Model

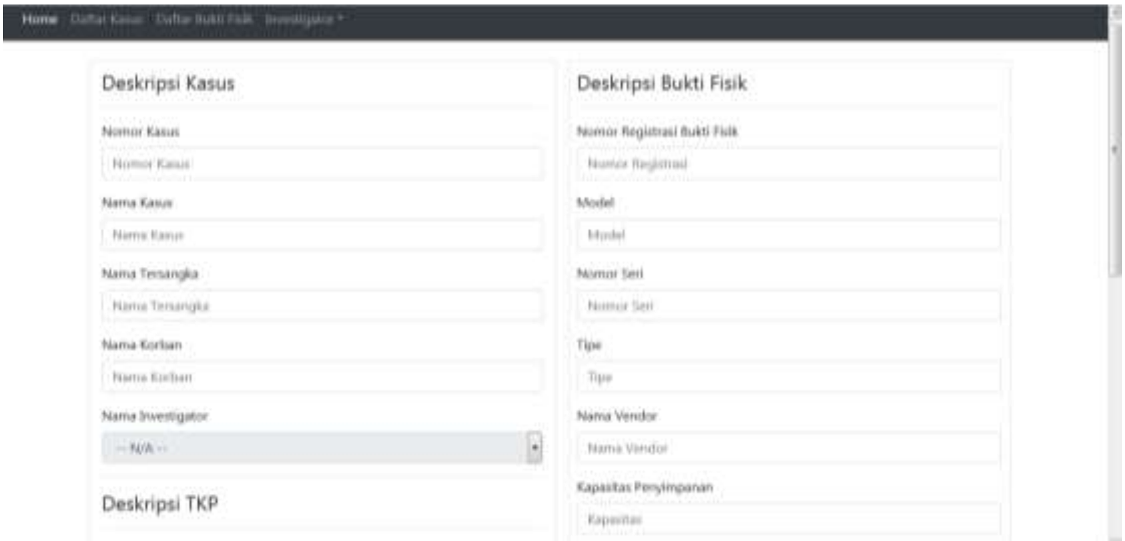
Nomor Seri: Nomor Seri

Tipe: Tipe

Nama Vendor: Nama Vendor

Kapasitas Penyimpanan: Kapasitas

Figure 10. Investigator Display



Deskripsi Kasus

Nomor Kasus: Nomor Kasus

Nama Kasus: Nama Kasus

Nama Tersangka: Nama Tersangka

Nama Korban: Nama Korban

Nama Investigator: -- N/A --

Deskripsi TKP

Deskripsi Bukti Fisik

Nomor Registrasi Bukti Fisik: Nomor Registrasi

Model: Model

Nomor Seri: Nomor Seri

Tipe: Tipe

Nama Vendor: Nama Vendor

Kapasitas Penyimpanan: Kapasitas

Figure 11. Officer Display

CONCLUSION

The results showed that this research had successfully implemented the concept of Data Inventory. It is expected that with the concept of Physical Evidence Management the control of physical evidence and all activities related to it can be maintained and documented properly.

REFERENCES

Bari, A., & Kasmawi, K. (2016). Sistem Informasi Manajemen Inventory Secara Online menggunakan Framework EasyUI. *INOVTEK Polbeng-Seri Informatika*, *1*(1), 78-86.

Bhosale, S. T., Patil, T., & Patil, P. (2015). SQLite: Light Database System. *International Journal of Computer Science and Mobile Computing*, 882-885.

Dogan, S., & Akbal, E. (2017, May). Analysis of mobile phones in digital forensics. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1241-1244). IEEE.

Harbawi, M., & Varol, A. (2017, April). An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In *2017 5th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-6). IEEE.

M. Yunus. (2016). Praktikum Sistem Basis Data (MySQL), STMIK Bumigora Mataram.

Marshall, A. M. (2009). *Digital forensics: Digital evidence in criminal investigations*. John Wiley & Sons.

Prayudi, Y., & Sn, A. (2015). Digital chain of custody: State of the art. *International Journal of Computer Applications*, *114*(5).

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2014). Digital evidence cabinets: A proposed framework for handling digital chain of custody. *International Journal of Computer Applications*, *107*(9).

Turner, P. (2006). Selective and intelligent imaging using digital evidence bags. *digital investigation*, *3*, 59-64.

Widatama, K., Prayudi, Y., & Sugiantoro, B. (2018). Application of RC4 Cryptography Method to Support XML Security on Digital Chain of Custody Data Storage. *International Journal of Cyber-Security and Digital Forensics*, *7*(3), 230-238.