khazanah informatika

Jurnal Ilmu Komputer dan Informatika

Design Thinking Method to Develop a Digital Evidence Handling Management Application

Erika Ramadhani [1]*, Amrullah Sidiq [1]
[1]Faculty of Industrial Technology, Department of Informatics
Universitas Islam Indonesia
Yogyakarta
*erika@uii.ac.id

Abstract - Handling digital evidence in forensics is a very crucial task. Incorrect handling can cause the evidence to become invalid as proof of a crime in court. The procedure of handling digital evidence, starting from its collection, usage, and storage, affects its acceptability in the judicial process. Therefore, a digital evidence management system becomes imperative for police researchers and investigators. This study aims at designing such a system using the design thinking method, which goes through five stages: empathy, definition, idea, prototype, and test. The result of the study is a web-based system prototype. The prototype user testing attains a system usability scale (SUS) value of 60. The SUS value means that the prototype is in the category of marginal low and indicates that the prototype does not meet the feasibility and needs improvement.

Keywords: digital forensics, digital evidence, digital evidence handling, design thinking

Article info: *submitted January 1, 2020, revised Fecruary 22, 2021, accepted September 25, 2021*

1. Introduction

Each country has a different system of jurisdictions. So with these differences, the way of handling evidence against digital data is also different. In Indonesia, there are two laboratories that are already popular in handling digital evidence, namely: the Indonesian Police Forensic Laboratory Center (Puslabfor Polri) and the Indonesian Islamic University's Center for Digital Forensic Studies (Pusfid UII). Currently, the two laboratories have implemented procedures for implementing digital forensics that are in accordance with digital forensics rules. However, each laboratory certainly has different rules in handling digital evidence. In Indonesia, there is no specific standard that addresses the handling of digital evidence. Every agency that has a digital forensics division will have a standard for handling digital evidence independently. So by looking at this situation, there is no uniformity in the handling of digital evidence in Indonesia. The absence of specific standards in the process of handling digital evidence sometimes makes it difficult for an investigator to determine which procedure is best to use.

Procedures in handling digital evidence need to be carried out in accordance with certain rules and standards. This is because a digital evidence must have the feasibility to be used as evidence in the realm of justice. Handling that is not in accordance with procedures can make the digital evidence unfit for use in trial. For example, in 2016 Indonesia was shocked by the case of cyanide coffee. The case at that time had evidence in the form of digital data, namely video data from CCTV at the scene. However, at that time digital forensic science was just developing in Indonesia, so the trial process and the process of investigating digital evidence seemed difficult in the process. One opinion is that this is because the court is not ready to accept digital evidence to be used as evidence. At that time, there was no full socialization of legal experts and courts on how to treat digital evidence. As a result, the authenticity of the evidence is questioned. This makes it more difficult to determine who the perpetrator is.

Another problem faced in the handling of digital evidence is that digital evidence is very easy to modify, so that the authenticity of the data may be lost along with the wrong treatment process for handling digital data [1]. So that it is easy to modify it, this is what causes the process of handling digital evidence to be more difficult to do compared to handling physical evidence [2]. Handling digital evidence according to rules and standards is very crucial. Research conducted by Matthew Braidd [3] states that digital evidence that can be used in the realm of trial must have five criteria: admissible, authentic, complete, reliable, and believable.

Then the research conducted by Schatz [4] states that there are two decisive aspects: the legal aspect and the technical aspect. Based on several explanations of these problems, in the process of handling digital evidence, special procedures are needed.

Currently, there are many procedures and standards in the handling of digital evidence, but it will not cover all investigators who fully understand the handling. sometimes the process of handling digital evidence is still done manually and has not been stored digitally and follows digital standards and rules. So, to make it easier for an investigator to handle digital evidence and make it easier to manage digital evidence, a web-based digital evidence management system was created..

Before implementing a system to be built, the first step is to design the system. This is done to conduct a needs analysis of user needs. The user of the system in question is an investigator and analyst.

The system will be designed using a design thinking approach. Design thinking is an iterative process in which developers seek to understand users and their assumptions, and redefine the problem in an attempt to identify alternative strategies and solutions. The design thinking approach provides a solution-based approach in solving problems [5]. The choice of this design thinking approach method is used because the design can be done by looking at empathy from the user's side. The use of design thinking can help to question the problem, its assumptions, and its implications. This method also involves a lot of experimentation, such as sketching, prototyping, testing, and trying out concepts and ideas.

To meet the standards in the management of digital evidence handling that will be poured into web-based applications, a system business process rule is needed. The system business process in handling digital evidence refers to the framework that has been made in the research of Lizarti, et al [6].

The results of this study are in the form of a system prototype which will then be tested using usability testing. The result of usability testing is 60 which the prototype that has been designed still does not meet the eligibility criteria for use. This is because the system is still difficult to use and still not consistent in providing its features.

2. Method

The method of designing a digital evidence handling system follows a design thinking approach. Design thinking is an innovative and sustainable method of development. It is said to be innovative and sustainable because this method is based on user needs. So that the design of a system will always be adjusted to the user's needs for the system [7]. Users of this system have been described in Table 4, namely first responders and forensic analysts. The need in question is the need for features that will be implemented into the application according to the needs when handling digital evidence. There are several core stages of the design thinking method: empathy, definition, idea, prototype, and test. The research flow that has been collaborated with design thinking is depicted in Figure 1.

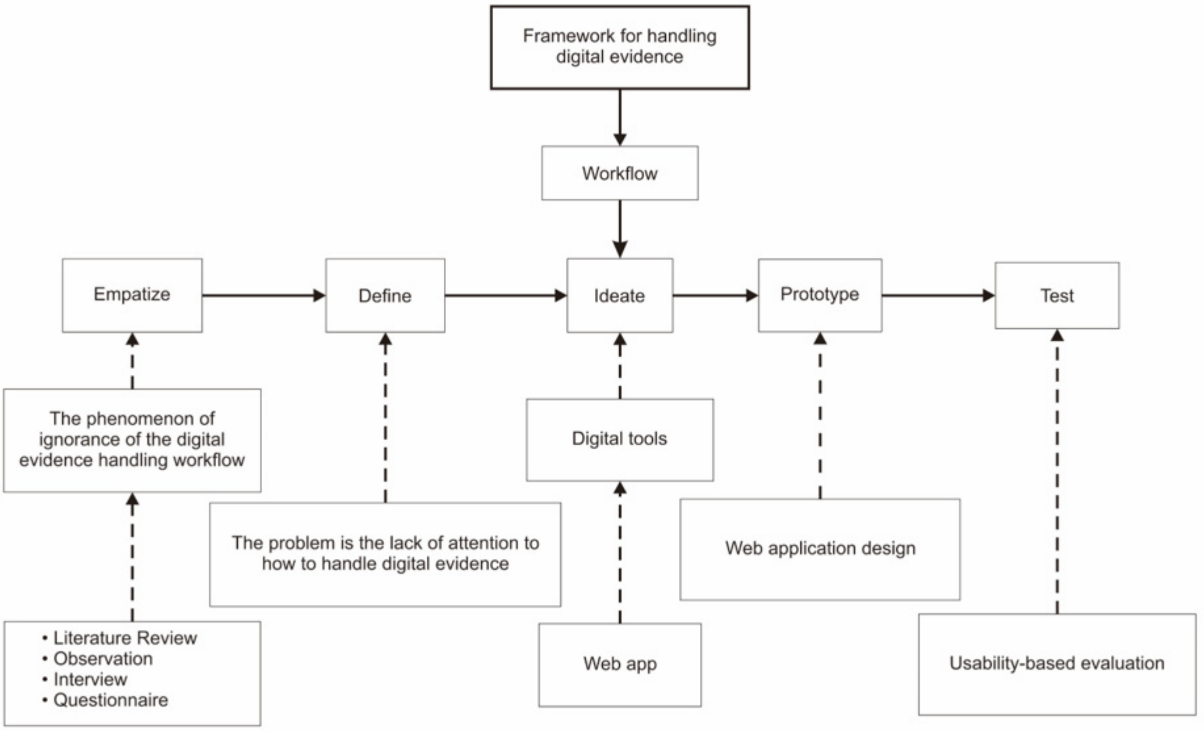
Framework for handling digital evidence
Workflow
Empatize
Define
Ideate
Prototype
Test
The phenomenon of ignorance of the digital evidence handling workflow
The problem is the lack of attention to how to handle digital evidence
Digital tools
Web application design
• Literature Review
• Observation
• Interview
• Questionnaire
Web app
Usability-based evaluation

Figure 1.The workflow

The description related to Figure 1 is as follows:

a. Empathy

In this stage, the process of literature review, observation, interviews, and giving questionnaires to prospective users is carried out. This is done to the phenomenon of ignorance of the flow of handling digital evidence. So that this stage aims to equalize the perception of needs between users and the system to be built.

The literature review was carried out by taking sources from Google Scholar, Scopus, and Science Direct with a span of 10 years of research on the theme of handling digital evidence. The selection of these three study sources is due to obtain a richer and more complete study. In this paper, the number of literatures obtained is 175 literatures, then 3 literatures are selected according to the problems in the management process for handling digital evidence.

Observations were made by participating in discussions related to digital forensics with the Kominfo and government agencies. Discussions were held by attending seminars related to the handling of digital evidence and digital forensic laboratory standards.

The observation process is a process of checking the frameworks for handling digital evidence and existing rules. Then observe the actors involved in the process of handling digital evidence. Based on the paper written by Subektiningsih, that the actors involved in the process of digital forensics activities are: (1) First responders; (2) Investigators, Digital Investigators, Forensic Investigators; (3) Police officers; (4) IT Professional.

The next stage is interviews with experts and practitioners who are experienced in the world of digital forensics. Interviews were conducted to find out what problems were encountered at the digital forensics stage, especially the process of handling digital evidence. The interview process was carried out by giving questionnaires to two practitioners as well as academics and 1 practitioner. Interviews were conducted with 3 digital forensics experts, namely academics and practitioners. Interviews were conducted simultaneously with giving questionnaires related to problems in digital forensics in general and the process of handling digital evidence. The questionnaire was given by asking questions related to the theme of the paper.

b. Definition

This stage is a continuation of the first stage which is the process of defining what needs will be given to the system to be built based on the problems encountered in the first stage..

The problem definition process uses a point of view template by describing the problem from the user's side, needs, and point of view. User descriptions are taken from the interview process with digital forensics experts who were carried out at the empathy stage.

The result of the definition process in the form of features to be created will have three actors: system admin, main responder, and forensic analyst. The features that will be provided on the system include: (1) The system has integrated storage media with the cloud; (2) The system has good data communication security, in accordance with data communication security rules; (3) The system has a data authentication model regarding who can access the data.

c. Idea

This stage is the determination of the solution to the system to be built. This stage is a stage for brainstorming, noting all ideas. The digital tool that will be used in this system is a web application.

Brainstorming is done by referring to the process of empathy which is described in the form of mapping ideas. The results of the mapping are then taken from the core ideas that will be implemented using the now wow how matrix. The selection of ideas is done using the Now Wow How Matrix method by sorting the ideas obtained during brainstorming into three quadrants. The three quadrants are How, Now, and Wow. Now is an idea that can be implemented immediately without seeing its novelty. Wow is an implementable and innovative idea. How is an idea that can be implemented in the future.

d. Prototype

This stage has entered the design model of the system to be created. In this paper, a prototype model is made based on the usertask flow and application flowchart. Usertask flow is used to map the flow of system usage based on the user side. Then the application flowchart is used to map how the application flows to the user.

e. Test

The model that has been made based on the previous stages will be tested on potential users, if there are improvements, an improvement process will be carried out and will be re-tested to potential users. The testing process is carried out using usability testing with the System Usability Scale (SUS) method to see how feasible the application is. Data was taken using a questionnaire. The questionnaire was addressed to 3 digital forensics experts, namely academics and practitioners.

The SUS method uses a Likert Scale with a coverage of 10 statements. Questionnaire participants will give a rating of 1 to 5 based on how much they agree with the statements given. 5 means strongly agree and 1 means completely disagree. Based on the SUS method, to get the SUS score, the result of the average score of each odd-numbered question is subtracted by 1 point and 5 points is subtracted from the result of the average score of each even-numbered question. After subtracting, the odd-numbered and even-numbered questions are added up and the result is multiplied by 2.5.

The overall result of the calculation is a score of 100. This calculation is not a percentage, the results directly point to the score of the assessed system.

To determine the level of user acceptance, the method of writing made by Brooke, 2013 [8] is used. Determination by looking at the level of user acceptance by dividing it into three categories: not acceptable, marginal, and acceptable can be seen in Figure 2.

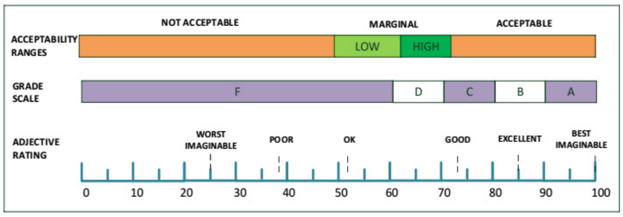

Figure 8. SUS Score [8]

3. Result

The following is the result of a system design based on a design thinking approach.

a. Empathy

This stage is carried out several steps including literature review, observation, and interviews with experts and potential users. Table 1 is the result of a literature review related to the problems faced in digital forensics. The literature was selected based on the focus of research related to the theme of the paper and based on the nearest 10 years. The literature selection was taken from several journal sources using the Google Scholar search engine. Research on handling digital evidence is focused on security and the digital chain of custody.

Table 1. Literature review of problems in digital forensics

Researcher	Title	Problem
Prayudi dkk, 2015 [8]	Digital Chain of Custody: State of The Art	The challenge faced by investigators is how to handle digital evidence
Sadiku dkk, 2017 [9]	Digital Chain of Custody	The most important part of the investigation process is the digital chain of custody (COC).
Richter & Kuntze, 2010 [10]	Securing Digital Evidence	Every piece of evidence in order to be used and support the legal process must have proper procedures in handling digital evidence

The results of observations on digital forensics rules and frameworks can be seen in Table 2. The results of observations refer to the results of studies of research journal literature. Litertaute review of digital forensic frameworks is presented in Table3.

Table 2. Observation of digital forensics rules and framework

Framework/ Rule	Information
Association of Chief Police Officer (ACPO)	Consists of five stages: preparation, preserving, collecting, confirming, identifying.
SOP Laboratorium Forensika Digital POLRI	The procedure consists of 15 SOPs related to digital forensics
Association of Chief Police Officer (ACPO)	Consists of five stages: preparation, preserving, collecting, confirming, identifying.
National Institute of Justice (NIJ) U.S Department of Justice	Consists of five things that are carried out in conducting digital forensic analysis, making policies and procedures, digital evidence assessment, digital evidence retrieval, digital evidence analysis, and documentation and reporting
Jurisdiction Rules No, 10/2020	Regarding the procedures for handling digital evidence by the Indonesian National Police

Table 3. Literature review of digital forensics framework

Researcher	Title	Information
Rhee, 2012 [11]	Framework of multimedia forensic system	Multimedia forensics framework using composition
Lizarti, 2017 [12]	Penerapan composite logic dalam mengkolaborasi framework multimedia forensik	Building a multimedia forensics framework using a composite logic approach
Ledesma & M.S., 2015 [13]	A proposed framework for forensic image enhancement	Digital image forensics framework in the image enhancement section
AlShaikh dan Sedky, 2015 [14]	Post incident analysis framework for automated video forensic investigation	Post incident framework for video forensics investigation automation
SWDGE, 2010 [15]	SWDGE Minimum requirement for quality assurance in the processing of Digital and Multimedia Evidence	Minimum requirement for multimedia forensic investigation

b. Definition

The problem definition process is carried out by defining the problem based on the point of view referred to from the results of the literature review that has been carried out in the empathize section. Table 4 is the result of defining the problem from the user side of the system. In Table 4, the definition of users who will use the system is two people, namely first responders and forensic analysts.

Table 3. Point of view template for defining problems from the user's point of view

User	Needs
First responders (network administrators, investigators, law enforcement officers)	Media to protect, integrate and preserve evidence obtained from crime scenes.
Forensic Analyst	Media for safe storage and retrieval of evidence

The results of the interview stage, some of the problems faced in handling digital evidence for multimedia data are the absence of operational standards for the process of handling digital evidence. In addition, there is a lack of knowledge on how to operate the handling of digital evidence owned by actors. Definition of functions, features, and elements: in this section will be defined service requirements that will exist in a system.

c. Idea

The ideas of the process of looking for ideas are taken from the previous process of empathizing and defining. There are three user needs that serve as a reference for designing applications in this paper. These requirements consist of application features, management, and digital tools. Application features relate to the services that will exist in the application. Management of digital facilities relates to the media used to implement the system.

In the digital facilities section, the results of the brainstorming noted the need for digital facilities that can be used on the system, namely web applications and mobile applications. Then the results of brainstorming for management include: flow of use of digital evidence, framework for handling digital evidence, storage media, mechanisms, and personas involved in the system. For application features, the results of brainstorming are the type of storage media, data communication security, chat, and file sharing.

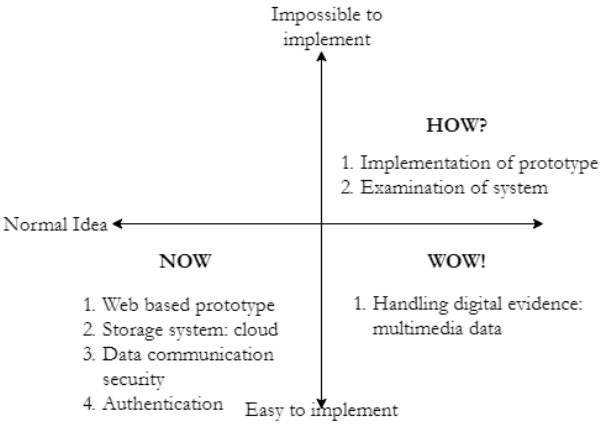

Figure 3. Now Wow How Matriks

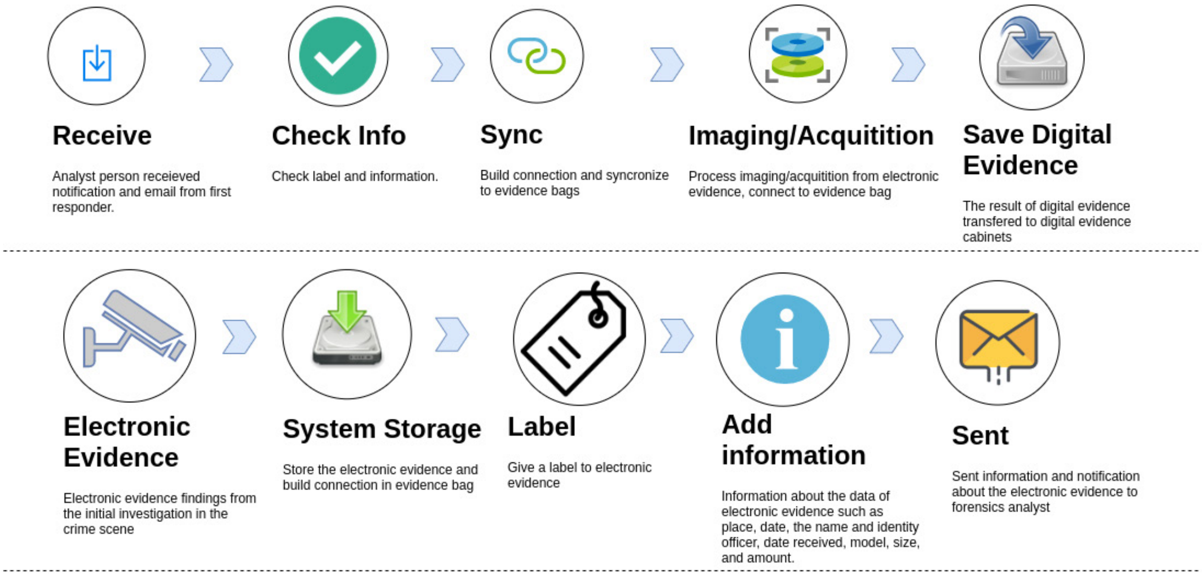
Receive
Analyst person receieved notification and email from first responder.
Check Info
Check label and information.
Sync
Build connection and syncronize to evidence bags
Imaging/Acquitition
Process imaging/acquitition from electronic evidence, connect to evidence bag
Save Digital Evidence
The result of digital evidence transfered to digital evidence cabinets
Electronic Evidence
Electronic evidence findings from the initial investigation in the crime scene
System Storage
Store the electronic evidence and build connection in evidence bag
Label
Give a label to electronic evidence
Add information
Information about the data of electronic evidence such as place, date, the name and identity officer, date received, model, size, and amount.
Sent
Sent information and notification about the electronic evidence to forensics analyst

Figure 4. User task flow

The ideas from the brainstorming results are then selected using the Now Wow How matrix. The selected ideas are taken based on the parameters now, wow, and how. The results of the now wow how matrix are as follows:

1. How: prototype implementation and testing
2. Wow: handling of digital evidence for multimedia data
3. Now: web-based prototypes, storage media using cloud technology, data communication security, and user authentication.

Based on the matrix shown in Figure 3, the implementation is chosen in the now matrix section: a web-based prototype using cloud-based storage media, data communication that has security, and there is an authentication system for system users..

d. Prototype

The business process of handling digital evidence is referred to from research conducted by Prayudi et al. The stage of handling digital evidence involves an officer, investigator, law enforcement, and first responder. So that in the prototype to be made, the actors involved are first responders, forensic analysts, and system admins. To determine the activities of the actors involved, it refers to the basic assumptions of the digital forensics business model proposed by Prayudi et al [16].

So that the user task flow is made based on the digital forensics business model proposed by Prayudi, et al. The usertask flow is depicted in Figure 4. Main responders: find evidence and collect evidence and then give it to forensic analysts. So that what can be done to the main responders in the system are: (1) Providing notifications to forensic analysts to carry out imaging actions/acquisition of electronic evidence via email; (2) Record information and information regarding evidence through a system in the form of photos and information on evidence labels (name of sending institution, name of sending officer including complete identity, amount of evidence, brands of evidence, size); (3) Storing evidence in the evidence bag (a stand-alone system).

Forensic analyst: performs the acquisition/imaging of electronic evidence into digital evidence. The process of acquisition/imaging and analysis is done outside the system. So that forensic analysts use the system to: (1) Connect and request authentication with the evidence bag system; (2) Record information on electronic evidence (name of sending institution, name of sending officer including complete identity, date received, amount of evidence, brands of evidence, size); (3) Storing the acquisition results on cloud storage media called digital evidence cabinet.

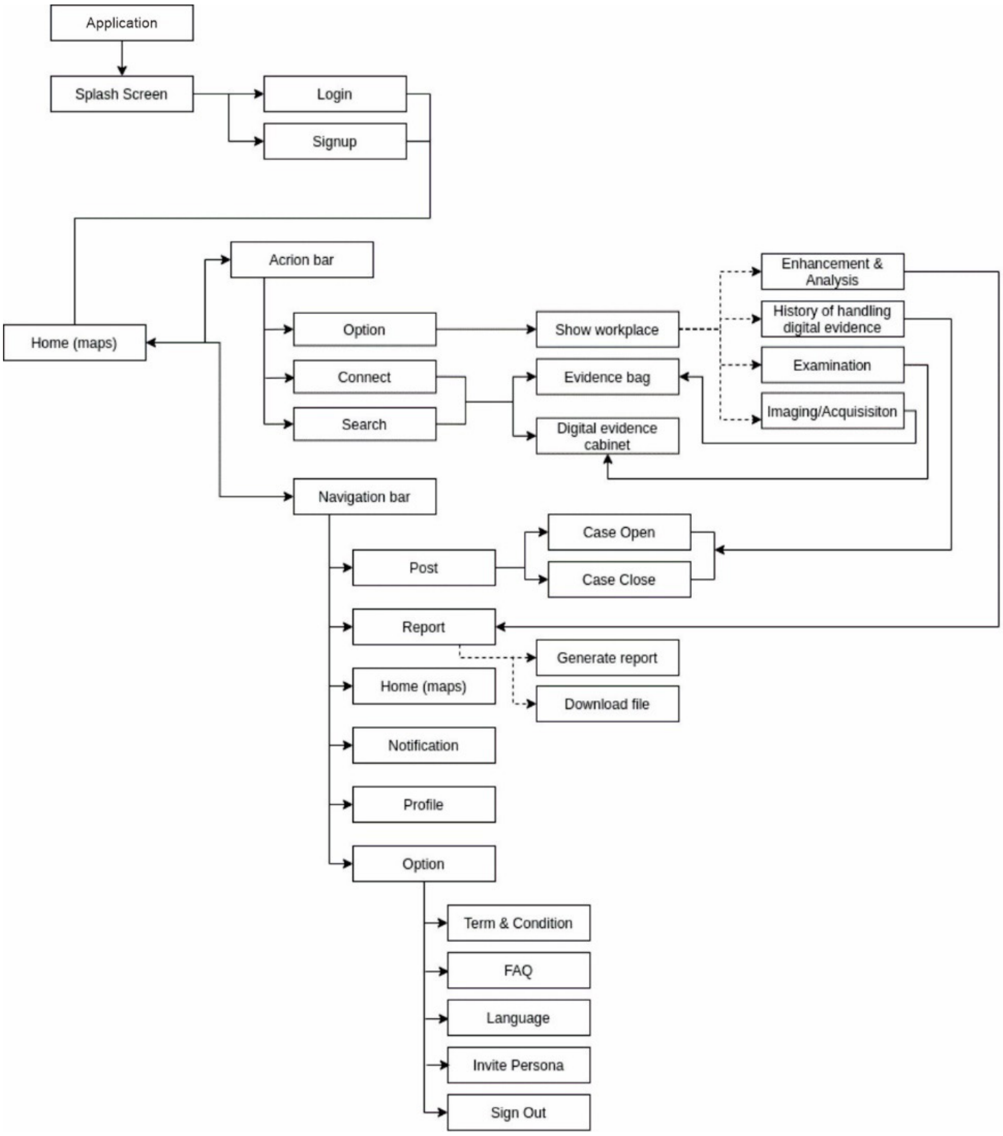

Figure 5. Flowchart of the application

The flowchart stages shown in Figure 5 are the workflow of the prototype to be made. This process begins with a splash page in the form of a logo display from the application that has been created. Furthermore, the user will enter the login page or sign up if the user does not have an account. After logging in, the user will enter the home page where there is an action bar in the middle of the page and a navigation bar at the top of the page.

In the action bar there are 3 options, namely the button option which refers to the show workplace page which contains enhancement & analysis, history of handling digital evidence, examination and imaging/acquisition, then connect and search buttons which refer to the evidence bag folder and digital evidence cabinet folder.

While in the navigation bar there are five choices, namely home which refers to the first page after the user logs in, then the case button which refers to the case open and case closed pages, then the report button which refers to the generate report page and download the file, after that there is a button options that refer to the terms & conditions page, FAQ, language, invite persona, and sign out, and the last button profile which refers to the profile page, and notification button.

After the prototype is made, then testing is carried out on the user. The results of improvements to the prototype are carried out in two iterations. The first iteration is an improvement in the connection process for access to digital evidence bags and digital evidence cabinets. Then the second iteration, improvements to the navigation bar in the post.

5. Test

At this stage, trials will be carried out on the prototype that has been made in the previous sub-chapter using usability testing by giving questionnaires to several potential users. The results of the questionnaires that have been given will be assessed using the System Usability Scale (SUS) to get the measurement results of the prototype being tested for potential users. The results of the questionnaire were then calculated using a predetermined formula to get the SUS score. The results of the SUS score assessment are shown in Table 5.

Table 4. SUS score calculation results

No	Question	Average
1	I will use this system again	3.5
2	I find this application system complicated to use but it could be simpler	2.5
3	I find this application system easy to use	3.5
4	I feel that I need the help of other people or technicians to use this application	3
5	I found various features well integrated in the system	4
6	I feel there are a lot of inconsistent things in this app	2.5
7	I think many users will quickly learn this system	3.5
8	I find this feature very handy when used	3
9	I can use this system well	3.5
10	I need to get used to it first in using this system	3

The results of the calculation provide the SUS value of 60. In the SUS assessment, the system can be categorized as acceptable if the SUS value is more than 70. Based on the calculation of the SUS value, the Digital Evidence Handling Management prototype gets a score of 60. The value of 60 is included in the marginal low category. Marginal low has a minimum value of 50. The Digital Evidence Handling Management Prototype does not meet the eligibility category because it does not meet the acceptable category. The causes of not meeting the acceptable category can be seen in Table 5, the smallest value of 2.5 indicates that users still find difficulties to use the application and feel that there are still parts that are not consistent in the application.

4. Conclusion

The study has constructed a prototype of digital evidence handling management application. The prototype user testing gives a SUS value as low as 60, which falls into the marginal-low category. The system still needs improvement in terms of convenience and consistency. The design thinking method shows that the design process focuses more on exploring problems and providing solutions. For this reason, as a refinement of the system, in the future, more in-depth research should be carried out related to the design and implementation directly into a system. The recommended method for system improvement is the user-centered design method because it focuses more on user needs and is suitable for software development.

Acknowledgement

I express my gratitude and appreciation to all reviewers at Khazanah Informatika. In addition, thanks to UII Informatics Engineering for its contribution, so that this paper can be completed properly.

Reference

[1] A. Antwi-Boasiako and H. Venter, “A model for digital evidence admissibility assessment,” in IFIP Advances in Information and Communication Technology, 2017, vol. 511, pp. 23–38, doi: 10.1007/978-3-319-67208-3_2.

[2] Y. Prayudi and A. SN, “Digital Chain of Custody: State of The Art,” Int. *J. Comput. Appl.*, vol. 114,

no. 5, pp. 1–9, Mar. 2015, doi: 10.5120/19971-1856

[3] Matthew Braid, "Collecting Electronic Evidence After a System Compromise," 2001. https://www.auscert.org.au/publications/2017-09-11-collecting-electronic-evidence-after-sy (accessed Feb. 23, 2021).

[4] B. Schatz, "Digital Evidence: Representation and Assurance," 2007

[5] T. Y. S. Rikke Friis Dam, "What is Design Thinking and Why Is It So Popular? | Interaction Design Foundation (IxDF)," 2020. https://www.interaction-design.org/literature/article/what-is-design-thinking-and-why-is-it-so-popular (accessed Mar. 04, 2021).

[6] N. Lizarti, B. Sugiantoro, and Y. Prayudi, "PENERAPAN COMPOSITE LOGIC DALAM MENGKOLABORASIKAN FRAMEWORK TERKAIT MULTIMEDIA FORENSIK," JISKa, vol. 2, no. 1, pp. 26–33, 2017

[7] C. Müller-roterberg, "Handbook of Design Thinking," no. January, 2019

[8] Brooke, John. (2013). SUS: a retrospective. Journal of Usability Studies. 8. 29-40.

[9] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody," 2014. Accessed: Aug. 28, 2020. [Online]. Available: http://www.dynotech.com/articles/digitalevidence.shtml.

[10] J. Richter, N. Kuntze, and C. Rudolph, "Securing digital evidence," in *5th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2010*, 2010, pp. 119–130, doi: 10.1109/SADFE.2010.31.

[11] K. Rhee, "Framework of multimedia forensic system," in *2012 7th International Conference on Computing and Convergence Technology (ICCCT)*, 2012, pp. 1084–1087, Accessed: Aug. 28, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/6530496.

[12] N. Lizarti *et al.*, "PENERAPAN COMPOSITE LOGIC DALAM MENGKOLABORASIKAN FRAMEWORK TERKAIT MULTIMEDIA FORENSIK," 2017

[13] Ledesma, S. Aguila, and M.S., "A proposed framework for forensic image enhancement," University of Colorado at Denver, 2015.

[14] A. AlShaikh and M. Sedky, "Post Incident Analysis Framework for Automated Video Forensic Investigation," *Int. J. Comput. Appl.*, vol. 129, no. 17, pp. 38–44, Nov. 2015, doi: 10.5120/ijca2015907187.

[15] SWDGE, "SWGDE Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence," 2010. https://www.swgde.org/documents/published (accessed Aug. 30, 2020).

[16] Y. Prayudi, A. Ashari, and T. K Priyambodo, "Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody," Int. J. Comput. Appl., vol. 107, no. 9, pp. 30–36, 2014, doi: 10.5120/18781-0106.