ILKOM Jurnal Ilmiah Vol. 13, No. 1, April 2021, pp. 58-66
Accredited 2nd by RISTEKBRIN No. 200/M/KPT/2020; E-ISSN 2548-7779 | P-ISSN 2087-1716

Research Article Open Access (CC–BY-SA)

Forensic storage framework development using composite logic method

Helmi Rachman [a, 1, *]; Bambang Sugiantoro [b, 2]; Yudi Prayudi [a, 3]
[a] *Universitas Islam Indonesia, Jalan Kaliurang km.14, Yogyakarta 55584, Indonesia*
[b] *Universitas Islam Sunan Kalijagaam, Jl. Marsda Adisucipto, Yogyakarta 55281, Indonesia*
[1] *17917108@students.uii.ac.id;* [2] *bambang.sugiantoro@uin-suka.ac.id;* [3] *prayudi@uii.ac.id*
** Corresponding author*

Article history: Received March 16, 2021; Revised April 24, 2021; Accepted April 30, 2021; Available online April 30, 2021

Abstract

Increasing number of information technology users allows possibility for crimes to take advantage of information technology to continue increasing either directly and indirectly. Criminals often use computer devices to commit crimes. This is a major concern so that the need for handling digital evidences becomes significantly urgent. Therefore, a forensic storage framework is required for managing digital evidences. This framework is designed by applying the composite logic method to determine role model of each variable or the initial pattern of the stages to be collaborated. Composite logic produces a role model that is to generate patterns in order to achieve the same goal. This method collaborates framework for handling the pre-existing hdd, ssd, and vmware to be in turn combined into a forensic storage framework. Based on the results of the test, this study proposes a new framework called forensic storage framework which comprises of four main stages, namely preparation, collection, analysis and report. The advantage of this framework is that it can be used to handle digital evidences in four storages which are SSD, HDD, VmWare, and cloud.

Keywords: Storage Forensics; Composite Logic; Framework

Introduction

Advances in technology have provided many benefits for many computer users. This computer system is used as a tool that helps in personal life, education, commercial, government, etc. [1]. Unfortunately, the ease of internet access helps some criminals to commit fraud, intrusion and attacks that can damage user privacy [2]. Along with the increasing number of users of information technology, the opportunities for crimes that utilize information technology continue to increase both directly and indirectly. The use of the internet causes crimes that were originally carried out conventionally, continue to develop into a modern crime that causes a greater level of harm and has a very broad impact. It is undeniable that internet technology has a large negative impact besides its benefits.

Based on information from kominfo.go.id, the proliferation of digital crimes has placed Indonesia as the second highest cybercrime perpetrator in the world. Examples of digital crime are defamation of artists through a prostitution site, criminal acts via e-commerce, hackers who disrupt the website of certain entities, ATM skimming, etc. Digital evidence is needed to prosecute the criminals who have been involved in this cybercrime. Because digital evidence is stored in a storage, an acquisition action is needed for the respective storage media. Various types of storage such as hard disks, solid state drives, cloud storage and virtual hard drives cause many problems in handling the digital evidence to be encountered in the proving process. For instance, in hard disk handling, there are some difficulties in recovering deleted data, because hard disks have a complex set of components, so criminals can hide evidence of their crimes [3].

Virtual storage media is widely used by cyber criminals because this storage media has a very complex nature due to the volatility of VMs. Evidence in a VM can be easily lost when moved or deleted. This causes difficulty for investigators in the investigation process [4]. The difference in the handling of these four storage media causes investigators to have difficulty in the investigation process. Therefore, new standard framework is required to assist investigators in solving these problems. There are more than one hundred digital forensic investigation procedures that have been developed worldwide [5]. investigators must have guidelines in the investigation process to handle cases on digital evidence [6]. To catch and prosecute criminals who are involved in digital crimes, investigators must use consistent and clear forensic procedures to obtain valid digital evidences [1]. Applicable legal regulations require evidence to have integrity, authenticity, reproducibility, non-interference, and minimalist. Hence, the credibility of

http://dx.doi.org/10.33096/ilkom.v13i1.811.58-66

digital evidence is one of the important elements of digital forensics. Digital evidence includes physical computer evidence, digital audio, digital video, cell phones, digital fax machines etc. [7].

In handling cases related to digital evidence, investigators must have guidelines in the investigation process [6]. With the increasing number of digital-based evidence, the need for rapid identification, analysis, and interpretation of digital evidence becomes increasingly important [8]. The need for forensic investigations for the handling of digital evidence is very important. This is because, handling crime cases related to digital evidence requires digital forensics investigation [9]. Digital forensics has four main stages, namely Collection, Examination, Analysis and Reporting [10]. The need for handling digital evidence is a major concern in digital forensics. A framework is urgently required in the digital forensics investigation process, Several studies have developed many frameworks for handling digital evidence, for instance, Audio forensics framework [11], Multimedia forensics [12], Forensic cloud computing [13], Integrated Digital Forensics Investigation Framework (IDFIF) [14], Digital Evidence Collection Framework in Social Media [15].

However, the current framework for the acquisition process on storage for handling digital evidence emphasizes general investigations and does not provide a specific stage of acquisition. This framework will be the main guide for investigators in resolving cases related to digital evidence. Many previous studies have created a framework for digital forensics case investigations. However, most of these frameworks are designed for the general forensic investigation process. The acquisition process is one of the important components in the digital forensic investigation process. Errors that occur during the acquisition process cause damage in evidences. Therefore, it is necessary to design a special framework to accommodate all types of digital evidence. Due to the urgent need for a framework for handling cases related to digital evidence, this study is to propose a framework that can accommodate all types of digital evidence. This research will combine four existing storage forensics framework into one new framework which employs composite logic method.

Composite Logic is a method used to determine the role model of each variable or initial pattern of the stages to be collaborated. The Composite Logic method will produce a role model which is to produce patterns that can create the same goal. Previous research [16] used the Composite Logic method to create a distributed modeling process. This research develops model-based distributed software by proposing split, edit, and collaboration activities based on the composite model so that it becomes a formal sound modularization mechanism that allows for local consistency checks and systematic transformations.

Method

The method contains the stages or research procedures and the algorithms used in the research, the problem formulas studied in more detail, and the system design if needed. The stages of research are carried out to explain the sequence of systematic steps and provide guidelines for solving problems, analyzing research results, and the difficulties encountered. The steps in this research can be seen in **Figure 1**.

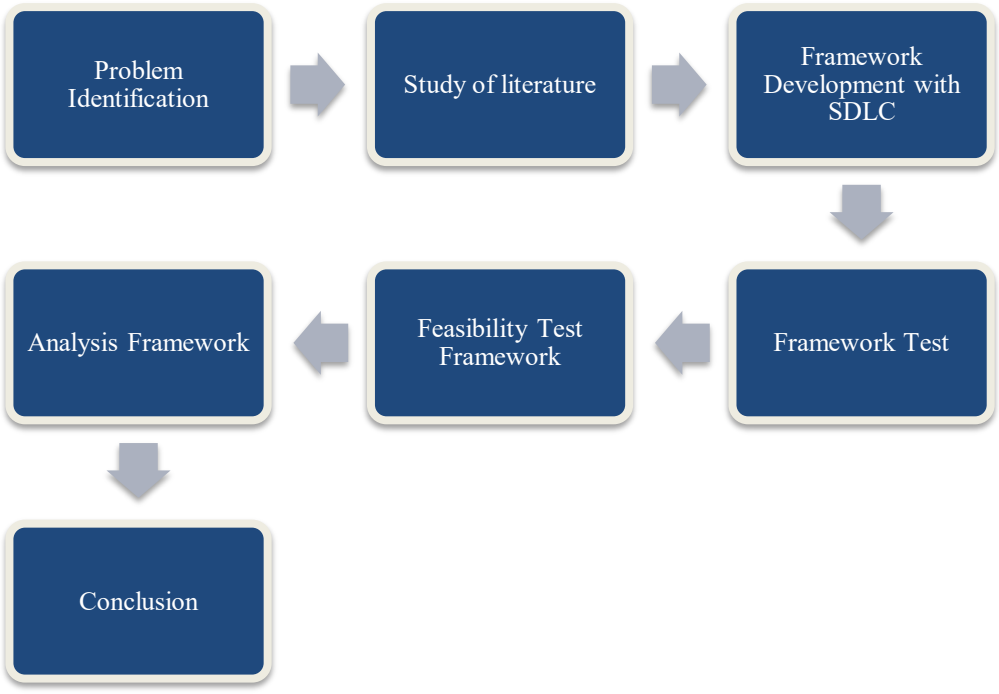

Figure 1. The flow of research methods

Figure 1 describes the research methodology to complete this research. This research method is used to develop an acquisition and processing framework in the handling of digital evidence. This research method includes several main stages; problem identification, literature study, framework development with the composite logic method, framework testing, framework feasibility testing, framework analysis and making a conclusion related to the results of making a framework to develop an acquisition and processing framework in handling digital evidence.

Results and Discussion

This part is a section to write research results that are described in detail, clearly and sequentially. The results of the research are presented in the form of tables, graphs or other illustrations with the discussions that are presented in a structured and systematic way. A description of the performance, weaknesses, and strengths of the research results must be explained.

A. Framework design using the Composite Logic method

Composite Logic is a method that can summarize complex multi-dimensional reality. This method is used to support decision-making and can be used in the interest of reducing the size of a series of indicators without changing the main information base and facilitating the process of interpretation in many separate indicators. This method can be applied in determining the role model of each variable, or the initial pattern of the stages that want to be collaborated on. Collaboration on several model structures can be conducted with this method to become a unified model that still maintains the initial structure and hierarchy.

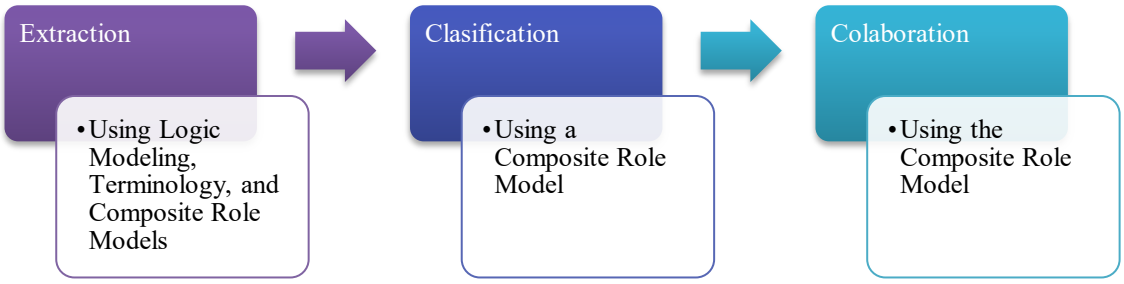

Figure 2. Composite Logic Implementation Scheme

Figure 2 is the modeling stage of Composite Logic which consists of three stages; the process of extraction, classification and collaboration. The following are the description:

1. Extraction: The Use of Logic Modeling, Terminology and Composite Role Models.
2. Classification: The Use of Composite Role Model.
3. Collaboration: The Use of the Composite Role Model.

B. Identification of Storage Forensics

At this stage, four types of Storage Forensics Frameworks that have existed previously will be identified. Several storage frameworks will be developed and combined into one framework for the digital evidence handling process, which is more focused on the acquisition process. In these 4 types of storage, each has its characteristics and differences in handling. It is necessary to have a new standard framework to help investigators not have difficulty in the investigation process to solve these problems in one go. The reason for choosing these four frameworks is because these four frameworks represent each framework for handling forensic storage so that it will be easier to collaborate using the composite logic method.

Consider the importance of a framework for handling cases related to digital evidence originating from storage, this research will design a framework that can accommodate all types of digital evidence originating from storage. This identification process will be carried out using the composite logic method based on naming and terminology. This process will simplify the logic modelling to classify the stages based on naming and terminology. There are four types of storage forensics framework developed in this study including shown in **Table 1**:

1. A research on the investigation method of digital forensics for a VMware Workstation's virtual machine, has six stages of investigation.[17]
2. The Cloud Storage Forensic Framework has seven stages of investigation [18]
3. Importance of Forensics Image of Hard Disk Using Different Forensics Tools By Preserving The Integrity of Digital Evidence has seven stages [19]
4. Solid State Device (SSD) Forensics has eight stages. [20]

Table 1. Results of Related Storage Forensic Identification

No	A research on the investigation method of digital forensics for a VMware Workstation's virtual machine	Digital Forensics Framework for Cloud Computing Environment	Importance of Forensics Image of Hard Disk Using Different Forensics Tools by Preserving the Integrity of Digital Evidence	Solid State Device (SSD) Forensics
1	Copy Vm Image	Commence	Identification	Incident
2	Extract filesystem metadata & File Carving	Preparation	Search and Seizure	Identification
3	Recover VM Image	Evidence Source Identification and Preservation	Acquisition	Seizure
4	Mount Image	Collection	Authentication	Imaging
5	Analyze	Examination & Partial Analysis	Analysis	Hashing
6	Report	Presentation	Presentation	Analysis
7		Complete	Preservation	Report
8				Preservation

C. Related Storage Forensics Framework Collaboration

At this stage, collaboration results will be carried out from identifying the Storage Forensic Framework related to the implementation of the Composite Logic scheme. Furthermore, the stages resulting from the collaboration are used to build a Storage Forensic framework that will be used in handling digital evidence.

1. Extraction With Logic Modeling, Terminology, and Composite Role Models.

   This extraction process also uses six basic elements from the template logic model: Activity, Output, Rationale, Assumption, Impact, and Outcomes. Furthermore, to determine the impact indicator, the composite role model is used; Prohibit, Implies and Don't care. The explanation of each stage of the basic elements from the logic model template is as follows.

   a. Activity is a stage to meet the needs of the output.
   b. Output is the stage of the results of the activities that become inputs
   c. Rationale is a step in terminology obtained from related literature sources.
   d. Assumption is a stage that contains facts or opinions that are believed to be true and have an influence on outcomes.
   e. Impact is the stage of the analysis of the rationale and assumption in interrelated stages. Determination of the impact of the table logic model is conducted by adapting the role model of the Composite Logic model:
      - A stage "n" is said to be "implies" if it collaborates with other stages. This indicator can cause a new name after collaboration because it has the same terminology with other stages
      - A stage "n" is said to be "Prohibit" if it is a stage with general terminology that is considered important but is not contained in other Storage Forensics Frameworks. This indicator can lead to an immediate addition at this stage
      - A stage "n" is said to be "don't care" if the stage must remain in the original stage because it cannot be collaborated and does not have the same terminology as the other stages.
   f. Outcomes are the final results that are applied after considering the existing assumptions and ratios.

2. Classification using Composite Logic Model

   This extraction process also uses six basic elements from the template logic model: Activity, Output, Rationale, Assumption, Impact, and Outcomes. Furthermore, to determine the impact indicator, the role model from the composite is used; Prohibit, Implies and Don't care. The explanation of each stage of the basic elements of the logic model template is shown in **Figure 3**.

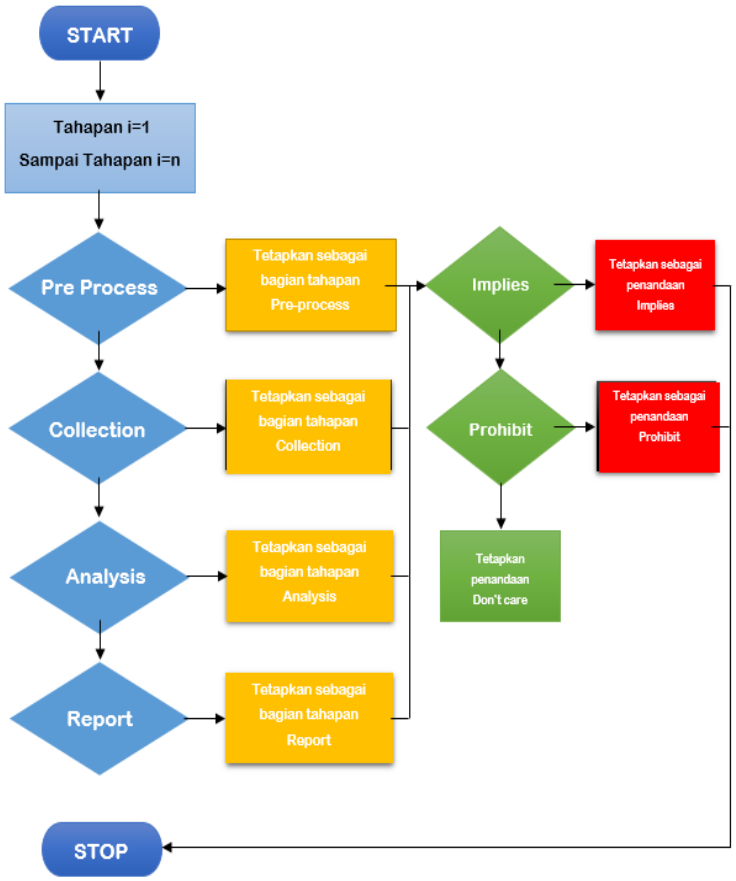

Figure 3. Flowchart of the Classification Process Based on the Role Model.

This classification process is carried out based on the Output indicators and role indicators conducted in the previous extraction process. The classification process *i* is the stage and *n* is the processed number of stages in each framework. The results of this classification will produce a table that visualizes the role model indicators. The indicating indicator is red, the prohibit indicator is green, and the Don't Care indicator is blue. The visualization process with coloring is made to make it easier to distinguish existing indicators. Classification result is shown in **Table 2**.

Table 2. Classification result

No	Preparation	Collection	Analysis	Report
1	Copy Vm Image	Identification	Analyze	Report
2	Incident	Identification	Analysis	Report
3	Commence	Evidence Source Identification and Preservation	Authentication	Preservation
4	Preparation	Extract filesystem metadata & File Carving	Analysis	Presentation
5		Collection	Examination and Analysis	Presentation
6		Recover VM Image		Complete
7		Mount Image		
8		Seizure		
9		Search and Seizure		
10		Hashing		
11		Imaging		
12		Acquisition		
13		Preservation		

: Stages with the “Implies” role model
: Stages with the “Prohibit” role model
: Stages with the "Don't Care" role model

A stage n is said to be "Implies" if it collaborates with other stages, this indicator can cause a new name after being collaborated because it has the same terminology with other stages.

a. For each entry role model, it is carried out using the following formula. Logical implication formula (1)

$$(A \Rightarrow B) \quad (1)$$

b. A step n is said to be "Prohibit" if it is a step with general terminology, considered important but not contained in other forensic storage frameworks. This indicator can lead to the direct addition of this stage. Logical implication formula (2)

$$(A \Rightarrow B) \quad (2)$$

c. stage n is said to be "Don't care" if the stage must remain in the original stage because it cannot be collaborated and does not have the same terminology as the other stages.

3. Collaboration using Composite Role Model

After the classification process, the next stage that will be carried out is the Composite Role Model's collaboration stage. At this stage, the Implies role model collaboration will be carried out which has the same naming and terminology, so that this indicator causes a new name to be given after the collaboration process is carried out. Terminology collaboration results is show in **Table 3**.

Table 3. Terminology Collaboration Results

No	Preparation	Collection	Analysis	Report
1	Incident	Identification	Analyze	Presentation
2	Commence	Extract File System Meta Data & File carving	Assesment	Report
3	Preparation	Recover VM Image		Complete
4	Copy VM Image	Mount Image		
5		Seizure		
6		Acquisition of Evidence		
7		Hashing		
8		Preservation		

4. Framework Design

After collaborating using Composite Logic, then a framework is produced from the collaboration, which will be used as a framework design in handling forensic digital storage evidence. Framework of design is shown in **Table 4**. The preparation of this framework follows the following requirements:

a. The stage that will be determined as the main stage of the new framework is the stage that has been identified in the output and has been written in the table of classification results for the forensic storage framework to be described in the form of activities.
b. The results of the collaboration stages have been compiled, sorted, and shown in **Table 3**. The stage has a suitable hierarchy because of the influence of applying the role model on the stage obtained from the identification process.
c. The design of this framework will be evaluated based on previous research.

Table 4. Framework of Design Results

No	Stages of the Design Result Framework	ID
Stage of Preparation		**P**
1	Preparation	**P1**
2	Identification	**P2**
3	Incident	**P3**
4	Commence	**P4**
5	Copy VM Image	**P5**
Stage of Collection		**C**
6	Extract File System Meta Data & File Carving	**C1**
7	Recover VM Image	**C2**
8	Mount Image	**C3**
9	Seizure	**C4**
10	Acquisition of Evidence	**C5**

No	Stages of the Design Result Framework	ID
11	Hashing	**C6**
12	Preservation	**C7**
Stage of Analysis		**A**
13	Analysis	**A1**
14	Assesment	**A2**
Stage of Report		**R**
15	Presentation	**R1**
16	Report	**R2**
17	Complete	**R3**

The flow in the collaborative framework can be seen in **Figure 4**. This flow describes the process from the initial to the final stages in the collaborative framework stage which will then be used as the Storage Forensic Framework.

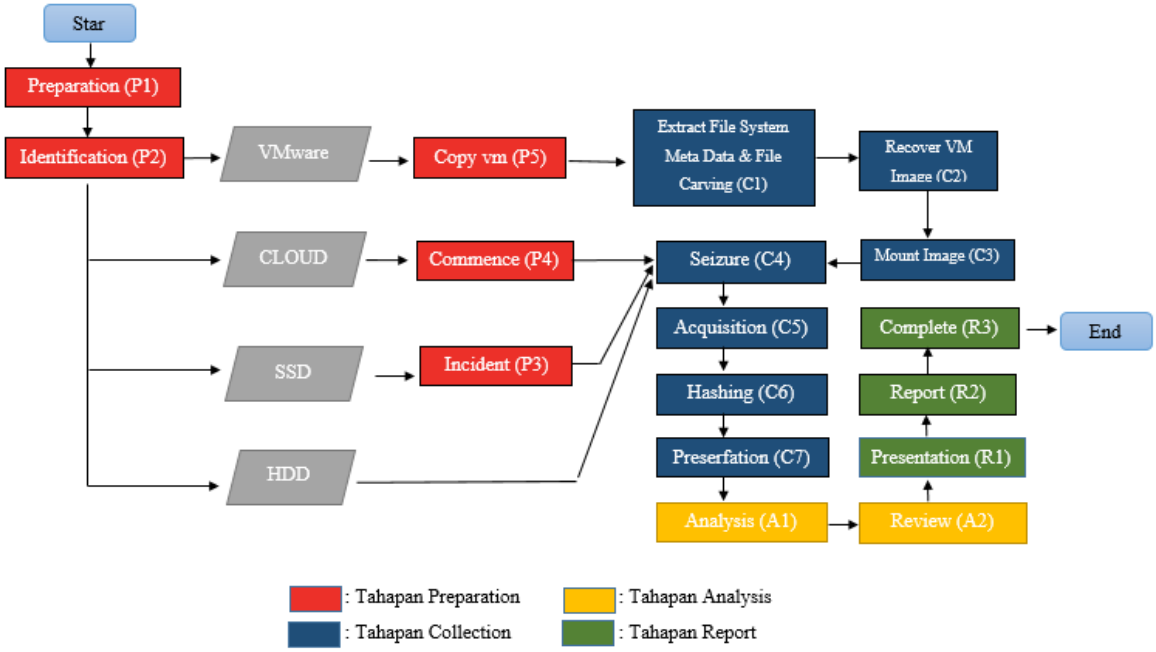

Figure 4. Flow of the Design Result Framework

5. Framework Evaluation

This stage will evaluate the initial framework that has been designed. The evaluation stage, as in **Table 5** is carried out as a comparison and to find out that the design framework is in line with the need to build a Storage Forensic Framework.

Table 5. Framework Evaluation Table

No	Stages in Digital Forensics Investigation Models	Steps in the Storage Forensics Framework	
A research on the investigation method of digital forensics for a VMware Workstation's virtual machine		Yes	No
1	Copy Vm Image	✓	
2	Extract filesystem metadata & File Carving	✓	
3	Recover VM Image	✓	
4	Mount Image	✓	
5	Analyze	✓	
6	Report		
Cloud Storage Forensic Framework		Yes	No
7	Commence	✓	
8	Preparation	✓	
9	Evidence Source Identification and Preservation		✓
10	Collection		✓
11	Examination & Partial Analysis		✓
12	Presentation	✓	
13	Complate	✓	

No	Stages in Digital Forensics Investigation Models	Steps in the Storage Forensics Framework	
Importance of Forensics Image of Hard Disk Using Different Forensics Tools		Yes	No
14	Identification	✓	
15	Search and Seizure		✓
16	Acquisition	✓	
17	Authentication	✓	
18	Analysis	✓	
19	Presentation	✓	
20	Preservation	✓	
Frameworks Solid State Device (SSD) Forensics		Yes	No
21	Incident	✓	
22	Identification	✓	
23	Seizure	✓	
24	Imaging		✓
25	Hashing	✓	
26	Analysis	✓	
27	Report	✓	
28	Preservation	✓	

In **Table 5**, there are several stages of the results of the new framework design that are not contained in the stages of the Digital Forensics Investigation Models framework, which are used as the basis for the design of the new framework. In addition, in the digital evidence collection framework in Forensic Storage, the number of framework stages is less than the number of stages in the framework used as the basis for the design. This happens because several stages in the Forensic Storage Framework have been collaborated and given a new name.

Conclusion

The conclusions obtained from this research is that the design of the acquisition framework and the process in handling digital evidence can be conducted using the Composite Logic method by collaborating with several existing frameworks. In general, this framework has covered all the requirements for designing the acquisition framework and the process of handling digital evidence in storage forensics.

Reference

[1] F. Cohen, "Two models of digital forensic examination," *4th Int. Work. Syst. Approaches to Digit. Forensic Eng. SADFE 2009*, vol. 1, no. 3, pp. 42–53, 2009, doi: 10.1109/SADFE.2009.8.

[2] M. R. Gregg Gunsch, Clint Carr, "An Examination of Digital Forensic Models," *4th Int. Work. Syst. Approaches to Digit. Forensic Eng. SADFE 2009*, vol. 1, no. 3, pp. 42–53, 2009, doi: 10.1109/SADFE.2009.8.

[3] A. Alenezi, R. K. Hussein, R. J. Walters, and G. B. Wills, "A Framework for Cloud Forensic Readiness in Organizations," *Proc. - 5th IEEE Int. Conf. Mob. Cloud Comput. Serv. Eng. MobileCloud 2017*, pp. 199–204, 2017, doi: 10.1109/MobileCloud.2017.12.

[4] P. Tobin, N.-A. Le-Khac, and T. Kechadi, "Forensic Analysis of Virtual Hard Drives," *J. Digit. Forensics, Secur. Law*, vol. 12, no. 1, 2017, doi: 10.15394/jdfsl.2017.1438.

[5] S. Perumal, "Digital Forensic Model Based On Malaysian Investigation Process," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 8, pp. 38–44, 2009, doi: 10.1504/IJESDF.2010.033780.

[6] O. Takwa, C. R. Belgacem, and D. Adel, "A New Digital Investigation Frameworks Comparison Method," *Int. J. Comput. Tech. -–*, vol. 3, no. 4, pp. 6–10, 2016, [Online]. Available: http://www.ijctjournal.org.

[7] V. Baryamureeba and T. Florence, "The Enhanced Digital Investigation Process Model," *Asian J. Inf. Technol.*, vol. 5, pp. 790–794, 2004.

[8] R. Mislan, J. Goldman, S. Debrota, M. Rogers, and T. Wedge, "Computer Forensics Field Triage Process Model," *J. Digit. Forensics, Secur. Law*, pp. 27–40, 2006, doi: 10.15394/jdfsl.2006.1004.

[9] S. Garfinkel *et al.*, "Bringing Science to Digital Forensics with Standardized Forensic Corpora By Bringing science to digital forensics with standardized forensic corpora," 2009, doi: 10.1016/j.diin.2009.06.016.

[10] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," 2006, doi: 10.6028/NIST.SP.800-86.

[11] R. Inggi, B. Sugiantoro, and Y. Prayudi, "Penerapan System Development Life Cycle (Sdlc) Dalam (Sdlc) Dalam Mengembangkan," *SemanTIK*, vol. 4, no. 2, pp. 193–200, 2018, doi: 10.5281/zenodo.2528444.

[12] N. Lizarti *et al.*, "PENERAPAN COMPOSITE LOGIC DALAM MENGKOLABORASIKAN," no. March 2018, 2017, doi: 10.14421/jiska.2017.21-04.

[13] M. E. Alex and R. Kishore, "Forensics framework for cloud computing," *Comput. Electr. Eng.*, vol. 60, pp. 193–205, 2017, doi: 10.1016/j.compeleceng.2017.02.006.

[14] Y. D. Rahayu and Y. Prayudi, "Membangun Integrated Digital Forensics Investigation Framework (Idfif) Menggunakan Metode Sequential Logic," *Semin. Nas. Teknol. Inf. dan Komun.*, no. March, pp. 2089–9813,

2014.
[15] M. N. Al Jumah, B. Sugiantoro, and Y. Prayudi, "Penerapan Metode Composite Logic Untuk Perancangan Framework Pengumpulan Bukti Digital Pada Media Sosial," *Ilk. J. Ilm.*, vol. 11, no. 2, pp. 135–142, 2019, doi: 10.33096/ilkom.v11i2.442.135-142.
[16] D. Strüber, G. Taentzer, S. Jurack, and T. Schäfer, "Towards a distributed modeling process based on composite models," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7793 LNCS, pp. 6–20, 2013, doi: 10.1007/978-3-642-37057-1_2.
[17] S. Lim, B. Yoo, J. Park, K. D. Byun, and S. Lee, "A research on the investigation method of digital forensics for a VMware Workstation's virtual machine," *Math. Comput. Model.*, vol. 55, no. 1–2, pp. 151–160, 2012, doi: 10.1016/j.mcm.2011.02.011.
[18] Y. Y. Teing, A. Dehghantanha, K. K. R. Choo, and L. T. Yang, "Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study," *Comput. Electr. Eng.*, vol. 58, no. 2017, pp. 350–363, 2017, doi: 10.1016/j.compeleceng.2016.08.020.
[19] K. N. Mahajan, S. S. Chafale, and V. G. Mulik, "International Journal of Advance Engineering and Research Importance of Forensic Image of Hard Disk Using Different Forensic Tools By Preserving The Integrity of Digital Evidence," pp. 272–279, 2018.
[20] N. Reddy, "Solid State Device (SSD) Forensics," doi: 10.1007/978-1-4842-4460-9.