Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014

Adi Setya [1], Abba Suganda [2]

[1,2] *Computer Science Departement, Binus Graduate Program - Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia*

[1] adi.setya@binus.ac.id, [2] eagirsang@binus.edu

***Abstract*— Social media is a place that people use to socialize. In addition to socializing, social media is also often used as a crime medium by certain people. In the evidentiary process, law enforcers have the duty to present the evidence used by the suspect in committing his crime. The method used in collecting digital evidence from social media must have a clear scientific basis and guidelines. If the method used is not known as a theory or method in digital forensics, this will undermine all expert testimony and evidence presented in the court. Making a framework that can be recognized by all judicial administrators (judges, public prosecutors, attorneys for defendants, witnesses and defendants) is a solution that can be used as a standard so that the evidence process runs well. The framework that has been created by the researcher is an update from the previous framework. The framework design is made using the Composite Logic method. The composite logic method will collaborate with the Digital Forensics Investigation Models framework to produce a new framework. Based on existing data and facts, this research has produced a framework with better performance than the previous framework.**

Keywords: **Forensic digital, digital proof, social media acquisition, SNI 27037 :2014**

I. INTRODUCTION

Social media has become a major need in society. However, social media is often used as a medium for committing crimes. With so many crimes that use social media, it is necessary to design a framework to collect digital evidence on social media. The framework is a blueprint that explains how elements of information technology and information management work together as a single unit [1]. Framework is a reference that is used to help complete a goal. Digital evidence or electronic evidence is any evidentiary information stored or transmitted in digital form which the parties to a legal case can use for court hearings. Before accepting digital evidence, the court will determine whether the evidence is relevant, authentic, hearsay and whether a copy is acceptable or an original is required.

Reflecting on a judicial process that questioned the strength of the evidence presented in the court. In the trial process, the statement of the digital forensic expert actually made a person's position biased. It may be that there is no strong evidence that confirms someone's involvement in a case because the methods used are not known as theories or methods in digital forensics. This will undermine all expert testimony and evidence presented in the court [2]. Making a framework that can be recognized by all judicial administrators (judges, public prosecutors, attorneys for defendants, witnesses and defendants) is a solution that can be used as a standard so that the evidence process runs well.

SNI is a standard that is well known by the public. The application of SNI to all forms of activity is intended to protect the public interest, state security, and national economic development. Therefore, the framework design is carried out using the Composite Logic method and taking into account the steps stipulated in applicable standards such as SNI 27037:2014, namely regarding specific guidelines related to activities in handling digital evidence. The framework in previous research [3] regarding SNI 27037:2014 is a general framework so it needs adjustments so that it can be used as a framework for collecting digital evidence from social media.

In proving a crime, a scientific proof process is needed. Each stage in the collection of digital evidence must follow the applicable procedures and the process can be accounted for in court. The stages of the process must be stated in a rule and there are procedures that can be used to audit the process. These stages must be carried out in succession so that when these stages are missed in the investigation process, of course it will become a problem and can be sued in court and the results of the investigation carried out are canceled due to procedures that are not carried out [3].

In a previous study [4], a Digital Evidence Collection Framework on Social Media has been created that can be used to collect information from social media, but the framework has not accommodated the collection of

personal information such as chat communication on Facebook Messenger, and detailed profile information hidden by users. This research will try to design a framework that can collect more information. Not only open source data, but also personal data. The solution that will be offered in this research is how to create a framework for collecting digital evidence from social media that can collect information that is private and still refers to national standards that can be recognized by all judicial administrators. The application of Composite Logic can create a new framework, so that the Digital Evidence Collection framework on Social Media can achieve better performance by referring to SNI 27037:2014.

II. METHOD

A. Composite Logic

According to [5] the composite logic model is a model that provides a basis for the selection and combination of variables into a composite indicator to meet the achievement of an organization's goals. Composite Logic models can provide an overview of how several objects collaborate, one or two roles that work together in a pattern to achieve the same goal. A role represents the point of view of several objects that work together by holding on to a goal. Logic modelling can direct each object, activity, role and goal to be achieved in an objective reasoning that can describe the sequence of cause and effect relationships and effects of the connectedness between these objects so that they can relate the problem (situation) to an intervention (input and output), and outcomes [6]. The following is an analogy to the logic model template that the researcher uses in the study as shown in the Fig. 1-3.

The Composite Logic stage is used to combine several model structures into a unified model that maintains the hierarchy or initial arrangement of the existing model framework. The most important thing in the Composite Logic model is to determine the role model of each variable or initial pattern that you want to collaborate on. The role model describes how several objects collaborate, one or two roles simultaneously in a pattern to achieve the same goal. A role represents the point of view of several objects that work together by holding on to a goal. This modelling can assist researchers in exploring the interrelationships of different activities with the same goal. This makes it easier for researchers to classify and collaborate with several frameworks which will eventually produce a set of frameworks [7].

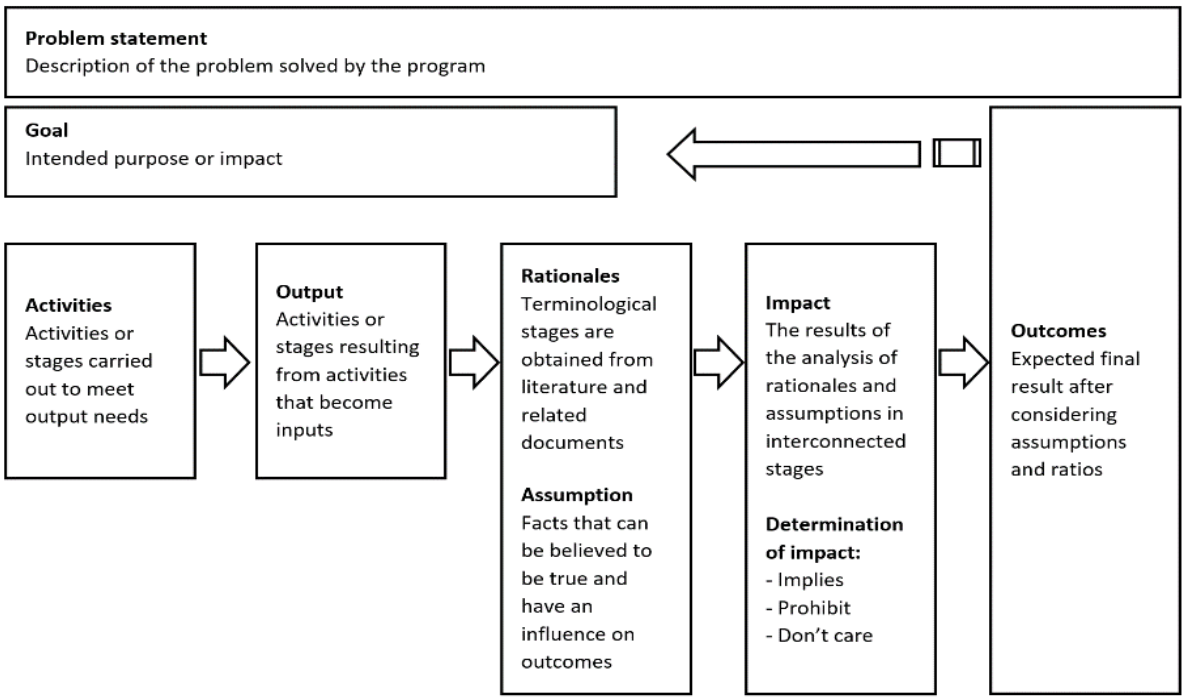

Fig. 1 Logic model template

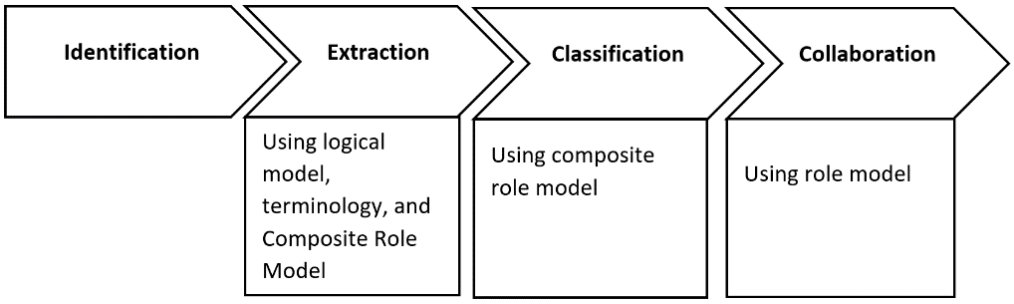

Fig. 2 Composite logic implementation scheme

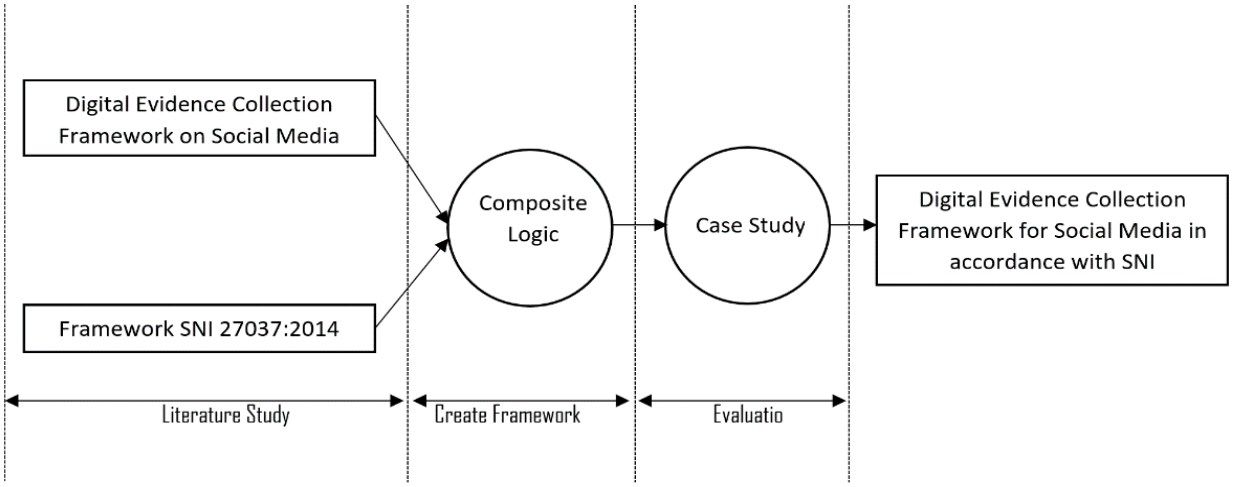

Fig. 3 The concept

Composite logic schemes such as Fig. 2 have other advantages in that they can summarize complex multi-dimensional realities with a view to supporting decision makers and are easier to interpret for many separate indicators and reduce the apparent size of a set of indicators without dropping the underlying information base. Despite some of the advantages that composites have, there are some disadvantages, including being able to send misleading policy messages if they are poorly constructed or misinterpreted. In addition, it can invite simple policy conclusions that are likely to be misinterpreted, and the selection of indicators and weights can be the subject of political disputes [5].

B. The Concept

This research was conducted by combining the Digital Forensics Investigation Framework and the SNI 27037:2014 framework so as to produce a new framework for collecting digital evidence from social media in accordance with Indonesian National Standards.

According to Fig. 3, at the literature study stage there are 2 frameworks that are used as references. The first is the old version of the Framework for Collecting Digital Evidence on Social Media and the second is SNI 27037:2014 regarding specific guidelines related to activities for handling digital evidence. The two frameworks are collaborated with composite logic to combine the two model structures into a unified model that maintains the hierarchy or initial arrangement of the existing model framework. After the new framework is created, it is continued with the evaluation stage, namely by comparing and calculating between the application of the Digital Evidence Collection Framework on Social Media (Framework v1) and the Digital Evidence Collection Framework on Social Media according to SNI 27037:2014 (Framework v2) against the real conditions of digital evidence collection on social media. The evaluation stage was carried out to answer the questions, whether the v2 Framework managed to achieve better performance than the v1 Framework and whether the v2 Framework succeeded in obtaining private data from

social media accounts according to the problems described in the initial section. If these two things are met, it can be concluded that a new framework has been created with better performance than the previous framework.

C. Method Steps

Details about the sequence of steps that are made systematically and can be used as clear guidelines in solving problems, analysing research results, and the difficulties encountered. The steps or stages in this research can be seen in the following Fig. 4.

The first step taken is problem identification. This is done to obtain and find research topics that will be investigated further and identify the problems needed to create a framework for collecting digital evidence on social media in accordance with SNI 27037:2014. Literature studies are carried out to collect reference materials related to research, either through books, articles, papers, journals, papers, and websites.

Then proceed with Digital Evidence Analysis on Social Media. At this stage, it will describe what content data can be posted by social media users. The next stage is the creation of the framework. The framework design is made using the Composite Logic method. The composite logic method will collaborate with the Digital Forensics Investigation Models framework to produce a new framework.

Followed by the testing phase, namely by applying the old version of the Digital Evidence Collection Framework on Social Media (first framework) and the digital evidence collection framework on social media according to SNI 27037:2014 (second framework) to the real conditions of digital evidence collection on social media. Next is the Framework Analysis stage. This stage is an evaluation process of the framework that has been designed. Evaluation of the new framework that has been created to see if the new framework can achieve better performance than the previous framework.

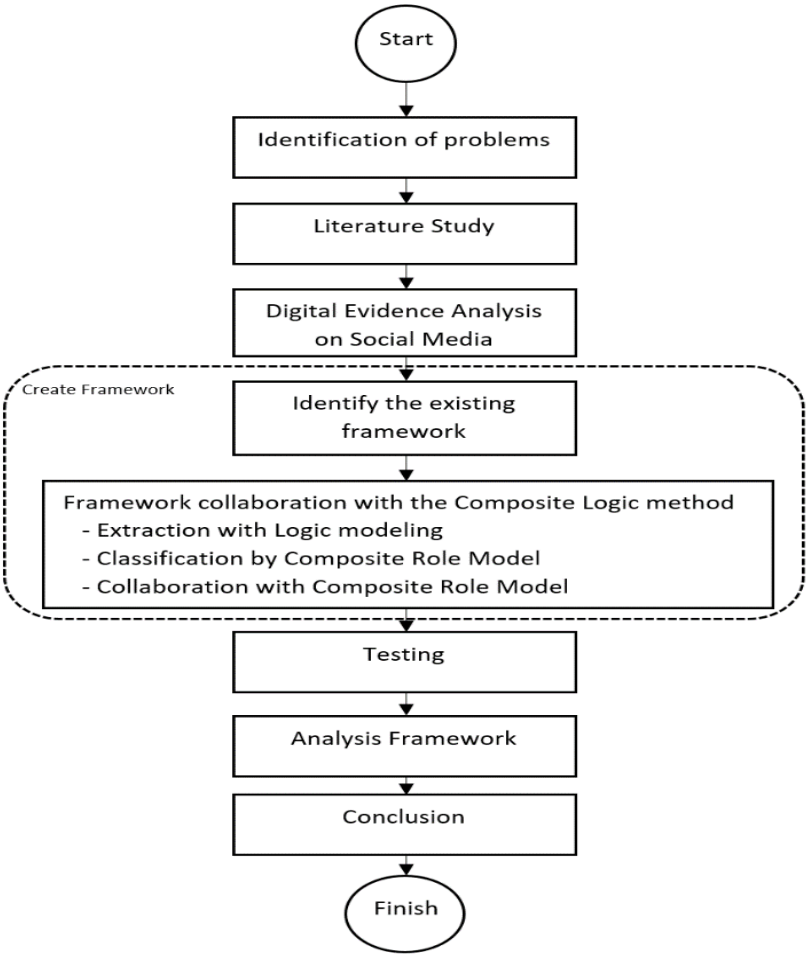

Fig. 4 Research steps

III. RESULTS AND DISCUSSION

A. Analysis of Digital Evidence on Social Media

Social media accounts are logical information that is on the server of each provider and can be accessed via the internet. It is necessary to search using special keywords such as account name [8]. The data logic on the server that is running is data that is vulnerable to change at any time, so the main priority for securing it is to quickly carry out the acquisition process.

In this study, the social media used was Facebook. A Facebook account has been created to be used as a measurement of the implementation of the framework. There are 44 data that will try to be collected with the implementation of the new framework. Each data is divided into several types based on the status of publication. There are 4 types of data in this study, namely: “Public”, “Private”, “Friends”, “Only me”.

B. Previous Framework

There are the following is the identification of the framework related to the research. The first framework, namely the Framework for Collecting Digital Evidence on Social Media, consists of 18 stages. The second framework, the SNI 27037:2014 framework, consists of 22 stages. Details of the stages can be seen in Table I.

C. Composite Logic implementation

Followed by the extraction stage with a logic model. The extraction process is carried out on all existing stages of Digital Forensics Investigation Models. This extraction process uses the Composite Logic Application Scheme. Determination of impact indicators using a role model from the composite, namely "Prohibit", "Implies" and "Don't care".

From each extraction process that has been carried out for each stage of the framework, it will be classified according to the output variables and into three roles, namely prohibit, implies and don't care. The output variables are taken from 4 main stages regulated in SNI 27037:2014, namely the stages of identification, collection, acquisition, and preservation [3]. This classification process is carried out to facilitate the process of the next stage, namely the collaboration process. Classification details can be seen in Table II.

After classification, the next stage is the collaboration process. The results of the collaboration can be seen in Table III.

TABLE I
FRAMEWORK RELATED TO THE RESEARCH

Framework	Stages
Collecting Digital Evidence on Social Media	Planning; Preparation; Internet; Approach Strategy; Collection; Identification; Usage/User Profiles; Triage; Examination; Reconnaissance; Transport & Storage; Preservation; Case Specific; Chronology Timeline; Analysis; Prof & Defence; Presentation; Archive of Evidence
SNI 27037:2014	Investigation planning; Equipment preparation & team direction; Crime scene security risk assessment; Crime scene security; Search for evidence; Identification of evidence; Determining the priority of evidence; Documentation; Recording of evidence (Chain of custody); Determine whether evidence is confiscated or acquired at the crime scene; Confiscate evidence; Provide evidence label; Packing evidence; Collect verbal statements from witnesses; Examination of the security aspects of evidence data; Determination of the acquisition model carried out; Acquisition implementation; Verification of acquisition results; Provide seal of evidence; Checking the security aspects of the transfer of evidence; Transfer of evidence; Storage of evidence

TABLE II
CLASSIFICATION PROCESS

Main stages	Stages	Impact Indicators
Identification	Investigation Planning	Implies
	Team Preparation & Direction	Implies
	Crime Scene Security Risk Assessment	Don't Care
	Crime Scene Security	Don't Care
	Search For Evidence	Implies
	Identification Of Evidence	Implies
	Determining The Priority Of Evidence	Implies
	Documentation	Don't Care
	Determine Whether Evidence Is Confiscated Or Acquired At The Crime Scene	Implies
	Planning (Preparation)	Implies
	Preparation	Implies
	Internet	Prohibit
	Approach Strategy	Implies
	Triage	Implies
Collection	Confiscate Evidence	Don't Care
	Provide Evidence Label	Don't Care
Acquisition	Examination Of The Security Aspects Of Evidence	Don't Care
	Determination Of The Acquisition Model Carried Out	Don't Care
	Acquisition Implementation	Implies
	Verification Of Acquisition Results	Implies
	Collection	Implies
	Identification	Implies
Preservation	Recording Of Evidence / Coc (Chain Of Custody)	Implies
	Packing Evidence	Prohibit
	Collect Verbal Statements From Witnesses	Implies
	Provide Seal Of Evidence	Don't Care
	Checking The Security Aspects Of The Transfer Of Evidence	Implies
	Transfer Of Evidence	Implies
	Storage Of Evidence	Implies
	Usage/User Profiles	Implies
	Examination	Implies
	Reconnaissance	Implies
	Transport & Storage	Implies
	Preservation	Implies
	Case Specific	Implies
	Chronology Timeline	Implies
	Analysis	Implies
	Prof & Defense	Implies
	Presentation	Implies
	Archive Of Evidence	Implies

TABLE III
COLLABORATION PROCESS

Main stages	Stages
Identification	Investigation Planning and Administration; Crime scene security; Crime scene security risk assessment; Define an evidence collection strategy; Internet; Social media account search; Documentation
Collection	confiscate evidence; Provide evidence labels
Acquisition	Examination of the security aspects of evidence; Determination of the acquisition model carried out; Acquisition implementation; Acquisition hash verification
Preservation	Handover chain recording; Collecting Additional Information; Packing evidence; Provide seal of evidence; preserving the state of physical evidence; Submission to Digital Forensics Laboratory

After collaborating with Composite Logic, a framework is then produced that will be used as a framework for collecting digital evidence on social media. The making of this framework follows several provisions including:

- In the extraction process there is an identification of the output which will then be used as the naming of the main stages because it is a goal of each activity or activity.
- The collaboration process is arranged based on the sequence and influence of the application of the role model on each stage obtained from the identification process.
- This framework will be evaluated by applying it in case studies of social media evidence collection.

In accordance with SNI 27037:2014, this new framework is also divided into 4 main stages, namely identification, collection, acquisition, and preservation. The explanation of each stage is as follows:

1) Identification

- Investigation Planning and Administration
  This investigative and administrative planning stage includes the preparation of strategies related to the investigation to be carried out. Starting from the planning tools used, technical investigation planning, and other related matters [3]. Prepare all needs, both administrative and technical matters for the investigation process. Obtain authorization from the local enforcement team and obtain a search warrant to confiscate evidence [9]. Prepare tools, techniques, search warrants, and management support [10].
- Crime scene security risk assessment
  Maintain the security of the investigation team and evidence. For example, to assess whether at a crime scene there are weapons or materials that can cause physical damage [3].
- Crime scene security
  Protect evidence. Security is also carried out to limit not everyone can enter the crime scene and only people who have been authorized by the team [3].
- Define an evidence-gathering strategy
  Dynamically formulate an approach based on the potential and impact on the observer of the specific technology involved, including determining the priority of evidence / forensic triage and determining which evidence is confiscated or acquired at the crime scene. The application of triage can be applied as an initial identification [11].
- Internet
  Setting up an Internet network is necessary for examining artefacts related to Internet activities, such as instant messaging (IM), e-mail, and web browsing [12].
- Search social media accounts
  Social media accounts are logical information that is on the server of each provider and can be accessed via the internet. A search is required using special keywords such as account names. After doing a search, you will find 1 or more social media accounts. Followed by identifying unique or specific information such as username and ID.
- Documentation
  All activities related to finding evidence must be documented. And the documentation here also covers all aspects of the process carried out from the identification stage to the final stage of the investigation which must always be documented [3].

2) Collection

- Seizing evidence
  In Article 1 point 16 of the KUHAP (Criminal Procedure Code) Confiscation is a series of actions by investigators to take over and or keep under the control of movable or immovable objects, tangible or intangible for the benefit of evidence in investigation, prosecution and trial [13].
  In this case the confiscation of social media is the confiscation of intangible objects. Investigators' actions to take over intangible objects in the form of social media accounts must also be included in the Digital Evidence Collection framework on Social Media. As with the process of securing social media accounts in general, the confiscation of social media accounts also applies the same thing, namely by changing passwords and replacing 2-step verification. This aims to take over the control status of social media accounts, which were initially controlled by the suspect, turned to be controlled by investigators and secure all content on the account from possible manipulation by the previous owner or suspect.
- Provide a label of evidence.
  Labelling all evidence to facilitate the reconstruction process and make it easier to identify the evidence [3]. This is done with the aim

of making it easier to identify if at one time the evidence collection process there are several social media accounts that will be processed at once.

3) Acquisition

- Examination of the security aspects of evidence
  Inspection of security aspects to ensure that the acquisition process carried out will not damage the evidence [3].
- Determination of the acquisition model carried out
  On computer equipment, the acquisition process is divided into 3 types, namely acquisitions on powered devices, acquisitions on non-lit devices and partial acquisitions [3]. The acquisition of social media is carried out by considering the availability of data compression features and downloading social media data provided by service providers. If the service provider has data compression and data download features, the acquisition process can take advantage of these features. However, if the service provider does not have this feature, the acquisition process must use another acquisition method, namely by utilizing certain software that has social media data retrieval functions such as Oxygen Forensics, Ufed Cloud Analyzer and others. With Oxygen Forensic Investigators can use any combination of username and password or token retrieved from a mobile device or PC to gain access to cloud storage even when two-factor authentication is enabled on the selected service [14]. With Ufed Cloud Analyzer collect accessible and cloud-based social media data and collect new evidence hidden in social media and cloud-based personal data archives [15].
- Acquisition implementation
  The hard drive acquisition process is different from the social media acquisition process. In the hard disk acquisition process, it is done by copying data in a bit stream image, which is copying each bit by bit [16]. While the acquisition of social media is done by extracting or downloading all information on a social media account by using the credentials or passwords that have been obtained in the previous stage, namely confiscation. Implementation of the acquisition process in accordance with the acquisition method that has been previously determined. This stage is carried out to duplicate digital evidence using acceptable standard digital procedures. The results of the acquisition will be stored in external storage media in the form of DVD, flash disk or hard disk.
- Verify the hash of the acquisition
  Hash function is one of the functions that provide services for verification and authentication because this function produces a unique value for each input [17]. Verification is carried out to ensure that the acquired data is identical to the original data. Verification can be done using a hash function. In the social media acquisition process, hash verification aims to identify the confiscated items in the form of documents and electronic information. In identifying confiscated items, we need to keep in mind the principle of the status quo of the crime scene. Status Quo is a condition where the crime scene (TKP) has not changed, it is still in intact condition like the original / initial state. The hash value can be used in court to explain that the confiscated goods have not changed during the examination process.

4) Preservation

- Handover chain recording
  Chain of custody (COC) is a procedure for recording/documenting chronological evidence from the time the evidence is found, the duplication process, the storage of evidence either physically or digitally to the presentation and final decision on the evidence. Chain of custody is used to ensure the integrity and originality of evidence [18]. The results of the analysis or initial examination can be used as a guide for a digital forensic laboratory. This can be stated in the minutes of confiscation [13]. Metrological traceability is an activity to ensure that the measurement process carried out has a traceable value to International Units [19]. COC and confiscation minutes have my terminology, which is to record information about ownership, when the evidence was duplicated and to whom the evidence was submitted.
- Collecting Additional Information
  This is done to get more clues and find information related to the evidence found. When compelling evidence is found in digital media, it is important to demonstrate a connection between that evidence and a specific and identifiable suspect. This stage also includes Reconnaissance which is an exploration carried out to obtain additional information. One of the goals of this stage is to find out from which digital device the social media account was accessed. Because the mobile

forensics method can be used to get traces and forensic evidence from social media [20]. So that a connection will be obtained between the suspect's digital device and social media accounts.

- Packing evidence
  Packing or carrying out the process of packaging evidence by inserting evidence into the evidence wrapping equipment. Pay attention to the security aspect of the evidence when it will be packaged [3]. For confiscated objects as referred to in Article 38 in conjunction with 39 in conjunction with 129 of the Criminal Procedure Code, the evidence is packaged/sealed [21].
- Provide a seal of evidence
  Packaged evidence must be sealed to ensure that during the transfer process the evidence remains in its packaging and is useful in maintaining the integrity of the evidence [3].
- Preserving the state of physical evidence
  In transferring evidence, officers must be careful and always pay attention to the security of evidence. Evidence must be stored in a storage area that has good security facilities and good storage facilities. For example, it must have facilities to keep the temperature of the storage room not too hot or too cold so that it can cause damage to evidence. All evidence collected must be placed in a safe place as it is important that the evidence is safe from tempering and it is necessary to maintain the integrity of the evidence. Isolate, secure and preserve the state of physical and digital evidence. This includes preventing people from using digital devices or allowing other electromagnetic devices to be used within the affected radius. Security aspect checks are carried out to ensure the evidence is safe during the process of transferring evidence from the crime scene to a storage area or digital forensic laboratory.
- Submission to digital forensic laboratory
  The social media analysis process involves four different steps, namely data discovery, collection, preparation, and analysis [22]. However, if it refers to the position of the expert who must be independent and not involved in the investigation (confiscation) process, the analysis stage and the reporting stage are separate activities from the digital evidence collection framework on social media. The analysis and reporting stages are the stages that apply in the digital forensic laboratory. This was also conveyed [3] at the final stage of the security aspect of the transfer of evidence, namely ensuring that the evidence is safe during the transfer process to the laboratory. The digital forensic laboratory will apply other frameworks according to the storage media used by investigators to store cloned/extracted results from social media. The laboratory will keep all evidence that may need to be used for reference in the near future and may also need to be used for evidentiary purposes [23]. After conducting the examination, the digital forensic officer will issue a separate report in accordance with the framework and SOPs that apply in the digital forensic laboratory.
  After the minutes of the digital forensic laboratory are published, on this basis the investigator can conduct an examination of the digital forensic officer as a Digital Forensic Expert. Experts are independent parties and are not involved in the investigation process. In a court [24] an opinion is expressed, the expert cannot provide information at the trial because if they are involved and assist the police in the investigation process.
  In this case the expert also cannot be involved in the confiscation process which is the investigator's authority in accordance with Article 1 number 16 [13]. This is what causes the Analysis and Reporting process which is the task of digital forensic experts and is separated from the Digital Evidence Collection process on Social Media.

The next stage is to apply the Digital Evidence Collection Framework on Social Media (Framework v1) and the Digital Evidence Collection Framework on Social Media according to SNI 27037:2014 (Framework v2) to the real conditions of digital evidence collection on social media. The collection process is applied to a Facebook account that has been created in the previous stage, namely to a Facebook account that has 44 data which is divided into 4 types of data.

After collecting by applying Framework v1 and v2, to find out the difference in the amount of data that was successfully obtained by giving a value of 0 for "data that cannot be obtained" and giving a value of 1 for "data that can be obtained". From the test results, the results of the application of Framework v1 as many as 18 data were successfully obtained. Meanwhile, in the application of Framework v2, 38 data were obtained. After knowing the value of each data obtained, the next step is to perform calculations using (1).

$$N_n = \left(\frac{\Sigma F_n}{\Sigma F_t}\right) x100 \quad (1)$$

Information:
N_n : The percentage value of the data that was successfully collected
ΣF_n : The amount of data that was successfully collected
ΣF_t : Total data on social media

Framework v1

$$N_n = \left(\frac{\Sigma F_n}{\Sigma F_t}\right) x100 \ = \left(\frac{18}{44}\right) x100 = \ 40.9\%$$

Framework v2

$$N_n = \left(\frac{\Sigma F_n}{\Sigma F_t}\right) x100 = \left(\frac{38}{44}\right) x100 = 86.36\%$$

Furthermore, the calculation of the difference in the final value of each framework with (2).

$$S = N_2 - N_1 \quad (2)$$

Information:
S : Difference Value
N_2 : Percentage Value Framework v2
N_1 : Percentage Value Framework v1

$$S = N_2 - N_1 = 86{,}36 - 40{,}9 = 45.46$$

The value of the S variable is positive, which means that the new framework has succeeded in achieving better performance than the previous framework. The percentage of data collection in the new framework is greater than the percentage of data collection in the old framework.

IV. CONCLUSION

Based on the data and facts obtained, the application of composite logic can create a new framework with better performance than the previous framework with reference to SNI 27037:2014. The research that has used the composite logic method is a collaboration of the Digital Evidence Collection Framework on Social Media and the Digital Forensic Investigation Framework SNI 27037: 2014. The stages in the two frameworks that have the same terminology have been combined and given a new name. Previous research has succeeded in making the collection of digital evidence from social media that is open source, but related to private data, it must be preceded by several more steps. This research has succeeded in making a framework with better performance by referring to SNI 27037:2014. This framework can be used to fulfill the needs of investigations by law enforcement and can comply with the applicable laws in Indonesia. In addition to obtaining private data, the advantage of this framework is that it guarantees the integrity of the data from the confiscation process to submission to the digital forensic laboratory. And in the end it will be presented in court as valid evidence to support proving a crime in the court process. In this study, data collection did not reach 100% performance. There were some data that were not collected, one of which was posting on the Facebook Page. In future research, it is necessary to create a framework that can collect this information so that it can link digital evidence on the Facebook Page with the suspect. The final result of this research is not a legal stipulation, so a study in the legal field is needed to become a standard operating procedure that applies in the investigation process.

REFERENCES

[1] R. Setiawan, "Perancangan Arsitektur Enterprise Untuk Perguruan Tinggi Swasta Menggunakan Togaf Adm," *J. Algoritm.*, vol. 12, no. 2, pp. 548–561, 2016.

[2] Lontar.id, "Ahli Digital Forensik Pertanyakan Kekuatan Alat Bukti Rekaman KPK - Lontar.id," 2019. https://lontar.id/ahli-digital-forensik-pertanyakan-kekuatan-alat-bukti-rekaman-kpk/ [accessed Oct. 10, 2020].

[3] D. Sudyana, B. Sugiantoro, and A. Luthfi, "Instrumen Evaluasi Framework Investigasi Forensika Digital Menggunakan SNI 27037:2014," *J. Inform. Sunan Kalijaga*, vol. 1, no. 2, pp. 75–83, 2016.

[4] 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.

[5] M. Nardo, M. Saisana, A. Saltelli, *Handbook of Contructing Compsoite Indicators: Methodology and user guide*. 2008.

[6] P. F. McCawley, "The Logic Model for program planning and evaluation," *Univ. Idaho*, pp. 1–5, 2002.

[7] 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.

[8] M. T. Anwar, "Analisis Pola Persebaran Pornografi pada Media Sosial dengan Social Network Analysis," *J. Buana Inform.*, vol. 9, no. 1, pp. 43–52, 2018.

[9] S. Perumal and N. Norwawi, "Integrated computer forensic investigation model based on Malaysian standards," *Int. J. Electron. Secur. Digit. Forensics*, vol. 3, no. 2, pp. 108–119, 2010.

[10] F. Cohen, "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.

[11] R. Rizal, "Network Forensics Untuk Mendeteksi Serangan Flooding Pada Perangkat Internet Of Things (IoT)," *J. Teknol. dan Sist. Komput.*, p. 67, 2018.

[12] M. K. Rogers *et al.*, "Journal of Digital Forensics , Security and Law Computer Forensics Field Triage Process Model Computer Forensics Field Triage Process Model," *J. Digit. Forensics, Secur. Law*, vol. 1, no. 2, pp. 1–21, 2006.

[13] KUHAP, "Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Kitab Undang Undang Hukum Acara Pidana (KUHAP)," *Kpk*, vol. 1951, no. 8, 1981.

[14] "Oxygen Forensics - Mobile forensic solutions: software and hardware." *https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective* [accessed Aug. 17, 2021].

[15] "Cellebrite UFED CLOUD | Access Cloud-Based Evidence." *https://www.cellebrite.com/en/ufed-cloud/* [accessed Aug. 17, 2021].

[16] Sunardi, I. Riadi, and M. H. Akbar, "Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 3, pp. 576–583, 2020.

[17] Y. Bin Pairin, "Kode Autentikasi Hash pada Pesan Teks Berbasis Android," *Eksplora Inform.*, vol. 8, no. 1, p. 6, 2018.

[18] Y. Prayudi and A. SN, "Digital Chain of Custody: State of The Art," *Int. J. Comput. Appl.*, vol. 114, no. 5, pp. 1–9, 2015.

[19] Ilham, "Ketertelusuran Metrologi atau Pengukuran dalam ISO IEC 17025 versi 2017 - LABMUTU," 2020. *https://www.labmutu.com/2020/04/ketertelusuran-metrologi.html* [accessed Jul. 21, 2021].

[20] M. S. Hartawan, A. Damuri, and A. S. Putra, "Pengolahan Data Untuk Menemukan Bukti Pada Mobile Forensik," 2020.

[21] U. M. Aruan, "Tata Cara Penyitaan Barang Bukti Tindak Pidana Menurut Kuhap," *Lex Crim.*, vol. 3, no. 2, pp. 77–85, 2014.

[22] S. Stieglitz, M. Mirbabaie, B. Ross, and C. Neuberger, "Social media analytics – Challenges in topic discovery, data collection, and data preparation," *Int. J. Inf. Manage.*, vol. 39, no. October 2017, pp. 156–168, 2018.

[23] G. Palmer, "A road map for digital forensic research," *Proc. Digit. Forensic Res. Conf. DFRWS 2001 USA*, pp. iii–42, 2001.

[24] M. Y. F. N. HERIANI, "Kedudukan Ahli dan Pendapatnya dalam Perkara Pidana - Hukumonline.com." *https://www.hukumonline.com/berita/baca/lt57bc379b6a154/kedudukan-ahli-dan-pendapatnya-dalam-perkara-pidana/* [accessed Jul. 28, 2021].