

Framework Design for the Retrieval of Instant Messaging in Social Media as Electronic Evidence

Linda Rosselina

*Electrical Engineering Department
Universitas Indonesia (UI)
Depok, Indonesia
linda.rosselina@depok.go.id*

Tofan Hermawan

*Electrical Engineering Department
Universitas Indonesia (UI)
Depok, Indonesia
h3rmawantofan@gmail.com*

Yohan Suryanto

*Electrical Engineering Department
Universitas Indonesia (UI)
Depok, Indonesia
yohan.suryanto@ui.ac.id*

Fahdiaz Alief

*Electrical Engineering Department
Universitas Indonesia (UI)
Depok, Indonesia
freddiziel@gmail.com*

Abstract— *The rapid growth of social media features not only brings many advantages but also causes problems. Mainly related to digital evidence when cybercrime occurs. One of the social media features that are currently popular is the unsend message feature in instant messaging applications such as Instagram, Whatsapp, Facebook Messenger, Skype, Viber, and Telegram. In cybercrime, the perpetrator can delete the messages and erase digital evidence, making it difficult to trace. Those artifact messages might be useful for law enforcement or forensic investigators to be used as digital evidence in court. Therefore, an effective and efficient framework is needed to guarantee the data integrity in the mobile forensic investigation process. This paper will discuss the review of several international standards on mobile forensics, namely NIST SP 800-101, ISO/IEC, and SWGDE. This paper also proposes a framework design to retrieve unsend data artifacts on social media according to official and widely used international mobile forensic standards.*

Keywords— *forensics framework, electronic evidence, instant messaging, unsend message feature, social media, international standards, NIST SP 800-101, ISO/IEC, SWGDE*

I. INTRODUCTION

Social media usage continues to increase, along with the development of digital technology [1]. The features offered by social media applications are increasingly sophisticated and diverse [1]. On the other hand, crime in cyberspace is also increasingly happening by utilizing this social media application. Social media can send pornographic content, threats of violence, intimidation, fraud, cyberbullying, illegal transactions, and other crimes [2]. When cybercrime cases occur, law enforcers need to obtain digital evidence to assist in the investigation process.

Nevertheless, social media has developed a new feature where users can delete messages sent at the receiver and sender (unsend data). In obtaining digital evidence, investigators need a specialized mobile forensic technique to recover digital evidence from mobile phones. This digital evidence can be used as electronic evidence in court as long as it can be accessed, displayed, and guaranteed integrity [3].

Investigations and litigation in law often involve more than one agency or organization. Cyberspace is open space without limits so that crime can occur across countries and continents. Thus, standards are needed to regulate the processes, procedures, and management of digital forensic aspects of cybercrime, both locally and internationally. Standards are set to ensure a product or service functions by its original purpose. The standard contains an explanation of the specified procedures and specifications. Standards are agreements that can significantly affect the reliability, safety, and efficiency of work [4]. International standards are an essential requirement that guarantees the enforcement of the regulations across jurisdictional and geographical boundaries. Standards provide essential frameworks needed by governments to increase national and international trust. In the industrial world, standards are needed to guarantee quality and gain consumer confidence. The use of guaranteed standards in handling mobile forensic cases will affect the integrity and accuracy of the data presented in court [5].

In some cases, digital evidence is incomplete, contaminated, invalid, making it challenging to uncover cybercrime [5]. All of this happened because of the lack of digital forensic governance in the organization. Therefore the forensic examiner must follow the digital forensic standards that have been formally established and recognized internationally. Several international standards are widely used as a reference in digital forensics, Scientific Working Group on Digital Evidence (SWGDE), standard ISO/IEC 27037:2012-Guidelines for identification, collection, acquisition, and preservation of digital evidence, and NIST SP 800-101 Rev.1:2014-Guidelines on Mobile Devices Forensics.

This paper discusses the comparison of the application of the NIST SP 800-101 Rev.1: 2014, ISO/ IEC 27037: 2012, and SWGDE standards on mobile forensics, specifically for the collection of data artifacts. As the results of this comparison, a framework design is proposed for retrieving instant messaging evidence in social media unsend features case. This framework is arranged to ensure data integrity in taking data artifacts unsend on social media.

II. MOBILE FORENSIC ON SOCIAL MEDIA

A. Mobile Forensic

Mobile devices have various and growing features. Cellular devices have microprocessors, ROMs, RAM, radio modules, digital signal processors, microphones, speakers, and various hardware keys, interfaces, and LCD screens. NAND or NOR memory on a mobile device stores the operating system used. Whereas in RAM, the code is executed. Each mobile device has different physical and technical characteristics [5]. Cellular devices can be classified into several types. The first is a cellphone that only has voice and message communication devices. The second is a smartphone that has more advanced multimedia capabilities and services. [6]

Mobile forensics is the science of finding digital evidence from cellular devices using recognized methods. The examiners can use commercial forensic software tools or open-source tools when needed. The forensic tool is designed to be able to calculate the integrity hash of the data obtained. This tool retrieves data without changing its content, from the handset's UICCs and internal memory. [6]

B. Unsend Message Features on Social Media

Competition in the social media industry is very tight. Every social media always updates its features to attract more users. An exciting feature developed by the social media industry is unsend messages features. These features can be used to delete message content from the sender's or recipient's side. In 2018 Instagram officially released the unsend message feature [7], while Line and Whatsapp issued the function with a duration of 24 and 7 hours respectively in 2017 [8], while Telegram is instant indefinitely starting to be introduced in 2019 [9]. Facebook Messenger has a feature that is the same as the duration of 10 minutes after sending it since 2019 [10]. Snapchat has a unique feature since 2018 that automatically deletes messages sent to senders and recipients after the application is closed but only applies to unread messages [11]. In contrast, Viber has had this feature since 2015 [12].

C. Mobile Device Tools Classification System

In digital forensics, it is crucial to know the various kinds of cellphone acquisition tools and devices. It is also essential to know what kind of data can be recovered with these tools. This classification is used to create a framework for comparing extraction methods using different tools to facilitate the digital forensic process. System classification tools are explained in Figure 1 below: [6]

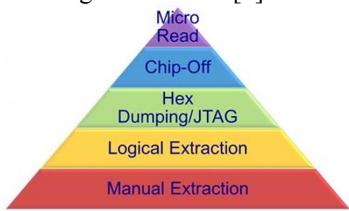


Fig. 1. Mobile Device Tool Classification System

D. Forensic Tools Capabilities

Forensic software seeks to meet the needs of conventional investigations with various devices in circulation [6]. More complicated situations, such as recovering data deleted from the device's memory, require more specialized tools and expertise.

The first step is to block or eliminate storage requests to the device, then calculate the hash value on the data file's contents and repeatedly verify that the entire file's value has not changed. Maintaining the integrity of the original data file obtained from the extraction of data sources is one of the forensic tools' critical characteristics. In a legal aspect, integrity is very critical. It is also crucial that investigation and analysis can be implemented repeatedly using the same baseline. [6]

III. SUMMARY OF FORENSIC INVESTIGATION STANDARD SWGDE, ISO/IEC 27037: 2012, AND NIST SP 800-101 REV.1:2014

Since 1984, the international community has developed digital forensic examination methods [13]. Different standards and models of forensic investigations have been adopted in various countries to identify, acquire, and preserve digital evidence [13]. Some digital forensic standards are explained in detail, while some are general. Some methods concentrate on forensic investigation's technical aspects, but others highlight the forensic examination's management aspects. This research will review several digital forensic standards that are widely used in investigations.

A. NIST SP 800-101 REV.1: 2014

This standard describes preserving, acquiring, examining, analyzing, and presenting electronic data as evidence. NIST sets a more specific explanation of mobile devices and the technology used in connection with digital forensic. This guide focuses primarily on cellular devices' characteristics, such as tablets with cellular voice and smartphones, essential in incident examinations. [6]

NIST SP 800-101 divides digital forensic procedures into 4 (four) phases, as described in Figure 2. Below [13]:

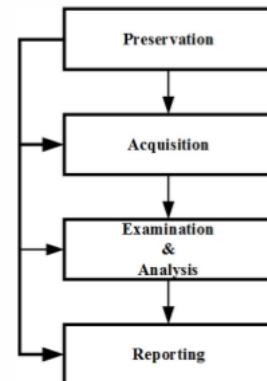


Fig. 2. Forensic process based on NIST SP 800-101

Phase 1: Preservation

This phase includes exploration, introduction, documentation, and collection the electronic evidence. It is crucial to conduct this preservation phase to use digital evidence in official trials or non-formal cases. Failure to store evidence in its entirety can endanger an investigation and result in loss of valuable information. [6] Activities to be carried out in this phase can be seen in Figure 3 below:

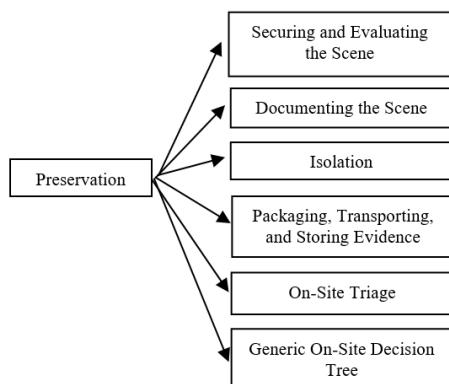


Fig. 3. Preservation Phase

Phase 2: Acquisition

This phase is the phase to get information from mobile devices or related media. Data collection on forensic investigations starts with obtaining information from a mobile device. The procedures, software, and methods used to investigate and make forensic copies of device content are mainly determined by the operating system, device type, and other mobile devices' characteristics. [6]

Phase 3: Examination and analysis

In this phase, digital evidence begins to be revealed, including hidden or removed, as the unsend message feature on social media. One can eliminate digital evidence by deleting or canceling messages that have been sent previously. Investigators can still get full digital evidence by using specific scientific methods. [6]

Phase 4: Reporting

This phase is to prepare a comprehensive review of all activities that have been carried out. The result of this investigation is a conclusion that can be used for the trial process. Proper documentation is needed for all activities and observations conducted during the investigation process to get fair reporting. The results of the test and inspection were also explained in the reporting phase. Reporting documents equipped with notes, photos, and results of the tools used. [6]

B. ISO/IEC 27037: 2012

This research uses ISO/ IEC 27037:2012 to compare with other standards. ISO/ IEC 27037:2012 is an international standard that provides guidelines for specific activities in handling digital evidence, namely identifying, collecting, acquiring, and preserving digital evidence that can have the

power of proof. International Standards guide the process of handling electronic evidence and implementing disciplinary procedures. It also facilitates organizations in interchanging substantial electronic evidence between legal authorities. [14]

Digital data is easily broken. It can change, be changed, or destroyed through improper handling or inspection. The person handling digital evidence must identify and control the risks and effects of digital evidence actions. Failure to handle digital devices in the right way can cause potential digital evidence in these digital devices to be unusable. [14]

Figure 4 shows the digital handling process of ISO/IEC 27037 [13]:

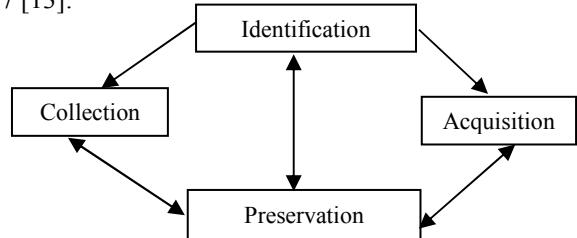


Fig 4. ISO/IEC 27037: 2012 Digital Handling Process

Phase1: Identification

The identification phase includes searching, identifying, and documenting potential digital data used as evidence at trial. Identification of potential electronic evidence related to cases is carried out on cellular devices, especially in the digital storage and processing section. Electronic evidence gathering is based on data priority and volatility. Identification of data volatility ensures the correct sequence of collection and acquisition phases. It also aims to obtain the best data and minimize damage to crucial digital evidence. [14]

Phase 2: Collection

The collection is the phase of handling digital evidence when the device moves from its initial location to a laboratory or other place that has been determined in the investigation for further analysis. Devices that contain potential digital evidence may be in one of two circumstances; when the system is on or when the system is dead. Various approaches and tools are needed, depending on the condition of the device. Local procedures can be applied to the approaches and tools used for the collection process. [14]

Phase 3: Acquisition

The acquisition phase involves producing copies of digital evidence and documenting the actions taken and the methods used. The investigator must adopt the right method in a different set of circumstances. The selection of specific procedures or tools also needs to be appropriately documented. [14]

Phase 4: Preservation

Preservation is the phase of securing crucial electronic evidence on cellular devices. This phase manages the whole

step of processing electronic evidence. The confidentiality of data must be guaranteed during the entire investigation process. In some cases, the confidentiality of potential digital evidence is a requirement, which must be met legally. [14]

C. SWGDE

Scientific Working Group on Digital Evidence (SWGDE) is an organization actively involved in digital and multimedia evidence. It encourages communication and cooperation to ensure quality and consistency in the world's forensic community. The document issued by SWGDE is a best practice for collecting, safekeeping and acquiring digital evidence from cellular devices. The techniques and methods in this document are designed to maintain evidence integrity and maximize data recovery. [16]

In SWGDE, the digital forensic process is divided into 3 (three) stages, namely Evidence Collection and Preservation, Evidence Handling, and Evidence Acquisition. [16]

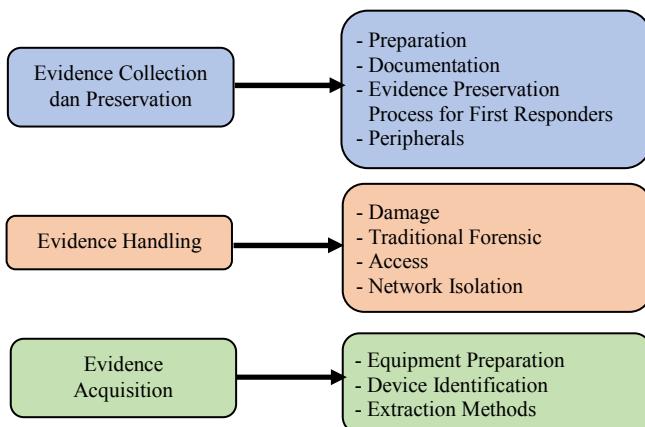


Fig 5. Digital Forensic Process of SWGDE

Phase 1: Evidence Collection & Preservation

At this stage, preparations are made, including determining the equipment and ensuring legal authority to collect digital evidence. Documenting under procedures and storing digital evidence.

Phase 2: Evidence Handling

Improper handling of mobile devices during storage and collection can cause loss of digital data. This procedure ensures that data recovery can run as well as possible. If there is damage to the evidence, then repairs must be under procedures and documented if it is carried out. Traditional forensic processes, such as fingerprints, must be completed on a mobile device before the digital forensic process. If the device is not appropriately handled during storage and collection, physical evidence can be contaminated and cannot be used. This stage ensures access to the device can be done (for example, a device that uses a password) and, after that, disconnects cellular devices from the network, to prevent remote destruction or modification. [16]

Phase 3: Evidence Acquisition

This stage includes the device's preparation, identification of the device, and selecting methods to carry out the extraction process. The device includes hardware and software used to carry out inspection and data extraction and analysis of evidence. The device must be tested and validated before being used in the investigation process. [16]

IV. COMPARISON AND PROPOSED FRAMEWORK

A comparison is made to determine the most appropriate data integrity method in retrieving an unsent data artifacts on social media based on a review of the three standards above. Table I describe features comparison of NIST SP 800-101, SWGDE, and ISO/IEC 27037.

TABLE I. FEATURES COMPARISON OF NIST SP 800-101, SWGDE, AND ISO/IEC 27037

Components	NIST SP 800-101	SWGDE	ISO/IEC 27037
Last Updated	May 2014	July 2019	October 2012
Description	Mid/Low-Level	Mid/Low-Level	High Level
References	Provide procedures for preserving, acquiring, examining, analyzing, and reporting digital evidence. Describe the forensic analysis of mobile devices in more detail	Provides best practices for the collection, preservation, and acquisition of evidence from mobile devices	Provides general references for identifying, collecting, acquiring, and preserving digital evidence
Phases	4	3	4
	- Preservation - Acquisition - Examination and Analysis - Reporting	- Evidence Collection and preservation - Evidence handling - Evidence Acquisition	- Identifying - Collecting - Acquiring - Preserving
Scope	Involves analyzing and examination process.	Designed to ensure the data integrity of electronic evidence	Covers the initial stages of the digital investigation process

Standard is a procedure that becomes a benchmark so that it must fulfill certain conditions to achieve a specific purpose. Some of the digital forensic standard requirements include auditable, repeatable, reproducible, and justifiable, as described in Table II below.

TABLE II. GENERAL REQUIREMENTS RESUME OF NIST SP 800-101, SWGDE, AND ISO/IEC 27037

General Requirements	Description	NIST SP 800-101	SWGDE	ISO/IEC 27037
Auditable	This requirement is reached if all activities carried out by Investigator can be evaluated by an independent assessor	✓	✓	✓

	or other official stakeholders. For this reason, proper documentation is essential.			
Repeatable	This requirement is reached if, after the initial test, the same test results can be repeatedly produced using the same instruments, conditions, procedures, and measurement methods at all times.	√	√	√
Reproducible	This requirement is reached if the same output can be reproduced anytime in different equipment and circumstances using the same assessment procedures.s	√	√	√
Justifiable	This requirement is fulfilled if all investigators' actions and methods in handling electronic evidence can be verified.	√	√	√

NIST SP 800-101, SWGDE, and ISO / IEC 27037 standards have different processes in handling electronic evidence data. Table III summarizes the processes according to each standard.

TABLE III. RESUME OF THE PROCESS IN HANDLING ELECTRONIC EVIDENCE DATA OF THREE STANDARDS

Digital Evidence Handling	Summary	NIST SP 800-101	SWGDE	ISO/IEC 27037
Identification	Identification is a phase of searching, recognizing, and documenting crucial data of digital evidence.	X	√	√
Collection	The collection is a phase of gathering the material things that contain crucial data of digital evidence.	X	√	√
Acquisition	The acquisition is a phase of creating duplicate data according to the provisions. The acquisition product is a crucial digital copy of evidence	√	√	√
Preservation	Preservation is a phase of maintaining and securing the originality dan integrity of digital evidence's crucial data.	√	√	√

Examination and Analysis	Examination and analysis is a phase of reviewing the technical aspect to make the evidence visible to be analyzed.	√	X	X
Reporting	Reporting is a phase of presenting the investigation process and result of the case.	√	X	X

Confidentiality, integrity, and availability, commonly referred to as CIA triads, is designed to guide an organization's information security policies. Table IV shows a comparison of this CIA model in NIST SP 800-101, SWGDE, and ISO/IEC 27037.

TABLE IV. COMPARISON OF THE CIA TRIAD MODEL IN THREE STANDARDS

CIA triad model	Description	NIST SP 800-101	SWGDE	ISO/IEC 27037
Confidentiality	The aspect of confidentiality, protects sensitive information from unauthorized access. In order to ensure data confidentiality, significant digital evidence must be preserved in the right way.	√	√	√
Integrity	This aspect ensures that digital evidence is accurate, trustworthy, and guaranteed that it is not modified in an inappropriate manner.	√	√	√
Availability	This aspect guarantees the availability of crucial digital evidence when it is necessary.	√	√	√

Based on the comparison, it can be concluded that each standard has advantages from each other. SWGDE focuses on handling the initial investigation process. ISO/ IEC has a complete scope in 4 (four) phases of the process. However, ISO/ IEC discusses more non-technical aspects, while SWGDE explains the technical aspects adequately. Meanwhile, NIST has a fairly comprehensive discussion of technical and non-technical aspects and is equipped with an examination, analysis, and reporting process. The drawback is not discussing details in the initial stages. It is necessary to integrate non-technical and technical aspects in several standards to get a comprehensive forensic investigation process specifically to get data from unsend messages features on social media.

Most examiners focus on the technical aspects of the digital forensic process. Figure 7 is the proposed framework based on several standards to get the best method in the investigation process. This framework aims to maintain the data integrity in retrieving data artifacts on unsend message social media features. The design consists of 9 (nine) steps representing the integration of each standard's technical and non-technical aspects. These steps are made to apply to the process of handling electronic evidence, especially in cases of retrieving data artifact.

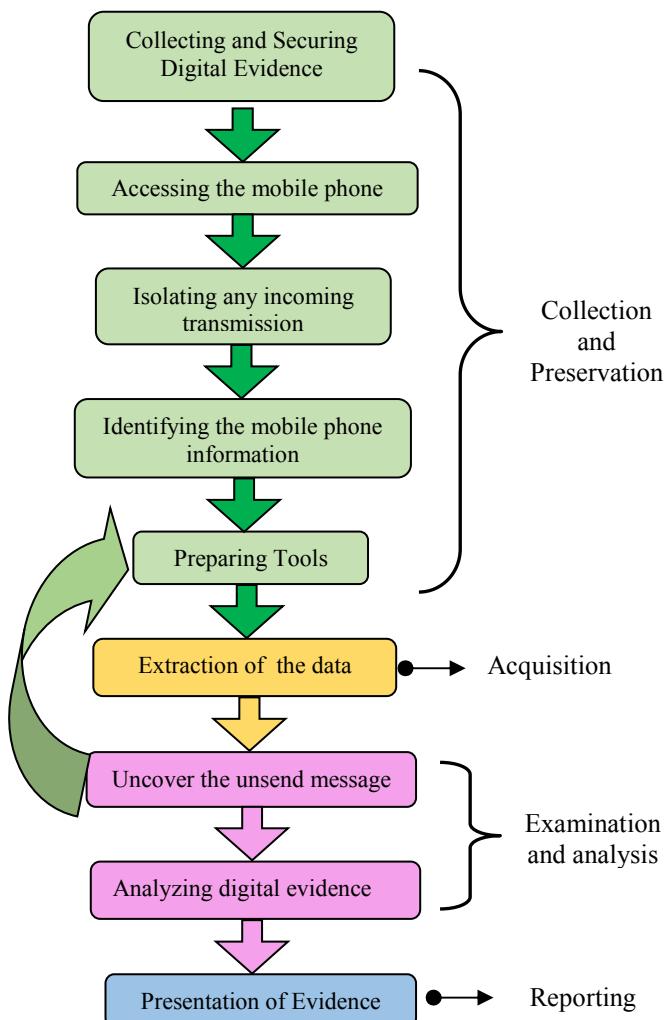


Fig. 6. Proposed Framework

The explanation below is 9 (nine) steps of the proposed framework, as mention in Fig. 6:

1. Collecting and Securing Digital Evidence

In this phase, a new investigation process begins. Electronic evidence is securely transferred to the investigation site. Collecting and securing digital evidence is crucial because incorrect handling will damage the data that might be needed—documentation of all the processes starting from this stage so that all evidence can be accounted for. Documentation is including photographs or details written description about the location and the device's condition.

2. Accessing the mobile phone

The approach and tools used in the investigation can vary depending on the device's condition. Electronic evidence on the device may be in a system of on or off state. If the device is found in a damaged condition, it is possible to repair it first because physical damage does not always damage the data. However, this repair must precisely follow the guidelines for handling the damaged device, and all of the processes must be documented carefully. Forensic examiners must also ensure that all supporting data is complete to access mobile phones such as PIN, passwords, secure codes, or fingerprints used on devices.

3. Isolating any incoming transmission

Mobile devices have the capability to reset to the original factory condition, and they may be performed remotely. It may clear all the user content and memory on the device. Blocking any incoming transmission is needed to ensure that the device's current data condition is not remotely modified or destroyed. Forensic examiners can use airplane mode or keep the mobile device in a faraday bag. Media cards and other hardware devices on mobile devices must not be removed.

4. Identifying the mobile phone information

The device's specification will determine what techniques and tools should be taken to investigate and extract the data process. Therefore, it is crucial to get the cellular device's specifications, including its IMEI (Mobile Equipment Identity), ESN (Electronic Serial Number), operating system, types, and properties. If the device is on, the information on the screen may assist in the identification process. This information determines the route that must be taken in making a forensic copy of the device's contents.

5. Preparing tools

This step is determined by the necessary equipment to take to the scene. Forensic examiners must prepare software and hardware used in the investigation process, whether to use proprietary or open-source software. Tool capabilities may vary according to device type, manufacturer, and model. Examiners may need to employ tools from multiple vendors and run acquisitions at multiple levels to maximize the volume of recovered data.

6. The data extraction

The next process is the data extraction to get the unsend messages from social media. Before extracting data, examiners may need to install some additional software to gain root access to the device's operating system or accept a wireless connection to extract data from the device. Because this technique can leave digital artifacts, the examiner must document the use of this method. Documentation includes all changes that cannot be avoided during the acquisition process. A single tool may not be able to extract all the data on the mobile device. Examiners can be manually resuming mobile device content or using the second forensic tool to provide additional data that cannot be recovered during the initial

extraction. Due to the dynamics of storage media properties in mobile devices, the hash values of multiple extractions from the same device may not be the same. Data integrity must be guaranteed to ensure that copies obtained since the initial process are not modified.

7. Uncover the unsend message

In this process, using the right forensic tools, digital data can be obtained from the device. Thus digital evidence can be revealed, including those that might be hidden or obscured. A copy of this evidence can be made as documentation for the benefit of the court. A single tool may not extract or present all data in a mobile device so that if this process fails, examiners need to return to step 5 (five) to get another tool.

8. Analyzing electronic evidence

In the analysis process, uncovering the unsend message will be examined further to find a significant relation. In addition to data directly present on the mobile device and associated external storage such as UICC / SIM or other media, the examiner should look for other data sources that may be of relevance to the device. This data can be synchronized on other devices such as smartwatches, tablets, and cloud-based mobile devices. This phase also analyzes the data that can be used as evidence in court.

9. Presentation of Evidence

The presentation is the final step to report the investigation process, result, and conclusion related to the case. In this step, the examiners presenting the findings to the authorities or in front of the trial. Presentations are made to explain things difficult to understand for the public so that the data can help the investigation process to find a suspect, or reveal a case. This stage involves the forensic techniques and tools used, including forensic expert testimony and the complete documentation.

V. CONCLUSION

This paper discusses an overview and comparison of international mobile forensic standards NIST SP 800-101, ISO/ IEC 27037, and SWGDE for retrieving unsend messages in Instant Messaging. From this review, it is known that a combination of standards is needed to produce a suitable framework in the mobile forensic investigation. We proposed a framework design to retrieve data on social media unsend message features.

It can be concluded that the application of an appropriate framework can influence data retrieval in the digital investigation process. The use of appropriate procedures will significantly assist in law enforcement and guarantee the integrity of the data.

REFERENCES

- [1] Ranul Deelaka Thantilage & Nhien-An Le-Khac, "Framework for the Retrieval of Social Media and Instant Messaging Evidence from Volatile Memory," 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering, 2019
- [2] Shortall, A., & Azhar, M. A. H. Bin. Forensic Acquisitions of WhatsAppData on Popular Mobile Platforms. International Conference on Emerging Security Technologies (EST), 2015:13–17
- [3] Law Indonesia No. 11 of 2008 concerning Electronic Information and Transactions
- [4] Marthie Grobler, "Digital Forensic Standards: International Progress," Proceedings of the South African Information Security Multi-Conference (SAISMIC2010), 2010
- [5] ISO/IEC 27037:2012 Information technology-Security techniques-Guidelines for identification, collection, acquisition, and preservation of digital evidence
- [6] NIST Special Publication 800-101 Revision 1. Guidelines on Mobile Device Forensics
- [7] <https://www.nottinghampost.com/news/uk-world-news/new-feature-instagram-lets-you-1050352> [accessed 04 April 2020]
- [8] <https://tekno.kompas.com/read/2017/12/14/20070037/septi-whatsapp-pesan-terkirim-di-line-kini-bisa-ditarik> [accessed 03 April 2020]
- [9] <https://tekno.kompas.com/read/2019/03/27/14420087/telegram-sudah-bisa-hapus-pesan-tanpa-batas-waktu-begini-caranya> [accessed 03 April 2020]
- [10] <https://www.liputan6.com/tekno/read/3888436/pengguna-facebook-messenger-kini-bisa-hapus-pesan-terkirim> [accesed 04 April 2020]
- [11] <https://inet.detik.com/cyberlife/d-4073182/pesan-terkirim-snapchat-kini-bisa-dihapus-tapi diakses> [accesed 04 April 2020]
- [12] <https://www.ubergizmo.com/2015/11/viber-update-delete-messages-sent/> [accessed 04 April 2020]
- [13] Akinola Ajijola, Pavol Zavarsky, Ron Ruhl, "A Review and Comparative Evaluation of Forensics Guidelines of NIS T SP 800-101 Rev. 1 :2014 and ISO/IEC 27037:2012," World Congress on Internet Security (WorldCIS-2014), 2014
- [14] ISO/ IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence
- [15] Ivans Kigwana, H.S. Venter, "A Digital Forensic Readiness Architecture for Online Examinations," SACJ 30 (1) July 2018, 2018
- [16] SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition
- [17] Michael Kohn, Jan H. P. Eloff, MS Olivier, "Framework for a Digital Forensic Investigation," Information and Computer Security Architectures Research Group (ICSA) Conference, 2006