Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones

Muhammad Saleh Jafri*[1], Suwanto Raharjo[2], M. Rudiyanto Arief [3]
[1] PJJ Study Program Master of Informatics Engineering Universitas AMIKOM Yogyakarta
[2] Informatics IST AKPRIND Yogyakarta
[3] Study Program Master of Informatics Engineering Universitas AMIKOM Yogyakarta
E-mail: *[1]**muhammads.1213@students.amikom.ac.id**, [2]wa2n@akprind.ac.id,
[3]rudy@amikom.ac.id

Abstract

A forensic investigator or analyst should implement an appropriate digital forensic framework to acquire valid digital evidence to be presented at court. Choosing an unsuitable digital forensic framework with the investigation process may lead to failure at acquiring or maintaining complete digital evidence. Missing a step or turning a certain step into another irrelevant step may lead to unclear results and invalid conclusions. Digital evidence extracted from risky electronic evidence cannot be accepted by the court. Accordingly, a forensic investigator or forensic analyst should refer to a structuralized standard structure to perform well.

Several internal digital forensic frameworks are available, one of which is the Good Practice Guide for Computer-based Electronic Evidence [1], an English issuance by ACPO (Association of Chief Police Officers) in cooperation with 7Safe. The digital forensic framework is commonly called the digital forensic framework from ACPO or the ACPO Framework.

This research brings into focus the analysis of the percentage of success rate for using the ACPO digital forensic framework or the ACPO Framework in comparison with another digital forensic framework, i.e., NIST Framework. This research is also aimed at examining the performance of a mobile forensic tool, i.e., Cellebrite's UFED Touch2 in comparison with another mobile forensic tool for digital evidence acquisition in smartphones.

The research objects were smartphones containing deleted WhatsApp messages. This research successfully implemented the ACPO Framework for digital evidence acquisition in smartphones using Cellebrite's UFED Touch2 as the mobile forensic tool.

Keywords *— Digital Forensic Framework, Mobile Forensic, Smartphone, ACPO Framework, Cellebrite's UFED Touch2*

1. INTRODUCTION

Using the Internet, smartphone users are now allowed to communicate using social media applications. Indonesia's most popular social media applications in 2020-2021 are demonstrated in Figure 1.

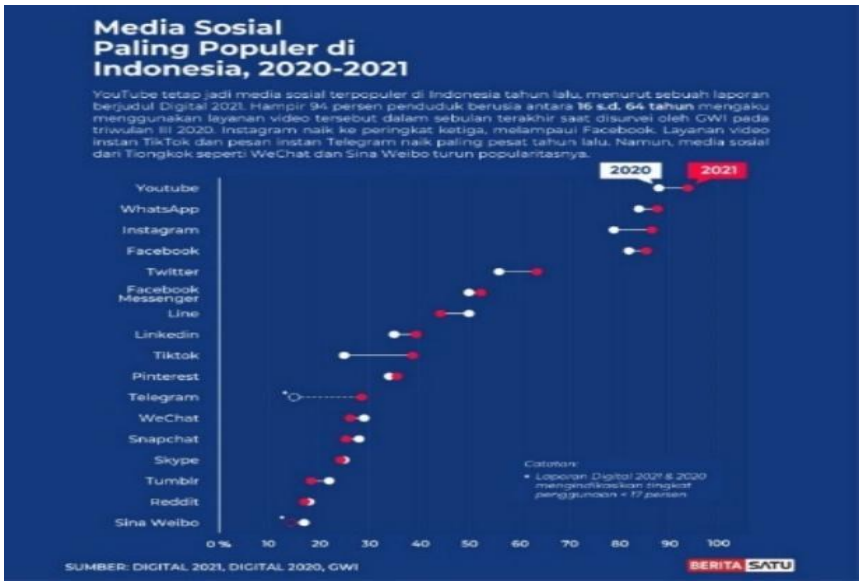

Figure 1 Indonesia's Most Popular Social Media Applications in 2020-2021

Figure 1 exhibits the most popular social media applications in 2020-2021, the data of which can be accessed at beritasatu.com [2].

In other words, the existence of social media potentially brings about crimes, committed by perpetrators, who, using social media, commit illegal acts, e.g., spreading of fake news/hoaxes, humiliation/defamation of a person or institution, incitement/provocation, cyberbullying, online prostitution/pornography, drug transactions, and others. Data of social media misuses are indicated in Figure 2.

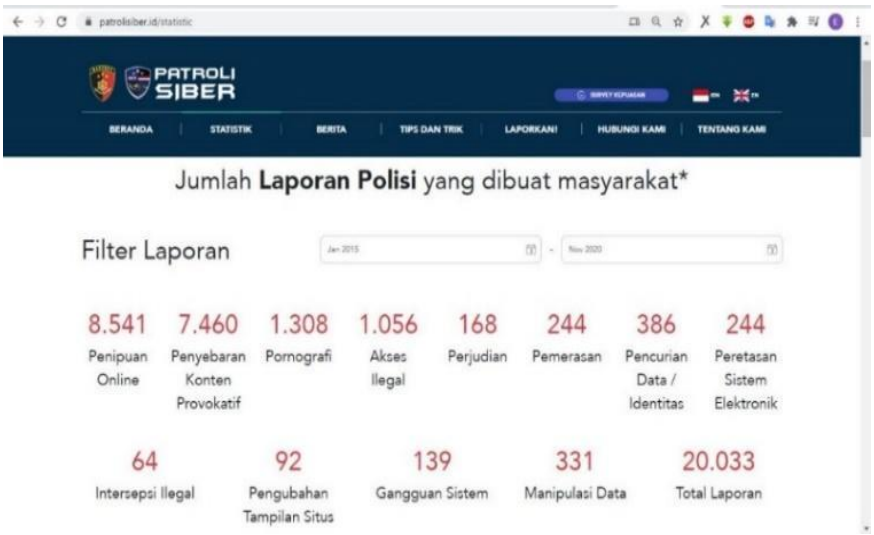

Figure 2 Police Report Data on Cybercrimes Reported by the Community. This survey was carried out in January 2015-November 2020 (patrolisiber.id)

Figure 2 delineates data on cybercrimes reported to Polri from January 2015-November 2020. They are available at the official site *Patroli Siber* managed by Polri [3]. Increasing community reports/complaints are indicative of a high number of unsettling and worrisome cybercrimes in Indonesia.

Digital evidence acquisition in digital forensic, in general, encompasses seizure, acquisition in digital media, analysis, digital evidence acquisition, and digital evidence reporting. Those activities are the responsibility of forensic investigators or analysts.

There are many international digital forensic frameworks, most of which are government-sponsored. In this regard, the government serves as a reference guiding in-charge apparatuses to act correctly and procedurally in investigating cybercrimes and computer-related crimes and analyzing evidence. Two popular references are the Good Practice Guide for Computer-based Electronic Evidence [1] issued by ACPO (Association of Chief Police Officers) in conjunction with 7Safe and Forensic Examination of Digital Evidence: A Guide for Law Enforcement [4] issued by NIJ (National Institute of Justice) under the auspices of the U.S. Department of Justice. NIST (National Institute of Standards and Technology) is a standardizing body under the auspices of the U.S. Department of Commerce. It has standards in mobile forensics, the name of which is NIST Special Publication 800-101 [5]. The standards regulate digital evidence security/acquisition levels, namely Manual Extraction, Logical Extraction, Physical Extraction, Chip-Off, and Micro Read. Digital Forensics Research Workshop (DFRWS) was convened in the United States in 2001 and attended by academicians, digital forensic researchers, and institutions concerning cybersecurity [6].

Emphasized in several digital forensic frameworks above, digital evidence investigation and analysis must be suitable with the standard process. Forensic investigators or analysts should opt for an appropriate digital forensic framework and mobile forensic tool. Selecting an inappropriate digital forensic framework and mobile forensic tools may lead to incomplete or lost digital evidence. Missing one step or turning a step into another irrelevant one may lead to unclear findings and invalid conclusions. Digital evidence extracted from risky electronic evidence is unacceptable in court.

Research on digital forensic frameworks was commenced by [7], who discussed network forensics at Klabat University, in which data from the server farm of the university's Network Operation Center (NOC) were collected and analyzed. The DFRWS (Digital Forensic Research Workshop) digital forensic network or the DFRWS Framework was applied to carry out network forensics at Klabat University. This research was aimed to analyze how frequently the system and network were interrupted by examining log servers and firewalls and to conduct handling and early detection of network interruptions.

[8] investigated digital forensic frameworks for mobile forensics. The research successfully acquired digital evidence using the National Institute of Justice (NIJ) framework. The stages were identifying, proposing a solution, pilot testing the solution, evaluating, and reporting the result. The research used some mobile forensic tools, i.e., MOBILedit Forensic, Wondershare dr. Fone for Android devices, and Belkasoft Evidence Center.

[9] observed digital forensic frameworks for mobile forensics. The research recovered deleted digital evidence using the NIST framework and Oxygen and Belkasoft as the mobile forensic tools.

And yet, the research left the ACPO digital forensic framework or the ACPO Framework, as well as a mobile forensic tool, namely Cellebrite's UFED Touch2, unresearched. Accordingly, research which implements the ACPO Framework for digital evidence acquisition in smartphones is important.

This research is aimed at identifying the percentage of success rate for using the ACPO digital forensic framework or the ACPO Framework in comparison with other digital forensic frameworks, notably the NIST Framework and Cellebrite's UFED Touch2 performance in comparison with other mobile forensic tool performances for digital evidence acquisition in smartphones.

2. RESEARCH METHOD

2.1. Research Methodology Flowchart

We took systematic steps in this research. Figure 3 delineates our research methodology flowchart.

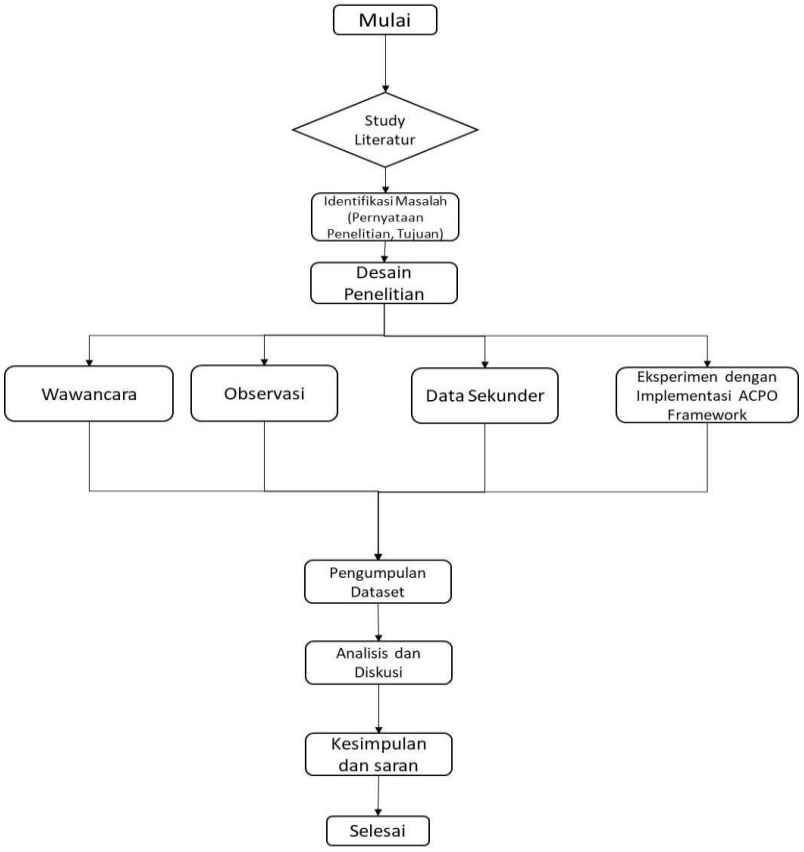

Figure 3. Research Methodology Flowchart

The following is a detailed description of Figure 3.

a. Literature Study

Before carrying out this research, we conducted a literature study of the ACPO Framework for digital evidence analysis and investigation by collecting several journals addressing the framework. We used the journals as a reference to execute this research.

b. Problem Identification

Problems or drawbacks in the previous research were identified by studying relevant references.

c. Research Design

The research design was made consistent with the identified problems.

d. Interview

Data and information were collected by interviewing respondents directly.

e. Observation

Data were collected by direct observation on the tested method using the predefined scenario.

f. Secondary Data

Secondary data were collected from sources compiled by other parties. We collected the data from books available in libraries/book stores, websites, and relevant previous research.

g. Experiment on the ACPO Framework

An experiment on the ACPO Framework was stepwise performed (simulating a criminal case, preparing materials and tools, connecting a smartphone to a mobile forensic tool, extracting data from the smartphone, and searching digital evidence information when digital evidence was found). The experimental stages were implemented by referring to the ACPO Framework stages, namely plan, capture, analyze, and present. The criminal case manipulated in this experiment was a fraud case using WhatsApp.

h. Material and Tool Preparation

The experiment material and tool (a laptop and the tested smartphone) were prepared, as well as the forensic material and tool (Cellebrite's UFED, either the software or hardware) experimented.

i. Dataset Collection

The dataset was collected by collecting all data sources (primary data, secondary data, and data from the experiment).

j. Analysis and Discussion

All data from the dataset or data sources were analyzed and discussed to draw a conclusion.

k. Conclusion and Suggestion

Conclusions were made to answer the research problem. Several suggestions were also afforded.

2.2. Research Area and Time

This research was carried out in Bid Labfor Polda Papua office, whereas the experiment was conducted at Laboratorium Komputer Forensik Subbid Komputer Forensik in March 1st-September 30th, 2021.

2.3. Materials and Tools

The experiment and forensic materials and tools used in this research were provided at Laboratorium Forensik Bid Labfor Polda Papua.

a. Experiment Materials and Tools
   1) A Dell Precision M400 notebook (specifications: OS Windows 7 Professional OS 64bit RAM 8 GB Core i7, HDD 1 TB).
   2) A SAMSUNG GALAXY J2 smartphone (specifications: OS Android 6.0 (Marshmallow), chipset MediaTek MT6737T (28 nm), RAM 1.5GB, internal memory 8GB).
   3) WD Elements Portable Hard Disk with USB 3.0 - 1TB – Black.

b. Forensic Materials and Tools
   1) Cellebrite's UFED Touch2.
   2) UFED Physical Analyzer V.7.38.051 (a software integrated with UFED Cellebrite's UFED Touch2).

   The experiment and forensic materials and tools are depicted in Figures 4, 5, and 6.

Figure 4 Dell Precision M400 Notebook

Figure 5 Cellebrite's UFED Touch2 Device

Figure 4 illustrates the Dell Precision M400 notebook we used for the experiment.

Figure 5 is the mobile forensic tool, i.e., Cellebrite's UFED Touch2, used for mobile forensics in this research.

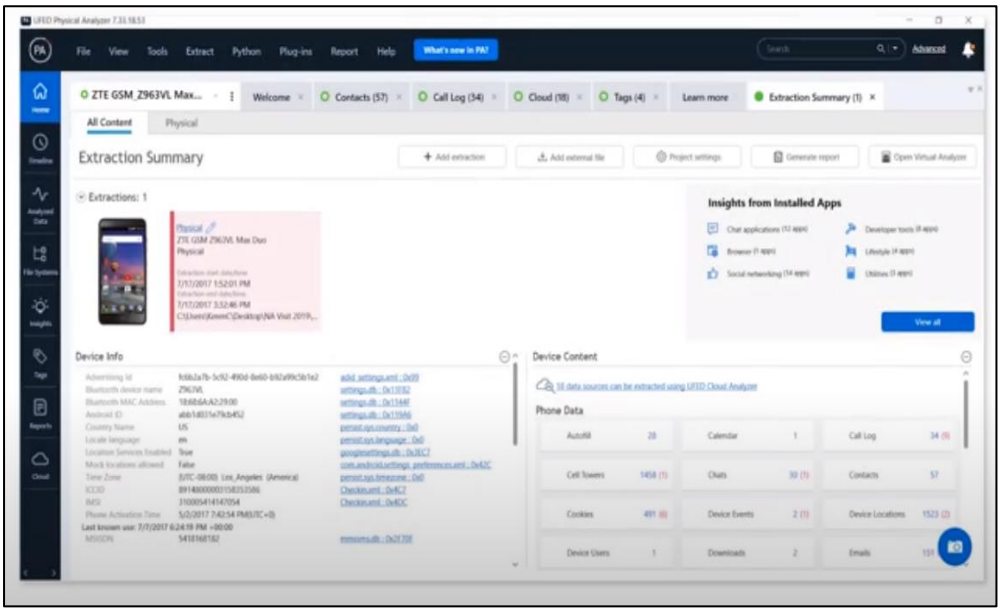

Figure 6 UFED Physical Analyzer V.7.38.051 Software

Figure 6 is the UFED Physical Analyzer V.7.38.051 used as the forensic material and tool to perform mobile forensics in this research.

Figure 7 A Samsung Galaxy J2 Smartphone

Figure 8 WD Elements Portable Hard Drive with USB 3.0 -1TB – Black

Figure 7 is the Samsung Galaxy J2 smartphone used as the experimental material and tool in this research.

Figure 8 is the WD Elements Portable Hard Drive with USB 3.0 - 1TB - Black used to store extracted data.

2.4. Literature Study

a. Digital Forensics

Digital computer forensics or digital forensics is a science or computer technology-based application for legal evidence acquisition (pro-justice). It is aimed at extracting scientific evidence of high technology crimes or cybercrimes, acquiring digital evidence to sentence the perpetrators [10].

b. Digital Evidence

Digital evidence is a term used to describe information or data regarded as evidence stored and extracted from a data store of a computer or other devices.

Digital evidence is classified into original digital evidence and duplicate digital evidence [11].

Original digital evidence is physical items and the data objects as regards the items at the time of seizure. Meanwhile, duplicate digital evidence refers to the accurate digital reproduction of all data objects stored in an original physical item. Digital evidence acquisition calls for a certain method and several tools and/or software. This is a systematic and scientific method in identifying, searching, finding, acquiring, and analyzing digital evidence from a computer, storage media, and electronic device. In the implementation, the method used should cater to the acceptability standard.

c. Mobile Forensics or Mobile Phone Forensics

Mobile forensics or mobile phone forensics is a science relating to the recovery process of digital evidence in a mobile device using methods suitable to forensic conditions [5][12].

The use of mobile phones, e.g., smartphones, with diverse types and operating systems for addressing crimes is increasing. Mobile phone forensics can assist us to combat criminal cases associated with mobile devices [13].

d. Digital Evidence Acquisition

[14] argues that, relating to mobile forensics, there are four digital evidence acquisition techniques, i.e., manual acquisition, logical acquisition, and physical acquisition. The manual acquisition is the easiest acquisition method, by which to extract data and information required, an investigator can access the mobile device investigated and open its data directly. This technique is applicable in all types of smartphones as long as they are not in lock mode. Logical acquisition is extracting an object located in a logical partition of mobile phone memory. Hence, using the technique, an investigator does not extract the data outside the partition, e.g., slack spaces. Most methods used in digital mobile forensics refer to the logical acquisition approach. This process is conducted by making a connection between the mobile phone and the investigator's computer using infrared, Bluetooth, or wire [15]. Forensic investigators use a set of AT instructions to extract specific potential evidence items from a mobile phone. A list of standard AT instructions for 3G mobile phones and the syntax is available in the reference [16]. Physical acquisition is information acquisition by duplicating (copying) all data on the memory chip of a mobile phone to its physical memory, e.g., an SD card and so forth. Two frequently used tools were Flasher Box and Joint Test Action Group (JTAG) [17].

e. Mobile Forensic Tools

Mobile forensics is considered a relatively new area of digital forensics, providing relatively new software and tools used for data extraction in mobile phones. Extracting tools may be either hardware or software, depending on how data are extracted from a mobile device. Various extracting tools are available in the market, as well as other new tools with innovative ideas. Most of the tools

available are commercial and open-source. However, procuring these tools is not easy because of privacy, security, and financial issues [18].

f. Cellebrite's UFED Touch

Cellebrite's UFED Touch is a set of standalone devices (software + hardware) used by forensic analysts and investigators to extract data from a mobile phone. This device enables digital evidence data extraction in a physical item, file system, password, and logical partition to be later investigated using mobile forensics [10]. In this research, we used a file system extraction. The mobile forensic tool used was Cellebrite's UFED Touch2, which was the property of Laboratorium Komputer Forensik Bid Labfor Polda Papua, where we conducted this research.

g. Framework

The term "framework" is often found in system or software development as the development blueprint or concept. A framework, by definition, constitutes a basic structure or concept to solve or cope with a complex problem [19]. In this research, we analyzed a digital forensic framework model in two articles discussing digital forensic frameworks for investigation.

h. ACPO (Association of Chief Police Officers) Digital Forensic Framework

ACPO stands for the Association of Chief Police Officers of England, Wales, and Northern Ireland. It is a private not-for-profit private limited company leading policy practice development in England, Wales, and Northern Ireland for years. ACPO was founded in 1948.

ACPO, in conjunction with 7Safe, issues guidelines or a document entitled Good Practice Guide for Computer-based Electronic Evidence [1] in England.

The guidelines or document is aimed at providing assistance for law enforcement agencies and all parties contributing to cyber security and cybercrime investigations. This document was updated by legislative and policy amendments and issued by needs. There are four fundamental principles in the documents [10], namely:

1) No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
2) In circumstances where a person finds it necessary to access original data held on a computer or storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3) An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4) The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

In this research, we used the ACPO Framework, whose stages are demonstrated in Figure 1.

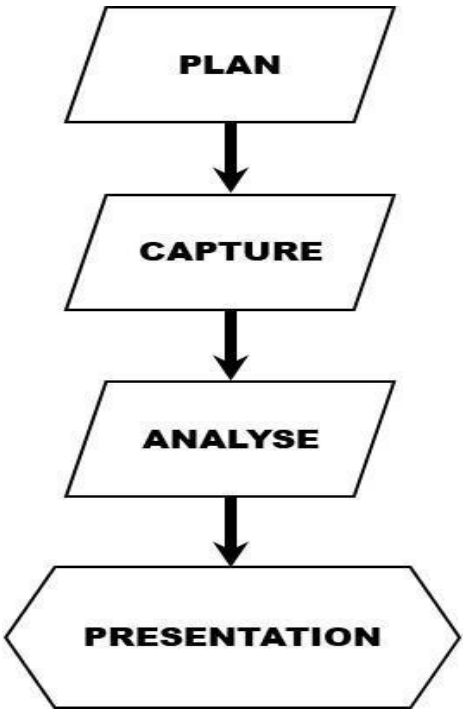

Figure 9 Stages by ACPO Framework

Figure 9 is the outline of stages by ACPO Framework [8], described in detail as follows:

1) Plan: This is a planning stage, where actions made during the research are planned. Planning is aimed at making the research process, including determining what software is used to acquire valid research data, well implemented.
2) Capture: In this stage, research data are recorded, stored, captured, and collected. Capturing research data can be performed using software or hardware available.
3) Analyze: This is an extensive analysis process undertaken to the collected data using a method justified in a technical manner to obtain useful information and answer questions which foster data collection and investigation. Data are analyzed and compared to find a valid research result.
4) Presentation: This stage is publishing research data, which are now useful and justified information. The research actions and results are stated in detail. Suggestions associated with the results are also conferred.

3. RESEARCH RESULTS AND DISCUSSION

This particular section addresses a series of experiments and evaluations. The experiment was carried out by implementing the ACPO Framework for digital evidence acquisition in a smartphone using Cellebrite's UFED Touch2 as the mobile forensic tool and comparing the result with digital evidence acquisition result using the NIST (National Institute of Standards and Technology) digital forensic framework, the research on which had been conducted by [9]. We also carried out an investigation into Cellebrite's UFED Touch2 for mobile forensics.

3.1. Initial Data

In the case simulation, the initial data in the tested smartphone was used to examine the performance of the mobile forensic tool used in recovering the data deleted using manual data deletion. Initial data were composed of contacts, messages, image files, and video files, as exhibited in Table 1.

Table 1 Initial Data in the Case Simulation

No.	Digital Evidence	Total
1	Contact	11
2	Message	47
3	Image	11

Initial data in the simulation were initial data stored in the tested smartphone.

3.2. Case Simulation

This research did not employ an actual criminal case and evidence but made a simulated case.

The case simulated in this research was an evidence deletion scenario. An investigator at the Police Criminal Investigation Unit had managed to find a smartphone unit of a fraud-committing perpetrator. The smartphone was regarded as (physical) electronic evidence, whose digital evidence would be extracted. The perpetrator had deleted the data (WhatsApp messages/chats) in the smartphone manually to commit the fraud.

The research scenario implementation stages are depicted in Figure 10.

Figure 10 Data Deletion Method Scenario

The data deletion method scenario was the evidence deletion scenario in this research.

The implementation of data (WhatsApp messages/chats) manual deletion in the smartphone to simulate a fraud crime is illustrated in Figure 11.

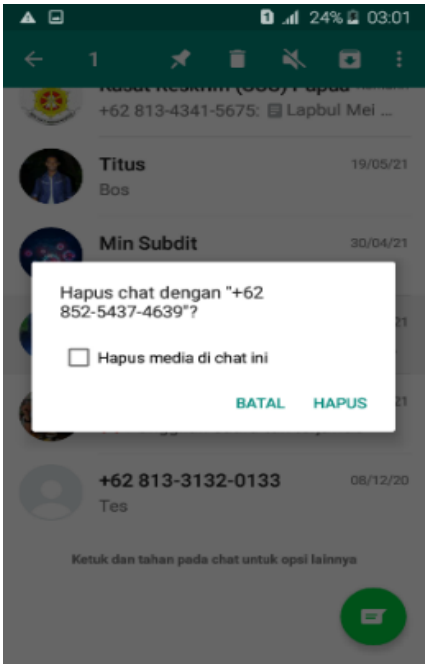

Figure 11 Implementation of Manual Evidence Deletion in the Smartphone

In this research, we recovered deleted data, consisting of contacts, messages, image files, video files, audio files, download histories, and so on, in the smartphone as evidence.

Deleted data recovery was carried out using a mobile forensic tool, i.e., Cellebrite's UFED Touch2 and the UFED Physical Analyzer V.7.38.051 software was used in digital evidence investigation and analysis processes. The smartphone was also used to analyze the ability of the mobile forensic tool in data recovery.

The results were presented in the form of data on the performance of the tool used for deleted data recovery.

3.3 Experiment Using the ACPO (Association of Chief Police Officers) Digital Forensic Framework or the ACPO Framework

We executed an experiment using the ACPO (Association of Chief Police Officers) digital forensic framework or the ACPO Framework and added one stage, namely criminal case simulation.

The research methodology flowchart by the ACPO (Association of Chief Police Officers) digital forensic framework or the ACPO Framework is displayed in Figure 12.

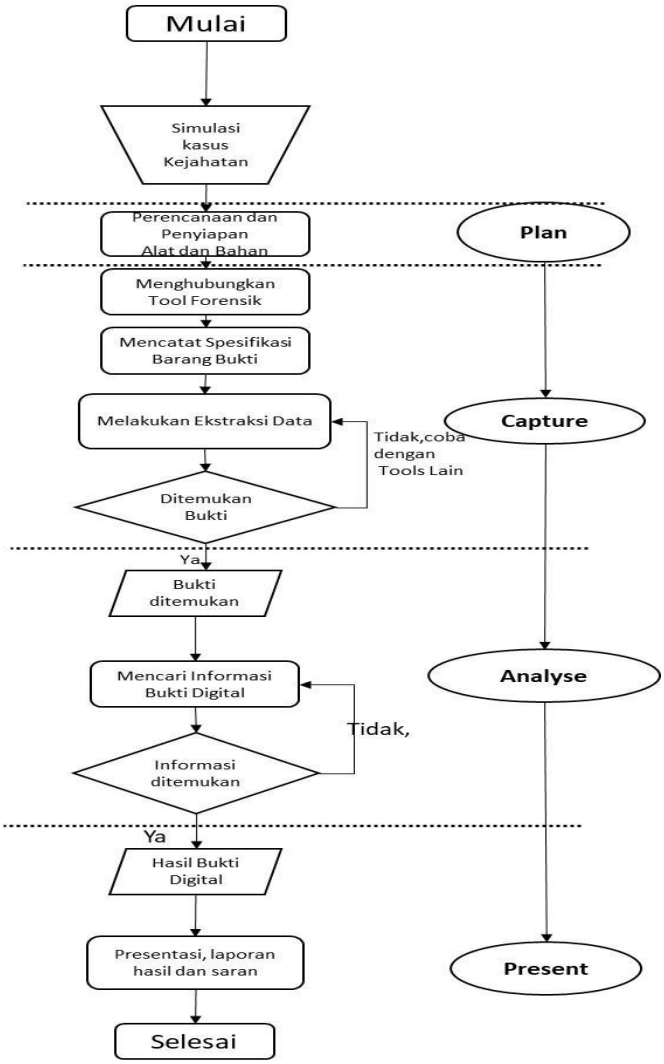

Figure 12 Research Methodology Flowchart by the ACPO (Association of Chief Police Officers) Digital Forensic Framework or the ACPO Framework

The research stages are described in detail as follows:

a. Planning and Determining Materials and Tools

In this stage, we carefully planned what actions forensic investigators or analysts at Laboratorium Komputer Forensic should take after electronic evidence from Police Criminal Investigation Unit who were handling the case was received. It had to be considered whether the digital evidence was alterable, lost, damaged (volatile) before electronic evidence investigation to acquire valid digital evidence. The forensic investigator or analyst executed a digital evidence investigation using mobile forensics. The mobile forensic materials and tools were then determined to investigate electronic evidence. In this research, we used Cellebrite's UFED Touch2 as the mobile forensic tool and the UFED Physical Analyzer V.7.38.051 software and other supporting devices, as indicated in Figures 6, 7, 8, 9, and 10.

b. Connecting the SAMSUNG Galaxy J2 Smartphone to Cellebrite's UFED Touch2

The tested SAMSUNG Galaxy J2 smartphone was connected to Cellebrite's UFED Touch2 and the external hard disk to duplicate the extraction result. A notebook, in which the UFED Physical Analyzer V.7.38.051 software was installed, was prepared.

After the smartphone was connected to Cellebrite's UFED Touch2, the investigator selected a certain brand or type suitable with the tested smartphone or selected the Auto-Detect (automatic detector) feature.

Figure 13 Connecting the Smartphone to Cellebrite's UFED Touch2

In figure 13, the Samsung Galaxy J2 smartphone was connected to Cellebrite's UFED Touch2 using a data cable.

c. Recording the Evidence Specifications

Evidence specification recording was a prerequisite in digital forensic procedures. In recording evidence specifications, an investigator or analyst could observe device specifications in the smartphone setting or identify them using the Auto Detect (automatic reading) feature of the smartphone through Cellebrite's UFED Touch2. The evidence specifications identified were recorded.

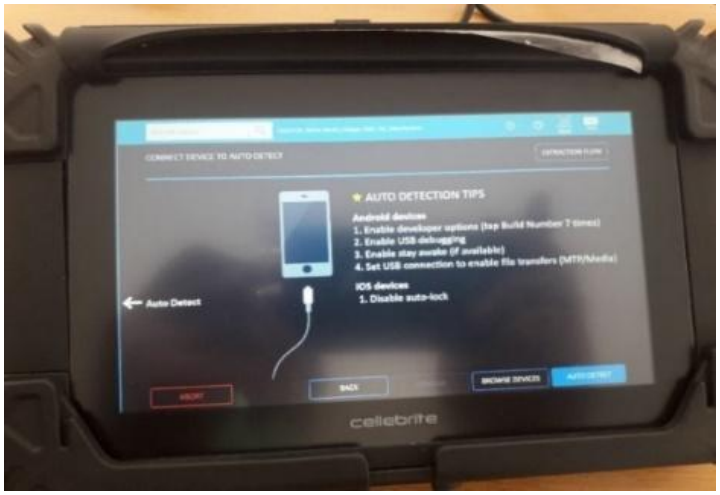

Figure 14 Auto Detect (Automatic Detector) Feature of the Smartphone

Figure 14 is the Auto-Detect (automatic detector) feature of the tested smartphone.

Figure 15 Samsung Galaxy J2 Smartphone Detected by Auto Detect (Automatic Detector)

Figure 15 is the result of automatic detection in the Samsung Galaxy J2 smartphone where information was extracted.

d. Extracting Data

In extracting data from a smartphone, we searched digital evidence information if finding the evidence but if no evidence was found, we conducted another experiment with a different extraction process. In this stage, data extraction was carried out using Cellebrite's UFED Touch2. It was file system extraction.

The options of contents extracted were Call Log, SMS, MMS, Contacts, Device Locations, Installed Applications, User Accounts, Data Files Application, Archives, Audio, Databases, Documents, and Images.

Figure 16 Contents Displayed on Cellebrite's UFED Touch during File System Extraction

Figure 16 is how content types were displayed on Cellebrite's UFED Touch during the process of file system extraction.

We only selected WhatsApp messages (chats) to be extracted. After extraction, the result was duplicated into the external hard disk prepared and transferred to the notebook. Digital evidence information search (analysis) was then conducted using the UFED Physical Analyzer V.7.38.051 software.

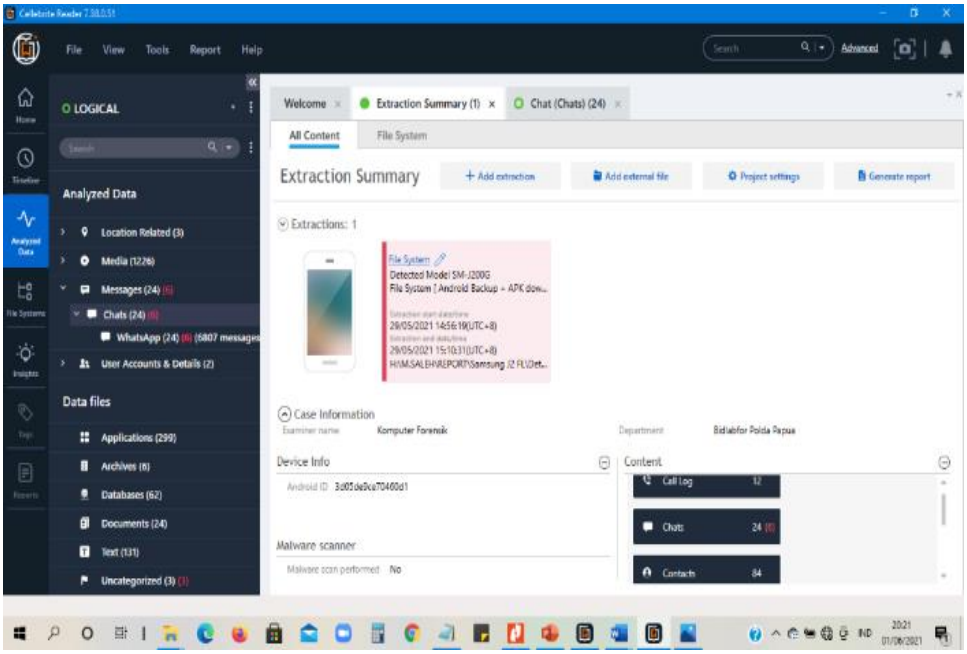

Figure 17 Result of the Extraction in the Samsung Galaxy J2 Smartphone Using File System Extraction Opened with the UFED Physical Analyzer V.7.38.051 Software

Figure 17 demonstrates the result of extraction in the Samsung Galaxy J2 smartphone using file system extraction. The result was opened using a notebook installed the UFED Physical Analyzer V.7.38.051 software and analyzed.

e. Digital Evidence Information Search (Analysis)

In this stage, digital evidence information search/analysis was executed on all extraction results duplicated into the external hard disk. The results were opened using the UFED Physical Analyzer V.7.38.051 software connected to the notebook and analyzed. A comparison between all results was made to acquire valid data on digital evidence investigation.

The analysis process using the UFED Physical Analyzer V.7.38.051 by searching information in messages, contacts, and images is depicted in Figure 18.

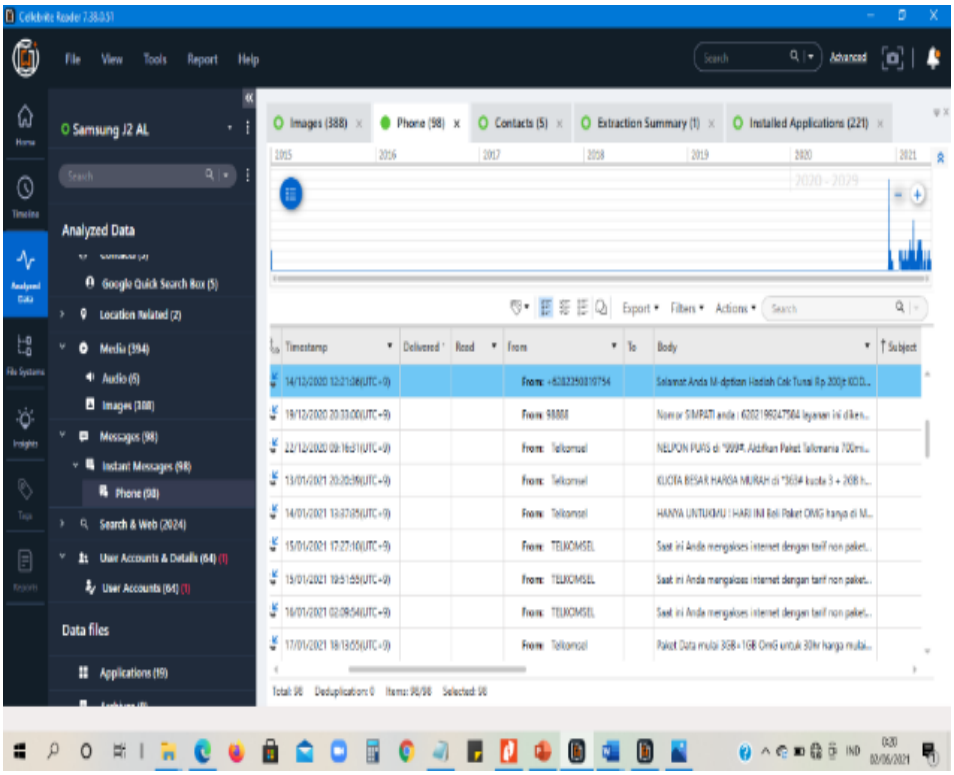

Figure 18 Messages in the Samsung Galaxy J2 Smartphone

Figure 18 exhibits the messages in the Samsung Galaxy J2 smartphone.
After extraction and digital evidence finding, digital evidence recovery was performed.

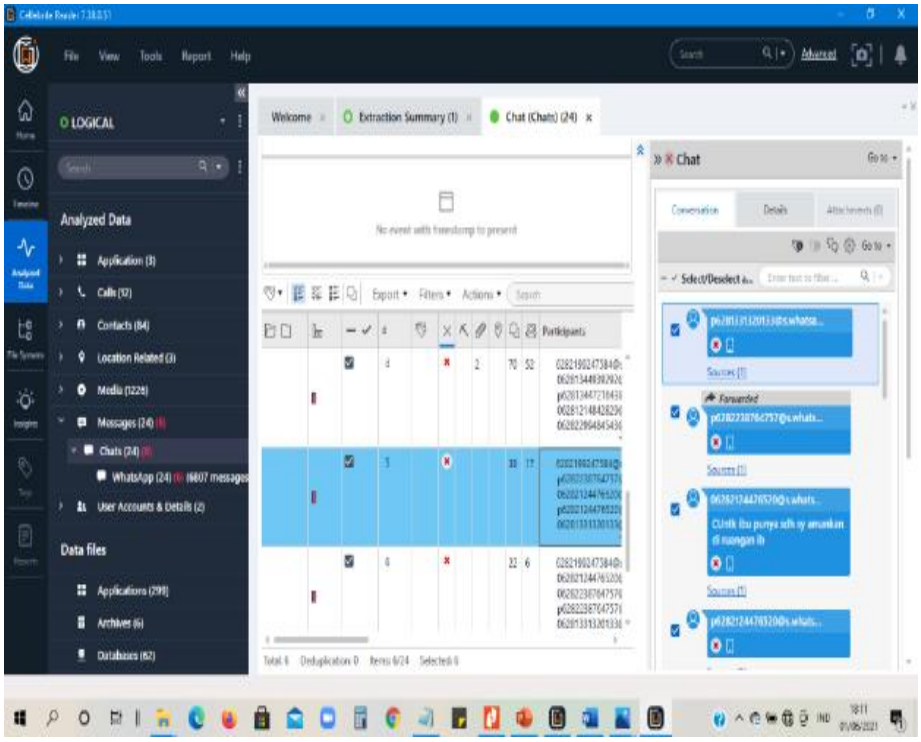

Figure 19 Chat Data Deleted from the Samsung Galaxy J2 Smartphone

Figure 19 indicates chat data deleted from the Samsung Galaxy J2 smartphone. Six of 24 chats had been deleted.

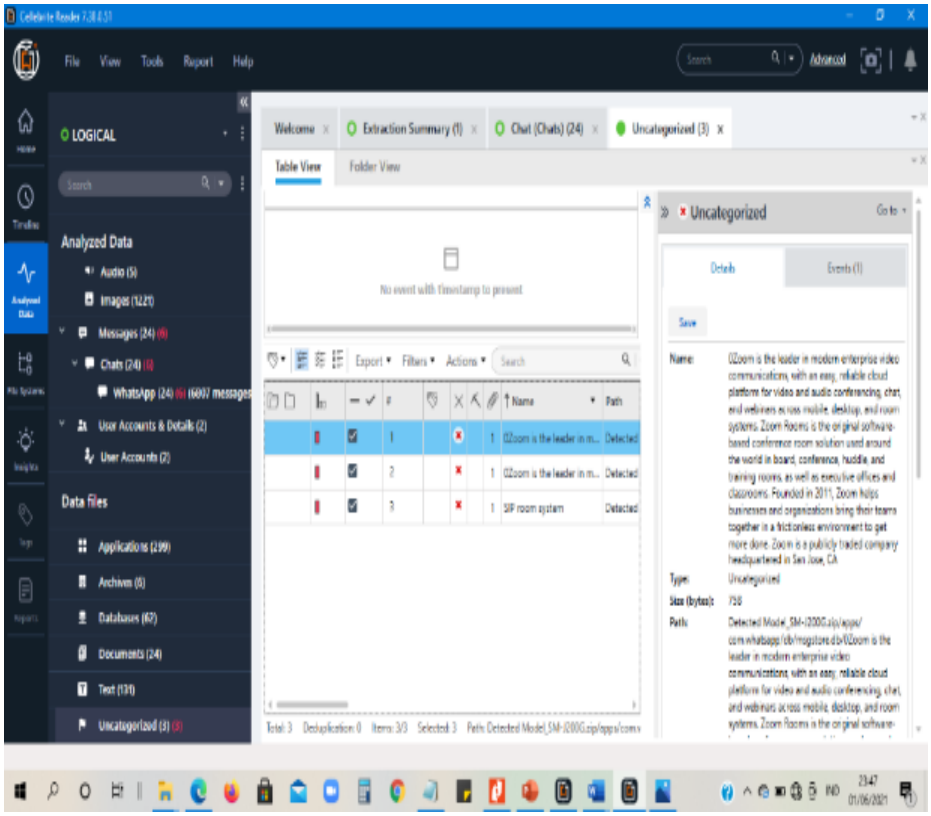

Figure 20 Uncategorized Data Deleted from the Samsung Galaxy J2 Smartphone

Figure 20 manifests uncategorized data deleted from the Samsung Galaxy J2 smartphone. Three chats had been deleted.

Six of 24 chats were deleted and three chats were uncategorized.

f. Presentation and Reporting

In this stage, digital evidence was presented in the form of a report as a publication of digital evidence investigation and extraction results.

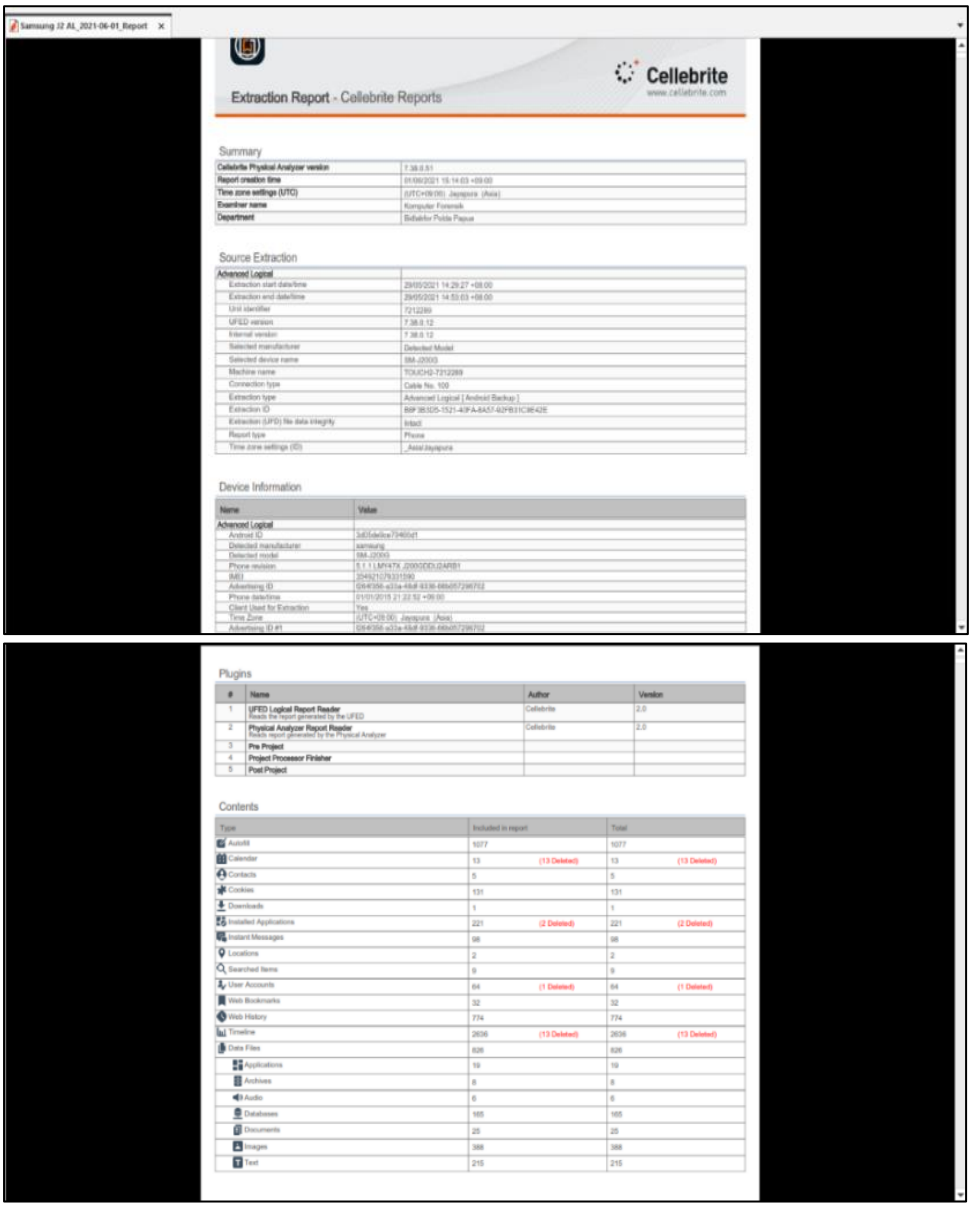

Figure 21 The Report of Extraction Using Cellebrite's UFED Touch2

Figure 21 is the report of extraction using Cellebrite's UFED Touch2.

Table 2 points out the experiment result on the ACPO Framework for digital evidence acquisition in the Samsung Galaxy J2 smartphone using Cellebrite's UFED Touch2 as the mobile forensic tool used.

Table 2 The Experiment Result Using the ACPO Framework

Category	Total	Deleted Data	Total
Call log	12	0	12
Chats	24	6	30
Contacts	5	0	5
Device locations	3	0	6
Installed applications	31	0	31
User accounts	2	0	2
Data file application	9	0	9
Applications	299	0	299
Archives	6	0	6
Audio	5	0	5
Database	62	0	62
Documents	24	0	24
Image	1221	0	1221
Text	131	0	131
Uncategorized	3	3	6

3.4. Comparison and Analysis

a. Experiment Result Using the ACPO Framework in Comparison with the NIST Framework [9]

This research was aimed at comparing the ACPO Framework and the NIST framework associated with recovering digital evidence manually deleted from the Samsung Galaxy J2 smartphone and comparing the percentage of success rate between mobile forensic tools used. The compared data from the experiment or pilot test are presented in Table 3.

Table 3 Experiment Result on the ACPO Framework in Comparison with the NIST Framework

Experiment Stages on the ACPO Framework (This Research)				Experiment Stages on the NIST Framework (Research by [9])				
No.	Category	Initial Simulation Data	Final Data from the Experiment (Cellebrite's UFED)	No.	Category	Initial Simulation Data	Final Data from the Experiment (Oxygen)	Final Data from the Experiment (Belkasoft)
1	Contacts	11	15	1	Contacts	11	11	0
2	Messages	47	30	2	Messages	25	7	9
3	Images	11	85	3	Images	13	13	13

Shows the result of digital evidence recovery in the Samsung Galaxy J2 smartphone using a manual deletion method The percentage of success rate with Cellebrite's UFED Touch2 (this research) was 118%, whereas Oxygen and Belkasoft (research by [9]) resulted in percentages of the success rate of 63% and 44%, respectively.

b. Experiment Stages by the ACPO Framework (This Research) in Comparison with Experiment Stages by the NIST Framework (Research by [9])

We made a comparison between experiment stages by the ACPO Framework (this research) and that by NIST Framework (research by [9]). The experiment stages are showcased in Table 4.

Table 4 Experiment Stages by the ACPO and NIIST Frameworks

No.		Experiment Stages by the ACPO Framework	No.		Experiment Stages by the NIST Framework [9]
i		Starting the experiment	i		Starting the experiment
ii		Simulating the crime	ii		Simulating the crime
I		*Plan*	I		*Collect*
	1	Planning and preparing materials and tools		1	Preparing materials and tools
				2	Activate the Airplane and USB Debugging modes
				3	Recording evidence specifications
II		*Capture*	II		*Examine*
	2	Connecting forensic tools		4	Connecting forensic tools
	3	Recording evidence specifications		5	Extracting data (if evidence was found, it could proceed to information search. If no evidence was found, another tool should be used)
	4	Extracting data (if evidence was found, it could proceed to information search. If no evidence was found, another tool should be used)			
III		*Analyze*	III		*Analyze*
	5	Searching digital evidence information (if a result was found, it could proceed to reporting. If there was no result, the process finished)		6	Searching digital evidence information (if a result was found, it could proceed to reporting. If there was no result, the process finished)
IV		*Present*	IV		*Report*
	6	Presenting and reporting		7	Reporting

As shown off in Table 3, the ACPO Framework had six stages, whereas NIST seven (in research by [9]).

After stages of both frameworks were compared and presented in a tabular form, a score of 0 (zero) was afforded to the stage non-existing in the frameworks and 1 (one) to the stage existing in the frameworks. The scoring was carried out to identify the difference in the number of stages between the two frameworks.

After the scoring, the percentages of success rate were calculated using the following formulas.

1) Percentage for the ACPO Framework

$$NI_1 = \frac{\sum TI_1 \times 100\%}{\sum TT}$$

Where:

$\sum TI_1$: the number of stages by the ACPO Framework

$\sum TT$: the total number of stages in the experiment

NI_1 : the percentage for the ACPO Framework

$$NI_1 = \frac{4}{6} \times 100\% = 66.6\%$$

The percentage for the ACPO Framework was 66.6%.

2) Percentage for the NIST Framework

$$NI_2 = \frac{\sum TI_2}{\sum TT} \times 100\%$$

Where:

$\sum TI_2$: the number of stages by the NIST Framework
$\sum TT$: the total number of stages in the experiment
NI_2 : the percentage for NIST Framework

$$NI_2 = \frac{4}{7} \times 100\% = 57.1\%$$

The percentage for the NIST Framework was then 57.1%.

3) Difference in Percentages between the ACPO and NIST Frameworks

The following formula was used to identify the difference in percentages between the two frameworks.

$$NI_1 - NI_2 = 66.6\% - 57.1\% = 8.9\%$$

According to the calculation, the difference in percentages between the ACPO Framework used in this research and the NIST Framework used by [9] was 8.9%.

4. CONCLUSION

We had successfully analyzed the implementation of the ACPO Framework for digital evidence acquisition in a smartphone.

The digital evidence deletion in the Samsung Galaxy J2 smartphone was conducted using a manual deletion method. The percentage of success rate with Cellebrite's UFED Touch2 (this research) was 118%, while the percentage of success rate with Oxygen and Belkasoft (research by [9]) were 63% and 44%, respectively.

Meanwhile, the percentage of the ACPO Framework (used in this research) was 66.6%, while the NIST Framework (used by [9]) had a percentage of 57.1%. The difference in percentages between the ACPO Framework used in this research and the NIST Framework used by [9] was 8.9%.

To sum up, based on percentages, the ACPO Framework had fewer stages relative to the NIST Framework used by [9] and Cellebrite's UFED Touch2 was more effective for digital evidence recovery in smartphones using a manual deletion method than Belkasoft and Oxygen. And yet, each mobile forensic tool had both strengths and weaknesses for digital evidence acquisition.

Today's smartphones come in various types and hence result in different difficulty levels in terms of digital evidence acquisition. This is challenging forensic investigators or analysts.

A suitable digital forensic framework with an investigation process will result in complete digital evidence acquisition. Stages of a digital forensic framework should comply

with the standard process to acquire a valid conclusion and make the digital evidence extracted from electronic evidence accepted in court.

5. SUGGESTED

Future researchers may perform an experiment using smartphones with Android 6.0, above, or others and another mobile forensic tool and a physical aq digital evidence acquisition.

Using an appropriate digital forensic framework, a forensic investigator or analyst can be more oriented during a mobile forensic process and therefore more contribute to the criminal evidence process in the legal process in court.

6. REFERENCES

[1] *Association of Chief Police Officers, "Good Practice Guide for Computer-Based Electronic Evidence Official release version 4 . 0," Director*, 2005.

[2] Yudo Dahono, "Data: Ini Media Sosial Paling Populer di Indonesia 2020-2021," 2021. https://www.beritasatu.com/digital/733355/data-ini-media-sosial-paling-populer-di-indonesia-20202021 (accessed Feb. 15, 2021).

[3] patrolisiber.id, "Statistik Jumlah Laporan Polisi yang dibuat masyarakat," 2020. https://patrolisiber.id/statistic (accessed Nov. 03, 2020).

[4] Y. Marumo, *"Forensic Examination of Soil Evidence," Japanese J. Forensic Sci. Technol.*, vol. 7, no. 2, pp. 95–111, 2003, doi: 10.3408/jafst.7.95.

[5] R. Ayers, W. Jansen, and S. Brothers, *"Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)," NIST Spec. Publ.*, vol. 1, no. 1, p. 85, 2014, [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.

[6] G. L. Palmer., *"A Road Map for Digital Forensic Research. Technical Report DTR-T0010-01, DFRWS,"* 2001.

[7] J. Moedjahedy, "Forensik komputer Studi Kasus: Universitas Klabat," *J. Sist. Inf. dan Teknol. Inf.*, vol. 5, no. 2, pp. 95–106, 2016.

[8] I. Riadi, S. Sunardi, and S. Sahiruddin, "Analisis Forensik *Recovery* pada *Smartphone* Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, pp. 87–95, 2019.

[9] M. R. Anton Yudhana, Abdul Fadlil, Setyawan, "Analisis *Recovery* Bukti Digital Skype berbasis *Smartphone* Android Menggunakan *Framework* NIST," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 682–690, 2020.

[10] Muhammad Nuh Al-Azhar, *Digital Forensic: Practical Guidelines for Computer Investigation*. Jakarta: Salemba Infotek, 2012.

[11] D. L. Shinder, *Scene of the Cybercrime: Computer Forensics Handbook*. 2002.

[12] I. Riadi, A. Yudhana, and M. C. F. Putra, *"Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," Sci. J. Informatics*, vol. 5, no. 2, pp. 235–247, 2018, doi: 10.15294/sji.v5i2.16545.

[13] I. R. Roni Anggara Putra, Abdul Fadlil, "Forensik *Mobile* pada *Smartwatch* Berbasis Android," *J. Rekayasa Teknol. Inf.*, vol. 1, pp. 41–47, 2017.
[14] D. Hariyadi *et al.*, "Analisis Barang Bukti Digital Aplikasi Paziim Pada Ponsel Cerdas Android dengan pendekatan *Logical Acquisition*," vol. 2, no. 2, pp. 52–56, 2019.
[15] S. Willassen, *"Chapter 16 Forensic Analysis Of Mobile Internal / External Memory," Memory*, p. 204, 2014.
[16] SAGEMCOM, *"AT Command Set for SAGEM HiLo/HiLoNC Modules."* SAGEMCOM, France, 2011.
[17] A. Abdulla, K. & Jones, *"Forensics data acquisition methods for mobile phones,"* 2012.
[18] I. Z. Yadi and Y. N. Kunang, "Analisis Forensik pada *Platform* Android," *Konik*, 2014.
[19] D. Naista, *Codeigniter Vs Laravel Kasus Membuat Website Pencari Kerja*. Yogyakarta: CV LOKOMEDIA, 2017.