Comparative Analysis Software on Android-Based IMO Messenger using National Institute of Justice and Association of Chief Police Officers

Imam Riadi*, Sunardi*, Yana Safitri*
Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Abstract- The need for effective digital forensic tools to assist law enforcement agencies in investigating criminal activities has increased due to the rapid growth of digital communication platforms. This research compares forensic software techniques used in the Android-based IMO Messenger application, specifically focusing on the Association of Chiefs of Police (ACPO) and National Institute of Justice (NIJ) frameworks. The tools used for examination are MOBILEedit Forensic Express and Autopsy. The evidence obtained includes chat logs, user IDs, data deletions, and group conversations based on digital data extracted from IMO Messenger tokens on Android smartphones. The aim of this study is to collect video evidence in cases of body shaming using the ACPO and NIJ) frameworks with testing tools MOBILedit Forensic Express Pro and Autopsy. Based on the search results, MOBILedit Forensic Express Pro achieved a 91.66% extraction rate. In contrast, using Autopsy yielded an extraction efficiency of 8.33%. The NIJ framework is considered the best because it supports the investigative process with the most comprehensive steps in investigating cases of body shaming using mobile forensic tools, thus yielding extractable results. Video has been identified as the best form of digital evidence that can be used to support legitimate legal claims. The findings of this research contribute to advancing mobile forensic knowledge in cases of physical shaming or cyberbullying within the ACPO and NIJ frameworks, benefiting investigators.

Keywords- Association of Chief Police Officers, Cyberbullying, Digital Investigation, IMO Messenger, Mobile Forensic, National Institute of Justice.

I. Introduction

Like the growth of smartphone technology with the Android operating system, which is already outfitted with a number of cutting-edge capabilities, the rate of technological advancement in the world today is very quick [1]. Benefits of having a smartphone are undeniable. The development of Android smartphone forensics has created both enormous potential and intriguing challenges [2].

Nearly all parties and people of all ages are indirectly interacting online thanks to the present technological breakthroughs. Cybercriminals will have more options thanks to applications on cellphones to use messenger to perpetrate crimes. Digital crime is the analysis of traces of criminal conduct to be used as evidence [3]. The Android smartphone itself is a hybrid device that can operate as a phone and also in a manner that is more streamlined and portable than a computer [4]. To make investigations easier in the field of digital forensics, numerous tools are used [5]. The development of Android smartphone forensics has created both enormous potential and intriguing challenges [6].

Instant messaging systems like IMO Messenger have grown in importance as the digital era has progressed as a means of communication [7]. Communication between people and sharing of opinions and significant social events are easier than ever [8]. A lot of dubiois and incorrect content is being produced and shared for beneficial purposes [9]. However, along with their advantages, programs like this also carry the risk of abuse, such as cyberbullying, which can have detrimental effects on the individuals impacted [10]. The greatest risk to instant messaging apps today is cybercrime. Investigators must perform forensic analysis on both the victim's and the suspect's devices in order to find digital evidence in order to combat short message-based cybercrime [11]. Cybercrime is an illegal activity that makes use of computer technology and advances in internet technology [12]. Crimes against people, crimes against things, crimes against organizations, and crimes against society all fall under this category of cybercrime [13]. One of the detrimental effects currently affecting teenagers is cyberbullying [14].

Investigators must look at messaging service artifacts if they find evidence of criminal offenses in IMO Messenger messages, given the difficulties outlined above. So it is necessary to use forensic handling, particularly mobile forensics, to assist in the conclusion of criminal cases [15]. In order to help investigators in cybercrime investigations employing mobile devices retrieve artifacts, decrypt data, and analyse it, mobile forensic technology is required [16]. Supportive tactics should also be used by investigators to guarantee a smooth and effective investigation. Android smartphone crime scene analysis is possible with the use of mobile device forensic procedures [17]. Figure 1 shows a number of areas of expertise in the field of digital forensic investigation.

Digital forensics has at least five subfields of research, as depicted in Figure 1. Forensics of mobile devices is one of them [18]. The capture or recovery of digital evidence from mobile devices is the focus of the subspecialty of digital forensics known as mobile device forensics [19]. The problem with forensics is that many of the forensic instruments are ineffective. Researchers have expressed concern about this, saying that each forensic tool has advantages and disadvantages [20].

The ACPO and the NIJ have developed forensic techniques that have been adapted for use in this research to collect digital evidence of criminal activity through stages of investigation and analysis [21]. The ACPO method is a study methodology that includes four core key elements: identification, preservation, analysis, and presentation [22]. The NIJ approach involves five stages, with the identification stage encompassing the classification of digital criminal evidence and the selection of data to aid the search for such evidence during the investigative process. To preserve the integrity of the evidence, techniques of identification, labelling, and recording are used in this step. A number of activities are part of the collection stage, which is where information is gathered to aid in the hunt for evidence of digital crime. At this step, procedures are used to extract information from pertinent data sources and guarantee the consistency of the evidence against tampering [23].

Studies on digital crimes have been undertaken by a number of researchers, including one titled "Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework [24]", However, because this study only used one framework, it was difficult to systematically find instances of cyberbullying. The evidence derived from the forensic results therefore requires further study. In a related study, "Cyberbullying Detection on Instant Messaging Services using Rocchio and Digital Forensics Research Workshop Framework [25]" assessment criteria were defined in order to successfully discover significant parameters.

Based on earlier research and unique backdrop challenges, this study has a solid foundation for conducting an experimental examination of the capacity of forensic tools in evaluating digital evidence from the IMO Messenger. In this article, the ability of two mobile forensic tools, notably ACPO and NIJ, to handle digital cases involving Android mobile devices is contrasted.

II. METHOD AND THEORITICAL FRAMEWORK

The investigation's research technique simulates a case study utilizing the ACPO and NIJ frameworks in order to assess the smartphone app IMO Messenger. The goal of this simulation is to contrast the two forensic frameworks and tools offered for the smartphone app IMO Messenger. The purpose of this is to locate communications and media files that have been utilized in illegal activity and turn them into evidence.

1) The research challenge serves as the basis for selecting the study topic that will be further explored. At this stage, detectives use a variety of techniques to obtain information about the scene and the timeline of the events.
2) A literature review is supposed to assemble all available data on the topic and the study object, as well as lay the groundwork for future research and new insights for each researcher. By doing this, it is ensured that the study can be cited in the future.
3) Case Study uses MOBILedit Forensic Express Pro and Autopsy to conduct a forensic analysis of the IMO Messenger Android application. The investigation's flowchart is depicted in Figure 1 for the case study.

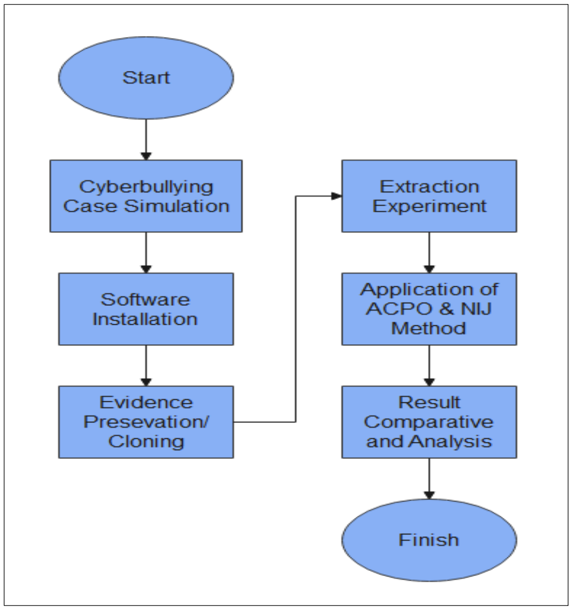

Start
Cyberbullying Case Simulation
Software Installation
Evidence Presevation/ Cloning
Extraction Experiment
Application of ACPO & NIJ Method
Result Comparative and Analysis
Finish

Figure 1. Investigation flowchart

Figure 1. showing the flowchart is explained as follows:

1) Creating a cyberbullying simulation: For this study, a cyberbullying simulation is created using the Imo application.
2) Installing forensic tool software on a PC or laptop that will be utilized for the collection and analysis of digital evidence is what an investigator does.
3) Evidence preservation/cloning: To preserve the integrity of the original data, the investigator must preserve the tangible evidence while the smartphone is in airplane mode.
4) Extraction Experiment: To extract data from the smartphone device, investigators employ a variety of forensic tools. The smartphone is physically imaged using MOBILedit Forensic Express Pro, and digital evidence from multimedia files is evaluated using Autopsy.
5) Implementation of ACPO and NIJ Methods: In this study, researchers evaluate two approaches to support investigators in conducting investigations. Planning, Capture, Analysis, and Presentation are the four stages of ACPO. Identification, Collection, Examination, Analysis, and Reporting are the five processes that make up NIJ.

Evaluation and Results Analysis: Each forensic tool's performance will be analysed and examined in light of the program's features and the digital evidence it produced. The study's goals, particularly the analysis of the IMO Messenger program, are catered to by the parameters used.

Case Scenario

Cyberbullying occurs in chat groups when the IMO Messenger program is being utilized. A fictitious simulation of a cyberbullying situation is showing Figure 2, which also shows how the victim and the bully communicate through message exchanges.

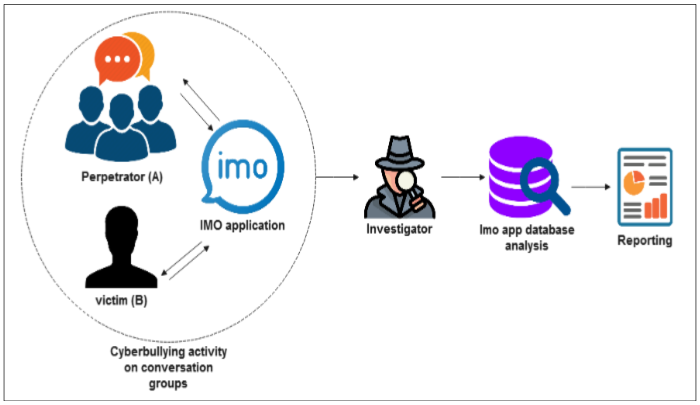

Perpetrator (A)
imo
IMO application
victim (B)
Cyberbullying activity on conversation groups
Investigator
Imo app database analysis
Reporting

Figure 2. Research scenarios of cyberbullying conversation cases

Figure 2. showing the simulation is carried out using conversations from a group chat on instant messaging. Bullying affects one member of the group. A case of cyberbullying between numerous attackers and a single victim is the scenario that is replicated. In this instance, the bullies pretend to have a chat with the victim through the IMO Messenger program, which results in cyberbullying. The victim's gadget in this hypothetical situation is a smartphone Samsung Galaxy Core 2.

Research Data Variable

Once the smartphone has been successfully obtained, a digital forensic method is used to compile proof of the illicit behavior. The outcomes of this evidence will be used as further justification at trial. The emphasis is on developing digital evidence search factors, as indicated in Table 1, to simplify the search for evidence.

Table 1 Research data variable

No.	Variables
1.	Device Information
2.	Application
3.	Account
4.	Friends
5.	Groups
6.	Chats
7.	Messages
8.	Images
9.	Video
10.	Media Files
11.	Cached Web Pages
12.	Documents

The digital forensic method will be carried out to gather pertinent pieces of evidence using the variables stated in the table.

Digital Forensic

Finding evidence from digital media, such as computers, mobile devices, servers, or networks, is the focus of the profession known as "digital forensics," which is consistent with the conclusion. It gives forensic teams the greatest methods and resources to crack cases. Child pornography cases, cybercrime, identity theft, online fraud, defamation, online threats, and other crimes that take advantage of information and communication technology, such as offenses related to terrorism, are a few examples of crimes that can be discovered utilizing digital forensics [26].

Cyberbullying

Any type of online bullying that affects kids or teens is referred to as cyberbullying, and the perpetrators are often other kids their age or peers. [27]. When a child or teenager is made fun of, insulted, intimidated, or degraded by another child or teenager using the internet, digital technology, or mobile phones, the incident occurs. Due to lax oversight of electronic devices and internet access, this behaviour is frequently carried out on purpose through recurrent electronic contact. [28].

IMO Messenger

IMO Messenger is an Instant Messenger program that provides real-time data transfer over the internet and enables users to share photographs, videos, and audio calls as well as text messages for group chats. IMO Messenger has the potential to be used as a tool for illegal activities including drug trafficking and cyberstalking, which involve using the internet or electronic devices to harass an individual, a group of people, or certain organizations [29].

Mobile Forensic

The recovery of digital evidence from mobile devices utilizing proper and defined scientific forensic settings is the focus of the scientific field known as mobile forensics (MF) [1]. Additionally, this branch has become crucial due to the rise in users, demand for mobile-based services, and sporadic changes in mobile technologies like ubiquity and pervasiveness as well as the quickly developing Internet of Things (IoT) technology, which necessitates device connectivity [30].

Mobiledit Forensic Express Pro

A mobile device forensics tool called MOBILedit Forensic Express can retrieve erased information such as passwords, contact information, chat history, graphic files, phone logs, and multimedia communications. From a variety of installed applications, including Skype, Dropbox, Facebook, WhatsApp, etc., MOBILedit may retrieve application cache history and online browser data [31].

Autopsy

Law enforcement organizations, corporate investigators, the military, and others use Autopsy, an open source and digital forensic investigation program. Sleuth Kit is used by Autopsy to examine pictures. Sleuth kit makes it possible to examine digital files and retrieve deleted content [32].

Tools and Material

In order to obtain artifacts for this investigation from the IMO Messenger program, tools must be used. Hardware tools and forensic software tools are the two categories of research instruments. Table 1 lists the research items that were used in this experiment.

Table 2 Software and Hardware

No.	Hardware and Software	Function
1.	PC	A method for transmitting digital data from smartphones to storage devices so that it can be analyzed
2.	MOBILedit Forensic Express Pro	Used for the IMO Messenger app on a smartphone physical imaging process or data backup
3.	Autopsy	Utilized for additional media file analysis on extracted files
4.	USB Connector	Used to grant complete access to a smartphone from a computer
5.	Portable Power Suplly	Is a gadget that boosts a smartphone's battery life and keeps the devices "on" state constant
6.	Faraday Bag	A container for protecting cellphones from data transmission

III. RESULT AND FINDINGS

This section will go over how to use the ACPO and NIJ framework in IMO Messenger forensics. MOBILEdit Forensic Express Pro. These results employ digital data that comes from the various reporting files. MOBILEdit Forensics Express Pro provides the ability to acquire data logically and physically. Utilizing MOBILEdit Forensics Express Pro, data from smartphone devices may be extracted. The IMEI (International Mobile Equipment Identity) of a mobile phone, as well as the ICCID and IMSI of an unregistered SIM card, may all be found with MOBILEdit Forensic Express Pro. It was successful at locating contact details, text messages, videos, photographs, and other data with MOBILEdit Forensic Express Pro.

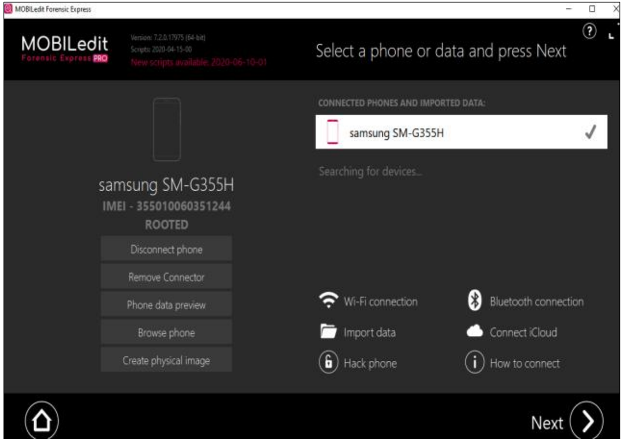
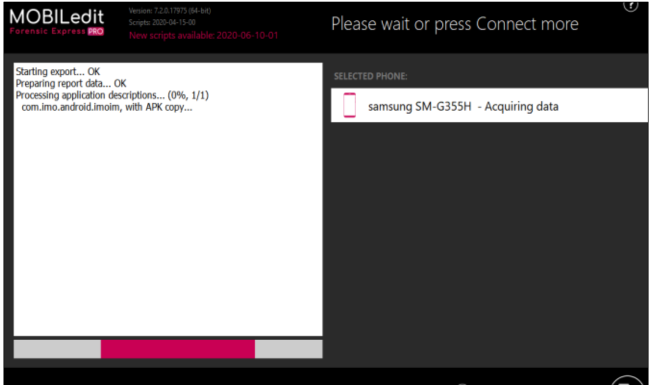


Figure 3 The initial stage of acquisition usage MOBILEdit Forensic Express Pro

Figure 3. is the initial phase of the data acquisition process from a smartphone or physical evidence using the MOBILEedit Forensic Express Pro tool, which involves connecting the evidence item to a PC or laptop using a USB cable.


MOBILedit
Forensic Express PRO
Version: 7.2.0.17975 (64-bit)
Scripts: 2020-04-15-00
New scripts available: 2020-06-10-01
Please wait or press Connect more
SELECTED PHONE:
samsung SM-G355H - Acquiring data

```
Starting export... OK
Preparing report data... OK
Processing application descriptions... (0%, 1/1)
  com.imo.android.imoim, with APK copy...
```

Figure 4 The process of obtaining digital evidence usage MOBILEdit Forensic Express Pro

Figure 4. illustrates the process of obtaining digital evidence. The digital evidence obtained consists of a reporting file in PDF format. Within this file, there are several pieces of evidence, one of which is a video artefact.

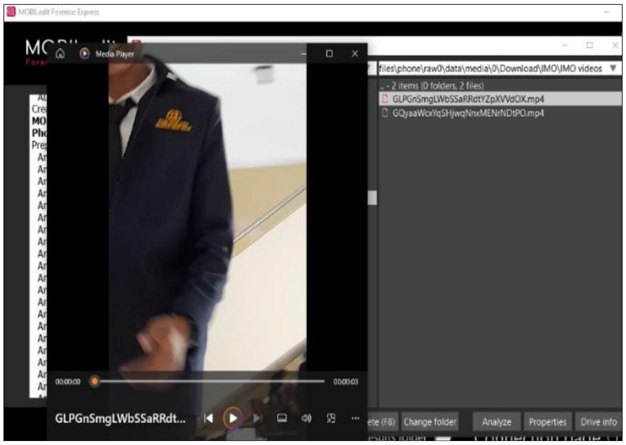
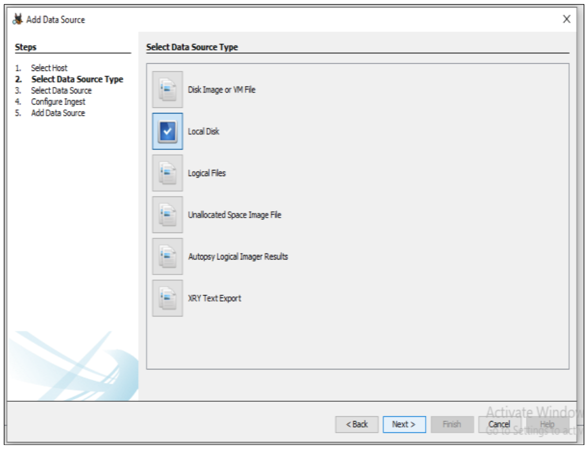

MOBILedit Forensic Express
Media Player
files\phone\raw0\data\media\0\Download\IMO\IMO videos
.. - 2 items (0 folders, 2 files)
GLPGnSmgLWbSSaRRdtYZpXVVdOX.mp4
GQyaaWcxYqSHjwqNnxMENrNDtPO.mp4
00:00:00
00:00:03
GLPGnSmgLWbSSaRRdt...
ete (F8)
Change folder
Analyze
Properties
Drive info

Figure 5 Digital image on MOBILEdit Forensic Express Pro

Figure 5. show video artefacts finds using MOBILEdit Forensic Express Pro.

Autopsy

Data from numerous sources, including as hard drives, mobile devices, and other storage media, are analysed using the tool or digital forensic software known as Autopsy. Digital forensic experts frequently use autopsy to look into digital evidence connected to criminal cases or particular situations. This program can help with the extraction, processing, and visualization of data that can offer insights about pertinent digital activities and trails. Figure 6 displays the extraction outcomes from the Autopsy tool, which acquired a video artifact as digital evidence.


Add Data Source

Steps

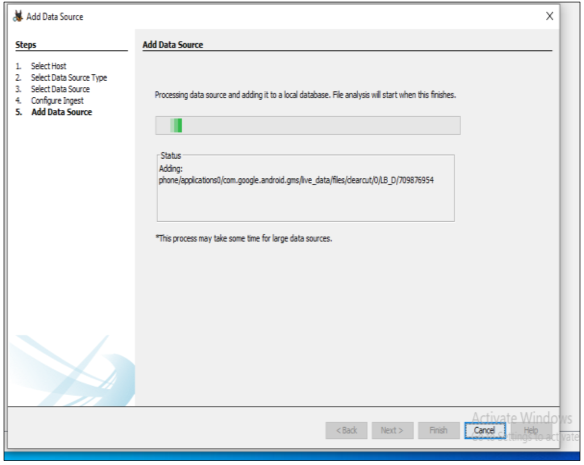
1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

- Disk Image or VM File
- ☑ Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

Figure 6 Selecting a data source type using Autopsy

Figure 6. represents the stage of selecting the data type to be used with Autopsy. In this research, the data type used is the local disk.


Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Add Data Source

Processing data source and adding it to a local database. File analysis will start when this finishes.

Status
Adding:
phone/applications0/com.google.android.gms/live_data/files/clearcut/0/LB_D/709876954

*This process may take some time for large data sources.

Figure 7 The process of digital imaging using Autopsy

Figure 7. showing the process of digital imaging using Autopsy. The obtained data is then analyzed.

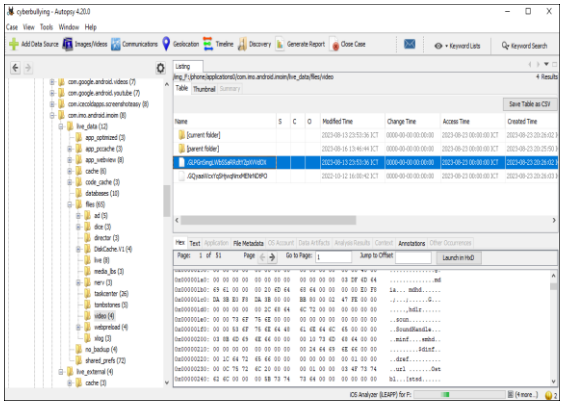


Figure 8 Digital image on Autopsy

In the cyberbullying case scenario, the outcomes of the digital forensic evidence analysis can be compared to the data from the found evidence. The finest tools for verification are MOBILEdit Forensic Express Pro since it can gather a wide range of evidence, including text messages, images, videos, user IDs, deleted data, and group information. Using the Autopsy program, however, only permits acquiring digital proof in the form of video recordings. The videos that were all collected as evidence end up being the most crucial and crucial pieces of information in the cyberbullying case. Table 2 displays the outcomes of a comparison of digital evidence based on the capabilities of forensic tools.

Table 3 Results of forensics tools

		Forensics Tools	
Framework	Evidence Parameter	MOBILEdit Forensic Express Pro	Autopsy
ACPO	Device Information	✓	✗
	Application	✓	✗
	Account	✓	✗
	Friends	✓	✗
	Groups	✓	✗
	Chats	✓	✗
	Messages	✓	✗
	Images	✓	✗
	Video	✓	✓
	Media Files	✓	✗
	Cached Web Pages	✗	✗
	Documents	✓	✗
NIJ	Device Information	✓	✗
	Application	✓	✗
	Account	✓	✗
	Friends	✓	✗
	Groups	✓	✗
	Chats	✓	✗
	Messages	✓	✗
	Images	✓	✗

	Video	✓	✓
	Media Files	✓	x
	Cached Web Pages	x	x
	Documents	✓	x
Percentage%		91.66	8.33

According to the experimental findings, researchers used index numbers in computations to determine each forensic tool's usefulness. (3.1) demonstrates how to determine the index number as the overall score index.

$$Pon = \frac{\sum pn}{\sum po}\ x\ 100\% \tag{3.1}$$

Note that the Equation Pon is the instant messaging application's anti-forensic vulnerability percentage score, ∑pn is total digital data obtained, and ∑po is all of the instant messenger application's digital data.

MOBILEdit Forensic Express: $Pon = \frac{11}{12}\ x\ 100\% = 91.66\%$ (3.2)

Autopsy: $Pon = \frac{1}{12}\ x\ 100\% = 8.33\%$ (3.3)

According to the ACPO and NIJ approaches, the only distinctions are in the framework's stages. The four stages of the ACPO approach are planning, acquisition, analysis, and presentation. The 5 steps of the NIJ are identification, collection, examination, analysis, and reporting. The NIJ technique is more extensive, thorough, and understandable. The ability of forensic instruments to locate evidence based on specified criteria, MOBILEdit Forensic Express Pro has a significant benefit because it uses (3.1) to determine an index for each forensic tool. With 91.66%, it has the highest index value. The index value for autopsy is 8.33%.

IV. CONCLUSION

The IMO Messenger application cyberbullying examples have been examined utilizing the ACPO and NIJ frameworks. Below are a few analysis findings from the inquiry. The NIJ framework is said to be the best since it supports the investigative process by including the most thorough stages. Video is the predominate form of evidence, according to the total forensic tool verification. The mobile forensic tool with the highest capability, MOBILedit Forensic Express Pro, is 91.66%. A capability with an index value of 8.33% is Autopsy. Research showing that the MOBILedit Forensic Express Pro forensic tool excels in data extraction skills forms the basis for the comparative outcomes of all forensic products. The objectives of the study are met, allowing the researcher to discover and evaluate both forensic.

Acknowledgment

Thank you to the research team in this article who contributed to the completion of the data and information.

REFERENCES

[1] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative Analysis of Android Mobile Forensics Tools," *2020 IEEE Conf. Comput. Appl. ICCA 2020*, pp. 1–6, 2020, doi: 10.1109/ICCA49400.2020.9022838.

[2] M. ALThebaity, S. Mishra, and M. Kumar Shukla, "Forensic Analysis of Third-party Mobile Application," *Helix*, vol. 10, no. 4, pp. 32–38, 2020, doi: 10.29042/2020-10-4-32-38.

[3] D. Yuliana, T. Yuniati, and B. Parga Zen, "Analisis Forensik Terhadap Kasus Cyberbullying Pada Instagram Dan Whatsapp Menggunakan Metode National Institute of Justice (NIJ)," *Cyber Secur. dan Forensik Digit.*, vol. 5, no. 2, pp. 52–59, 2022, doi: 10.14421/csecurity.2022.5.2.3734.

[4] A. Amorim, F. Pereira, C. Alves, and O. García, "Species assignment in forensics and the challenge of hybrids," *Forensic Sci. Int. Genet.*, vol. 48, 2020, doi: 10.1016/j.fsigen.2020.102333.

[5] J. Hou, Y. Li, J. Yu, and W. Shi, "A Survey on Digital Forensics in Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 1–15, 2020, doi: 10.1109/JIOT.2019.2940713.

[6] J. Qiu, J. Zhang, W. Luo, L. Pan, S. Nepal, and Y. Xiang, "A Survey of Android Malware Detection with Deep Neural Models," *ACM Comput. Surv.*, vol. 53, no. 6, 2021, doi: 10.1145/3417978.

[7] D. P. Harahap, "Implementasi Digital Forensik Aplikasi Dompet Digital Dan Pesan Instan Pada Android Dengan Menggunakan Metode NIST," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 6, no. 1, pp. 533–541, 2023, doi: 10.30865/komik.v6i1.5715.

[8] A. Yavari, H. Hassanpour, B. R. Cami, and M. Mahdavi, "Election Prediction Based on Sentiment Analysis using Twitter Data," *Int. J. Eng. Trans. B Appl.*, vol. 35, no. 2, pp. 372–379, 2022, doi: 10.5829/ije.2022.35.02b.13.

[9] M. Farhoodi, A. T. Eshlaghy, and M. R. Motadel, "A Proposed Model for Persian Stance Detection on Social Media," *Int. J. Eng. Trans. C Asp.*, vol. 36, no. 6, pp. 1048–1059, 2023, doi: 10.5829/ije.2023.36.06c.03.

[10] G. M. Abaido, "Cyberbullying on social media platforms among university students in the United Arab Emirates," *Int. J. Adolesc. Youth*, vol. 25, no. 1, pp. 407–420, 2020, doi: 10.1080/02673843.2019.1669059.

[11] A. Ademiluyi, C. Li, and A. Park, "Implications and Preventions of Cyberbullying and Social Exclusion in Social Media: Systematic Review," *JMIR Form. Res.*, vol. 6, no. 1, pp. 1–12, 2022, doi: 10.2196/30286.

[12] R. Y. Patil and S. R. Devane, "Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime," *J. King Saud*

Univ. - Comput. Inf. Sci., vol. 34, no. 5, pp. 2031–2044, 2022, doi: 10.1016/j.jksuci.2019.11.016.

[13] H. F. Hansen, "Analysis of NIST Methods on Facebook Messenger For Forensic Evidence," *JIRK*, vol. 1, pp. 695–702, 2022, doi: 10.2307/3412739.

[14] M. Yao, C. Chelmis, and D. S. Zois, "Cyberbullying ends here: Towards robust detection of cyberbullying in social media," *Web Conf. 2019 - Proc. World Wide Web Conf. WWW 2019*, pp. 3427–3433, 2019, doi: 10.1145/3308558.3313462.

[15] E. Akbal, I. Baloglu, T. Tuncer, and S. Dogan, "Forensic analysis of BiP Messenger on android smartphones," *Aust. J. Forensic Sci.*, vol. 52, no. 5, pp. 590–609, 2019, doi: 10.1080/00450618.2019.1610064.

[16] M. K. Bhatia, P. Gambhir, S. Sinha, and S. K. Singh, "A Comparative Analysis of OS Forensics Tools," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 11, pp. 494–502, 2022, doi: 10.22214/ijraset.2022.47346.

[17] T. Hermawan and L. Roselina, "Android Forensic Tools Analysis for Unsend Chat on Social Media," pp. 233–238, 2021.

[18] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. Media Inform. Budidarma*, vol. 6, no. 2, pp. 1263–1271, Apr. 2022, doi: 10.30865/mib.v6i2.3946.

[19] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," vol. 3, no. 1, pp. 13–21, 2018.

[20] M. El-tayeb, A. Taha, and Z. Taha, "Ingénierie des Systèmes d ' Information Streamed Video Reconstruction for Firefox Browser Forensics," *Int. Inf. Eng. Technol. Assoc.*, vol. 26, no. 4, pp. 337–344, 2021.

[21] K. A. Latif, R. Hammad, T. T. Sujaka, K. Marzuki, and A. S. Anas, "Forensic Whatsapp Investigation Analysis on Bluestack Simulator Device Using Live Forensic Method With ACPO Standard," *Int. J. Inf. Syst. Technol. Akreditasi*, vol. 5, no. 3, pp. 331–338, 2021.

[22] R. I. Ferguson, K. Renaud, S. Wilford, and A. Irons, "PRECEPT: a framework for ethical digital forensics investigations," *J. Intellect. Cap.*, vol. 21, no. 2, pp. 257–290, 2020, doi: 10.1108/JIC-05-2019-0097.

[23] T. Feucht, "The National Institute of Justice (NIJ)," *Encycl. Res. Methods Criminol. Crim. Justice Vol. II Parts 5-8*, vol. II, pp. 800–803, 2021, doi: 10.1002/9781119111931.ch152.

[24] Y. Safitri, Sunardi, and I. Riadi, "Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework," *J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 22, no. 3, pp. 651–664, 2023, doi: 10.30812/matrik.v22i3.2987.

[25] I. Riadi, Sunardi, and P. Widiandana, "Cyberbullying Detection on Instant Messaging Services Using Rocchio and Digital Forensics Research Workshop Framework," *J. Eng. Sci. Technol.*, vol. 17, no. 2, pp. 1408–1421, 2022.

[26] J. Choi, J. Yu, S. Hyun, and H. Kim, "Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger," *Digit. Investig.*, vol. 28, pp. S50–S59, 2019, doi: 10.1016/j.diin.2019.01.011.

[27] H. Nurhairani and I. Riadi, "Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method," *Int. J. Comput. Appl.*, vol. 177, no. 27, pp. 35–42, 2019, doi: 10.5120/ijca2019919749.

[28] M. A. Al-Garadi *et al.*, "Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges," *IEEE Access*, vol. 7, pp. 70701–70718, 2019, doi: 10.1109/ACCESS.2019.2918354.

[29] A. N. Ichsan and I. Riadi, "Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method," *Int. J. Comput. Appl.*, vol. 174, no. 18, pp. 34–40, 2021, doi: 10.5120/ijca2021921076.

[30] I. Riadi, H. Herman, and N. H. Siregar, "Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 3, pp. 489–502, 2022, doi: 10.30812/matrik.v21i3.1620.

[31] Sunardi, Herman, and S. R. Ardiningtias, "A Comparative Analysis of Digital Forensic Investigation Tools on Facebook Messenger Applications," *J. Cyber Secur. Mobil.*, vol. 11, no. 5, pp. 655–672, 2022, doi: 10.13052/jcsm2245-1439.1151.

[32] H. Adamu, A. A. Ahmad, A. Hassan, and S. B. Gambasha, "Web Browser Forensic Tools: Autopsy, BHE and Net Analysis," *Int. J. Res. Innov. Appl. Sci.*, vol. 06, no. 05, pp. 103–107, 2021, doi: 10.51584/ijrias.2021.6506.

AUTHORS

Imam Riadi –Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Sunardi – Universitas Ahmad Dahlan, Yogyakarta, Indonesia.
Yana Safitri- Universitas Ahmad Dahlan, Yogyakarta, Indonesia.
Correspondence Author– **Yana Safitri** Master Program of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia