Mobile Forensics in Human Trafficking Investigation Services Using Mobile Laboratory

Muammar[1], Imam Riadi [2*], Rusydi Umar[3]

[1,3] *Master Program of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[2] *Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
*corr-author: imam.riadi@is.uad.ac.id

Abstract - This research examines the application of a mobile digital forensic laboratory developed by the Digital Forensics Center (DFC) at UMP to handle digital evidence directly at crime scenes, specifically in human trafficking cases. Integrating the Association of Chief Police Officers' (ACPO) methods, this mobile lab facilitates the investigative process, from planning to evidence collection and analysis, without delaying transport to a central lab, thereby speeding response times and minimizing evidence degradation. We employed Magnet Axiom and DF-Tools to analyze WhatsApp data. Each demonstrated varying performance in identifying key digital evidence such as text messages, media, and group chats. DF-Tools showed an advantage in identifying multimedia artifacts with a 69.48% data acquisition success rate, compared to Magnet Axiom at 68.57%. Additionally, police bolstered their efforts to uncover human trafficking networks by implementing Base Transceiver Station (BTS)-based location tracking techniques to pinpoint suspect and victim locations via phone data or identity numbers. The research findings demonstrate that mobile labs enable rapid on-site responses, offer flexibility in collecting and securing digital evidence, and enhance efficiency and effectiveness of digital forensic investigations.

Keywords: ACPO framework; digital forensics; human trafficking; mobile laboratory; whatsapp forensics

I. INTRODUCTION

The internet has evolved rapidly, with users worldwide exceeding 3.8 billion people [1]. It is now accessible from various locations, including smartphones. Smartphones have become an integral part of daily life for many people. In Indonesia, with a population reaching 274.9 million in 2021, smartphone usage has become part of the lifestyle [2], [3]. The increasing use of smartphones as a communication tool makes it possible for WhatsApp Messenger to be misused for criminal activities, including cybercrime, as outlined in the Information and Electronic Transactions Law No. 11 of 2008 [4]. In cases of crime, the use of smartphones can impact victims of modern slavery and human trafficking [5]. There were 90,354 identified human trafficking victims globally in 2021, according to the U.S. Department of State in 2022, which details the global human trafficking data from 2011 to 2021, as shown in Fig. 1.

South and Central Asia reported the highest number of human trafficking victims, totalling 38,426, representing a 113.64% increase in victims compared to ten years earlier [6]. Technology has made communication more manageable for people. While advancements bring positive effects, they also have negative consequences, such as enabling crimes through online applications. These crimes inevitably leave digital evidence behind [7].

Digital forensics is a branch of science that applies investigative and analytical techniques to computer media or digital storage media to discover, acquire, examine, and preserve evidence in criminal cases so that it can be legally accountable [8], [9]. Digital forensics involves efforts to collect digital evidence related to a crime that has occurred [10], such as instant messaging applications that may serve as media for criminal activities. Instant messaging is a real-time communication channel that uses text, graphics, voice, or video [11]. Social media content is crucial for the police conducting criminal investigations [12], [13]. To investigate cybercrimes based on instant messaging, such as human trafficking cases, the police must analyse the suspect's device to find digital evidence. Instant messaging applications have implemented end-to-end encryption technology to prevent privacy violations such as mass surveillance by intelligence agencies [14]. Forensic handling in cybercrime cases involving computers or smartphones follows four stages: preparation, processing crime scenes, examining evidence in a digital forensic laboratory, and reporting findings. This process is outlined in Integrated Digital Forensic Investigation Framework Version 2, designed to comprehensively cover all aspects of digital forensic investigation [15].

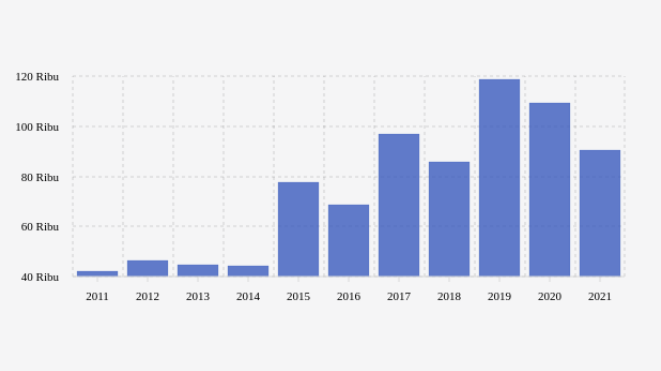


Fig. 1 The number of human trafficking victims globally according to Databooks Katadata.co.id

Indonesia's lack of digital forensic laboratories has been a major barrier to handling digital evidence in cybercrime cases, as such facilities are limited to major cities. Mobile forensic laboratories provide a solution by enabling direct analysis at crime scenes, speeding up evidence collection and reducing risks of evidence loss or data contamination, especially in remote areas. Despite limitations in equipment and human resources, mobile labs can improve investigation efficiency, particularly in human trafficking cases requiring quick responses. This research is crucial as it assesses mobile labs' effectiveness in replacing traditional forensic processes and generating strong evidence within a short timeframe.

Previous research conducted forensic processes using DFRWS Framework [16], [17] for forensic processes. The research also focused on Signal Messenger [17], Facebook [18] and Michat [16]. This research focuses on WhatsApp Messenger, specifically examining media artefacts, text messages (chats), user IDs, and groups. The main objective is to search for digital evidence in human trafficking cases on WhatsApp. Unlike previous studies that typically used physical laboratories, this research utilized mobile lab Digital Forensic Center (DFC) of Muhammadiyah University of Purwokerto (UMP), using the framework from Association of Chief Police Officers (ACPO) and two forensic tools: Magnet Axiom and DF-Tools. The goal is to demonstrate that digital forensic investigations can be effectively conducted at crime scenes with a mobile lab, reducing evidence loss risk and enabling initial evidence handling. This research provides insights into the advantages and challenges of mobile forensic investigations, serves as a reference for future studies, and encourages further development in using mobile labs for digital investigations.

II. METHOD

In this research, mobile digital forensic investigations were conducted using mobile laboratory of Digital Forensic Center (DFC) at Muhammadiyah University of Purwokerto (UMP), simulating a human trafficking case. The ACPO framework offers significant advantages in digital forensic investigations using a mobile laboratory, particularly in human trafficking cases with evidence from WhatsApp data. Compared to NIST, which focuses more on in-depth analysis in a fixed laboratory, ACPO is more flexible and practical for field operations. With simple and structured procedures, ACPO enables rapid collection, preservation, and analysis of evidence to prevent data loss or overwriting, especially in scenarios involving deleted chat data. Tools such as Magnet Axiom and DF-Tools facilitate data recovery directly at the scene, making it more efficient for urgent case investigations. Furthermore, the ACPO framework ensures that every step of evidence handling complies with legal standards, making inquiry results admissible in court. Stages of the research can be seen in Fig. 2.

This research was conducted in several stages, as follows:

A. Literature Review

This stage gathered data from previous research across various sources such as journals, articles, and books. Literature review was conducted using websites like Google Scholar, ResearchGate, and Science Direct. Keywords used in the search include "Human Trafficking," "Instant Messaging," "Digital Forensics," and "ACPO Framework." Information obtained serves as a basis for consideration and reference in conducting mobile digital forensics investigations.

B. Case Simulation

This stage implemented a Human Trafficking case scenario on WhatsApp instant messaging application. The scenario uses perpetrator's smartphone. In this scenario, Human Trafficking perpetrator is apprehended, and Android smartphone is secured as evidence. Scenario is illustrated in Fig. 3.

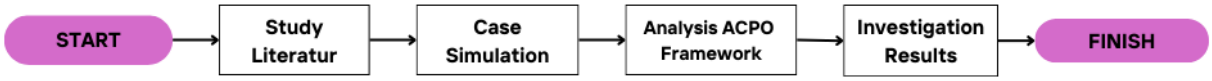


Fig. 2 Research stages methodology

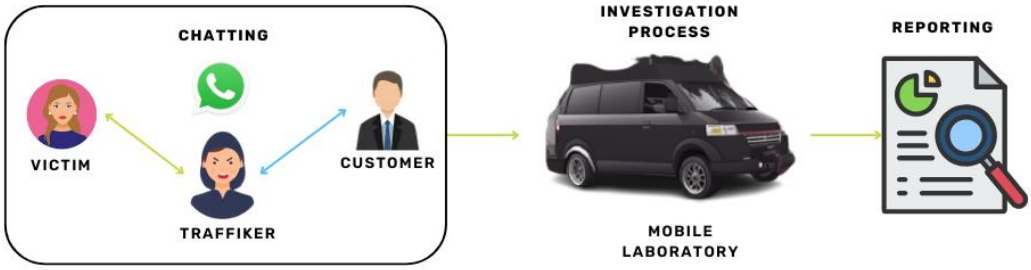


Fig. 3 Case simulation

Fig. 3 illustrates a case simulation where a perpetrator offers a job to a victim. After accepting an offer, the victim realizes the perpetrator has sold them. The victim reported the incident to the police, who discovered that perpetrator deleted 20 image files from the chat to destroy evidence. Following the victim's report, a Samsung A51 smartphone, identified as evidence, is secured by the police. A mobile laboratory is then sent to the crime scene to conduct a digital forensic investigation into a human trafficking case.

C. Forensic Analysis

At this stage, the simulation data was analysed using ACPO 7Safe, titled "Good Practice Guide for Computer-based Electronic Evidence" [19]. This framework was chosen for its comprehensive guidelines and suitability for rapid digital evidence investigations using a mobile laboratory. ACPO was selected for its advantages for mobile laboratories like DFC UMP, particularly its flexibility in handling various mobile forensic scenarios, focusing on practical guidance to assist investigators in documenting and collecting evidence at the crime scene. This approach allows investigators at mobile laboratories like DFC UMP to secure and analyse evidence directly, reducing the risk of evidence alteration or loss from transporting evidence to a physical lab. This is especially crucial in human trafficking cases, where time is critical to follow up on communication evidence in apps like WhatsApp. The ACPO framework is applied in the mobile investigation process with four main stages, as shown in Fig. 4.

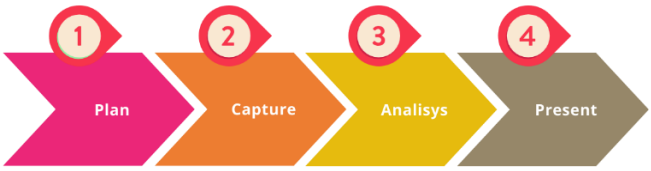


Fig. 4 ACPO framework

This research focuses on several variables: media, text messages, user IDs, and groups. These variables are analysed to assist in finding digital evidence related to human trafficking cases using Forensic Magnet Axiom and DF-Tool. Fig. 4 outlines the stages of ACPO framework [20] as follows:

- Plan : The planning phase includes the laboratory's mobile plan, determining actions, tools, and software used, and assuring that the investigation process follows mobile digital forensics procedures that address data privacy challenges while facilitating rapid acquisition in crime scenes.
- Capture : At this stage, the evidence data is documented, stored, retrieved, and collected. Data extraction from mobile devices is done quickly and securely, supported by specialised extraction tools, both software and hardware, available in the mobile laboratory.
- Analysis : This is an extensive process of collecting data using technically justified methods to obtain helpful information and answer the questions that prompted data collection and investigation. Data is analysed and compared to obtain valid results.

- Present : Final stage presents the analysed data, along with recommendations for further action.

D. Forensic Results Investigation

Final stage is a forensic investigation of results as a reference for developing human trafficking cases and accelerating the completion of investigations. These results are processed into data on the location of other suspected perpetrators using BTS and GPS.

III. RESULT AND DISCUSSION

This research describes the digital forensic procedure employing a mobile lab that enables all phases of the ACPO framework, from planning to reporting, to be carried out on-site at the crime scene. Flexibility is one of the benefits of DFC UMP's mobile laboratory. It speeds up the inquiry and minimizes possibility of evidence degradation by offering a quick answer without requiring transmission of evidence to a central laboratory. Compared to a static laboratory, this advantage is essential in cybercrime cases involving human trafficking networks since it allows for quicker evidence handling, development of cases involving additional suspects, and more effective case resolution.

A. Plan

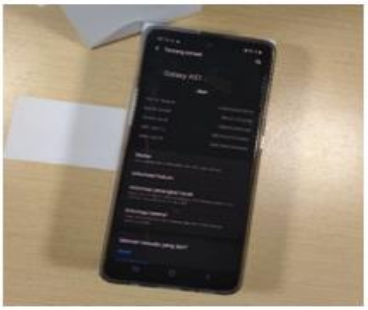
This process commenced with the development of a plan for evidence handling, which included the mobile laboratory's journey to the crime site in accordance with an official order from authorities. This was done to reduce risk of evidence loss when transferring to a central laboratory. Evidence, including smartphones of the perpetrator and victim, was documented while they were still operational upon arrival at the site. In order to guarantee the integrity of evidence, this procedure adhered to the ACPO and 7Safe guidelines. The initial step was to activate Developer Options to prevent evidence tampering and activate Airplane mode to terminate smartphone's internet connection. In order to extract evidence from WhatsApp in conformance with ACPO standards, this research employed Magnet Axiom and DF-Tools software, as well as forensic hardware in a mobile laboratory like Lenovo ThinkCentre Neo 50a PC and Samsung Galaxy A51 smartphone as digital evidence [20]. Fig. 5 illustrates the documentation procedure of evidence (Samsung Galaxy A51 smartphone) at this stage.

B. Capture

Digital evidence acquisition was carried out during acquisition phase using mobile laboratory equipment. Despite limitations in tools and absence of variable variations in this study, field investigation team ensured that the collection of validated evidence followed established procedures. Fig. 6 illustrates digital evidence acquisition process.

Forensic techniques aim to capture critical data such as text chats, media, and user IDs as digital evidence in Human Trafficking cases. The smartphone evidence was analysed using Magnet Axiom and DF-Tools WhatsApp. The the capture results are shown in Fig. 7 and 8.

Fig. 7 shows the digital evidence data acquisition process using Magnet Axiom Process forensic tool with the connected Galaxy A51 device for data extraction. The results were stored in digital storage of the mobile forensic laboratory. Fig. 8 shows the WhatsApp data extraction process using DF-Tool.



Device Name	**Samsung Galaxy A51 SM-A515F**
Serial Number	RR8NC098WNM
IMEI (slot 1)	350475672948981
IMEI (slot 2)	358760472948980
Sim Card	Yes
Platform	Android

Fig. 5 Smartphone evidence

Fig. 6 Investigator analysis officer

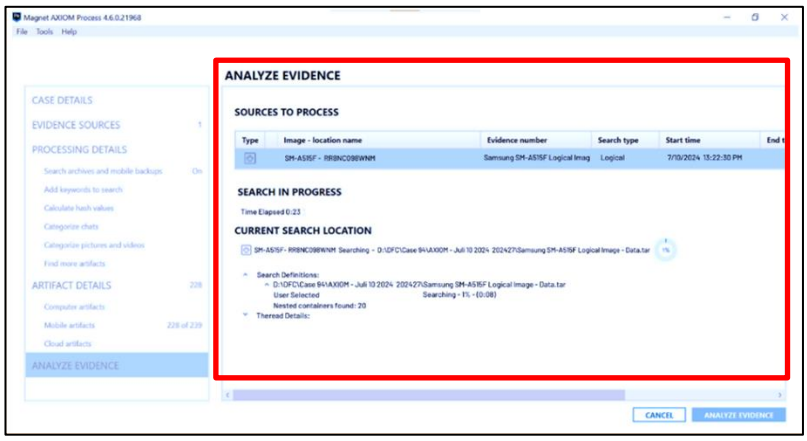


Fig. 7 Magnet Axiom capture result

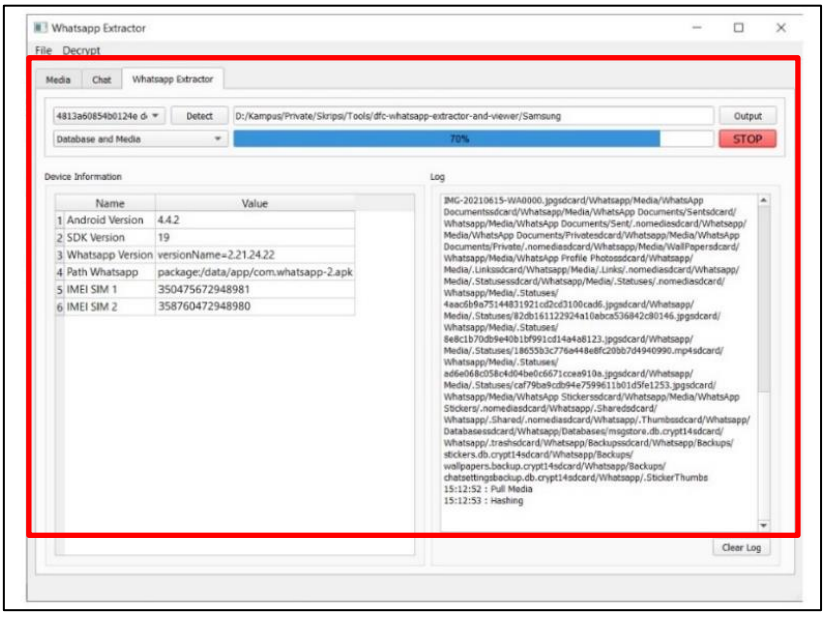


Fig. 8 DF-Tools WhatsApp capture result

DF-Tool features an automatic data extraction process. Monitoring results show that DF-Tool successfully retrieved artefacts, which were compressed into a .rar file, as demonstrated in Fig. 9, representing WhatsApp data acquisition results.

WhatsApp data acquisition results from WhatsApp forensic tool, as shown in Fig. 9, display artefacts and required data extracted according to folders present on the smartphone, including the accompanying hash validation values.

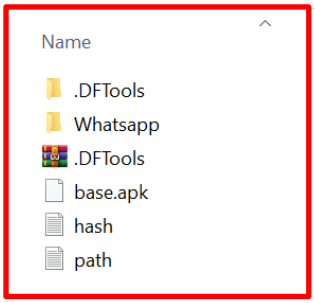


Fig. 9 Report acquisition DF-Tools WhatsApp

C. Analysis

Forensic analysis was conducted in the mobile laboratory after obtaining data from (Capture) data extraction process. In this analysis, information discovered during examination was cross-referenced to ensure consistency with the pre-established simulation data. This process aimed to gather and filter valid, processable digital evidence, which was then used to support further investigation for use in court. In this investigation, the investigators used two primary forensic applications: Magnet Axiom Examine and DF-Tools Viewers WhatsApp. The analysis focused on text information from conversations and media. Magnet Axiom was used for in-depth analysis and to match evidence related to images, audio, and text information according to the above case simulation, specifically examining conversations between traffickers and customers preparing for a transaction, as illustrated in Fig. 10.

Fig. 10 explains the conversation between traffickers and customers who asked about payment methods; the traffickers explained that payments can be made via bank transfer or payment applications. Data extraction using Magnet Axiom can produce data artefacts that can be reviewed and analysed, as shown in Fig. 11.

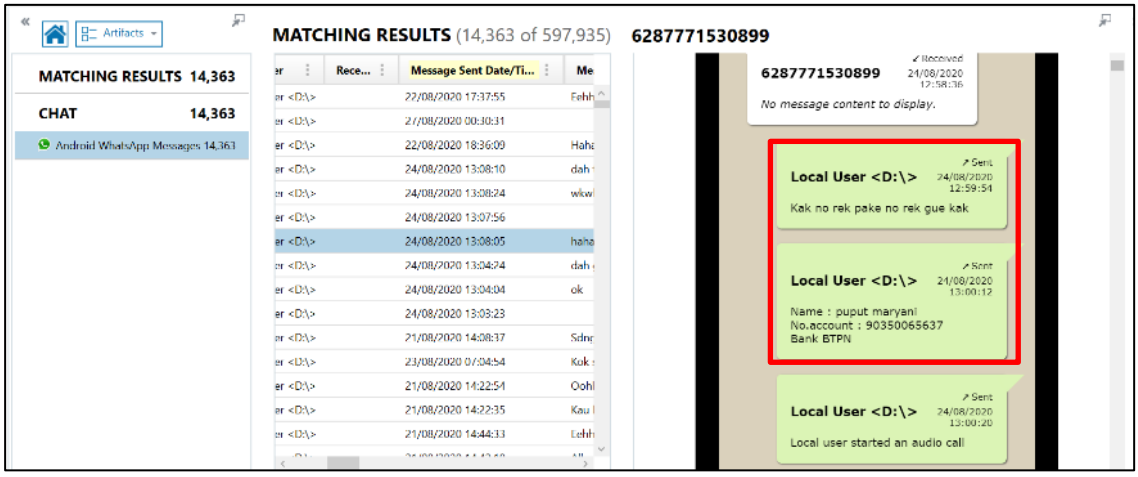


Fig. 10 Report chat Magnet Axiom

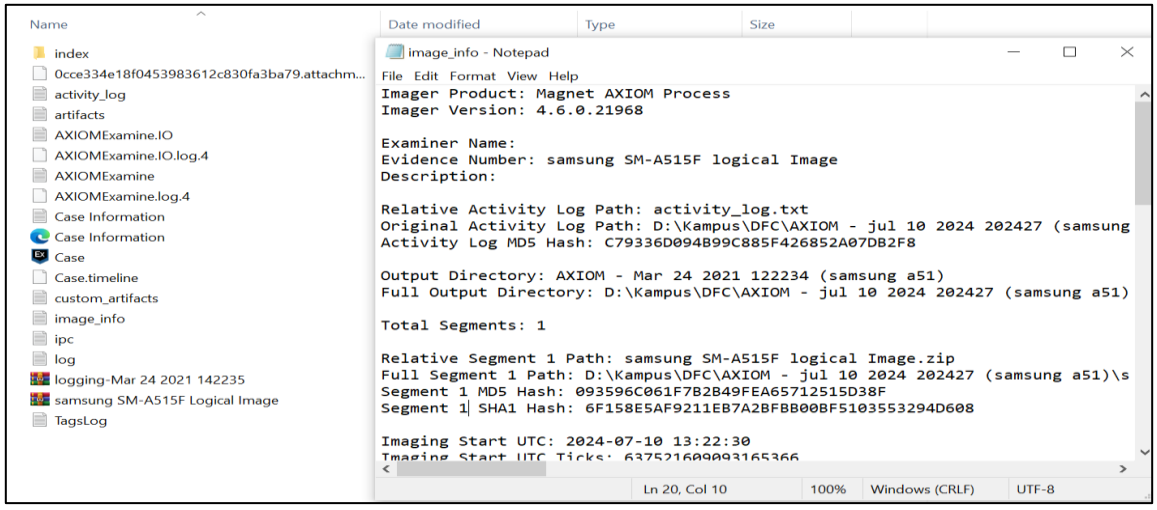


Fig. 11 Full report on the results of the acquisition of the Magnet Axiom application

Meanwhile, DF-Tool WhatsApp was used to extract and analyse conversation data from the WhatsApp application, which included job offers similar to those in the case simulation above, displaying conversations between traffickers and victims, as shown in Fig. 12.

Data extraction in the DF-Tools application can produce data artefacts that can be reviewed and analysed, as in Fig. 13.

The investigators then compiled all the analysed evidence to create a comprehensive report. Report was prepared using a pre-existing template, which expedited preparation of results directly in the DFC UMP mobile laboratory. This approach facilitated understanding for non-experts, ensuring that the information presented can be clearly interpreted and effectively used in further investigative processes.

D. Present

Presentation stage explains that the researchers successfully collected digital evidence including conversations, user IDs, media, and groups. This research focused on analyzing conversations stored in device's database. The researchers employed an index number formula (1) to assess performance of forensic tools used, aiming to provide a more accurate evaluation of tools' effectiveness in identifying and collecting digital evidence.

$$P_{ar} = \frac{\sum ar0}{\sum arT} \times 100 \quad (1)$$

Note:
P_{ar} = Forensic tool accuracy index number
$\dot{a}rT$ = Total number of variables used
$\dot{a}r0$ = Number of variables detected [17].

The findings highlight mobile forensics as an efficient and reliable method for forensic investigations using mobile laboratory, particularly on Android platform. This is supported by the performance index calculations of the forensic tools used, as shown in Table I, where Magnet Axiom and DF-Tools demonstrate variations in performance in identifying and collecting digital evidence.

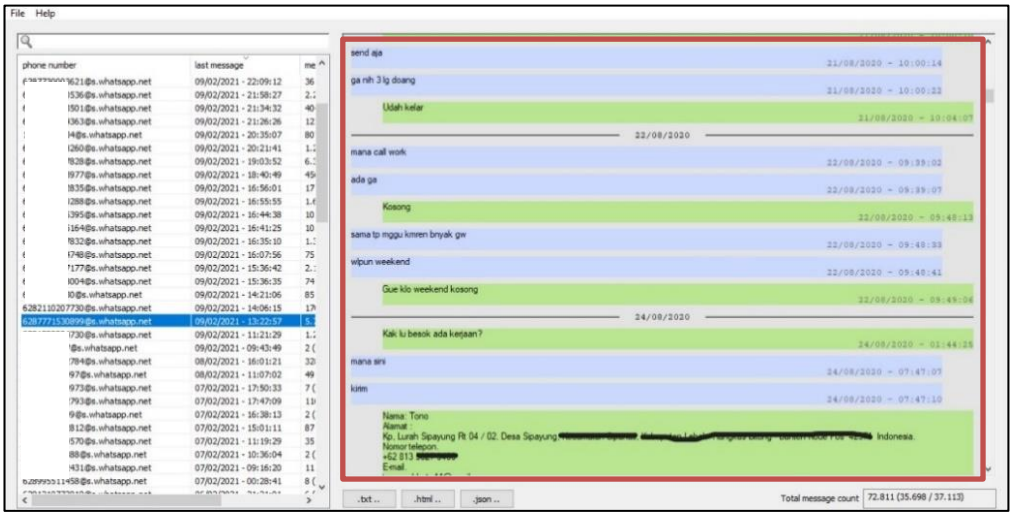


Fig. 12 View chat results from the acquisition of the DF-Tools application

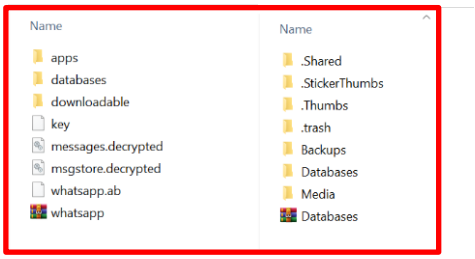


Fig. 13 Report on the results of the acquisition of the DF-Tools application

TABLE I
ACQUISITION SUCCESS

Digital evidence	Digital evidence obtained		
	Magnet Axiom	***DF-Tools***	**Submitted evidence**
ID Chat	86	99	110
Grup	4	5	5
Image	3410	3423	5000
Audio	43	68	68
Document	31	28	31
Video	29	29	40
Percentage Success	**68,5%**	**69,4%**	**100%**

Based on Table I, findings of digital evidence show performance variations between forensic tools Magnet Axiom (68.5%) and DF-Tools (69.4%). The difference in success rates between the two tools is minimal and may not be statistically significant. Of the 110 text chat IDs sent, Magnet Axiom successfully found 86 text chats, while DF-Tools found 99 text chat IDs. Both tools were able to identify Group Chats, with Magnet Axiom finding 4 out of 5 groups sent, while DF-Tools found all five groups. In terms of image files, there were 5000 artefact files, 20 of which had been deleted. Magnet Axiom found only 3410 image files, and the deleted files in chat could not be recovered, whereas DF-Tools found 3423 image files, with 13 of them being deleted files. For audio files, Magnet Axiom found 43 out of 68 audio files, while DF-Tools found all 68 audio files. Regarding documents, Magnet Axiom found 31 files, while DF-Tools found 28 papers. Both tools successfully found 29 out of 40 video artifacts. Neither of the tools could recover 100% of data, as the smartphone was not rooted or given full access. So, this limitation occurred. Rooting was not performed to achieve process efficiency.

These results show that both tools have different performances in identifying specific types of artefacts. Magnet Axiom has limitations in identifying deleted files in chats, while DF-Tools is more effective in recovering deleted image files. Overall, the performance difference between the two tools indicates that DF-Tools is slightly more effective, particularly for deleted data, although the difference is only 0.9%. Therefore, mobile forensics using the ACPO framework can be an effective method, as both tools perform well in a short and rapid process.

E. Investigation

Investigation stage discusses case development which involves tracking estimated location using phone number or digital identity number of other suspected perpetrators. This investigation aims to create a more detailed and comprehensive timeline of events. The concept of location tracking based on data found refers to the patent proposed by [21], which discusses location determination based on Base Transceiver Station (BTS), as illustrated in Fig. 12. A BTS (Base Transceiver Station) or transmitter station can determine its location using information received from nearby BTSs or signals sent by mobile devices to neighbouring BTS.

Fig. 12 illustrates steps taken to trace the locations of other suspected perpetrators. The process begins with the collection of signal data from Base Transceiver Stations (BTS) and GPS data from relevant mobile devices, including alleged phone number or IMEI. This signal data is then processed to determine signal strength and estimate the device's location using triangulation methods, taking into account BTS identity, signal reception time, signal strength (RSSI - Received Signal Strength Indicator), and Timing Advance (TA). Next, GPS data is used to verify and strengthen location estimates, as well as to analyse timing to understand the sequence of movements. Integrated data is then visualised using mapping software to identify movement patterns, which helps in uncovering relationships between suspects and locations. Afterwards, the obtained location data is compiled into a report to be presented to authorities or telecommunications operators for follow-up based on the findings; this stage can be conducted directly in the mobile laboratory. This stage of investigation is crucial as it assists the police in thoroughly uncovering human trafficking cases. By following these steps, the integration of BTS and GPS data not only enhances accuracy of locating other suspected perpetrators but also strengthens overall investigation process, especially in dismantling networks in cases where timely and accurate information is essential.

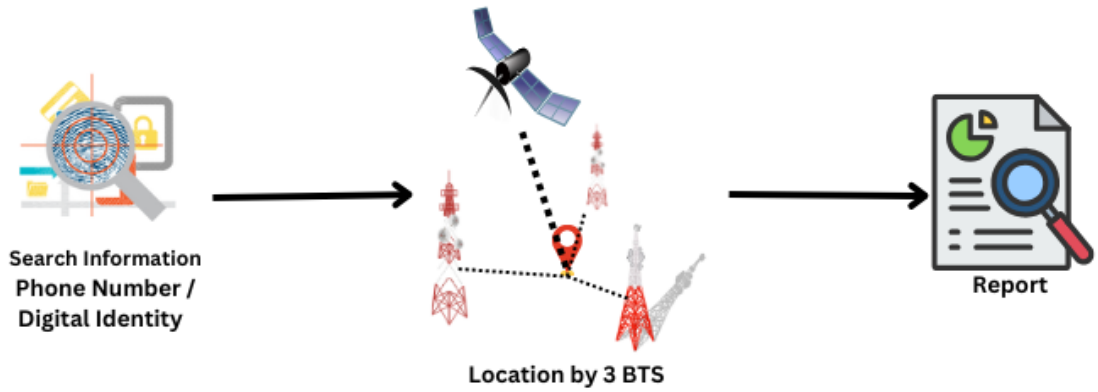


Fig. 12 Tracking location by BTS

IV. CONCLUSION

This research examined the use of the DFC UMP mobile digital forensics laboratory as an innovative method for handling digital evidence at the crime scene within ACPO framework. The mobility of this laboratory enhances quick response times. It reduces risk of evidence tampering or damage, which is critical in human trafficking cases involving perpetrators and victims in different locations. Various tools, such as Magnet Axiom and DF-Tools, are used to handle investigations in obtaining digital evidence from WhatsApp, including chat IDs, groups, images, audio, documents, and videos, particularly in scenarios involving deleted image chats. Authentication of evidence can be verified through file hashing, and the success rate in finding evidence based on parameters reaches 100%, which is in line with the capabilities of the forensic tools. The results of this research align with the research objectives, revealing that rapid field investigations can be conducted with a success rate of 69.4% for DF-tools, especially in recovering deleted evidence. To improve accuracy, it is recommended that future research conduct rooting processes to obtain more specific and accurate data. This research introduces case development by tracking the locations of other suspected perpetrators by utilising data in the forms of phone numbers or identity numbers, allowing for estimated location information to be discovered through BTS and GPS tracking methods, which leverage BTS Identity, RSSI, TA, and the latest GPS data. This approach strengthens coordination between investigators and network operators in efforts to thoroughly uncover the human trafficking network, thereby enhancing efficiency and effectiveness of the investigation. Despite the findings, this research has limitations as it does not cover variables such as device or operating system variations. These limitations are acknowledged as part of the research discussion to contextualise findings and provide direction for future research that includes more diverse and complex scenarios.

ACKNOWLEDGEMENT

This research was supported by the Directorate of Research, Technology, and Community Service Ministry of Education, Culture, Research and Technology, Indonesia, under Grant No. 107/E5/PG.02.00.PL/2024; 0609.12/LL5-INT/AL.04/2024; 069/PTM/LPPM/UAD/VI/2024. We want to express our deepest gratitude to the Digital Forensics Center (DFC) UMP laboratory for their invaluable support and resources throughout this research.

REFERENCES

[1] I. Riadi, A. Yudhana, and M. Al Barra, "Forensik Mobile pada Layanan Media Sosial LinkedIn," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 6, no. 1, pp. 9–20, 2021, doi: 10.14421/jiska.2021.61-02.

[2] A. Alanda, D. Satria, H. A. Mooduto, and B. Kurniawan, "Mobile Application Security Penetration Testing Based on OWASP," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 846, no. 1, 2020, doi: 10.1088/1757-899X/846/1/012036.

[3] S. K. Saad, R. Umar, and A. Fadlil, "Analisis Forensik Aplikasi Dropbox pada Android menggunakan Metode NIJ pada Kasus Penyembunyian Berkas," *J. Sains Komput. Inform. (J-SAKTI*, vol. 4, no. September, p. 293, 2020, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jsakti/article/view/221/203 (accessed Jul. 10, 2024).

[4] N. Saputri and R. Indrayani, "Analisis Data Forensik Investigasi Kasus Peredaran Narkoba Pada Smartphone Berbasis Android," *Djtechno J. Teknol. Inf.*, vol. 3, no. 2, pp. 156–166, 2022, doi: 10.46576/djtechno.v3i2.2597.

[5] K. A. Hogan and D. Roe-Sepowitz, "Providing Services to Victims of Human Trafficking During the COVID-19 Pandemic: A Social Service Agency State-Wide Survey," *J. Soc. Serv. Res.*, vol. 49, no. 3, pp. 357–376, 2023, doi: 10.1080/01488376.2023.2232827.

[6] C. M. Annur, "Ada 90 Ribu Korban Perdagangan Manusia di Seluruh Dunia pada 2021," Katadata Media Network, 2021.

[7] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 118–134, 2020, doi: 10.25299/itjrd.2021.vol5(2).4664.

[8] S. Sotnik, T. Shakurova, and V. Lyashenko, "Development Features Web-Applications," *Int. J. Acad. Appl. Res.*, vol. 7, no. 1, pp. 2643–9603, 2023, [Online]. Available: www.ijeais.org/ijaar (accessed Jul. 11, 2024).

[9] Sunardi, I. Riadi, and M. H. Akbar, "Application of Static Forensics Method for Extracting Steganographic Files on Digital Evidence Using the DFRWS Framework," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 3, pp. 576–583, 2020, doi: 10.29207/resti.v4i3.1906.

[10] I. Riadi, S. Sunardi, and A. Hadi, "Analisis Bukti Digital TRIM Enable SSD NVMe Menggunakan Metode Static Forensics," *JUITA J. Inform.*, vol. 8, no. 1, p. 65, 2020, doi: 10.30595/juita.v8i1.6584.

[11] R. N. Dasmen and F. Kurniawan, "Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media SosialDigital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial," *Techno.Com*, vol. 20, no. 4, pp. 527–539, 2021, doi: 10.33633/tc.v20i4.5170.

[12] M. El-Tayeb, A. Taha, and Z. Taha, "Streamed Video Reconstruction for Firefox Browser Forensics," *Ing. des*

Syst. d'Information, vol. 26, no. 4, pp. 337–344, 2021, doi: 10.18280/ISI.260401.

[13] A. Setya and A. Suganda, "Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014," *JUITA J. Inform.*, vol. 10, no. 1, p. 127, 2022, doi: 10.30595/juita.v10i1.13149.

[14] J. Son, Y. W. Kim, D. Bin Oh, and K. Kim, "Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema," *Forensic Sci. Int. Digit. Investig.*, vol. 40, p. 301347, 2022, doi: 10.1016/j.fsidi.2022.301347.

[15] B. Actoriano and I. Riadi, "Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2," *Int. J. Cyber-Security Digit. Forensic*, vol. 7, no. 4, pp. 410–419, 2018, [Online]. Available: https://www.researchgate.net/publication/327592240 (accessed Jul. 10, 2024).

[16] 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, p. 1263, 2022, doi: 10.30865/mib.v6i2.3946.

[17] 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.

[18] R. A. Bintang, R. Umar, and A. Yudhana, "Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST," *Techno (Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.

[19] J. Williams, *ACPO Good Practice Guide for Digital Evidence*, 5.0., vol. 71, no. 10. England, Wales & Northern Ireland. It: Police Cenral e-Crime Unit, 2012.

[20] F. Anggraini, H. Herman, and A. Yudhana, "Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers," *JURIKOM (Jurnal Ris. Komputer)*, vol. 9, no. 4, p. 1117, 2022, doi: 10.30865/jurikom.v9i4.4738.

[21] M. N. A. and S. D. Chapman, "SYSTEMAND METHOD FOR DETERMINING A BASE TRANSCEIVER STATION LOCATION," US 7,751,833 B2, 2013.