Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research, and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 7 No. 2 (2023) 286 - 292 ISSN Media Electronic: 2580-0760

Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework

Imam Riadi[1], Anton Yudhana[2], Galih Pramuja Inngam Fanani[3*]
[1]Department of Information System, Universitas Ahmad Dahlan
[2]Department of Electrical Engineering, Universitas Ahmad Dahlan
[3]Department of Informatics, Universitas Ahmad Dahlan
imam.riadi@is.uad.ac.id[1], eyudhana@ee.uad.ac.id[2], galih2008048035@webmail.uad.ac.id[3]

Abstract

Instant Messaging (IM) is a popular and widely used communication application. MiChat is a multi-platform instant chat service with several features that can attract various segments of the population to use it as a tool for committing cybercrimes. A forensic framework and several forensic tools are needed to carry out physical evidence investigation procedures. This study focuses on analyzing and comparing the forensic tools used during the research, based on defined digital evidence parameters and applying a specific mobile forensic framework. The results show that Final Mobile Forensic has the highest ability to obtain digital evidence and can recover deleted data, while Oxygen Forensic Detective has advantages in terms of audio, images, and video but cannot recover data. The best framework is DFRWS, which has the most complete stages so that it can support the investigation process. The best digital evidence is text chat and contacts, which can be used to support valid legal claims.

Keywords: digital forensic; mobile forensic; michat; smartphone

1. Introduction

Android smartphones have been in vogue over the last decade. Android-based smartphones are one of the most popular types of smartphones and have had many users over the last decade [1]. Due to the very high demand for mobility, on the other hand, the price is also very varied. Figure 1 shows the number of smartphone users from the last 7 years in the world. By 2022, the number of smartphone users will have increased significantly, further increasing to around 6,000 million users in the world [2].

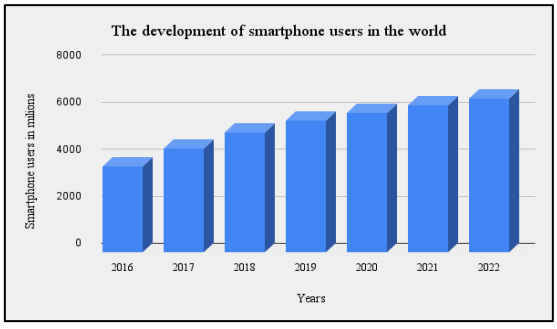

Figure 1. Smartphone Users in The World

The more versions of Android there are, the more various applications appear. One of them is Instant Messaging (IM) applications such as WhatsApp, LINE, Telegram, and Signal [3–5]. Android smartphones are so widely used that they make them an unavoidable source of forensic analysis from a criminal and non-criminal perspective [6], [7]. The increasing usage of social networking apps may potentially raise the likelihood of cybercrime. Online prostitution, sextortion, drug trafficking, and cyberbullying are some of the cybercrimes that are currently active [8], [9]. Data based on (Numbeo) shows that Venezuela is a country with the highest crime index in the world, reaching 83.16, and Indonesia occupies the 15th position for crime rates in Asia with an index value of 46.06, just above Vietnam, out of a total of 44 listed Asian countries [10]. In Indonesia, there are several cases of crimes involving short messaging applications. One of them is the MiChat application, which is very popular in Indonesia with 50 million downloads on Google Play [11]. Michat functionally helps communicate among users, such as through various media sharing or chatting. Michat is often associated with abusive activity for criminal purposes [12], [13]. Various cases involving the MiChat application in Indonesia are

Accepted: 29-09-2022 | Received in revised: 02-02-2023 | Published: 26-03-2023

shown in Table 1. These are cases in the last 5 years that occurred in Indonesia through the Michat application [14–18].

Table 1. Michat Cases That Occurred in Indonesia

No.	Year	Case
1.	2022	Dissemination of identity and immoral documents via MiChat in West Sumatra.
2.	2021	Drug trafficking through the MiChat Application in West Java and East Java.
3.	2020	Online fraud via MiChat in Samarinda
4.	2019	Human trafficking via Michat in North Sulawesi
5.	2018	The murder of Sisca Icun Sulastri by Hidayat who met via Michat in South Jakarta in Cimahi

Based on the issues outlined above, if investigators find evidence of criminal infringement on a MiChat message, they should look at the messaging service artifact to find out what happened. Therefore, there is a need for forensic handling, especially mobile forensics, in helping to solve crime cases [19]. Mobile forensic tools are needed that can help investigators extract artifacts, decrypt, and analyze data in dealing with cybercrime cases involving mobile devices [20]. Investigators also need to use supporting methods to assist the handling process in a structured and efficient manner. Crime scenes on Android devices can be solved with mobile device forensics techniques [21]. Several branches of science in the field of digital forensic studies can be seen in Figure 2.

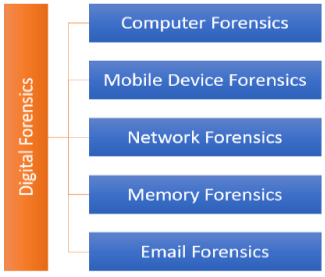

Figure 2. Five Substations of Digital Forensics.

As seen in Figure 2, digital forensics comprises at least five research subfields. Mobile device forensics is one of them. Mobile device forensics is digital forensics concerned with the acquisition or recovery of digital evidence from mobile devices. The issue with forensics is that many forensic technologies do not function properly [22]. This is also a concern of researchers; they say that every forensic tool has advantages and disadvantages. Another study conducted by Dogan and Akbal used the 2014 edition of MOBILedit Forensics and Oxygen Forensic Suite. Digital crime investigations using smartphone devices must be handled by utilizing various forensic instruments with different capabilities. Based on the results of this study, MOBILedit Forensics has an advantage in terms of run time, and Oxygen Forensic Suite 2014 has an advantage in finding artifacts [23].

According to research findings conducted by Salem et al., a comparison of forensic tools between Cellebrite UFED and XRY was made. XRY outperformed Cellebrite UFED in obtaining most types of digital evidence artifacts, whereas in maintaining the integrity of the authenticity of the evidence, Cellebrite UFED excelled [24].

Padmanabhan et al., also compared and analyzed commercial (paid) and open source forensic tools. Several forensic tools compared include Autopsy, SANS SIFT, MOBILedit Forensics, and Cellebrite UFED. According to the findings of this study, open source forensic tools are more widely used, with the advantages of GUI-based applications with terminal commands, logging capabilities, and fault-tolerant warnings. Meanwhile, commercial forensic tools excel in terms of processing speed, data extraction accuracy, analytical capabilities, and the capacity to retrieve lost data [25].

The researchers have grounds to undertake an experiment on forensic tool competence assessment in MiChat digital evidence examination based on the preceding study and certain background difficulties.

This article focuses on the comparison of the analysis of the capabilities of five mobile forensic tools using two methods, namely the Association of Chief Police Officers (ACPO) and the Digital Forensics Research Workshop (DFRWS), in handling digital cases involving android devices.

2. Research Methods

2.1. Stages of Research

In this study, researchers used a case study simulation by applying 2 frameworks, namely ACPO and DFRWS, to analyze the MiChat application on smartphones. This simulation was carried out with the aim of comparing the two frameworks and forensic tools on the MiChat application on smartphones to find evidence of messages and media files used to commit crimes and make the contents of these messages evidence. In summary, the methods and processes of the research phase are described in Figure 3.

Figure 3. Methods and Phase of Research

Figure 2 shows a research method with several phase, namely: The research problem is the initial stage in obtaining and determining the research subject for future investigation. It begins at this level by examining diverse occurrences, events, and information collected in various methods; The literature review is expected to unearth all information related to the problems to be studied and the object of research, as well as provide a

DOI: https://doi.org/10.29207/resti.v7i2.4547

foundation for the direction of research to be carried out and serve as a starting point for each researcher so that research can be used as a reference in the future; Case Study is a forensic framework-based investigation of an Android-based MiChat application using four (four) tools: Mobiledit Forensic Express, DB Browser for SQLite, Oxygen Forensic Detective, and Final Mobile Forensics. The results of the overall analysis process will be compared. As shown in Figure 4.

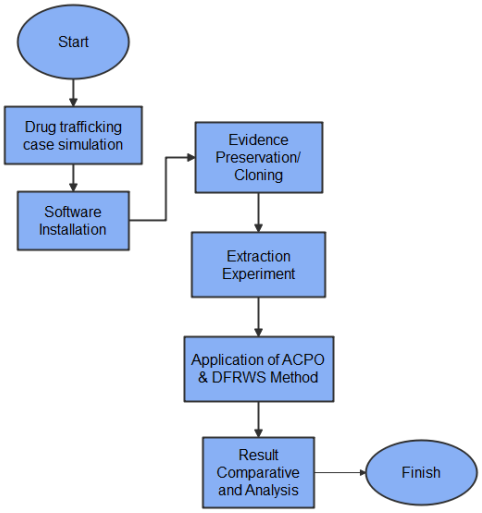

Figure 4. Case Process of Research Phase

The flowchart can be described as Drug trafficking case simulation: The drug trafficking case simulation in this study involves the MiChat application; Software Installation: Researchers as investigators install forensic tool software on computers or notebooks that will be used for the acquisition and analysis of digital evidence; Evidence Preservation/Cloning: Investigators must carry out maintenance of physical evidence in airplane mode to maintain the integrity of the original data, before cloning or backing up data from smartphone devices; Extraction Experiments: investigators carry out extractions on smartphone devices with several forensic tools. Using MOBILedit Forensic Express for smartphone physical imaging processes, DB Browser for SQLite for MiChat application database analysis, Oxygen Forensic Detective, and Final Mobile Forensic are used to analyze digital evidence from multimedia files; Use of ACPO and DFRWS Methods: In this study, researchers used two frameworks to compare a more appropriate framework to assist investigators in conducting investigations. ACPO has 4 stages, namely: plan, capture, analysis, and presentation [26]. Meanwhile, DFRWS has six stages, namely: identification, preservation, collection, examination, analysis, and presentation [27]; Evaluation and Analysis of Results: The performance of each forensic tool will be evaluated and analyzed based on the software characteristics and digital evidence gathered from each device. The settings employed are tailored to the study goals, namely MiChat application analysis; Conclusion is the process of all the stages that have been completed in this research, from the handling of physical evidence and obtaining digital items in the form of variables related to conversation time, conversation message content, and profiles of perpetrators and victims on MiChat, where the data can be analyzed to see if there was a criminal act, to the final stage of creating a final report to be presented.

2.2. Research Case Scenario

The scenario of this research is drug trafficking transactions between dealers and drug users using the MiChat application. Figure 5 is a conceptual simulation of a drug trafficking case, showing the communication process between the perpetrator and the victim in sending messages.

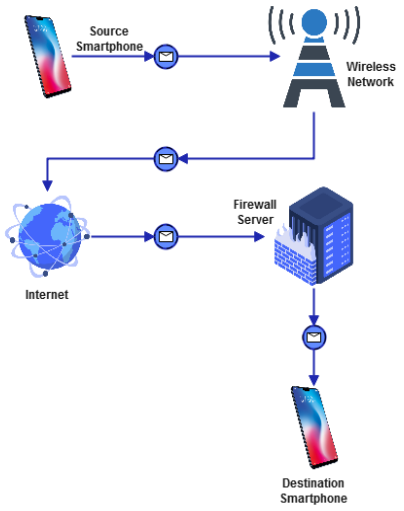

Figure 5. Research Scenarios of Drug Trafficking Cases

There are two smartphone users who use the MiChat application, which is connected to the internet network. Drug dealers offer drugs through the MiChat app to camouflage themselves from cyber cops. Drug dealers make buying and selling transactions through the chat feature on the MiChat application via the internet network, and the message will arrive at the MiChat server before it reaches the user.

Data will be collected from the crime of drug trafficking, investigators find transcripts of conversations between perpetrators and victims that have been stored in the database.

2.3. Research Tools

This research, in the process, requires tools used to obtain artifacts from the MiChat application. The research tool consists of two categories: hardware and forensic software. The explanation of the research materials used in this experiment can be seen in Table 2.

DOI: https://doi.org/10.29207/resti.v7i2.4547

Tabel 2. Software and Supporting Hardware

Hardware and Software	Function
PC	Used to carry out the process of transferring digital data from smartphones to storage media for the analysis process
MOBILedit Forensic Express	Used for the physical imaging process or data backup of the MiChat application on a smartphone
Final Mobile Forensic	Used for further analysis of media files on extracted files.
DB Browser for SQL	Used for further analysis of extracted database files
Oxygen Forensic Detective	Used for further analysis of media files on extracted files
USB Connector/ USB Dongle	Used to connect a smartphone to a computer to get full access to the smartphone
Portable Power Suplly	Is a device to increase smartphone battery power and is used to maintain the condition of the smartphone in an "on" condition.
Faraday Bag	A bag that is used to secure smartphones from data communication.

3. Results and Discussions

3.1 Oxygen Forensic Detective

Oxygen Forensic is capable of doing both logical and physical acquisitions. Oxygen Forensic was able to obtain information from a smartphone device.

Figure 6 is the Oxygen forensically collected Michat app conversation text artifact. Only physical acquisitions can produce those text message artifacts. Investigators can use oxygen forensics to dig up call logs, text message conversations, calendar notes, and app activity logs based on a chronological timeline as shown in Figure 7. This tool is quite beneficial for analyzing the time period established by the Ministry of Justice [6].

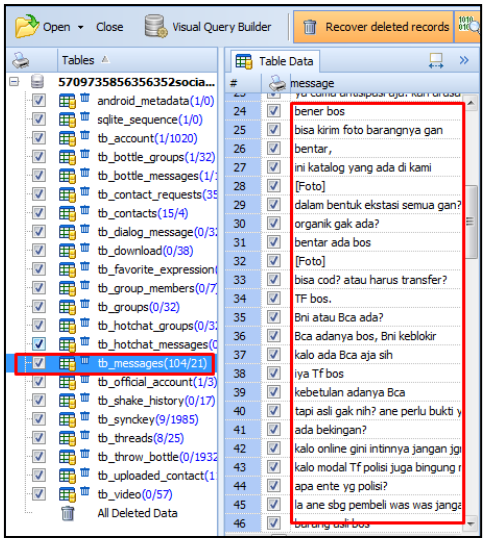

Figure 6. Digital text chat on Oxygen Forensic Detective tools

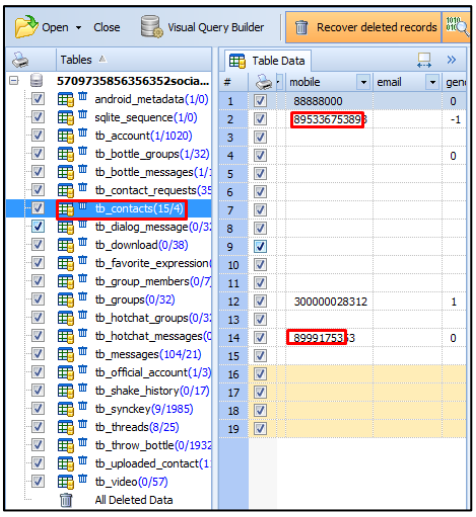

Figure 7. Digital Contact data on Oxygen Forensic Detective tools

3.2 MOBILedit Forensic Express

MOBILedit forensics, like oxygen forensics, may undertake both logical and physical acquisitions. MOBILedit Forensic was effective in obtaining information from a smartphone device. MOBILedit can recognize the IMEI (International Mobile Equipment Identity) numbers of both mobile phones as well as the IMSI and ICCID (Integrated Circuit Card Identifier) of registered SIM cards. MOBILedit successfully obtains contact information, text messages, and photographs from the MiChat app. However, video artifacts are not displayed in the MOBILedit acquisition. Figure 8. shows image artifacts with brief information regarding file paths, file sizes, file creation, and change. Image files can include information on how these files were created.

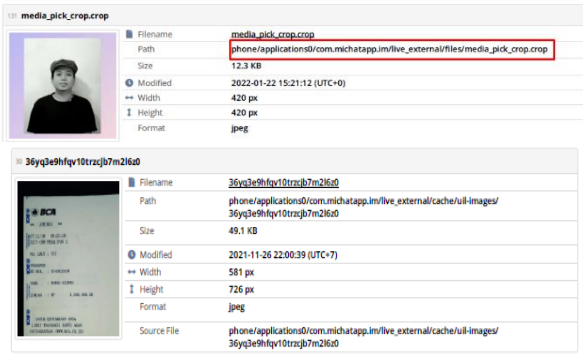

Figure 8. Digital Images on MOBILedit Forensic Express

3.3 DB Browser for SQLite

Based on the results of the analysis of previous tools, there are indications of drug trafficking transactions. To obtain more detailed data, an analysis of the next tool is carried out. The results of the examination using the DB Browser for SQLite tool do not produce images or photos due to software limitations, but the conversation data is obtained in full. The analysis shows exactly the same conversations as those featured in Oxygen

DOI: https://doi.org/10.29207/resti.v7i2.4547

Forensic. Figure 9 shows the results of conversational analysis using DB Browser for SQLite.

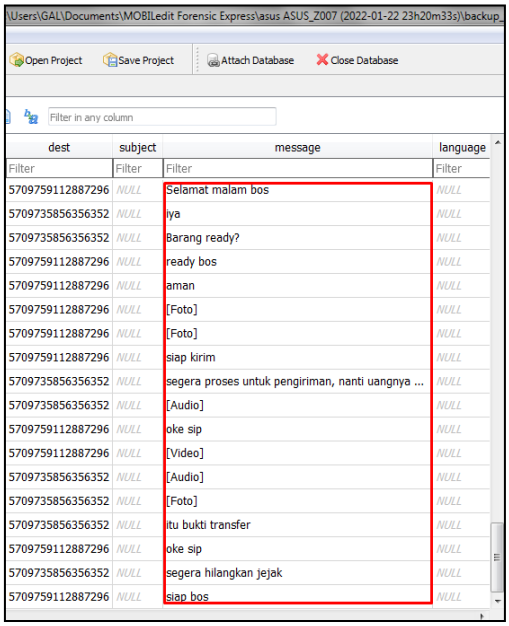

Figure 9. Digital Chat on DB Browser for SQLite

3.4 Final Mobile Forensics

Analysis using Final Mobile Forensics also found digital data in the form of audio, video, web caches, and timestamps as shown in Figure 10. Evidence that deleted image and audio files can be recovered with the original file size with high quality. Video files are found and analyzed according to the specified parameters.

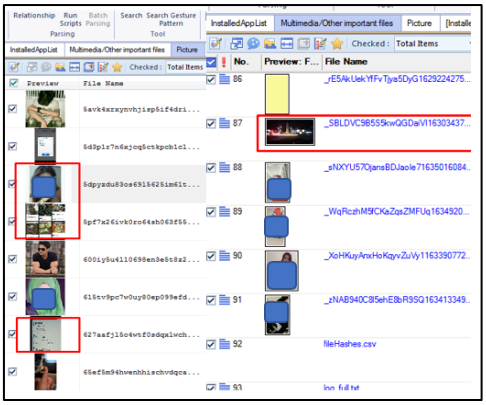

Figure 10. Digital Images and Video Data On Final Mobile Forensic Tools

3.5 Discusion

The results of the analysis of digital forensic evidence in the case scenario of drug trafficking can be compared with the data of evidence found. The results of the verification of the best digital evidence data are text chat and contacts because all forensic tools used are able to acquire the evidence. All the evidence obtained, chat messages and contacts became the most important and main data points for drug trafficking cases. The results of the comparison of digital evidence based on the capabilities of forensic tools are shown in Table 3.

Table 3. Comparison Results of Forensic Tools

Metode	Evidence Parameters	Tools Forensic			
		Mobil Edit Express	DB Browser for SQL	Oxigen Forensic Detectiv	Final Mobile Forensic
ACPO	Text Chat	✓	✓	✓	✓
	Contact	✓	✓	✓	✓
	Images	✓	-	✓	✓
	Audio	✓	-	✓	✓
	Video	-	-	✓	✓
	Cache web	-	-	-	✓
	Timestmap	-	-	✓	✓
DFRWS	Text Chat	✓	✓	✓	✓
	Contact	✓	✓	✓	✓
	Images	✓	-	✓	✓
	Audio	✓	-	✓	✓
	Video	-	-	✓	✓
	Cache web	-	-	-	✓
	Timestmap	-	-	✓	✓

According to the experimental results, to evaluate the effectiveness of each forensic tool, researchers performed calculations using index numbers. The index number is calculated as the overall score index, as shown in equation 1.

$$par = \frac{\sum ar0}{\sum arT}\ x\ 100\% \quad (1)$$

Par is the Index number as a percentage, ar0 is the Forensic Tools-obtained Evidence, and arT is the Total Digital Evidence/Artifact.

Based on the ACPO and DFWRS methods, there are only differences in the stages of the framework. Acpo has 4 stages of the process, namely plan, capture, analysis, and presentation. Meanwhile, DFRWS has six phases, starting with identification, preservation, collection, examination, analysis, and the final phase of the presentation.The complete DFRWS method is clearer and more detailed. From the ability of forensic tools used to find evidence based on predetermined parameters, Final Mobile Forensic has a strong advantage by calculating the index of each forensic tool using equation 1. It has the highest index value of 100%. MOBILedit Forensic Express has an index value of 57.1%, DB Browser for SQL has an index value of 28.6%, and Oxygen Forensic Detective has an index value of 85.7%.

4. Conclusion

According to the findings of the investigations and analyses of drug trafficking cases, the MiChat

DOI: https://doi.org/10.29207/resti.v7i2.4547

application uses two ACPO and DFRWS frameworks, with evidence parameters namely chat text files, contacts, images, audio, video, web cache, and timestamp. Overall, the results of the comparison and analysis can be concluded that the most appropriate and best mobile forensics method is DFRWS. The best evidence, based on the overall verification of forensic tools, is text chat and contact. The highest capability of mobile forensic tools is 100%, namely Final Mobile Forensic, MOBILedit Forensic Express has the ability with an index value of 57.1%, DB Browser for SQL has an index value of 28.6%, and Oxygen Forensic Detective has an index value of 85.7%. The results of the comparison of all forensic tools are based on research that shows that final mobile forensic tools have full power capabilities and even available timestamp specifications. This study is in accordance with the objectives of the researcher, so that the researcher can find and compare the two forensic tools based on the evidence.

Acknowledgment

Thank you to the Ahmad Dahlan University MTI Study Program for facilitating the Research Laboratory to conduct experiments and providing a forum for developing journal research.

Reference

[1] 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.

[2] S. O'Dea, "Number of smartphone subscriptions worldwide from 2016 to 2027," *www.statista.com*, 2022. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (accessed Jul. 07, 2022).

[3] I. Riadi, S. Sunardi, and M. E. Rauli, "IWhatsApp Digital Evidence identification on Proprietary Operating Systems Using Live Forensics," *J. Tek. Elektro*, vol. 10, no. 1, pp. 18–22, 2018, doi: 10.15294/jte.v10i1.14070.

[4] A. Menahil, W. Iqbal, M. Iftikhar, W. Bin Shahid, K. Mansoor, and S. Rubab, "Forensic Analysis of Social Networking Applications on an Android Smartphone," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/5567592.

[5] M. R. Setyawan, A. Yudhana, and A. Fadlil, "Data Acquisition On Messenger Skype Using The National Institute Of Justice Method," *Syst. Inf. Syst. Informatics J.*, vol. 5, no. 2, pp. 13–18, Mar. 2020, doi: 10.29080/systemic.v5i2.724.

[6] R. Umar, I. Riadi, and B. F. Muthohirin, "Acquisition of Email Service Based Android Using NIST," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 3, no. 3, pp. 263–270, 2018, doi: 10.22219/kinetik.v3i4.637.

[7] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 155–160, 2017, [Online]. Available: https://www.researchgate.net/publication/317620078

[8] A. Sanchez, N. Han, and P. Jones, "Mexico: Organized Crime and Drug Trafficking Organizations Related papers T he St rat egic Implicat ions of t he Cárt el de Jalisco Nueva Generación," 2015. [Online]. Available: www.crs.gov

[9] Y. F. Amilia and D. Wahyudi, "Investigating the Crime of Prostitution Online," vol. 2, pp. 45–56, 2021, doi: https://doi.org/10.22437/pampas.v2i1.12413.

[10] Numbeo, "No Crime Index by Country 2022 Mid-Year," *www.numbeo.com*, 2022. https://www.numbeo.com/crime/rankings_by_country.jsp (accessed Jul. 07, 2022).

[11] M. Rauf, A. Prasetio, S. Sos, and M. Si, "Communication Activities Match Search Applications on Michat Media," in *e-Proceeding of Management*, 2021, pp. 1559–1571.

[12] G. Fanani, I. Riadi, and A. Yudhana, "Michat Application Forensic Analysis Using Digital Forensics Research Workshop Method," vol. 6, no. 2, pp. 1263–1271, 2022, doi: 10.30865/mib.v6i2.3946.

[13] K. D. O. Mahendra and I. K. Ari Mogi, "Digital Forensic Analysis Of Michat Application On Android As Digital Proof In Handling Online Prostitution Cases," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 9, no. 3, p. 381, Feb. 2021, doi: 10.24843/JLK.2021.v09.i03.p09.

[14] Y. Pasha, "Nyambi Trades Drugs, Police Arrested Prostitutes in MiChat," *jabar.idntimes.com*, 2020. https://jabar.idntimes.com/news/jabar/bagus-f/nyambi-dagang-narkoba-psk-di-michat-ditangkap-polisi (accessed Jul. 08, 2020).

[15] L. Utama and A. Hari, "North Sulawesi Police Unravel Human Trafficking Through the MiChat Application," *viva.co.id*, 2019. https://www.viva.co.id/berita/nasional/1182565-polda-sulut-bongkar-perdagangan-manusia-lewat-aplikasi-michat (accessed Jul. 08, 2022).

[16] A. Anwar, "Sisca Icun Sulastri's murder, this is how MiChat is abused," *Tempo.co*, 2018. https://metro.tempo.co/read/1158644/pembunuhan-sisca-icun-sulastri-begini-michat-disalahgunakan (accessed Jul. 08, 2002).

[17] S. Maulana, "The Story of a Man in Samarinda, Fooled by Open BO MiChat to Lose Millions of Rupiah," *suarakaltim.id*, 2021. https://kaltim.suara.com/read/2021/04/14/164208/kisah-pria-di-samarinda-tertipu-open-bo-michat-hingga-rugi-jutaan-rupiah?page=all (accessed Jul. 08, 2022).

[18] Humas Polres Pessel, "Spreading Immoral Documents via MiChat, 19-year-old Student Arrested by Ditreskrimsus West Sumatra Police," *Kriminal*, 2022. https://pesisirselatan.sumbar.polri.go.id/index.php/2022/04/26/sebarkan-dokumen-asusila-lewat-michat-mahasiswa-19-tahun-diamankan-ditreskrimsus-polda-sumbar/ (accessed Jul. 08, 2022).

[19] O. Osho and S. O. Ohida, "Comparative Evaluation of Mobile Forensic Tools," *Int. J. Inf. Technol. Comput. Sci.*, vol. 8, no. 1, pp. 74–83, 2016, doi: 10.5815/ijitcs.2016.01.09.

[20] S. Singh and S. Kumar, "Qualitative Assessment of Digital Forensic Tools," *Asian J. Electr. Sci.*, vol. 9, no. 1, pp. 25–32, 2020, doi: 10.51983/ajes-2020.9.1.2372.

[21] 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, Feb. 2021, doi: 10.5120/ijca2021921076.

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

[23] S. Dogan and E. Akbal, "Analysis of mobile phones in digital forensics," *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2017 - Proc.*, pp. 1241–1244, 2017, doi: 10.23919/MIPRO.2017.7973613.

[24] F. E. Salamh, U. Karabiyik, M. K. Rogers, and E. T. Matson, "A comparative uav forensic analysis: Static and live digital evidence traceability challenges," *Drones*, vol. 5, no. 2, 2021, doi: 10.3390/drones5020042.

[25] R. Padmanabhan, K. Lobo, M. Ghelani, D. Sujan, and M. Shirole, "Comparative analysis of commercial and open source mobile device forensic tools," *2016 9th Int. Conf. Contemp. Comput. IC3 2016*, 2017, doi: 10.1109/IC3.2016.7880238.

[26] I. Riadi, R. Umar, and M. A. Aziz, "Web Forensics Instant Messaging Service Using Association of Chief Police Officers (ACPO) Methods," *Mob. Forensics*, vol. 1, no. 1, p. 30, Sep.

2019, doi: 10.12928/mf.v1i1.705.
[27] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Comparative analysis of Forensic Tools on Twitter applications using the DFRWS method," *J. RESTI*, vol. 1, no. 3, pp. 829–836, 2017, doi: https://doi.org/10.29207/resti.v4i5.2152.

DOI: https://doi.org/10.29207/resti.v7i2.4547