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. 6 No. 2 (2022) 213 - 219 ISSN Media Electronic: 2580-0760

Live Forensic to Identify the Digital Evidence on the Desktop-based WhatsApp

Triawan Adi Cahyanto[1], Muhammad Ainul Rizal[2], Ari Eko Wardoyo[3], Taufiq Timur Warisaji[4], Daryanto[5]
[1,2,3,4,5]Department of Informatics, Faculty of Engineering, Universitas Muhammadiyah Jember
[1]triawanac@unmuhjember.ac.id*, [2]muhammad.ainul.rizal@gmail.com, [3]arieko@unmuhjember.ac.id,
[4]taufiqtimur@unmuhjember.ac.id, [5]daryanto@unmuhjember.ac.id

Abstract

The live forensics method was used to acquire lawful digital evidence data from device memory in the WhatsApp application, particularly for desktop-based WhatsApp. There has been little research on live forensics on desktop-based WhatsApp applications. These studies involve mimicking crime cases in cyberspace using the Instant Messenger application. Much of the acquisition process is completed only once, even though many possible conditions may arise during the purchase process. Investigators or experts can employ digital evidence data discovery to identify crimes that have occurred. The stages of research carried out in detecting digital evidence are data collecting, the examination process, and the acquisition of analysis and reporting outcomes. During the data-gathering phase, a case simulation dataset was obtained. The examination process stage results in the integrity of the duplicated data; data reduction is performed on data related to fundamental operating system components, influential application features, and incomplete data. According to the investigation findings, there are difficulties in looking for digital evidence, and the features of each digital evidence vary. The simulation file contained many reports on the finds of digital evidence. As a data acquisition method, the characteristics of live forensics are limited to the data retrieval process in RAM. Based on these findings, it is possible to conclude that the data collection and examination processing were completed effectively. The analysis results were acquired, and the report was presented with the indicated digital evidence. Further study can be paired with chip-off procedures on RAM devices for data recovery.

Keywords: Live Forensics, Data Acquisition, Digital Artifact, Volatile Data, Dekstop-based WhatsApp

1. Introduction

Various techniques or methods can assist the identification process of digital evidence, one of which is live forensics. The live forensics method is a technique for identifying digital evidence when the equipment or system evidence is in operating condition [1]–[3]. The live forensics method is appropriate for handling volatile data characteristics [4, 5]. Volatile data in Random Access Memory (RAM) describes all activities in a system [6]. Based on this explanation, it can be concluded that the live forensics method is a very appropriate choice for handling and as a form of assistance in the identification process of digital evidence of criminal cases related to volatile data. Based on this description, several previous research results are needed as a reference. Based on this background, the state of the art several studies became the basis of this research. Research on the application of live forensics on desktop-based WhatsApp applications (WAD) is still limited, but several studies on the topic of live forensics have been carried out by [7]–[13]. These studies are in the form of simulating a crime case in cyberspace with the involvement of an Instant Messenger (IM) application. The following process is in data acquisition on the perpetrator's device, and data analysis is carried out based on the acquisition results. The acquisition process is only carried out once, while the reality on the ground is that various possible conditions can occur during the acquisition process—this possibility, such as when the IM application is logged out while the data has been deleted.

Digital forensics has become an essential part of handling cases in cyberspace. Digital forensics is categorized as a branch of science focusing on taking legal evidence or recognizing it at trial based on data sources from storage media such as hard drives, flash drives, RAM, and others [14]. Along with technology development, it has increased cybercriminals using information technology to support crime using IM applications as a communication medium [15]. The

Accepted: 03-02-2022 | Received in revised: 07-04-2022 | Published: 20-04-2022

resolution or prevention of these crimes can be completed in terms of technical aspects through digital forensic science. The field of digital forensics is divided into sub-fields of digital forensics, especially related to the handling of the characteristics of digital evidence being studied, such as mobile forensics, live forensics, network forensics, and others. The digital forensics study in this study focuses on the discussion of live forensics methods to identify digital evidence in WAD applications.

Digital evidence in WAD applications is characteristic of volatile data, so live forensics techniques are appropriate for identification. Analyzing digital evidence is carried out through the stages of data acquisition and analysis of the data acquired from the WAD application with various possible challenges or scenarios. The determination and use of the live forensics method in this research are closely related to data collection, examination, analysis, and reporting to obtain several research objectives. This research is expected to be a compliment and an explanation for the shortcomings found in previous studies. The results or the final output of this research are expected to assist investigators or experts in implementing the data acquisition process with a live forensics approach to WAD applications and analysis of the data acquired by WAD applications with various possible challenges or scenarios that can occur.

Based on the formulation of the problem, the objectives of this research were set, namely (i) collecting data and examining the process and (ii) obtaining the results of analysis and reporting (reporting). Furthermore, the benefits of this research are expected to complement and explain the shortcomings found in several previous studies, and the output of this research can be used as assistance for investigators or experts. Based on this, the information submitted by investigators or experts can be recognized and declared legal to be used as legal evidence at trial.

2. Research Methods

This research was carried out in a laboratory within the Department of Informatics, Faculty of Engineering, Universitas Muhammadiyah Jember, from November 2021 to January 2022. Research materials and tools are needed to achieve each research goal through several implementation stages. The research material used is a dataset in the form of a simulation of death threats and terror cases from the WAD application [16]. The research tools used are (i) two computers, Lenovo G40 and Lenovo 3493EQG, (ii) Google Pixel smartphone, (iii) Samsung hard drives, (iv) FTK Imager application, and (v) Hashmyfile application.

The research method is an algorithm for achieving each research goal [17]–[19]. The selection of the algorithm used is in the form of a flowchart. The research method is in the form of a flowchart, as shown in figure 1.

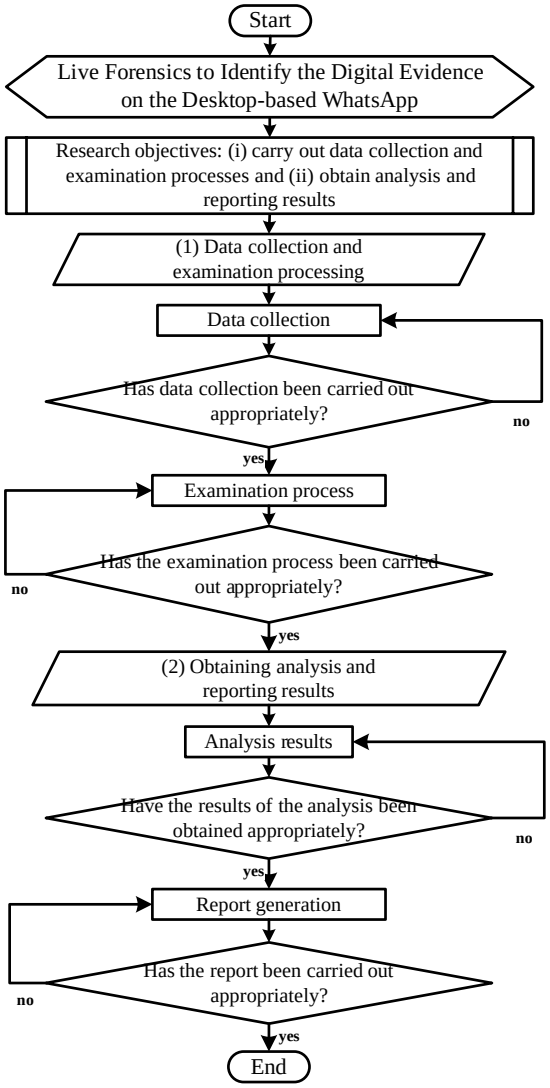


Figure 1. The research method is in the form of a flowchart.

Based on figure 1, it can be explained that there are four essential stages in this research, namely (i) the stage of data collection and examination process and (ii) the stage of obtaining the results of analysis and reporting. The data collection stage begins with creating primary data, namely case simulation datasets. The case data simulation is classified into three data; namely, simulation-1 elements consist of intact simulation data, no activity is given, simulation-2 is given exercise in the form of leaving WhatsApp (WA) on a cellphone, and simulation-3 is given chat data deletion activities. The next stage is based on the three conditions of the simulation data in the form of applying live forensics as a data acquisition mechanism when the device is in working condition.

DOI: https://doi.org/10.29207/resti.v6i2.3849

The stages of the examination process consist of verifying the authenticity of the dataset, reducing it, and searching for digital evidence. The steps of obtaining the analysis results focus on challenges in finding digital evidence and explaining the characteristics of digital evidence findings. The stages of making reports are carried out to summarize the results of digital proof.

3. Results and Discussions

3.1 Data Collection and Examination Process

The data collection phase consists of (i) making simulations of death threats and terror cases using WAD. A dataset will be obtained as primary data for this research in case simulations. When creating case simulations, specific challenges related to the data acquisition process are encountered. The data acquired only applies to activity data stored in RAM so that data outside of that (e.g., data on the hard drive) is not analyzed in more detail—the flow of case simulation creation is shown in figure 2.

Figure 2. Threat case simulation design.

Based on figure 2, it can be explained that (i) the case simulation was made by using two computers (the perpetrator's computer and the investigator's computer) and a hard drive as a storage medium for the duplicated files resulting from the data acquisition. (ii) The application of the live forensics method is carried out in making case simulations because this method is very suitable for data acquisition techniques in RAM, as the results of research by Mcdown et al. [11]. The case simulation is divided into three conditions: the condition when the WAD application activity is regular, the state when the WAD application activity exits the mobile version of the WA, and the situation when the WAD application activity is deleting data. These three conditions are often encountered in everyday life, so the possibility of problems related to these conditions has also been found, based on the results of research from Utami et al.; Riadi et al.; and Anwar et al. [13], [20], [21]. The examination process begins with (i) verification of the authenticity of the dataset consisting of three simulation data files. Guarantee is intended to ensure no changes to the data after the data acquisition process. The hashmyfile application is used for data integrity verification. The hashmyfile application is a display for data integrity verification, as shown in figure 3.

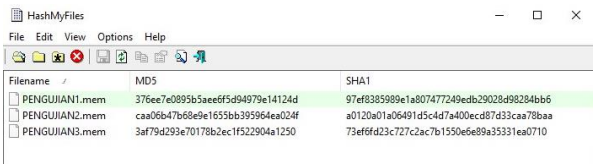
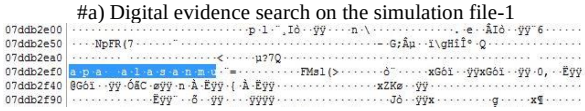


Figure 3. Hashmyfile application display for data integrity verification

The file shown in figure 3 is when the acquisition is complete. Data integrity verification is performed only for cloned files so that the original files are still stored. The data integrity verification stage is carried out by comparing the original file's hash value to the duplicated file's hash value, both MD5 and SHA1, and the resulting hash value must be the same. The data reduction stage needs to be carried out to obtain significant results from the search for digital evidence—the acquisition of volatile data from activities stored in RAM, mainly in incomplete pieces of information. Data reduction is carried out on data relating to the essential components of the operating system, obfuscation of data on application features, and incomplete data. The digital evidence search stage is carried out manually to ensure that pieces of information, which are generally vague, can be understood and interpreted as digital evidence. The search for digital evidence was carried out using the FTK Imager application on three simulation data files. The display of the search for digital proof of the simulation file is shown in figure 4.

#a) Digital evidence search on the simulation file-1



#b) Digital evidence search on the simulation file-2

Figure 4. Display of digital evidence search on the simulation file

Based on figure 4, it can be shown that the digital evidence data for simulation-1 and simulation-2 have been found. The data from simulation-3 did not find chat data, as was the case with chat data found in simulation-1 and simulation-2 data. This is because the data acquisition process is carried out after the message deletion process. Based on the search for digital evidence, there were data findings from (i) the simulation-1 totaling fifteen data, including telephone numbers of perpetrators and victims, conversation texts, multimedia files, and call trace log activities; (ii) the simulation-2 consists of ten data including telephone numbers, conversation texts, multimedia files, and call trace log activities; while (iii) there are six simulations-3 processes which include traces of phone numbers from perpetrators and victims without clear

DOI: https://doi.org/10.29207/resti.v6i2.3849

information, multimedia files, call tracking activity logs, and no text conversation data found.

3.2 Results of Analysis and Reporting

The stage of obtaining the analysis results begins with (i) challenges in finding digital evidence. The first challenge is finding pieces of text that are not intact. Various things cause the incomplete condition, in this case, the data storage mechanism in RAM [11] as the results of previous research by Mcdown et al., but some data are intact. Incomplete data files often occur, caused by various factors, in this case, simulation, by the communication and data acquisition processes, because both works simultaneously. The storage location of the found multimedia files has been identified if the file data (e.g., images, documents, audio, etc.) have been downloaded. The data recovery process for file discovery failed to be carried out because the data acquisition process was only limited to the virtual environment (RAM). It needed special techniques (e.g., removing the chip in RAM so that the data was successfully retrieved). The next stage is the analysis results in the form of the characteristics of digital evidence findings.

Display of digital data findings in simulation-1, as shown in table 1.

Table 1. Display of digital data evidence findings on the simulation file-1

Digital evidence finding	Characteristics	*Timestamp*
Victim's phone number (6282231249XXX)	name"Jur Kompas"shortName".Jur"profilePic" vhttps://web.*WhatsApp*.com/pp? t=s&u=6282231249XXX	-
Criminal's phone number (6282226249XXX)	7D58B52802","ack":3,"from":"6282226249XXX @c.us","to":"6282231249XXX	-
(Text): maksud kamu apa?	Complete text data and follow the evidence from the victim's cellphone	-
(Text): membongkar tentang saya tanpa bukti yang jelas	Complete text data and follow the evidence from the victim's cellphone	-
(Text): Saya dapet faktanya dari sumber yang valid dan bisa dibuktikan	Complete text data and follow the evidence from the victim's cellphone	-
(Text): saya bisa bunuh	Incomplete text data	-
(Text): apa alasanmu	Complete text data and follow the evidence from the victim's cellphone	
(Text): itu rumah kamu kan	Complete text data and follow the evidence from the victim's cellphone	-
(Text): Ancaman anda sudah saya laporkan ke polisi	Complete text data and follow the evidence from the victim's cellphone	-
Filename voicemail	*WhatsApp* Ptt 2022-01-23 at 10.13.15.ogg	10:13
Filename picture	Rumah Jur 2022-01-23.jpg	-
Filename picture	W.h.a.t.s.A.p.p. .I.m.a.g.e. .2.0.2.2.-.0.1.-.2.3. .a.t. .1.0...3.1...3.8...j.p.e.g	10:31
Incoming call	2022-01-2310:15:48.025:[*log* voip:incoming_signaling(pairedphone): {"id":"CF616CA68B5545E50859B0C A03 5229A1" ,"type":"offer","from":"6282231249XXX	10:15
Incoming call	2022-01-2310:16:48.025:[*log* voip:incoming_signaling(pairedphone): {"id":"CF616CA68B5545E50859B0C A03 5229A1" ,"type":"offer","from":"6282231249XXX	10:16
Incoming call	2022-01-23 10:46:12.469:[*log*][main-process][voip-native] voip:L3: 03:46:12.439 wa_capability_def.cc participant 6282231249XXX@s.*WhatsApp*.net has capability	10:46

Based on table 1, it can be explained that the digital evidence found in the form of data on telephone numbers, the text of conversations between the perpetrator and the victim, data on image and sound filenames, traces of incoming voice calls from the victim and voice calls out of the perpetrator. The discovery of the characteristics of digital evidence, including (i) some text data in intact condition, so that they can be recognized and interpreted, while text data is not in intact condition, it is necessary to carry out further analysis until finally understandable information is obtained; (ii) multimedia files can only be recognized from the file name and file storage location, while the file has failed to perform data recovery; and (iii) telephone number data is intact so that it can be appropriately interpreted.

Display digital data evidence findings in simulation-2, as shown in table 2.

Based on table 2, it can be explained that the acquisition of digital evidence in the form of data on telephone numbers and text of conversations made by the perpetrator and the victim, data on image and sound filenames, traces of incoming voice calls from the victim and voice calls out of the perpetrator. The characteristics of the digital evidence found are generally the same as the simulation-1. Still, there are some differences which include (i) the victim's phone number data was not found as in the simulation-1, (ii) the findings obtained were only traced numbers without

DOI: https://doi.org/10.29207/resti.v6i2.3849

Table 2. Display of digital data evidence findings on the simulation file-2

Digital evidence finding	Characteristics	*Timestamp*
Victim's phone number (6282231249XXX)	7D58B52802","ack":3,"from":"6282226249XXX @c.us","to":"6282231249XXX	-
Criminal's phone number (6282226249XXX)	7D58B52802","ack":3,"from":"6282226249XXX @c.us","to":"6282231249XXX	-
(Text) Saya dapet faktanya dari sumber yang valid dan bisa dibuktikan	Complete text data and follow the evidence from the victim's cellphone	-
(Text) saya bisa bunuh	Incomplete text data	-
(Text) apa alasanmu ?	Complete text data and follow the evidence from the victim's cellphone	-
Filename voicemail	*WhatsApp* Ptt 2022-01-23 at 10.13.15.ogg	10:13
Filename picture	Rumah Jur 2022-01-23.jpg	-
Filename picture	W.h.a.t.s.A.p.p. .I.m.a.g.e. .2.0.2.2.-.0.1.-.2.3. .a.t. .1.0...3.1...3.8....lnk	10:31
Incoming call	2022-01-2310:15:48.025:[*log* voip:incoming_signaling(pairedphone): {"id":"CF616CA68B5545E50859B0C A03 5229A1" ,"type":"offer","from":"6282231249XXX	10:15
Incoming call	2022-01-2310:16:48.025:[*log* voip:incoming_signaling(pairedphone): {"id":"CF616CA68B5545E50859B0C A03 5229A1" ,"type":"offer","from":"6282231249XXX	10:16
Outgoing call	2022-01-23 10:46:12.469:[*log*][main-process][voip-native] voip:L3: 03:46:12.439 wa_capability_def.cc participant 6282231249XXX@s.*WhatsApp*.net has capability	10:46

contact information, and (iii) the names of the multimedia files found are the same as those found in the simulation-1, but there are differences in the file name extensions, namely in simulation-2 with the *.ink extension, while in simulation-1 it has the *.jpeg extension, and (iv) found timestamp descriptions of some messages.

Display digital data evidence findings in simulation-3, as shown in table 3.

Table 3. Display of digital data evidence findings on the simulation file-3

Digital evidence finding	Characteristics	*Timestamp*
Victim's phone number (6282231249XXX)	7D58B52802","ack":3,"from":"6282226249XXX @c.us","to":"6282231249XXX	-
Criminal's phone number (6282226249XXX)	7D58B52802","ack":3,"from":"6282226249XXX @c.us","to":"6282231249XXX	-
Filename voicemail	*WhatsApp* Ptt 2022-01-23 at 10.13.15.ogg	10:13
Filename picture	Rumah Jur 2022-01-23.jpg	-
Filename picture	W.h.a.t.s.A.p.p. .I.m.a.g.e. .2.0.2.2.-.0.1.-.2.3. .a.t. .1.0...3.1...3.8....lnk	10:31
Outgoing call	2022-01-23 10:46:11.923:[*log*] voip:incoming_signaling(peer):{"peer_jid":"6282231249XXX@s.*WhatsApp*.net","isContact":true	10:46

Based on table 3, it can be explained that the acquisition of digital evidence in the form of traces of telephone numbers, names of multimedia files, and traces of calls. The characteristics of the digital evidence found are generally the same as the simulation-1 and simulation-2. Still, there are some differences which include (i) no conversational text data found, (ii) voice message file names and picture file names found, (iii) found call trace files, and (iv) found timestamp descriptions of some messages.

Based on the results of the analysis of the data acquisition of digital evidence on the three simulation data, it can be concluded that each simulation data shows different results. A comparison is displayed in a bar chart against digital evidence findings based on three simulation data, as shown in figure 5.

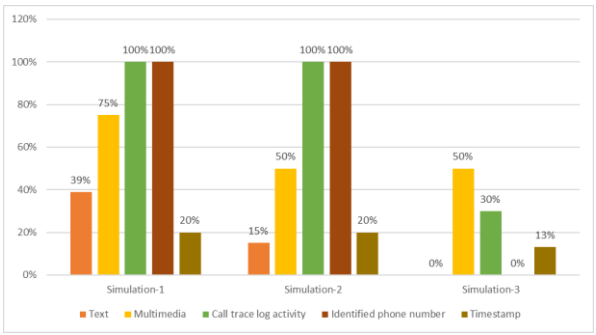


Figure 5. Comparison display in bar chart form against digital evidence findings based on three simulation data

DOI: https://doi.org/10.29207/resti.v6i2.3849

Based on figure 5, it can be explained that there is a percentage of digital evidence findings for each condition. Simulation-1 data in text data content of 39%, 75% of multimedia files, 100% of call trace log activities, 100% of identified phone numbers, and 20% of timestamp data of 100%. Simulation-2 data consists of 15% text data, 50% multimedia files, 100% call trace activity logs, 100% identified phone numbers, and 20% timestamp data. Simulation-3 data is data with 50% payload in multimedia files by 100%, call trace log activity by 100%, and timestamp data by 13%.

4. Conclusion

A case simulation dataset consisting of three different conditions and similarities to the actual conditions was successfully simulated in the data collection stage. Phases of the examination process resulted in the integrity of the duplicated data and declared valid. Data reduction is carried out on data relating to the essential components of the operating system, application features with data obfuscation, and incomplete data. The search for digital evidence has succeeded in obtaining data that can be understood and interpreted based on initial data. Most of the condition is in pieces of data or incomplete data. The results of the analysis succeeded in finding challenges in the search for digital evidence, namely related to the condition of the data findings that were intact, incomplete, incomplete data, and data storage locations. The characteristics of the result of digital evidence are temporary data because they are in RAM, and data recovery cannot be made, even though the location of the storage area has been found. Most of the digital evidence reports were found in all data in the simulation file, except for the text file and the contact's identity in the simulation data-3. The characteristics of live forensics as a method for data acquisition are limited to only the data retrieval process in RAM, so the data obtained is temporary and cannot be recovered from the files found, in this case, in the form of multimedia files. Further research can be combined with chip-off techniques on RAM devices to retrieve data so that the files found can be accessed and presented as factual evidence in digital form and not just temporary data.

Acknowledgment

Thank you to the Department of Informatics, Universitas Muhammadiyah Jember, for providing laboratory facilities to the author and all members of the group of “KDK” with network and data communication who helped and provided convenience so that this research could be completed.

References

[1] M. A. Yaqin, T. A. Cahyanto, and N. Q. Fitriyah, “Metode Live Memory Acquisition untuk Pencarian Artefak Digital Perangkat Memori Laptop Berdasarkan Simulasi Kasus Kejahatan Siber,” vol. 2, no. 2, pp. 87–94, 2021, doi: https://doi.org/10.37148/bios.v2i2.28.

[2] D. S. Yudhistira, I. Riadi, and Y. Prayudi, “Live Forensics Analysis Method For Random Access Memory On Laptop Devices,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. 4, pp. 188–192, 2018, [Online]. Available: https://www.researchgate.net/publication/324994027_Live_Forensics_Analysis_Method_For_Random_Access_Memory_On_Laptop_Devices.

[3] R. Umar, A. Yudhana, and M. Nur Faiz, “Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary,” *Pros. Konf. Nas. Ke- 4 Asos. Progr. Pascasarj. Perguru. Tinggi Muhammadiyah*, pp. 207–211, 2016, [Online]. Available: https://mti.uad.ac.id/download/analisis-kinerja-metode-live-forensics-untuk-investigasi-random-access-memory-pada-sistem-proprietary/.

[4] M. S. Ahmad, I. Riadi, and Y. Prayudi, “Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man in the Middle Attack Berbasis Evil Twin,” *Ilk. J. Ilm.*, vol. 9, no. 1, pp. 1–8, 2017, doi: 10.33096/ilkom.v9i1.103.1-8.

[5] S. Rahman and M. N. A. Khan, “Review of Live Forensic Analysis Techniques,” *Int. J. Hybrid Inf. Technol.*, vol. 8, no. 2, pp. 379–388, 2015, doi: 10.14257/ijhit.2015.8.2.35.

[6] M. N. Faiz, R. Umar, and A. Yudhana, “Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary,” *Ilk. J. Ilm.*, vol. 8, no. 3, pp. 242–247, 2016, doi: 10.33096/ilkom.v8i3.79.242-247.

[7] A. Socała and M. Cohen, “Automatic profile generation for live linux memory analysis,” *DFRWS 2016 EU - Proc. 3rd Annu. DFRWS Eur.*, vol. 16, pp. S11–S24, 2016, doi: 10.1016/j.diin.2016.01.004.

[8] T. D. Larasati and B. C. Hidayanto, “Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10,” no. November, p. 200, 2017, [Online]. Available: https://repository.its.ac.id/42778/1/5213100099-Undergraduate_Theses.pdf.

[9] M. P. Gupta, “Capturing Ephemeral Evidence Using Live Forensics,” *IOSR J. Electron. Commun. Eng.*, pp. 109–113, 2013, [Online]. Available: https://www.iosrjournals.org/iosr-jece/papers/NCNS/109-113.pdf.

[10] A. Yudhana, I. Riadi, and I. Zuhriyanto, “Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS),” *J. TECHNO*, vol. 20, no. 2, pp. 125–130, 2019, doi: 10.30595/techno.v20i2.4594.

[11] R. J. Mcdown, C. Varol, L. Carvajal, and L. Chen, “In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes,” *J. Forensic Sci.*, vol. 61, no. January, pp. 110–116, 2016, doi: 10.1111/1556-4029.12979.

[12] B. Actoriano and I. Riadi, “Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2,” *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 4, pp. 410–419, 2018, doi: 10.17781/P002480.

[13] S. D. Utami, C. Carudin, and A. A. Ridha, “Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik,” *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.

[14] M. Riskiyadi, “Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime,” *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020, doi: https://doi.org/10.14421/csecurity.2020.3.2.2144.

[15] I. Riadi and P. Widiandana, “Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics Research Workshop,” *J. RESTI (Rekayasa Sist. Dan Teknol. Informasi)*, vol. 4, no. 4, pp. 730–735, 2020, doi: https://doi.org/10.29207/resti.v4i4.2161.

[16] M. A. Rizal, “Dataset Hasil Akuisisi.” 2022, [Online]. Available: https://drive.google.com/drive/folders/1IC_l5s_qty1JU2oiOo

DOI: https://doi.org/10.29207/resti.v6i2.3849

TIiyL4WPSZkFh6?usp=sharing.

[17] A. Goeritno, D. Nurmansyah, and Maswan, "Safety instrumented systems to investigate the system of instrumentation and process control on the steam purification system," *Int. J. Saf. Secur. Eng.*, vol. 10, no. 5, pp. 609–616, 2020, doi: 10.18280/ijsse.100504.

[18] A. Goeritno, I. Nugraha, S. Rasiman, and A. Johan, "Injection current into the power transformer as an internal fault phenomena for measuring the differential relay performance," *Instrum. Mes. Metrol.*, vol. 19, no. 6, pp. 443–451, 2020, doi: 10.18280/I2M.190605.

[19] A. Goeritno and F. Hendryan, "Monitoring dan Kendali Tegangan Jaringan Listrik Fase-tiga melalui Smartphone," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 6, no. 1, pp. 32–40, 2022, doi: 10.29207/resti.v6i1.3662.

[20] I. Riadi, S. Sunardi, and M. E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *J. Tek. Elektro*, vol. 10, no. 1, pp. 18–22, 2018, doi: 10.15294/jte.v10i1.14070.

[21] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.

DOI: https://doi.org/10.29207/resti.v6i2.3849