JURNAL RESISTOR | ISSN 2598-7542 | E-ISSN 2598-9650
Vol. 6 No 1 – April 2023 | https://s.id/jurnalresistor
DOI : https://doi.org/10.31598
Publishing : Prahasta Publisher

Digital Forensic Tools And Techniques For Handling Digital Evidence

Khairunnisak Nur Isnaini[1], Wahyu Widodo[2]

[1,2]Informatic, Faculty of Computer Science, Universitas Amikom Purwokerto
Purwokerto, Indonesia

e-mail: nisak@amikompurwokerto.ac.id[1], mr.wahyuwidodo@gmail.com[2]

Received : December, 2022	Accepted : April, 2023	Published : April, 2023

Abstract

The development of information security issues in many sectors makes the skill of mastering digital forensic highly needed. Digital forensic is recently used not only to support legal proceedings but also to investigate many incidents like digital data manipulation, site hacking, and terrorism. In mastering the skill of digital forensic, investigators should have knowledge about the techniques and tools that will be used. This research is proposed to help investigators in enhancing and developing their skills in revealing the content of digital evidence with the result reviews from each area in the forensic field. The review in this study is based on the focus of the forensic area by giving detailed information about the functions, limitations, and advantages as well as the specific techniques of forensics that leads to the techniques of live forensic or static forensic. This research also discusses the non-technical things that affect the performance of forensic investigation including operational activities, investigated activities, and legal elements. Thus, the result of this research is expected to be beneficial for helping investigators in determining the appropriate tools to investigate the digital evidence. The further research can develop the activities of anti-forensics that can hinder the investigation processes.

Keywords: *Digital Forensic Tool (DFT), Forensic Technique, Digital Evidence, Live Forensic, Static Forensic*

Abstrak

Berkembangnya isu keamaman informasi yang merambah ke beragam sektor membuat kebutuhan kemampuan di bidang ilmu digital forensik semakin meningkat. Kini ilmu digital forensik tidak hanya digunakan untuk kebutuhan proses hukum semata. Hal tersebut selaras dengan beberapa insiden yang terjadi seperti halnya manipulasi data digital, peretasan situs, hingga kasus terorisme. Dalam pemenuhan kebutuhan kemampuan digital forensik, seorang investigator perlu memiliki pengetahuan yang cukup terkait teknik dan alat-alat forensik yang akan digunakan. Penelitian ini bertujuan untuk menambah dan mengembangkan pengetahuan seorang investigator dalam mengungkap isi dari barang bukti digital yang di analisis dari masing-masing fokus area forensic. Penelitian ini menghasilkan review penggunaan alat-alat forensik berdasarkan fokus area forensik masing-masing yang merinci fungsi dan batasan-batasan atau kekurangannya serta teknik forensic yang spesifik mengarah pada teknik live forensic maupun static forensic. Penelitian ini juga membahas hal-hal non-teknis yang dapat mempengaruhi kinerja investigasi forensik secara keseluruhan berupa aktivitas operasional, aktivitas investigasi, dan unsur hukum. Diharapkan dapat membantu investigator dalam memilih alat yang tepat dalam melakukan investigasi barang bukti digital yang ditemukan. Penelitian ke depan dapat dikembangkan dari aktivitas-aktivitas anti forensik yang dapat menghambat proses investigasi.

Kata Kunci: *Digital Forensic Tool (DFT), Forensic Technique, Digital Evidence, Live Forensic, Static Forensic*

1. INTRODUCTION

Digital forensic is a sequence of procedures in collecting, analyzing, and making a report in a digital data [1]. Forensic field is used to investigate crime using science that relates to digital evidence [2]. Digital forensic is also used to reveal some facts so that a case can be brought to a court [3].

Forensic digital is currently advancing not only for law enforcement but also for the private sector [4]. The example of a case in the private sector is the investigation of illegal activity in a company (in house) and intrusion investigation (from the characteristics and effect of a network) [5]. Meanwhile, there are a lot of universities in Indonesia that currently begin to open the study program majoring forensic digital from the vocation to magister. The opening of that study program seems like answering the challenges in the digital era and the developing security issue. Universitas Muhammadiyah Malang recently opened the study in vocational education [6] and Universitas Telkom opened it in master degree with the program of Digital Forensic & Cyber Security [7]. It is expected that the graduate can fulfill the needs of experts in Forensic Examiner, Computer Forensic Analyst, etc.

The need of digital forensic is in line with the enhancement of information security issues as seen in the cases of hacking in Indonesia. Based on the report by Direktorat Operasi Keamanan Siber (Directorate of Cybersecurity Operation) [8], the cases of hacking are dominantly found in regional governments with 133 cases. Then, 76 cases are found in the academic sector and 54 cases are found in the private sector. Thus, Digital Forensic Readiness started to be implemented in several companies as a planning for pre-incident forensic investigation [9].

Forensic digital has a large area in its specialization. According to [10] it can be classified based on its digital evidence. It can be physical or logical depending on the result of analysis conducted by the investigator. Several focuses of the digital forensic area are computer forensic, mobile forensic, audio forensic, video forensic, image forensic, and cyber forensic. The enhancement of knowledge and phenomenon affects the enhancement of forensic science as seen on the existence of forensic study that relates to IoT.

Working on handling and revealing cases that have digital evidence needs a special skill to determine appropriate technique. Generally, there are two techniques that can be applied to reveal the content of digital evidence. They are static forensic and live forensic. Static forensic technique is commonly applied to investigate storage media in certain servers [11]. It is used when the computer is off so that the acquisition and analysis of digital evidence can be accomplished without turning on the computer [12]. Besides, live forensic techniques are techniques of collecting, analyzing and providing information in the form of reports from any kind of forensic tools [13]. It can be applied in the running system [14]. The technique targets the volatile data of the computer that is taken when the systems are running [15]. Therefore, the technique can be used according to the conditions, one of which is when analyzing the hacking case.

Digital Forensic Tools (DFT) consists of several hardware and software that can be used to recover and restore the integrity of information from digital evidence [16]. DFT is used to provide protection against illegal access to sensitive information, cybercrime, extortion, and etc. [17]. Collecting information using DFT needs a matrix that includes the parts of the used tools so that it can give accurate results according to the specification and capacity [18].

Previous researchers have discussed the similar topic specifically. One of the researchers [19] has conducted the comparative study of analysis and investigation techniques in forensic digital. The comparison is based on Digital Forensic Tools with the type of Open Source. This comparative study is considered to be able to help the investigators in revealing the running cases. Live forensic technique is specifically used

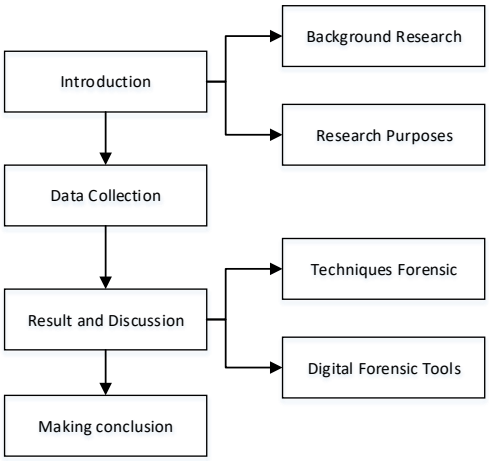
by [20] to identify digital evidence in desktop-based WhatsApp.

Other research by [21] also discusses forensic analysis using Exiftools to analyze hash values and Forevid Video to analyze image results derived from video. Both fall into the static or traditional forensic analysis.

Axiom Magnet and Oxygen Forensic, to analyze the digital evidence taken from Instagram. It reveals that Axiom Magnet is more accurate in measuring and analyzing information from the digital evidence. Furthermore, [22] carried out research about the classification and evaluation of various digital forensic tools. The result shows that the selected tools for comparison material cannot reveal the basic concept of fake image detector so that it needs literature, algorithm, and engineering and concept mapping according to the digital evidence found. In a research [23], forensic tools are used to compare the result of analysis in Twitter. It reveals that Mobile Edit Forensic Express is better than Belk soft Evidence. Research [24] uses MOBILedit Forensic Express as a tool for imaging processes in order to keep the originality of digital evidence in cyber bullying cases in WhatsApp Group. It is proven that the imaging process has been succeed to be exported and formatted in Ms. Excel. The file contains complete information. Network Tools Forensic that is used by [25] are Windump, Network Miner and Wireshark. Windump is used to record the traffic on the device while the other two tools are used to record the traffic on the network.

2. RESEARCH METHOD

This is an exploratory research that is proposed to dig information about the cases that will be investigated because they have not been analyzed by the previous researchers [26]. Besides, according to [27] exploration research does not need hypotheses since its main focus is to collect as much information or data. The research flow can be seen on the following diagram



Picture 1. Research Flow

Based on the picture 1, the data is collected by reviewing a lot of literature to know about the content of scientific journals and articles. It is then regarded as the primer data. According to [28], data collection can be done by making a survey of literature and by studying the written material such as scientific journals and magazines as long as the researcher has mastered the knowledge. Another way to do data collection is by using case study. In this research, exploration is executed by the detailed study about the tools and the techniques in digital forensic. It is divided into several focuses, that is computer forensic, network forensic, network forensic, mobile forensic, and etc. In the result and discussion part, the analysis is focused on the information about the name and function used including the limitation of DFT [29]. Meanwhile, the techniques will be reviewed and classified based on the techniques of live forensic and static forensic. At the end of the step, conclusion is made based on the discussion that has been presented in the previous part.

3. RESULT AND DISCUSSION

3.1 Forensic Techniques

Generally, techniques of static forensic and live forensic can help investigators in revealing information from the digital evidence. Static forensic focuses on the process of obtaining evidence when the system is off, while live forensic focuses on the acquisition process of digital evidence when the system is still running. Here are the comparisons from many literature.

.

Table 1. Literature review of Forensic Techniques

No	Source	Types	Description
1	[30]	Live Forensic	The use of live forensic techniques can disclose more complete information. In image forensic cases, turning off the system can harm and lose the volatile data like the running process, network and installed system. Using live forensic techniques enables us to make some changes in running systems.
		Static forensic/Dead forensic	The use of dead forensic/static forensic is considered to avoid any possibilities in changing the data from the running systems or from the user interaction especially in part of data acquisition. This technique can keep the metadata integrity yet it is still possible to not obtain the data and information completely, especially from volatile data.
2	[11]	Static forensic/dead forensic	Offline acquisition techniques are considered can keep data integrity because online processes can make the data as evidence will be corrupted. In cloud computation, acquiring volatile data needs special techniques so that the content of information can be read clearly.
3	[12]	Static forensic	Static forensic techniques are used because it can reach the deleted data, web and user browsing history and network connection. These techniques need an imaging file as the copy for doing investigation or acquisition without ruining the original version of digital evidence.
4	[15]	Live Forensic	Live forensic techniques can be used to get the volatile digital evidence like malicious code or ransomware that infect the system when it is running. In the examined case, the user of EAS key is able to help the investigator in obtaining the result of acquisition although not all of the ransomware family can apply the similar technique.
5	[20]	Live forensic	Live Forensic techniques are precise to be used to acquire volatile data characteristics. In certain cases, live forensic technique is limited for processing the data obtained from memory.
6	[31]	Live Forensic	Live forensic techniques are assumed to collect the digital evidence using proper techniques and tools. In this case, live forensic technique can not be used to acquire evidence yet it can help the other cases like the computer or system attack. Live forensic techniques are seen as the most challenging techniques because the investigator needs to understand the basic techniques and tools according to the cases.

Based on table 1, information that is obtained from the result of literature review is that live forensic techniques tend to be used to acquire the volatile data more than the static forensic techniques. Secondly, static forensic techniques need the process of imaging files to maintain the quality and the integrity of digital evidence before conducting the identification process. Thirdly, in certain complex cases, live forensic techniques can run maximally if only it is supported by tools, algorithms, or another method. Fourthly, in cyber security, information will be more precisely acquired using live forensic since the identification process is conducted when the system is running.

3.2 Digital Forensic Tools

Table 2 presents the specific review of digital forensic tools based on each focus area. Several tools reviewed are tools that are commonly used by the investigators or researchers. The other tools are rarely used. Besides, tools that is reviewed are selected based on the recently cases happened in Indonesia, like immoral content in the form of image and video in internet [32], case of Jaksa Pinangki and Djoko Candra [33], hacking case of police member data using Sistem Informasi Personel Polri (SIP) [34], hacking case of Whatsapp account via mobile device [35], terorism cases with various forms of evidence [36].

Table 2. Specific Reviews of Several Digital Forensic Tools

No	Source	Types	Tool	Function	Limitation
1	[37]	Computer Forensic	Forensics Acquisition of Websites (FAW)	Obtaining information in the form of HTML code and image	There is no function that provides malware activity and it has not been tested to be used in various browsers and machines.
2	[38]	Computer Forensic	Computer Aided Investigate Environment (CAINE)	Analyzing, inversitating, and making a report using various tools	It is only running in Linux Ubuntu Operating System.
3	[39]	Computer Forensic	SANS Investigative Forensics Toolkit (SIFT)	Enabling to detect various types of incident responses based on open source	It is only running in Linux Ubuntu Operating System.
4	[40]	Memory Forensic	Bulk Extractor	Analyzing the content of image disk, file, directory file and extracting the content of email in the form of .rar and .zip	In the case study, Bulk Extractor cannot restore the compressed object to the original version except in the log file.
5	[41]	Memory Forensic	Digital Evidence & Forensics Toolkit	Providing a group of forensic tools that can be used to analyze the digital evidence focusing on response incidents, cyber intelligence, and forensic scenarios	The feature is still limited. There are no ghiro tools to analyze the digital image, hashcat to hack the password, and rarcrack to access the password of archives data. Moreover, the largest file size is 3,08 GB.
6	[42]	Memory Forensic	Volatility	Analyzing RAM in an operating system from the hash value of evidence that is saved, deleted and encrypted using HashCalc	It is an open-source framework to detect malware and incident response in traditional forensic using other supported tools.
7	[43]	Network Forensic	Wireshark	Detecting the traffic of network in real time when the data network package is obtained.	When the tools are utilized, the user name and password can be seen clearly to detect the running trafic. Besides, it is not efficient to handle the big data volume.
8	[44]	Network Forensic	TCPDump	Analyzing the network package that is based on the command-line so that it is able to provide information about the time, protocol used, source address, host destination and port.	It is not efficient to handle the big-size data package. It is also unable to translate the data in the application layer.
9	[44]	Network Forensic	Xplico	Providing a sniffing tool that is used to detect the traffic of a network and manipulate it to the normal form by the manipulators. It also can be used to extract audio from a data stream.	It takes a lot of time to extract data from the hard disk drive in real time.
10	[44]	Network Forensic	Snort	Providing a sniffing tool that is able to detect network infiltration. It also provides a real-time recorder.	It can not find the host or port name when detecting the network traffic because it focuses on collecting big network packages.
11	[44]	Network Forensic	Network Miner	Providing a tool that is used to detect data network packages by identifying port, mapping,	Providing a tool that is used to detect data network packages by identifying port, mapping, extracting audio from

				extracting audio from VoIP and predicting the detected threat.	VoIP and predicting the detected threat.
12	[44]	Network Forensic	NetIntercept	Providing a tool that is used to monitor and analyze the network encapsulated by hardware. This tool is also used to inspect and analyze at a good speed.	It costs a lot to analyze the package deeply.
13	[45]	Cloud Forensic	FROST	Getting the data from API log, virtual disk, and virtual log in doing forensic investigation. It is also used to save data log in a hash tree and process it in the form of cryptography.	It needs trust from the cloud provider because the provider has to make sure that the user can trust the operating system host, hardware, network and cloud employee.
14	[46], [47]	Cloud Forensic	UFED	Extracting data from social media platforms like facebook, instagram, etc. It also provides the backup file. [46].	Cloud providers might not come from trusted entities and depend on API suppliers to center information. [47].
15	[48], [49]	Email Forensic	MailXaminer	Investigating email from client [48]. It is also used to make a time limit when looking for a certain email.	It has no real-time working in doing investigations. [49]
16	[48], [49]	Email Forensic	Add4Mail	Searching for email using certain keywords, processing email conversion, and processing email data according to the needs. [48]	It can only browse keywords written by the users. [49]
17	[50], [48]	Email Forensic	eMailTrackerPro	Analyzing email header to detect IP address of device that is used by message sender so that it can be tracked [50].	There is no option for importing email, folder, or database. They should be manually imported to detect the email header. [48]
18	[48], [51]	Email Forensic	Paraben Email Examiner	Searching for email file or database folder and providing analysis report that can be selected according to the needs of investigation [48].	It does not provide IP address tracers based on geographic location, cannot display the open port in IP address and is unable to detect email header from the content of the message. [51].
19	[52], [53]	Mobile Forensic	Oxigen Forensic	Extracting tools of formation, contact, call log, sms, mms, email, calendar event, file limitation, etc. It can be well-functioned if the oxygen forensic extractor is connected to the oxygen forensic suite. [52]	This tool is unable to extract information about IMSI (International Mobile Subscriber Identity) and ICCID (Integrated Circuit Card Identifier) from SIM cards. Nevertheless, it is able to identify phone IMEI number, provider name of SIM card, device phone name, and operating system version of the phone [53]. It only works on Windows operating systems [52].
20	[54]	Mobile Forensic	MOBILedit	Identifying information of metadata devices such as serial number, IMEI (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), ICCID	In acquisition steps, it is unable to provide backup data as expected from the extracted data.

				(Integrated Circuit Card Identifier) and root status.	
21	[55]	Mobile Forensic	Dr.Fone	Providing open source applications that can restore all content in storage media. It also has features of restore, transfer, open key, and root.	Delete media features can only be accessed after payment. Besides, in extracting data, the IMEI number can not be tracked.
22	[56]	Mobile Forensic	Belkasoft	Extracting data and encrypted password using Physical Acquisition. In the trial version, all of the tools for forensic activity can be used for one month.	It is a paid tool so that it needs additional access to make a maximal and accurate acquisition. (comp anlysis)
23	[57]	Mobile Forensic	Magnet Axiom	Restoring digital evidence from mobile devices, computers and cloud. The tool can also extract data in detail.	It needs a rooting process in Physical Acquisition so that the significant data can be obtained.

Based on the explanation in table 2, it can be understood that there are various forensic digital tools that are classified into each focus area. It is presented after making a review to know deeper about the functions and the limitations as well as disadvantages. It is expected to be able to help and ease the investigator in determining the tools that are appropriate for handling cases.

Challenges and problems in digital forensic makes an investigator have techniques and tools that can handle the cases with various pieces of evidence. The challenges can be found in the form of volatile data, cryptography data, and any data that should be extracted. They also have to be able to identify the tools of anti-forensic. Data volume, data location and another result of metadata affects the forensic tools that will be used.

The other challenges affecting forensic handling are operational activity, investigation activity, and law material. Three of them are related to each other in handling the cases of forensic in terms of tools and techniques. Even if it is not directly related, it can be a threat that should be handled. In operational activity, the legal response of incident management and procedure of operational standard is important to be noted. For example, in an investigation, an investigator can not give fast and precise response to digital evidence found and is limited to take an action because of the unstandardized operating procedure. Moreover, an investigator should have a skill to carry out forensic steps. They cannot rely only on the tools and the techniques. Joining a training and getting the certificate easily to improve their competence does not mean that the investigator can easily get trust and legality. An investigator needs legal protection regarding the possibility of a privacy invasion and other law cases while handling forensic cases. Not all digital forensic cases are law cases as a form of law enforcement, some of them only need it in the personal or private sector.

4. CONCLUSION

In handling digital forensic, either for legal need or personal need, the company should pay attention to the technical and non-technical things. Technical things like chosen techniques and tools become principles in doing a forensic investigation. Besides, the non-technical things, like operational activity, investigation activity, and material law, can affect the performance of forensic investigations. This is because its relation to another material beyond the investigator and evidence such as the personal skill of the investigator that is certified and legally recognized.

Various forensic tools that are reviewed are expected to help investigators in choosing the appropriate tools to investigate digital evidence found in any forms and types. The further research can develop their analysis on the activities of anti forensic that can hinder the investigation process.

STATEMENT OF APPRECIATION

The researchers deliver thank to LPPM Universitas Amikom Purwokerto for funding the research by the program of Hibah Penelitian Dosen Muda Amikom and for the support from Pusat Studi Jaringan Berbasis Informasi so that the research can be accomplished.

REFERENCES

[1] J. Kävrestad, *Fundamentals of Digital Forensics*, Second Edi. Skovde, Sweden: Springer International Publishing, 2018.

[2] N. Iman, A. Susanto, and R. Inggi, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)," *J. Telekomun. dan Komput.*, vol. 9, no. 3, p. 186, 2020.

[3] R. Synthiana, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," *J. Litigasi*, vol. 21, no. 21, pp. 104–127, 2020.

[4] M. R. B. Kencana, "Minim Jumlah, Indonesia Butuh Banyak Tenaga Ahli Digital Forensik," *Liputan 6*, 2020.

[5] Admin, "Digital Forensik," *Forensic Digital.Com*, 2019. [Online]. Available: https://forensikdigital.com/digital-forensik/. [Accessed: 17-May-2022].

[6] Admin, "UMM Buka Program Studi Keamanan Siber dan Digital Forensik," *Republika*, 2020. [Online]. Available: https://www.umm.ac.id/id/arsip-koran/republika/umm-buka-program-studi-keamanan-siber-dan-digital-forensik.html. [Accessed: 21-May-2022].

[7] Admin, "Tel-U Menjadi Kampus Pertama Dengan Program Studi S2 Digital Forensic & Cyber Security," *Telkom University*, 2021. [Online]. Available: https://telkomuniversity.ac.id/tel-u-menjadi-kampus-pertama-dengan-program-studi-s2-digital-forensic-cyber-security/. [Accessed: 21-May-2022].

[8] Direktorat Operasi Keamanan Siber, "Laporan Bulanan Publik Hasil Monitoring Keamanan Siber Maret 2022," Jakarta, 2022.

[9] Y. P. Asep Sudirman, Bambang Sugiantoro,

"Kerangka Kerja Digital Forensic Readiness Pada Sebuah Organisasi (Studi Kasus : Pt Waditra Reka Cipta Bandung)," *Cyber Secur. dan Forensik Digit.*, vol. 2, no. 2, pp. 82–88, 2019.

[10] M. N. Al-Azhar, *Digital Forensic Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek, 2012.

[11] H. Simaremare, R. T. Putra, and R. Abdillah, "Digital forensic static acquisition analysis for cloud environments," *Int. J. Sci. Technol. Res.*, vol. 8, no. 11, pp. 1712–1716, 2019.

[12] A. Faiz and R. Imam, "Forensic Analysis of Frozen Hard Drive Using Static Forensics Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 1, 2017.

[13] D. Sudyana and N. Lizarti, "Digital Evidence Acquisition System on IAAS Cloud Computing Model using Live Forensic Method," *Sci. J. Informatics*, vol. 6, no. 1, pp. 125–137, 2019.

[14] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 1, no. 3, p. 108, 2017.

[15] S. R. Davies, R. Macfarlane, and W. J. Buchanan, "Evaluation of live forensic techniques in ransomware attack mitigation," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 300979, 2020.

[16] U. D. of H. Security, "System Assessment and Validation for Emergency Responders (SAVER)," United States, 2016.

[17] K. Ghazinour, D. M. Vakharia, K. C. Kannaji, and R. Satyakumar, "A study on digital forensic tools," in *International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017*, 2017, no. September, pp. 3136–3142.

[18] F. Flandrin, W. J. Buchanan, R. Macfarlane, B. Ramsay, and A. Smales, "Evaluating Digital Forensic Tools (DFTs)," in *7th Int Conf Cybercrime Forensics Education and Training (CFET)*, 2014, no. January 2015, pp. 1–16.

[19] N. Pansari and D. A. Agarwal, "A Comparative Study of Analysis and Investigation using Digital Forensics," *Int. J. Linguist. Comput. Appl.*, vol. 07, no. 02, pp. 16–20, 2020.

[20] T. A. Cahyanto, M. A. Rizal, A. E. Wardoyo, and T. T. Warisaji, "Live Forensic to Identify the Digital Evidence on the Desktop-based," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 158, pp. 213–219, 2022.

[21] K. N. Isnaini, H. Ashari, and A. P. Kuncoro, "Analisis Forensik untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode NIST," *J. Resist.*, vol. 3, no. 2, pp. 72–81, 2020.

[22] A. Parveen, Z. H. Khan, and S. N. Ahmad, "Classification and evaluation of digital forensic tools," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 6, pp. 3096–3106, 2020.

[23] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 829–836, 2020.

[24] I. Riadi, Sunardi, and P. Widiandana, "Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics Research Workshop," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 1, no. 3, pp. 730–735, 2017.

[25] F. Yasin, Abdul Fadlil, and Rusydi Umar, "Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 91–98, 2021.

[26] S. G. S. U. Rahardja, *Theory and Aplication of IT Research Metodologi Penelitian Teknologi Informasi*. Yogyakarta: CV ANDI OFFSET, 2011.

[27] Hardani and Dkk, *Buku Metode Penelitian Kualitatif dan Kuantitatif*, 1st ed., no. April. Yogyakarta: CV Pustaka Ilmu, 2020.

[28] Sukardarrumidi, *Metode Penelitian-Petunjuk Praktis Untuk Peneliti Pemula*. Yogyakarta: Gadjah Mada University Press, 2012.

[29] R. F. M. Román, N. M. L. Mora, J. P. N. Vicuña, and J. I. P. Orozco, "Digital forensics tools," *Int. J. Appl. Eng. Res.*, vol. 11, no. 19, pp. 9754–9762, 2016.

[30] M. Kolhe and P. Ahirao, "Live Vs Dead Computer Forensic Image Acquisition," *Int. J. Comput. Sci. Inf. Technol.*, vol. 8, no. 3, pp. 455–457, 2017.

[31] 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.

[32] F. Kurniawan, "Digital Forensik Bisa Kejar Pelaku Penyebar Konten Mesum di Internet," *Sindonews*, 2020. [Online]. Available: https://tekno.sindonews.com/read/224406/207/digital-forensik-bisa-kejar-pelaku-

penyebar-konten-mesum-di-internet-1604830310. [Accessed: 17-May-2022].

[33] L. N. Arunanta, "Ahli Digital Forensic Ungkap Foto Djoko Tjandra dan Pinangki Bertemu di Malaysia," *Detiknews*, 2021. [Online]. Available: https://news.detik.com/berita/d-5361122/ahli-digital-forensic-ungkap-foto-djoko-tjandra-dan-pinangki-bertemu-di-malaysia. [Accessed: 17-May-2022].

[34] A. S. Wardani, "Ini Jenis Data Pribadi Anggota Polri yang Diduga Bocor di Forum Online," *Liputan 6.com*, 2021. [Online]. Available: https://www.liputan6.com/tekno/read/4714141/ini-jenis-data-pribadi-anggota-polri-yang-diduga-bocor-di-forum-online. [Accessed: 17-May-2022].

[35] D. H. A. Putra, "Ahli Digital Forensik: Kasus Ravio, Motif Peretasan Baru di Indonesia," *Kumparan*, 2020. [Online]. Available: https://kumparan.com/kumparannews/ahli-digital-forensik-kasus-ravio-motif-peretasan-baru-di-indonesia-1tK7ifuiRQG/full. [Accessed: 17-May-2022].

[36] N. M. Achmad, "Dalam Persidangan Munarman, Ahli Digital Forensik Ungkap Isi Percakapan soal Perang Biologis, Wabah Corona hingga Baiat," *Kompas.com*, 2022. [Online]. Available: https://megapolitan.kompas.com/read/2022/02/14/15372981/dalam-persidangan-munarman-ahli-digital-forensik-ungkap-isi-percakapan?page=all. [Accessed: 17-May-2022].

[37] N. Aspinwall and L. Ave, "Forensic Acquisition of Websites (FAW) Tool Review," 2014.

[38] B. V Prasanthi, "Cyber Forensic Tools: A Review," *Int. J. Eng. Trends Technol.*, vol. 41, no. 5, pp. 266–271, 2016.

[39] S. Sharma, K. K. Ghanshala, and S. Mohan, "Advanced Digital Forensic IoT Based Secure Communication," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 4, pp. 664–671, 2020.

[40] S. L. Garfinkel, "Digital media triage with bulk data analysis and bulk-extractor," *Comput. Secur.*, vol. 32, no. March, pp. 56–72, 2013.

[41] Y. El Bahlouli and N. Hmina, "Digital Forensics : Development of a Forensics Appliance – Analysis and Recommendations," *Int. J. Emerg. Sci. Eng.*, vol. 6, no. 1, pp. 6–8, 2019.

[42] M. Parekh and S. Jani, "Memory Forensic: Acquisition and Analysis of Memory and Its Tools Comparison," *Int. J. Eng. Technol. Manag. Res.*, vol. 5, no. 2, pp. 90–95, 2020.

[43] S. Qureshi, S. Tunio, F. Akhtar, A. Wajahat, A. Nazir, and F. Ullah, "Network Forensics: A Comprehensive Review of Tools and Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 5, pp. 879–887, 2021.

[44] P. Kaur and N. Misra, "A Methodical Review on Network traffic monitoring and Analysis tools," *JAC A J. Compos. Theory*, vol. 12, no. 9, pp. 1964–1968, 2019.

[45] J. Dykstra and A. T. Sherman, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform," *Proc. Digit. Forensic Res. Conf. DFRWS 2013 USA*, vol. 10, pp. S87–S95, 2013.

[46] M. Patidar and P. Bansal, "Cloud Forensics: An Overall Research Perspective," in *International Journal of Scientific Research in Network Security and Communication*, 2018, vol. 6, no. 2, pp. 5–10.

[47] S. Naaz and F. Ahmad, "Comparitive Study of Cloud Forensics Tools," New York, 2016.

[48] A. Ghafarian, A. Mady, and K. Park, "An Empirical Analysis of Email Forensics Tools," *Int. J. Netw. Secur. Its Appl.*, vol. 12, no. 3, pp. 39–57, 2020.

[49] Mrityunjay, U. Chauhan, and S. Gupta, "Novel Approach for Email Forensics," *Int. J. Eng. Res. Technol.*, vol. 5, no. 10, pp. 1–6, 2017.

[50] M. Tariq Banday, "Techniques and Tools for Forensic Investigation of E-mail," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 6, pp. 227–241, 2011.

[51] T. Hadianto, W. Prasetyo, and R. B. Bahaweres, "Studi Banding Email Forensic Tools," *Stud. Inform. J. Sist. Inf.*, vol. 10, no. 1, pp. 53–61, 2017.

[52] A. Khan, "COMPARATIVE STUDY OF VARIOUS DIGITAL FORENSICS LOGICAL ACQUISITION TOOLS FOR ANDROID SMARTPHONE'S INTERNAL MEMORY: A CASE STUDY OF SAMSUNG GALAXY S5 AND S6," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 1, pp. 357–369, Feb. 2018.

[53] 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, Jan. 2016.

[54] I. Riadi, A. Fadlil, and A. Fauzan, "A Study of Mobile Forensic Tools Evaluation on Android-Based LINE Messenger," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 10, pp. 201–206, 2018.

[55] M. Khyati Gajjar and P. Sharma, “Android based Mobile Forensic and Comparison using various Tools,” *Int. Res. J. Eng. Technol.*, vol. 7, no. 4, pp. 1399–1404, 2020.

[56] H. H. Lwin, W. P. Aung, and K. K. Lin, “Comparative Analysis of Android Mobile Forensics Tools,” in *2020 IEEE Conference on Computer Applications(ICCA)*, 2020, pp. 1–6.

[57] 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.