

# **Forensic Browser on Line Messenger Services for Handling Cyberfraud using National Institute of Standard Technology Method**

Mifthahul Jannah  
Department of Information System  
Universitas Ahmad Dahlan  
Yogyakarta of Indonesia

Imam Riadi  
Department of Information System  
Universitas Ahmad Dahlan  
Yogyakarta of Indonesia

## **ABSTRACT**

Advances in information and communication technology play an important role in everyday life which is useful for interacting with one another. Each other and make it easier for humans to do some work. Line Messenger is an online chat application that sends a text message in real-time, in addition to text messages, other features of the Line messenger application are audio files, videos, and also photos or images using the internet network with the number of users reaching 217 million in 2016. Cyberfraud is a new type of fraud that uses modern cyber information technology, and its essence is still a fraud crime. This study will use a scenario about the Cyberfraud case from a conversation using an instant messenger application, namely Line which runs on the Chrome web browser using the NIST (National Institute of Standards and Technology) stages. This study uses several forensic tools in finding the digital evidence needed including namely FTK Imager, Belkasoft, Browser History Capturer, Browser History Viewer, and Browser History Examination. Digital evidence found in Belkasoft and FTK Imager was 60% with digital evidence of conversation text, Email, and account ID. In Browser History Capturer and Browser History Viewer as much 40% with digital evidence Photos and Links. Furthermore on Browser History Capturer and Browser History Examiner tools as much as 40% with digital evidence in the form of Links and Cached Web.

## **Keywords**

Cyberfraud, Line Messenger, NIST, Forensics, Browser

## **1. INTRODUCTION**

Technological advances Information and communication play a very important role in everyday life that is useful for interacting with each other and making it easier for humans to do some work [1]. Social media can disseminate all forms of information very quickly by sharing content in the form of videos, photos, and accompanied by interesting captions to support an upload on social media [2]. Line Messenger is an online chat application that sends a text message in real-time, in addition to text messages, other features of the Line messenger application are audio files, videos, and also photos or images using the internet network.[3]. Social media itself is very fast in spreading information without a filter before uploading it, therefore social media users must be smarter in using social media, but in fact, there are still many social media users who are easily fooled by accounts that are not clear, such incidents are categorized as Cyberfraud. To find digital evidence, techniques or stages are needed, in this

study, the stages used are NIST (Collection, Examination, Analysis, and Reporting) [4].

## **1.1 Study Literature**

### *1.1.1 Previous Study*

Mulia Fitiana, Khairan AR, and Jiwa Malem Masya (2020) entitled "Application of the National Institute Of Standard and Technology (NIST) method in Digital Forensic Analysis for Handling Cybercrime". In this study using the WhatsApp application on an android cellphone with pornography cases, the tools used to find evidence are KingRoot to root the smartphone, CWM (ClockworkMod) Recovery, FTK Imager to perform data imaging, WhatsApp viewer to describe the WhatsApp database that has been described. , and DB Browser for SQLite to open the wa.db folder to view the contact list on the smartphone. The evidence found as a result of the research is in the form of chats that have been deleted by the perpetrator and the contacts found on the perpetrator's smartphone [5].

Rauhulloh Ayatulloh Khomeini Noor Bintang, Rusydi Umar, and Anton Yudhana (2020) entitled "Analysis of Facebook Lite Social Media with Forensic Tools Using the NIST Method". The case contained in the research is posting hate speech on social media facebook lite, the tool used in conducting investigations, namely MOBILedit forensic pro to extract data from smartphones, to find the perpetrator's account by cloning the data so that it is a string value or original data. The evidence that was found in the study were 297 images with different sizes, filenames, widths, and 19 videos with different types of filename, path, size, modified [6].

Gregorius Hendita Artha Kusuma and Yusuf Fadhilah (2019) with the research title "E-Commerce Digital Forensic Analysis on Car Rental Websites Using the NIST Method". Cases that identify cybercrimes who use e-commerce websites by offering unreasonable prices on car rental services. The online tools used in the research are whoisdomainid.tools, ScamAdviser and statshow to view the address of the perpetrator via google map. Based on the results of website research on rental services that were examined after checking through the Scam Adviser tools, the eligibility to visit the website was only 58% and there was no online reputation, other evidence found in the IP research location was in the US but having an address in Yogyakarta [7].

Muhammad Abdul Aziz, Imam Riadi and Rusyi Umar (2018) with the research title "Forensic Analysis of Web-based Line Messenger Using the National Institute Of Justice (NIJ) Framework". The results of this research were obtained using the FTK Imager and SQLite tools by exploring the laptop

directory used as research to find the Line Messenger database in the Google Chrome browser which contained files and folders such as caches and logs [8].

Muhammad Irwan Syahib, Imam Riadi, and Rusydi Umar (2018) entitled "Digital Forensic Analysis of Beetalk Applications for Cybercrime Handling Using the NIST Method". The case in this study is Cybercrime, a forensic tool used by MOBILedit, OXIGEN Forensics, and Kingroot. The evidence found in this research is evidence of conversations between accounts A and account B, and photo caches [9].

### 1.1.2 Digital Forensics

Forensics is a science related to cyber law (cyberlaw), security or security on systems, and computer networks [10]. Digital forensics can be interpreted as a part of forensic science that covers the discovery and investigation of material (data) found on digital devices [11]. Digital Forensics basically can find digital evidence that is usually stored on temporary computer/mobile storage, permanent storage, USB, CD, network traffic, and others [12]. Digital Forensics is the application of science and computer technology for justice, which in this case is proving high-tech crimes or computers scientifically to be able to obtain digital evidence that can be used against violators [13].

### 1.1.3 Web Browser

Web Browser is a tool to perform various activities on the Internet by users. Users utilize browsers for various functions such as information retrieval, access to email accounts, e-commerce, banking creation, instant messaging, online blogs, access to social networks. Web browsers log a lot of data related to user activity. Information such as URLs visited by users, search terms, cookies, cache files, access times, and usage times are stored in memory on the system [14]. Web Browsers are diverse, with each having its characteristics. This allows users to choose their favorites or try different Web browsers at the same time. In this situation, it is difficult to trace the Web sites the user has visited if the forensic investigator can only analyze the log files of a particular Web browser [15].

### 1.1.4 Digital Evidence

Evidence is data information contained in an electronic device that will later be acquired to obtain digital evidence, examples of physical devices can be laptops, smartphones, and so on. The information obtained from the acquisition is what is called evidence [16]. Digital evidence can be found in the physical evidence is electronic which can be identified concretely so that the physical evidence can be acquired [17].

### 1.1.5 Line Messenger

Line Messenger is an instant messenger application by sharing interesting features, namely text conversation features, video calls, voice notes, and being able to send an image using the internet network in real-time [18]. Line Messenger users reach 217 million worldwide according to static data from the business of APPS website, the many users of Line messenger do not deny that internet crimes will occur, such as fraudulent buying and selling of goods online, means of buying and selling drugs or even frequent cyberbullying. occurs in adolescents who make mental down and are not confident [19].

### 1.1.6 Cybercrime

Cybercrime is anything that uses the internet network that aims to commit criminal acts using very sophisticated technology with the motive of abusing technology to reap the

benefits of losses obtained from other people [20]. Crimes on social media or cybercrime are very different from crimes that occur in person, the effect of cybercrime is very significant on victims [21]. Detailed cybercrimes (which victims think are genuine) are a major problem. Despite the existence of a body of relevant laws passed down by harmonization around the world and bargaining appointments with the police, the attributes of cybercrimes are severe enough to be announced, plots to hinder the customary investigation process [22].

### 1.1.7 Cyberfraud

Cyberfraud (also referred to as cyber-scams) is any type of fraud that exploits mass communication technologies (eg email, Instant Messenger, social networking sites) to trick people into spending money [23]. User of telecommunications and network technology is involved in the process of cyber fraud. Exploring the concept of Cyberfraud should also explain the concepts of telecommunication fraud and network fraud [24].

### 1.1.8 National Institute of Standard Technology

National Institute of Standard and Technology (NIST) provides a standardized method that can be used to solve problems and analyze digital evidence or the steps to obtain information from digital evidence [25]. National Institute of Standard and Technology (NIST) to obtain evidence related to electronics and digital, it has 4 stages as shown in Figure 1.



Figure 1. Stages of NIST

1. Collection  
Collection stage is the initial stage that used to identify and acquire physical evidence in the form of electronic and digital media related to criminal acts.
2. Examination  
This stage is a step to extract data that has been generated from the collection process, the resulting data will be extracted automatically by forensic applications or can be done manually.
3. Analysis  
Analysis is a step taken to identify the extracted data, the analysis is carried out by the applicable rules without violating the rules.
4. Reporting  
The process reporting is a step to report the results of the steps that have been done previously, the documented report should be written in its entirety and detail.

## 2. METHODOLOGY

### 2.1 Research Scenario

scenarios are needed to support this research, the scenario discusses how the stages that occur in browser forensics take place.

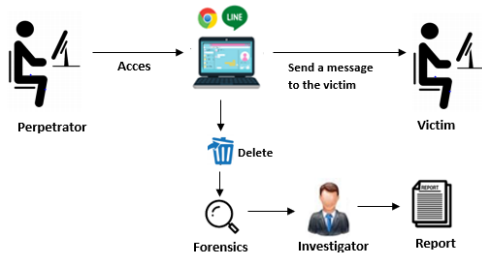


Figure 2. Research Scenario

Figure 2 Perpetrator using a laptop that has installed the chrome web browser and the Line Messenger extension on the chrome browser. Perpetrator send messages that trigger actions Cyberfraud. The victim asked the police for help by bringing a screenshot of the conversation between the victim and the perpetrator, the police formed a special team to resolve the case and arrest the perpetrator. When the police arrested the perpetrator, the police secured evidence at the crime scene, namely a laptop that was still faulty which was accessing Line Messenger on the chrome web browser where the perpetrator had deleted the chat history between the perpetrator and the victim.

## 2.2 Research Stages

This research uses stages based on the stages of the National Of Standards and Technology (NIST) which are carried out by live forensics. NIST has 4 stages, namely, Collection, Examination, Analysis, and Reporting.

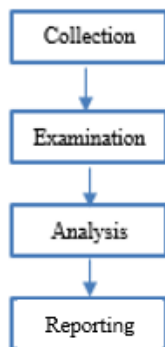


Figure 3. Stages of Implementation

Figure 3 is the investigator's stage in finding digital evidence. The following is an explanation of the implementation stages:

### 2.2.1 Collection

The collection stage is the stage of searching for data and information by investigators, as well as collecting evidence obtained at the crime scene (TKP). In this research, the evidence used is a laptop that is used by the Perpetrator to commit internet crimes. Information on physical evidence found in the research case scenario can be seen in table 1.

Table 1. Physical Evidence

No	Evidence	Figure	Description
1	Laptop of perpetrator		Laptop used by the perpetrator is branded Lenovo B41-35, the laptop was found in a crime scene and connected to Internet.
2	Charger Laptop of perpetrator or		Charger used 100-240V input and 20V output.

Table 1 is the documentation of physical evidence used by the perpetrator in committing a crime found at the location of the case.

### 2.2.2 Examination

Examination stage is the main stage in conducting an investigation, at this stage data acquisition will be carried out on physical evidence in the form of a laptop to obtain data and information on the perpetrator's crime.

#### 2.2.2.1 Belkasoft RAM Capturer

Belkasoft Live RAM Capturer is a forensic tool used to perform data acquisition on RAM on electronic evidence belonging to the perpetrator namely a laptop.

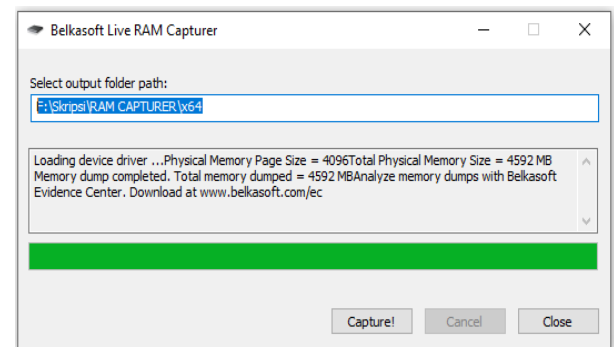


Figure 4. Process Acquisition of Belkasoft Live RAM Capturer

Based on Figure 4, the results obtained from the Belkasoft Live RAM Capturer tool are in the form of files with .mem extensions.

#### 2.2.2.2 FTK Imager

FTK imager is used to perform imaging on files that have been obtained from the acquisition of RAM.

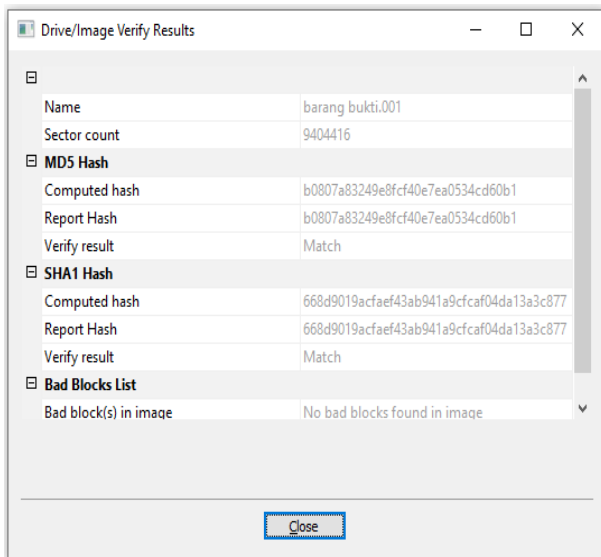


Figure 5. Hashing Results

Figure 5 shows the hashing results between MD5 and SHA1 files. The hash value from the two files matches which means that there is no change in the data.

### 2.2.2.3 Browser History Capturer

Browser History Capturer is used to acquire data on web browsers used by Perpetrator to commit internet crimes. Data obtained from browser acquisition can be in the form of web browsing history, cache, and archived history.

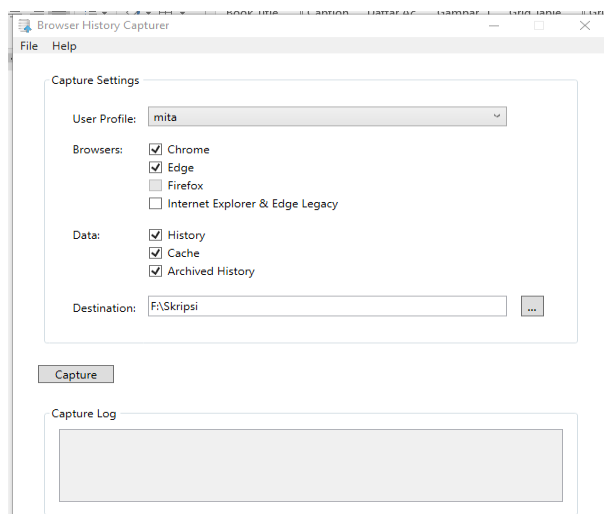


Figure 6. Process Acquisition of Browser History Capturer

Figure 6 shows that these tools can only be used on Chrome, Edge, Firefox, and Internet Explorer & Edge legacy web browsers, so they are not suitable for use by Macbook users who usually use the Safari web browser.

### 2.2.3 Analysis

Analysis is the stage of investigators to analyze data and information that has been obtained previously in order to obtain the required digital evidence. The results at this analysis stage will later be entered into the reporting table to see the differences in the results of several tools used in this research.

### 2.2.3.1 FTK Imager

Data obtained from the capture using the Belkasoft live RAM capturer with the .mem format which can be seen in Figure 7.

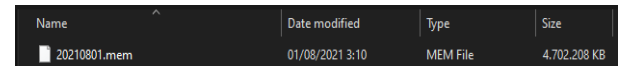


Figure 7. Belkasoft Live RAM Capturer Result

The acquired file in Figure 7 will then be analyzed using the FTK imager in collecting data and information. will be used as digital evidence. to make it easier for investigators to search for investigator data using keywords or parameters to be searched.

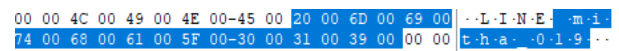


Figure 8. Id Line of Perpetrator

Based on Figure 8, investigators managed to find the ID of the perpetrator was "mitha\_019" which was used to deceive the victim according to the screenshot evidence provided by the victim to report the crime that had been committed by the perpetrator. The perpetrator's id is important information that will be used as digital evidence

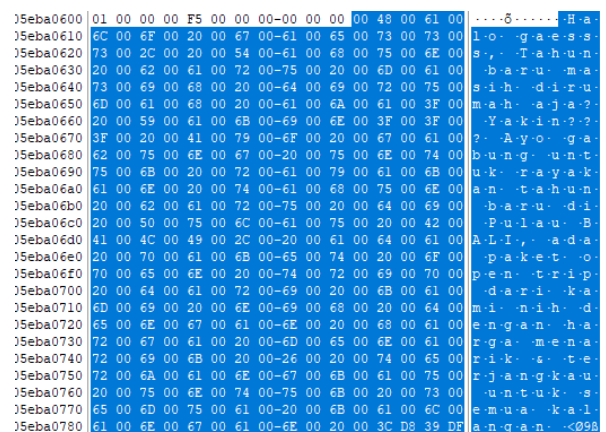


Figure 9. Evidence of Conversation 1

Figure 9 shows evidence of the first conversation that took place between the perpetrator and the victim which contained an offer of vacation tickets with, the sentence is similar to the screenshot given by the victim.

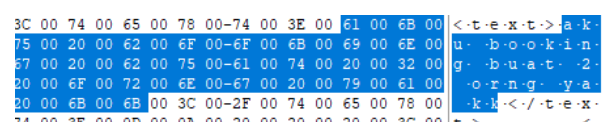


Figure 10. Evidence of Conversation 2

Figure 10 is a reply to a message from the victim to the perpetrator that the victim booked a ticket with a total of 2 people.

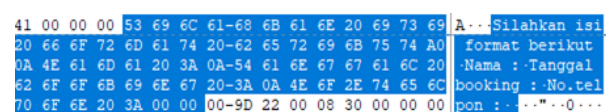


Figure 11. Evidence of Conversation 3



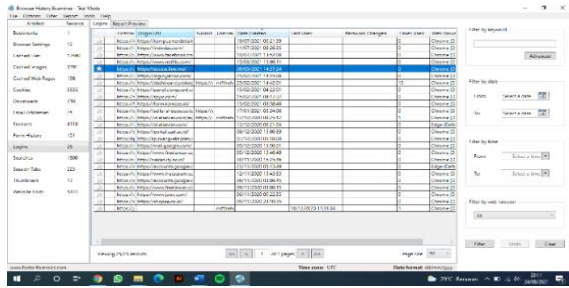


Figure19. History Login

Figure 19 is a history of logins that have been carried out by the perpetrator, the blue bar is digital evidence that the perpetrator has logged in to a LINE account via the chrome web browser.

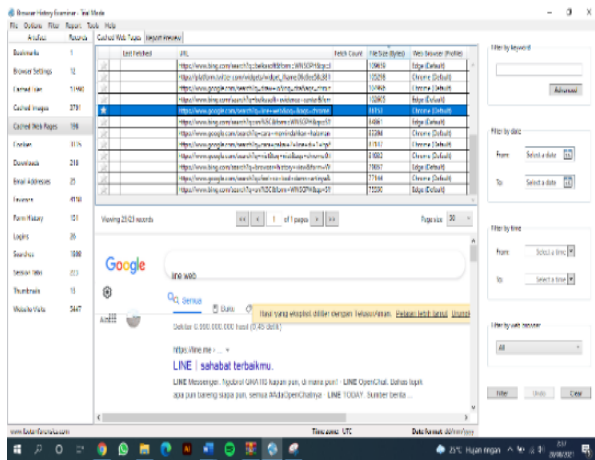


Figure20. Caches Web Pages

Figure 20 are the findings of cached web pages that have been visited by the perpetrator, based on the image above, the perpetrator has searched Line Messenger through the chrome browser with a file size of 86153 bytes.

## 2.2.4 Reporting


Reporting is the last stage of the National Institute of Standards and Technology (NIST) stage. At this stage, the investigator will make a report from the results obtained during an investigation of the evidence found at the crime scene (TKP), namely physical evidence in the form of a laptop where the perpetrator uses a chrome web browser to carry out internet crimes according to the scenario described. already made. At the reporting stage, it is a report of the results of the tools that have been used to find data and information about crimes committed by the Perpetrator. The following are the specifications of the evidence that can be seen in Table 2.

Table 2. Specifications of Physical Evidence

NO	Nama	Keterangan
1.	Processor	AMD A6-7310 APU @ 2,2 Ghz
2.	Graphics	AMD Radeon™ R4 Graphics
3.	Memory	4 Gb DDR3
4.	Hardisk	500 GB SATA
5.	Monitor	14 Inch
6.	OS	Windows 10 Pro

The results of the data found from the acquisition of RAM in carrying out the stages of browser forensics on chrome were carried out by the live forensic method. The results of the data found to be used as digital evidence can be in the form of interaction information between the victim and the perpetrator such as the message content, the perpetrator's account id, and the account password of the perpetrator, that can be seen in Table 3.

Table 3. Data Results Found

Information	Source	Content
Email	Perpetrator	mifthahuljannah36@gmail.com
Id Akun	Perpetrator	mitha_019
Text	Perpetrator	Hallo gaess, Tahun baru masih dirumah aja? Yakin??? Ayo gabung untuk rayakan tahun baru di Pulau BALI, ada trip dari kami nih dengan harga menarik & terjangkau untuk kalangan booking seat' mu segera karena kouta terbatas gaess
Text	Victim	Aku booking buat 2 orgn ya kk
Text	Perpetrator	Silahkan isi format berikut Nama: Tanggal booking: No.Telpon:
Text	Victim	Silahkan isi format berikut Nama: Nadila Tanggal booking: 4 agustus 2021 NO.Telpon: 085764808269
Text	Perpetrator	ok. Sertakan bukti transfer ya kan
Text	Perpetrator	baik kak. tiket dikirim pada tanggal 2 agustus ya
Text	Perpetrator	Ini udah tanggal 05 kk kok belum dikirim tiketnya kan saya booking tanggal 04
Picture	Perpetrator	

Based on Table 3, the evidence found from this research is the perpetrator's account ID, email, the text of the conversation between the perpetrator and the victim, and photos sent by the victim.

## 2.2.5 Result

Results found in this study in the form of image uploads that were sent by the perpetrator were found in the Browser History Capturer and Browser History Viewer tools, while the text of the conversation between the perpetrator and the victim was found using the Belkasoft and FTK Imager tools, where Belkasoft was used to acquire RAM. on the laptop and the FTK Imager is used to read the results of the RAM acquisition that has been obtained. In the Browser History

Capturer and Browser History Examiner tools, researchers only find evidence according to the scenario in the form of a web page browsing history link and account login.

**Table 4. Comparison of Results obtained from Several Tools**

No	Information Data	SoftwareForensic		
		Belkasoft & FTK Imager	Browser History Capturer & viewer	Browser History Capturer & examiner
1.	Link	✓	✓	✓
2.	Photos	-	✓	-
3.	Conversation Text	✓	-	-
4.	Account Id	✓	-	-
5.	Cached Web Pages	-	-	✓

Based on the results of Table 4, the evidence found using several tools forensic. Uploaded images that have been sent by the perpetrator have been found in the tools Browser History Capturer and Browser History Viewer, while the text of the conversation between the perpetrator and the victim has been found using the tools Belkasoft and FTK Imager, where Belkasoft is used to acquire RAM on the laptop and FTK Imager is used to read the results of the acquisition of RAM that has been obtained. In the tools, the Browser History Capturer and Browser History Examiner researcher only finds evidence according to the scenario in the form of a web page browsing history link and account login.

### 3. CONCLUSION

Digital forensic evidence for handling Cyberfraud using the chrome web browser is obtained by acquiring live forensic RAM on the perpetrator's laptop, digital evidence obtained in this study is in the form of text, cache, history or history of web pages that have been visited by the perpetrator while using the goods. physical evidence in the form of a laptop belonging to the perpetrator. Web browser usage activities recorded on the RAM of a laptop are volatile or temporary, where data will be lost if the device is not connected to power or turns off, so in this research forensics is carried out live to find data on the perpetrator's laptop to be used as evidence of a case. electronic crimes that often occur today. The results of the evidence carried out with the NIST stage assisted by several tools forensic were found in this study where the results from Belkasoft and FTK Imager were 60% with digital evidence of conversation text, Email, and account ID, Browser History Capturer and Browser History Viewer as many as 60%. 40% with Photo and Link digital evidence. Furthermore, the Browser History Capturer and Browser History Examiner tools are also 40% with digital evidence in the form of links and Cached Web Pages.

### 4. REFERENCES

- [1] D. A. González-Padilla and L. Tortolero-Blanco, "Social media influence in the COVID-19 pandemic," *Int. Braz J Urol*, vol. 46, no. Suppl 1, pp. 120–124, 2020, doi: 10.1590/S1677-5538.IBJU.2020.S121.
- [2] 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.
- [3] A. Fauzan, I. Riadi, and A. Fadlil, "Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 159–163, 2017, [Online]. Available: <http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752>.
- [4] D. T. Yuwono, A. Fadlil, and S. Sunardi, "Performance Comparison of Forensic Software for Carving Files using NIST Method," *J. Teknol. dan Sist. Komput.*, vol. 7, no. 3, pp. 89–92, 2019, doi: 10.14710/jtsiskom.7.3.2019.89-92.
- [5] M. Fitriana, K. A. AR, and J. M. Marsya, "Penerapana Metode National Institute of Standards and Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, p. 29, 2020, doi: 10.22373/cj.v4i1.7241.
- [6] R. A. Bintang, R. Umar, and A. Yudhana, "Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST," *Techno (Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.
- [7] G. H. A. Kusuma and Y. Fadhilah, "Analisis Forensik Digital E-Commerce pada Website Rental Mobil Menggunakan Metode NIST," *Pros. Semin. Nas. SISFOTEK*, vol. 3, no. 1, pp. 228–234, 2019.
- [8] M. A. Aziz, I. Riadi, and R. Umar, "Alanisis Forensik Line Messenger Berbasis WEB Menggunakan Framework National Institute of Justice (NIJ)," *Semin. Nas. Inform. 2018 (semnasIF 2018)*, vol. 2018, no. November, pp. 51–57, 2018.
- [9] M. I. Syahib, I. Riadi, and R. Umar, "Analisis Forensik Digital Aplikasi Beetalk untuk Penanganan Cybercrime Menggunakan Metode NIST," *Semin. Nas. Inform.*, vol. 2018, no. November, p. 134, 2018, [Online]. Available: <http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2629>.
- [10] F. Daryabar, M. H. Tadayon, A. Parsi, and H. Sadjadi, "Automated analysis method for forensic investigation of cloud applications on Android," *2016 8th Int. Symp. Telecommun. IST 2016*, pp. 145–150, 2017, doi: 10.1109/ISTEL.2016.7881799.
- [11] D. Hariyadi, H. Wijayanto, and I. D. Sari, "Analisis Barang Bukti Digital Aplikasi Paziim Pada Ponsel Cerdas Android Dengan Pendekatan Logical Acquisition," *Cybersecurity dan Forensik Digit.*, vol. 2, no. 2, pp. 1–5, 2019.
- [12] R. Umar and Sahiruddin, "Metode Nist Untuk Analisis Forensik Bukti Digital Pada Perangkat Android," *Pros. SENDU\_U\_2019*, pp. 978–979, 2019.
- [13] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "1490-Article Text-2859-1-10-20190413," *Akuisisi Bukti Digit. Pada Instagram Messenger Berbas. Android Menggunakan Metod. Natl. Inst. Justice*, vol. 4, pp. 219–227, 2018.
- [14] E. Akbal, F. Güneş, and A. Akbal, "Digital Forensic Analyses of Web Browser Records," *J. Softw.*, vol. 11,

- no. 7, pp. 631–637, 2016, doi: 10.17706/jsw.11.7.631-637.
- [15] R. Saputra and I. Riadi, “Forensic Browser of Twitter based on Web Services,” *Int. J. Comput. Appl.*, vol. 175, no. 29, pp. 34–39, 2020, doi: 10.5120/ijca2020920832.
- [16] P. W. Setyaningsih, Y. Prayudi, and B. Sugiantoro, “Manajemen Bukti Digital Hasil Akuisisi Dfxml,” *J. Tek. Inform.*, vol. 11, no. 1, pp. 47–54, 2018, doi: 10.15408/jti.v11i1.6680.
- [17] A. N. Ichsan and I. Riadi, “Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method,” *Int. J. Comput. Appl.*, vol. 174, no. 18, pp. 34–40, 2021, doi: 10.5120/ijca2021921076.
- [18] M. Alghizzawi, “The role of digital marketing in consumer behavior: A survey Want more papers like this? The role of digital marketing in consumer behavior: A survey,” *Int. J. Inf. Technol. Lang. Stud.*, vol. 3, no. 1, pp. 24–31, 2019, [Online]. Available: <http://journals.sfu.ca/ijitls>.
- [19] M. R. Setyawan, A. Yudhana, and A. Fadlil, “Identifikasi Bukti Digital Skype Di Smartphone Android Dengan Metode National Institute Of Justice ( NIJ ),” *Semnastek*, pp. 565–570, 2019.
- [20] F. Iqbal, B. C. M. Fung, M. Debbabi, R. Batool, and A. Marrington, “Wordnet-Based Criminal Networks Mining for Cybercrime Investigation,” *IEEE Access*, vol. 7, pp. 22740–22755, 2019, doi: 10.1109/ACCESS.2019.2891694.
- [21] W. Naro, A. Syatar, M. M. Amiruddin, I. Haq, A. Abubakar, and C. Risal, “Shariah assessment toward the prosecution of cybercrime in indonesia,” *Int. J. Criminol. Sociol.*, vol. 9, no. 1, pp. 572–586, 2020, doi: 10.6000/1929-4409.2020.09.56.
- [22] P. Mali, J. S. Sodhi, T. Singh, and S. Bansal, “Analysing the awareness of cyber crime and designing a relevant framework with respect to cyber warfare: An empirical study,” *Int. J. Mech. Eng. Technol.*, vol. 9, no. 2, pp. 110–124, 2018.
- [23] M. T. Whitty, “Predicting susceptibility to cyber-fraud victimhood,” *J. Financ. Crime*, vol. 26, no. 1, pp. 277–292, 2019, doi: 10.1108/JFC-10-2017-0095.
- [24] Z. Li, H. Zhang, M. Masum, H. Shahriar, and H. Haddad, “Cyber fraud prediction with supervised machine learning techniques,” *ACMSE 2020 - Proc. 2020 ACM Southeast Conf.*, pp. 176–180, 2020, doi: 10.1145/3374135.3385296.
- [25] T. Pandela and I. Riadi, “Browser Forensics on Web-based Tiktok Applications,” *Int. J. Comput. Appl.*, vol. 175, no. 34, pp. 47–52, 2020, doi: 10.5120/ijca2020920897.