Facebook Browser Investigation on Chrome using National Institute of Standards and Technology Method

Pangestu Windu Bahari
Department of Information System
UniversitasAhmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
Facebook is a social network or social media that allows users to add personal information with photos, contacts or information. The important role of the development of the internet for cybercrime or cybercrime, has led to the emergence of new types of crime, such as advertisements for buying and selling organs on Facebook services. The subject of this research is digital forensics on Facebook social media that runs on the Chrome browser to uncover criminal cases of buying and selling human organs online with digital evidence. The research was conducted using standards released by the National Institute of Standard Technology (NIST). When conducting research, scenarios are made in advance to run a simulation of the collection of evidence. The results obtained from this study are posts that have been deleted and the user account used to login to the Facebook service on the Chrome browser. For data acquisition using forensic tools FTK Imager, Belkasoft RAM Capture, and Browser History Capture, while for analysis using Browser History Examiner, Browser History Viewer, and also FTK. Details of digital evidence obtained from forensic tools are FTK Imager 60%, Belkasoft RAM Capture 60%, Browser History Capture 60%, Browser History Examiner 60% and Browser History Viewer 60%. The results obtained from this research are posts that have been deleted and the user account used to login to the Facebook service on the Chrome browser.

Keywords
Digital Forensic, Facebook, Cybercrime, Advertising buying and selling human organs, NIST, Web browser

1. INTRODUCTION
Technology has become a daily necessity for everyone, one of which is communication, communication can not only be done face-to-face, but also through technical intermediaries . Facebook is a social network or social media that allows users to add personal information with photos, contacts or information. Users can join the community to connect and interact with other users [2]. Computer technology and the internet that continue to develop can play an important role in the development of cybercrime or cybercrime, the internet causes the emergence of new types of crime, such as advertisements for buying and selling organs on Facebook services, with the increasing variety of human trafficking crimes, for example, advertisers promoting human organs for being sold through social media or websites is a cause for concern[3]. The existence of advertisements uploaded on social media has attracted some people to sell or buy because they are tempted by the price and will certainly increase the current crime rate. This study uses the NIST stage to obtain evidence and tools FTK Imager, Belkasoft RAM capture, Browser History Capture, Browser History Examiner, browser History Viewer [4]. With the increasing diversification of human trafficking crimes, for example, advertisers promoting human organs for sale via social media or websites are worth watching out for. The existence of websites and advertisements uploaded on social media has attracted some people to sell or buy because they are tempted by the price and will certainly increase the current crime rate. Living in this modern era, we can meet various online advertising needs every day, there should be regulations regarding advertising, but currently there are no regulations regarding online advertising [5].

1.1 Research Literature

1.1.1 Previous Research
The first previous research entitled “Comparative Design of Live Forensics on Instagram, Facebook and Twitter Social Media Security on Windows 10. This research uses the US National Institute of Justice (NIJ) method which is run with software (FTK Imager tools) as supporting material to determine the security of each social media (Facebook, Twitter, and Instagram). This study concludes that the live forensic method is very dependent on the condition of the computer being turned on because it requires data contained in RAM [6].

The second previous research entitled Investigation of Digital Forensics Design on Twitter Applications Using Live Forensics Methods. This research begins with creating a Twitter social media account, the tools used by FTK Imager as a manager for the data to be analyzed on social media accounts, when creating a Twitter social media account is done by cloning data and data Hashing its function is to ensure that Twitter social media accounts be a value representing the original string or the original account. That the social media accounts will be analyzed to obtain data that can be valid forensic data evidence [7].

The third previous research entitled "Analysis of Live Forensics for Comparison of Instant Messenger Applications on the Windows 10 Operating System. This research compares the security level of activity using instant messaging applications on the Windows 10 operating system. The messengers compared in this study are Line, Telegram and Facebook. Using the live forensic method, data collection and acquisition is carried out while the system is still running, then run the analysis [8].

The fourth previous research entitled"Digital Forensic Analysis of E-Commerce on Rental Websites Cars Using the NIST Method". In this research the tools that will be used to analyze data related to indications of fraud by scanning for website security identification are who is domains scam

adviser tools. [9].

The last previous research entitled "Analysis and Comparison of Applied Forensic Evidence" the Social Media Facebook and Twitter on Android Smartphones. This study uses the simulation method, the simulation method consists of several stages such as Problem Simulation, Conceptual Model the tools used in this research are Wonder share Dr. Phones for Android. Used to restore previously deleted data to eliminate forensic evidence. Get the conclusion that the data on social media Facebook and Twitter are not fully stored on the server. [10].

1.1.2 Digital Forensics

Forensic is the science of using scientific techniques or methods to provide correct evidence in a court or related legal examination [11]. Forensics is an activity to investigate and establish the truth or facts of a criminal event and other legal cases. In the field of technology, forensic analysis of digital or electronic evidence is called digital forensics or computer forensics [12].

1.1.3 Web Browser

Web browser is a software application for retrieving, presenting, and traversing information resources on the internet or the worldwide web (WWW) [13]. Information resources are identified by a Uniform Resource Identifier (URL) and can be web pages, images, videos, or other pieces of content [14].

1.1.4 Digital Evidence

Digital evidence is any information stored or transmitted in digital form that can be used for examination in court as evidence [15]. Digital evidence is very important to prove computer crime cases involving storage media devices [16].

1.1.5 Social Media

Social media is a tool or forum for conveying information where the process of communicating this information can be done more easily, quickly and personally. Great for business people, but creates a gap for cybercrime [17].

1.1.6 Facebook

Facebook is a social media that allows users to upload and view various things, such as images, text, and videos [18]. Facebook message links make it easy for users to get information. Facebook can be accessed through several platforms such as iOS, Android, and with a website interface on a computer browser [19]. This research focuses on links and posts and advertisements on Facebook that run on a computer browser platform [20].

1.1.7 Cybercrime

Cybercrime is a crime committed by a person or group of people by involving a computer or the internet [21]. The rapid development in the use of internet services ultimately invites the occurrence of crime, which is better known as Cybercrime [22]. There are various categories to explore what is meant by cybercrime, one of which is to divide it into two large groups, namely: Violent/potentially violent, and Non-Violent. Violent/Potentially violent is computer abuse that has a physical impact on other people [23].

1.1.8 National Institute of Standard Technology

National Institute of Standards and Technology (NIST) is one of the standards that can be used to perform digital forensic analysis [24].

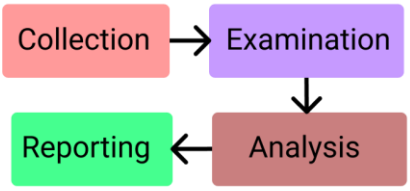


Figure 1.Stages of National Institute of Standard and Technology Method

Figure 1shows Stages of digital forensics National Institute of Standards Technology (NIST) includes:

a. Collection
   At this stage, identification, labeling, recording, and retrieval of data from relevant data sources are carried out by following procedures to maintain data integrity.
b. Examination
   The Next stage is processing the data that has been collected forensically using a combination of various scenarios, both automatic and manual, then assessing and releasing the data as needed while maintaining data integrity.
c. Analysis
   The next stage is to analyze the results of the examination by using methods that are technically and legally valid to obtain useful information in order to answer the questions that are the reason for the collection and examination.
d. Reporting
   Last reporting stage is the reporting stage, which is reporting the results of the analysis which includes a description of the actions taken, an explanation of the selected tools and procedures, determining other actions that need to be taken, then providing recommendations for improvements to policies, procedures, tools, and other aspects of the forensic process [25].

2. METHODOLOGY

2.1 Research Scenario

Case scenario is in the form of an advertisement for buying and selling human organs on social media Facebook, the advertisement in question can be in the form of a post.

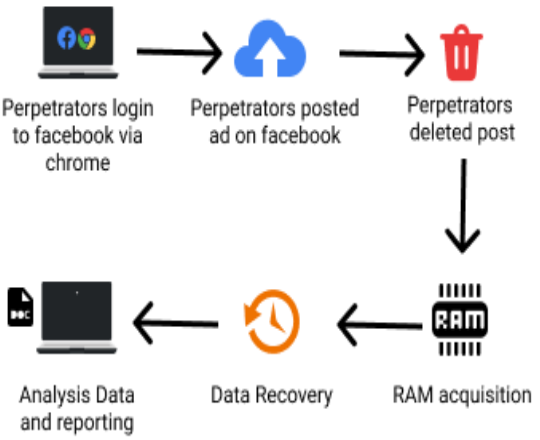


Figure 2. Test simulations performed in research

Figure 2 explains how the perpetrators post content of advertisements for buying and selling human organs on Facebook through the Chrome browser and delete them. Then an investigation is carried out in the condition of the device being turned on by acquiring ram using the Belkasoft Ram Capture forensic tools or utilizing the Capture memory feature from the FTK imager. The software is used to capture all activities that are running on the perpetrator's laptop ram.

2.2 Research Stages

Stages uses digital forensic standards released by the National Institute of Standard Technology (NIST) to find evidence that leads to advertisements for buying and selling human organs.

2.2.1 Collection

The stage collection is the beginning of a series of processes digital forensic carried out in this research. At this stage, the search, collection, and identification of digital evidence is carried out at the scene of the incident

Table 1.Evidence found at crime scene

No	Name of evidence	Picture	Description
1.	Laptop of Actor		The laptop brand found is Asus with a Core i3 processor, RAM capacity of 4GB, OS Windows 10 home single language found online
2.	Laptop charger		Adapter Asus laptop adapter. Found near the laptop.

Table 1 the evidence that has been obtained from the crime scene, the next step the evidence is submitted to the forensics to conduct a search for digital data related to the case.

2.2.2 Examination

Acquisition of data from evidence that has been secured, the evidence is the suspect's laptop which is used for advertising the sale and purchase of human organs online. The laptop is alive and connected to the internet, it is carried out live forensics because the data is volatile in RAM.

2.2.2.1 Belkasoft Live RAM Capture

The memory capture process is carried out using the forensic tools Belkassoft Live RAM Capturer. This forensic tool is used to acquire data stored in RAM. All activities that occur in RAM will be recorded, then become a file containing data that can be extracted for further analysis.

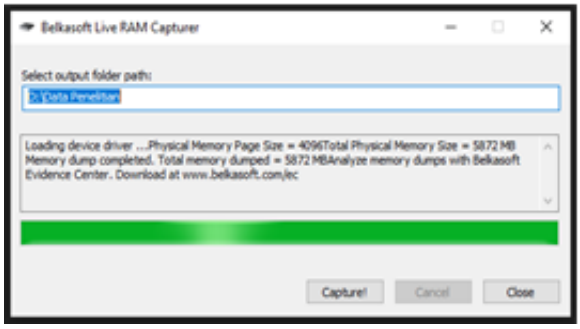


Figure 3.Belkasoft live RAM capture

Figure 3 is shows a display of the RAM acquisition process using Belkassoft Live RAM Caprturer, the results will be stored on partition D in the Research Data folder with a file size of 5872 megabytes (MB) according to a predetermined storage location. The result of RAM capture is a file in .mem format.

2.2.2.2 FTK Imager

Memory capture can also be done using the FTK Imager tool.

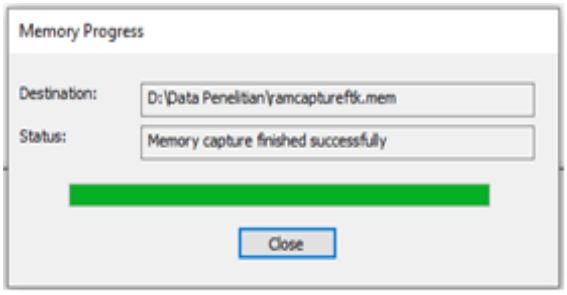


Figure 4. Memory capturefinishedsuccessfully

Figure 4 shows that the process Memory Capture has been completed and successful, the results of the process are then stored on partition D with the Research Data folder and the file name is ramcaptureftk.mem with a file size of 6,012,928 KB

2.2.2.3 Browser History Capture

Browser History Capture is a forensic tool that can be used in the chrome web browser acquisition process.

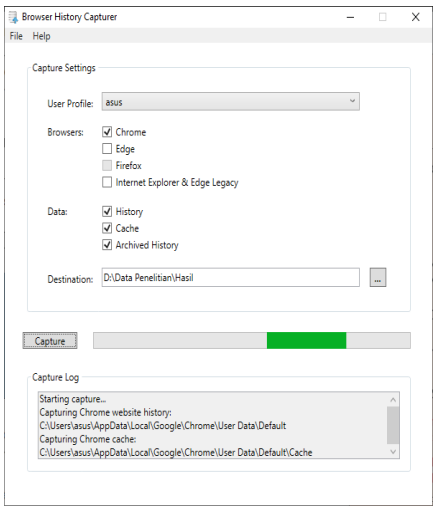


Figure 5.Start capture browsing history

Figure 5 shows that the capture process is in progress, when the process is complete, the results will be stored in the Research Data location.

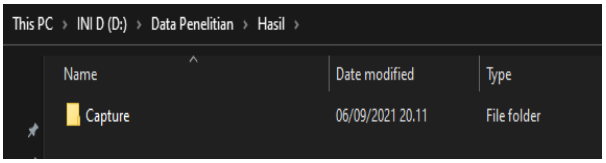


Figure 6.Browser History Capture

Figure 6shows results in that folder can be found sub folders containing historical data, and chrome data.

2.2.3 Analysis

The analysis process makes the results easy to read and understand and to determine whether there is evidence related to the case. In its implementation, tools are needed so that the data can be read, the tools used are as.

2.2.3.1 Browser History Examiner

The stage analysis uses this tool in order to read the data obtained from the browser history capture process. The data is extracted first.

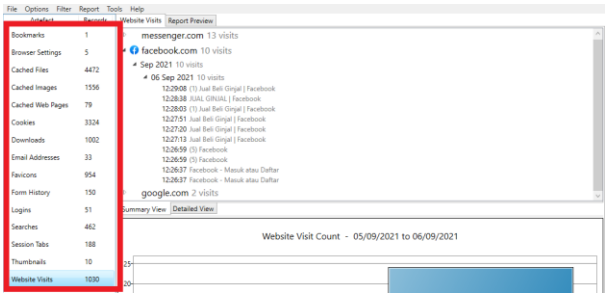


Figure7.The results of data extraction

Figure 7 is the result of extraction and information obtained from the Chrome browser such as Downloads, Bookmarks, Browser Settings, Chached files, Chached Images, Chached Web Pages, Cookies, Email Addresses, Favicons, FromHistory, Logins, Searches, Session Tabs, Thumbnails, Website Visits.

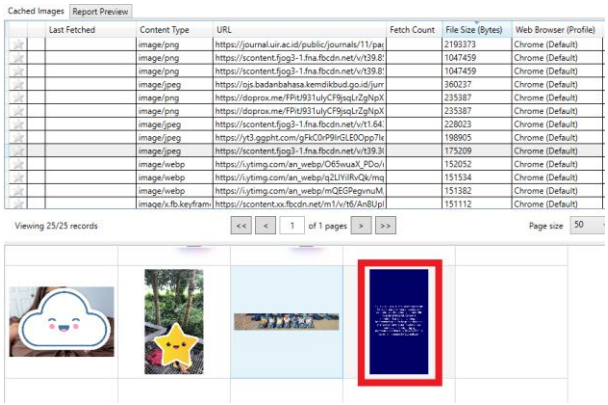


Figure8.Evidence found in cached images.

Figure 8displays cached images that were captured by forensic tools from the examination stage in the examiner's browser history. An image was found containing advertising content for buying and selling human organs from Facebook uploads that have been deleted.

2.2.3.2 Browser History Viewer

Browser History Viewer is a forensic tool that has the same use as Browser History Examiner, the only difference being that it has limited features.

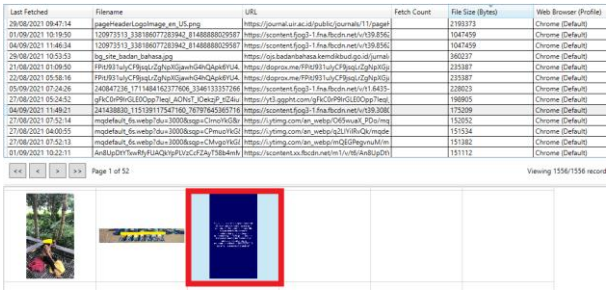


Figure 9.Browser history viewer

Figure 9shows initial view after extracting data in Browser History Viewer. The result was found similar images obtained fromthe Browser History Examiner tool. The history of visited websites is also the same. The difference is that this tool can use the "filter by keyword" feature to enter keywords that match what you are looking for so that the data obtained is more complete.

2.2.3.3 Analisis FTK Imager

In doing analysis, you can also use FTK imager tools. The data to be analyzed is obtained from the results of the examination using the FTK imager tool, namely the "20210906.mem" file. Click the Find button then the system will filter the data.

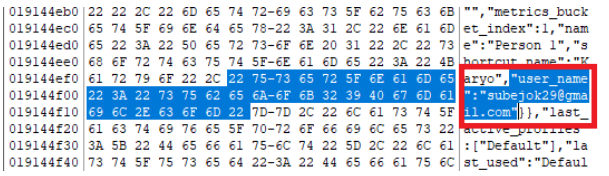


Figure 10.Criminal's facebook username

Figure 10shows username used to access Facebook.The data contains an email with the username subej***@gmail.com used by the perpetrator to carry out the action.

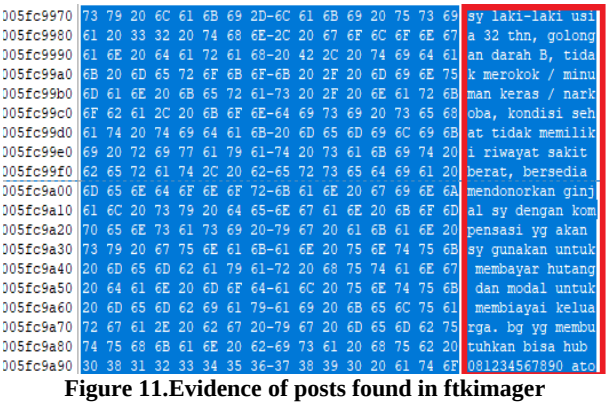


Figure 11.Evidence of posts found in ftkimager

Figure 11 found in the form of *text* from posts made by the perpetrators and has been deleted. The caption reads "I'm a 32 year old male, blood type B, doesn't smoke/alcohol/drugs,

healthy condition, no history of serious illness, willing to donate my kidney with compensation that I will use to pay debts and capital to support the family . For those who need it, you can call 08***4567890 and so on." Besides that, the suspect's username and password were also found and some comments from posts that have been deleted.

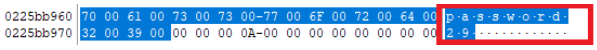


Figure 12.Password of the perpetrator

Figure 12shows password of the username of the perpetrator.The password of subejo***@gmail.com username was found. The password found is "pas**ord2*".

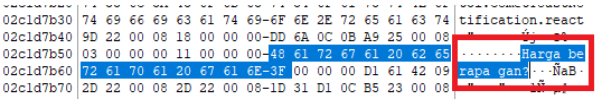


Figure 13. Comments that have been deleted

Figure 13shows comments that have been deleted, comments that read "How much, bro?". This comment was previously deleted and successfully restored.

2.2.4 Reporting

Reporting the results of the analysis includes an explanation of actions, and identification of data obtained from forensic tools.The Operation System used is Windows 10 Home Single Language. As for the software, it uses the Facebook web which is accessed via the Chrome browser. During acquisition and extraction, several forensic tools are used. Then the results obtained were analyzed so as to obtain evidence related to cases of buying and selling human organs.

Table 2. The comparison results of forensic tools

No	Forensic Tools	Software Forensic			
		Image	Text	Username	Password
1.	FTK Imager	-	✓	✓	✓
2.	Belkasoft RAM Capture	-	✓	✓	✓
3.	Browser History Capture	✓	-	✓	✓
4.	Browser History Examiner	✓	-	✓	✓
5.	Browser History Viewer	✓	-	✓	✓

Table 2 presents the evidence found by using forensic tools. The evidence is in the form of image, text, username, and password. The use of tools has been adapted to research needs. To perform the acquisition, use the FTK imager RAM capture feature,Belkasoft RAM Capture, and Browsers History Capture. Using more than one tool to ensure data accountability. Meanwhile, in the process, the extraction use the tools Browser History Examiner and Browser History Viewer. FTK Imager found data in the form of text, namely the sentence posted by the perpetrator along with comments on the post which had been previously deleted and successfully recovered. Then found also the username and password used by the perpetrator to access Facebook. In the Belkasoft RAM Capture tool, the same thing was found in the tool FTK imager. Evidence in the form of images was found using Browser History Capture, Browser History Examiner,and Browser History Viewer. In the three tools also found username and password.

2.2.5 Results

The evidence found from this research is image, text, username, and password.

Table 3. Finding Evidence from Research

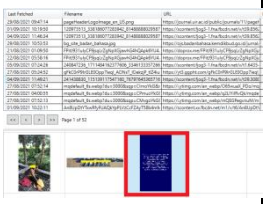
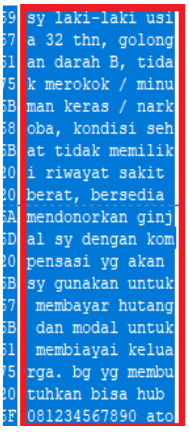
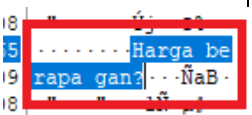
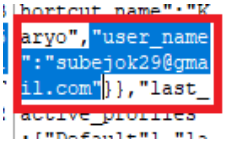
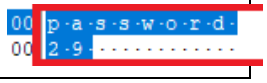
Evidence from the victim	Evidence found on the perpetrator's laptop
	**Post Image**  **Post Description and deleted comment**   **Username and Password**  

Table 3 shows the results from this research. Based on the results obtained, it was concluded that it was consistent with what the victim gave.

3. CONCLUSIONS

In a research conducted on the subject titleAnalysis of Digital Evidence for Facebook Services on Chrome Browser Using the NIST Method, conclusions can be drawn. The search for digital evidence was successfully carried out with the laptop on (Live Forensic), the acquisition was carried out first on the suspect's laptop, then the results from the acquisition were extracted and then analyzed according to NIST digital forensic standard procedures, by utilizing forensic tools so as to obtain evidence in the form of text and images. The details of digital evidence obtained from forensic tools are FTK Imager 60%, Belkasoft RAM Capture 60%, Browser History Capture 60%, Browser History Examiner 60% and Browser History Viewer 60%.The results obtained from this research are posts that have been deleted and the user account used to login to the Facebook service on the Chrome browser. From the results obtained, there are several shortcomings in the process of searching for digital evidence. Due to these shortcomings, further research is expected to enable the development of digital forensic stages and the development of old and new methods.

4. REFERENCES

[1] S. R. Ardiningtias *et al.*, "Investigasi Digital Pada Facebook Messenger," pp. 19–26, 2018.

[2] G. Atiko, R. H. Sudrajat, K. Nasionalita, and U. Telkom,Analysis of Tourism Promotion Strategies Through Social Media by the Ministry of Tourism (Descriptive Study on Instagram Account @Indtravel) 3(2):2349–58.

[3] I. Z. Yadi and Y. N. Kunang, "National Conference on Computer Science (KONIK) 2014 Forensic Analysis on Android Platform," *Konf. Nas. Ilmu Komput.*, p. 142, 2014,[Online].Available:http://eprints.binadarma.ac.id/2191/.

[4] Hadiyat and Yayat. 2017. "Online Prostitution Communication Patterns on Twitter." Journal of Communication and Development Research 18(2):125. Doi: 10.31346/Jpkp.V18i2.1219.

[5] Y. Prayudi and D. S. Afrianto, "Anticipation Of Cybercrime Using Computer Engineering," vol. 2007, no. Snati, 2007.

[6] P. T. Informasi and F. Tarbiyah 2020. "Application of National Institute of Standards and Technology (Nist) Methods in Digital Forensic Analysis for Handling Cyber Crime." 4:29–39.

[7] D. T. Yuwono and Y. W, "Comparative Analysis of File Carving with the Nist Method," J. Sains Komput. dan Teknol. Inf., vol. 2, no. 2, pp. 1–6, 2020, doi: 10.33084/jsakti.v2i2.1472

[8] N. Nasirudin, S. Sunardi, and I. Riadi, "Forensic Analysis of Android Smartphones Using NIST Method and MOBILedit Forensic Express Tool," J. Inform. Univ. Pamulang, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.

[9] T. Rochmadi, "Live Forensics for Anti-Forensic Analysis on a Web Browser Case Study Browzar," Indones. J. Bus. Intell., vol. 1, no. 1, p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.

[10] M. F. Sidiq and M. N. Faiz, "Review of Web Browser Forensics Tools to Support Digital Evidence Searching," J. Edukasi dan Penelit. Inform., vol. 5, no.1, p. 67, 2019, doi: 10.26418/jp.v5i1.31430.

[11] Y. Prayudi and D. S. Afrianto, "Anticipation of Cybercrime Using Computer Techniques." vol 2007, no. Snati,2007.

[12] T. Santoso. (1997) Sexuality and criminal law. Jakarta. Ind-Hill-Co. Hal. 134

[13] B. Raharjo, "More About Digital Forensics." pp. 384–387.

[14] I. Saputra and M. N. Azhar, "Analysis and Forensic Investigation of Digital Live Memory on Whatsapp Application." pp. 119–125, 2018.

[15] S. D. Utami, C. Carudin, and A. A. Ridha, "Live Forensic Analysis on Whatsapp Web for Proving Electronic Transaction Fraud Cases," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.

[16] J. P. Soepomo, "Forensic Analysis Of Digital Evidence On Frozen Solid State Drive Using The National Institute Of Standards And Technology (Nist) Method," Vol. 2, No. 2, Pp. 33–40, 2017.

[17] J. P. Soepomo, "Forensic analysis of the KakaoTalk application using the National Institute Standard Technology method," vol. 2018, no. November, pp. 129–133, 2018.

[18] P. Studi, T. Informatika, U. Ahmad, J. P. Soepomo, and S. H. J. Yogyakarta, "Forensic Analysis Instant Messenger Application," vol. 2, no. 2, pp. 25–32, 2017.

[19] W. Sanjaya, B. Sugiantoro, and Y. Prayudi, "A Offline Forensic Methods for Digital Analysis of Artifacts On TOR Browsers in Linux Operating Systems," JITU J. Inform. Technol. Commun., vol. 4, no. 2, pp. 41–51, 2020, doi: 10.36596/jitu.v4i2.345.

[20] P. Widiandana and I. Riadi, "Cyberbullying Forensic Investigation Analysis On Whatsapp Messenger Using The National Institute Of Standards And Technology (Nist) Method," pp. 488–493, 2019.

[21] 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.

[22] D. Zarella,(2010) The Social Media Marketing Book. Sebastopol: O'reilly Media.Inc.

[23] I. Zuhriyanto *et al.*,"Digital Forensic Design in Applications." *Semin. Nas. Inform.*, vol. 2018, no. November, pp. 86–91, 2018.

[24] D. A. Putri, and I. Riadi, "Forensic Mobile against Threat WhatsApp Services using National Institute of Standards Technology Method," vol. 183, no. 30, pp. 1–8, 2021.

[25] A. P. Utami, and I. Riadi, "Mobile Forensics Analysis of Line Messenger on Illegal Drug Transaction Case using National Institute of Standard Technology (NIST) Method," vol. 183, no. 32, pp. 23–33, 2021.