CENTIVE
VOL. 3, NO. 1, PP.744-749, DEC 2023
ISBN : 978-602-53004-0-0

Conference on Electrical Engineering, Informatics, Industrial Technology, and Creative Media 2023

Anti-Forensic Investigation Model Using Live Forensic Method on Private Web Browsing

Arya Satya Saputra [1], Wiwin Sulistyo [*2]

[1,2] *Teknik Informatika, Universitas Kristen Satya Wacana*
Jl. Dr. O. Notohamidjojo No.1 - 10, Blotongan, Kec. Sidorejo, Kota Salatiga, Jawa Tengah, Indonesia

[1] aryasatyasap@gmail.com
[2] wiwinsulistyo@uksw.edu

Received on 27-10-2023, revised on 27-11-2023, accepted on 11-12-2023

Abstract

For privacy protection, browsers developed incognito mode or private web browsing that does not store history data. Private web browsing can be used for crimes, but computer crimes definitely leave digital traces. It is necessary to have a forensic computer expert who will observe and analyze to obtain valid evidence. Private web browsing is an anti-forensic method because it intentionally uses private web browsing to find out something on the internet without storing data history. This research successfully found historical data on private web browsing for valid evidence. Data history for accessing the carding forum website and the marijuana buying and selling website is still stored in Random Access Memory (RAM), so it can be valid evidence. The Live-Forensic method retrieves Random Access Memory (RAM) data because Random Access Memory (RAM) stores all sources of information as long as the computer is turned on, which allows forensic computer experts to investigate quickly and accurately. From the tests conducted, the history data from private web browsing can still be found with the Live-Forensics method, even though the browser claims that it will not store history data.

Keywords: Private web browsing, Live-Forensics, Random Access Memory, Anti-Forensics

Corresponding Author:
*Wiwin Sulistyo
Teknik Informatika, Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo No.1 - 10, Blotongan, Kec. Sidorejo, Kota Salatiga, Jawa Tengah, Indonesia
Email: wiwinsulistyo@uksw.edu

I. INTRODUCTION

Anti-forensics is a technique or attempt to thwart an investigation, including avoiding event detection and interfering with the collection of needed information [1]. Web browser applications develop incognito mode or private web browsing features for privacy protection. Private web browsing is an Anti-Forensic method because it intentionally uses private web browsing to find out something on the internet without saving history data [2]. The incognito mode or private web browsing feature can be used for crime. The official website of the International Criminal Police Organization (INTERPOL) explains that in the Global Top Crime Trend 2022, there are several crimes such as Phishing and Online Scams, Synthetic Drug Trafficking, Online Child Sexual Exploitation and Abuse, and Cannabis Trafficking. Computer crimes must leave digital traces, so a forensic computer expert is needed who will secure and analyze to obtain valid evidence [3].

The Live-Forensics method is a method that performs Random Access Memory (RAM) data acquisition [4]. RAM stores computer information data as long as the computer is turned on [5]. Some previous studies

that become references are Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser, which explains that logs from private portable web browsing can be analyzed with volatility memory forensics tools and WinHex [6]. The research entitled Experimental Analysis of Web Browser Sessions Using Live Forensics Method explains the process of investigating logs from web browsing sessions with the Live-Forensics method, and his research also found evidence that could be used as a reference for court evidence [7]. The research entitled Digital Forensic Analysis Methodology for Private Browsing: Firefox and Chrome on Linux as a case study explains that logs on private web browsing with Firefox and Chrome browsers on Linux can be analyzed. The study took evidence on browsing history, email communication, and history of opening YouTube videos [8]. Based on the findings of previous comparable research, the Live-Forensics method has demonstrated its effectiveness in generating substantial evidence through the acquisition of RAM data. In addition, various studies shed light on the feasibility of analyzing the history of private web browsing activities.

This research tests anti-forensic techniques through the Live-Forensics method with a case study of open and closed private web browsing pages on the Linux operating system to assess their effectiveness in real-case scenarios. This research specifically investigates closed private web browsing pages. The purpose of comparing the two case studies is to ascertain whether there are any differences in findings between open and closed private web browsing pages. Based on the test results, this research produces digital evidence even though using anti-forensic techniques with case studies of open and closed private web browsing pages.

II. RESEARCH METHOD

This research follows the meticulous standardization stages developed by the National Institute of Standards and Technology (NIST) for digital forensic investigation. These stages, namely Collection, Examination, Analysis, and Reporting, are crucial in ensuring a systematic and reliable approach to analyzing digital evidence [9]. The significance of standardization in these stages cannot be understated, as it guarantees the use of a clear and accurate Standard Operating Procedure (SOP) when analyzing the data, which will serve as evidence in court. Two scenarios are needed to evaluate whether the history data on the private web browsing page, while still open, gives similar or different results compared to the closed private web browsing page.

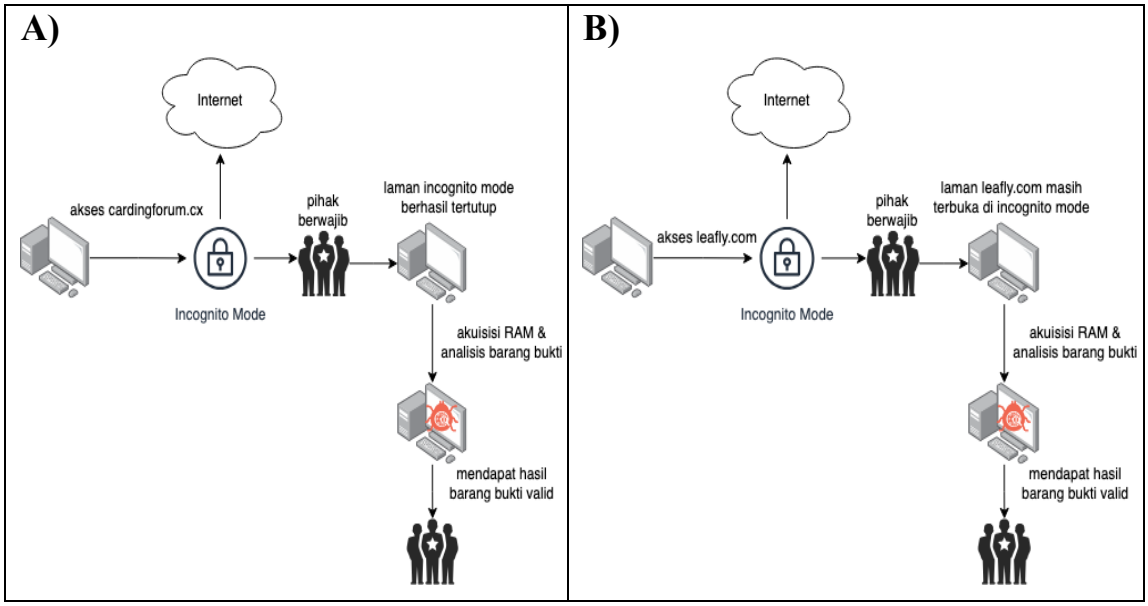

Figure 1. Explaining Carding Forum Scenario (A) and Leafy Scenario (B)

Referred to in Figure 1 Carding Forum Scenario (A), related to the test scenario, criminals access the carding forum website (cardingforum.cx) to sell other people's credit cards using incognito mode and are already in a closed state. Then, the authorities perform RAM acquisition and evidence analysis until they get the results of the evidence.

Then, in the Leafily scenario (B), criminals will access the marijuana buying and selling website (leafly.com) in incognito mode. Afterwards, the authorities apprehend the criminal while the private web browser page is still open. The authorities carry out RAM acquisition and analysis of evidence to obtain evidence results.

In the context of the forum carding scenario, the absence of open private web browsing pages requires a prolonged investigation, as it requires a thorough analysis of the available evidence. This technique can be categorized as Anti-Forensics, as it aims to hide or eliminate traces of the data source. In contrast, Leary's scenario found an open private web browsing page, which expedited the investigation as it provided clear instructions for analyzing the evidence.

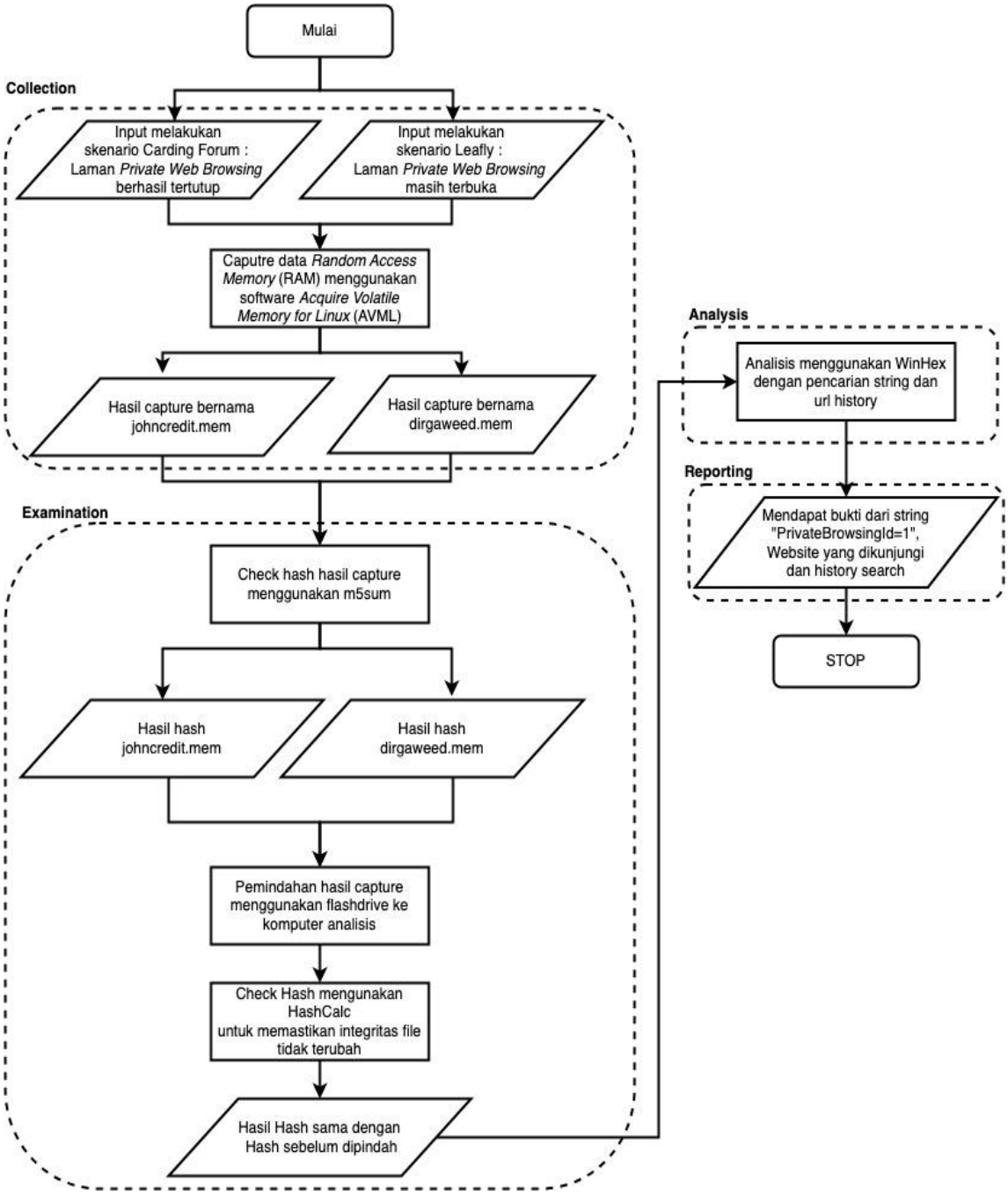

Figure 2. The research method refers to the NIST stages

Figure 2 is a research method that refers to the NIST stages in the implementation of Anti-Forensic investigations using the Live-Forensic method on private web browsing. In the first stage of the Collection stage, researchers create scenarios and are tested for this research. This research uses two scenarios: opening a private web browsing page that is still open and a private web browsing page that has been closed. Furthermore, at the Examination stage, researchers capture data from Random Access Memory (RAM) using AVML (Acquire Volatile Memory for Linux) software. After capturing data from Random Access Memory (RAM) has been completed, the researcher will perform a Hash Check on the capture file and then transfer the data using a Flash Disk to the computer that will be used for analysis. In the digital forensic investigation stage, there is one stage, namely maintaining data integrity to maintain its authenticity and not be modified. Therefore, researchers conducted a Hash Check on the evidence before and after being moved so that the hash remains the same and does not change [10]. At the Analysis stage, researchers use HashCalc software to get the Random Access Memory (RAM) hash, which is used as evidence that the integrity of the original capture data has not been changed. After the file is confirmed unchanged, researchers use WinHex software to analyze the evidence. At the Reporting stage, researchers found some evidence that could be used in court.

III. RESULTS AND DISCUSSION

A. *Acquisition of Random Access Memory*

The Random Access Memory (RAM) Acquisition stage refers to the Collection stage, which takes evidence from a computer as raw data for evidence analysis. To retrieve RAM data, use the Acquire Volatile Memory for Linux (AVML) application, which is acquired without having to know the Linux kernel of the device to be acquired. Acquisition of raw data from RAM with Linux commands in Figure 3.

```
—$ sudo ./avml /home/john/Desktop/johncredit.mem
```

Figure 3. RAM Data Acquisition

B. *Hash Check Before and After RAM Acquisition Data Transfer*

Check hash of raw files from Random Access Memory (RAM) refers to the Examination stage. Check hash by using md5sum software on Linux with the results in Figure 4 and Figure 5.

```
└─$ sudo md5sum johncredit.mem
[sudo] password for john:
5b8fd07c280bf09981e7a62a9bf68067  johncredit.mem
```

Figure 4. Hash of johncredit.mem

```
└─$ sudo md5sum dirgaweed.mem
ae6d6510c92a27184f036d5f4b58d84c  dirgaweed.mem
```

Figure 5. Hash of dirgaweed.mem

Next is the transfer of RAM acquisition data to the researcher's analysis device using Flash Drive storage media. After transferring the raw acquisition data from RAM using Flash Drive storage media, the researcher conducted a Hash Check using HashCalc software on the file data to ensure the integrity of the file was still the same and had not changed because the evidence must contain a definite causal correlation with the case and not be fabricated [8]. This is also part of the Standard Operating Procedure (SOP) for handling evidence. The Hash Check results are described in Figure 6 and Figure 7.

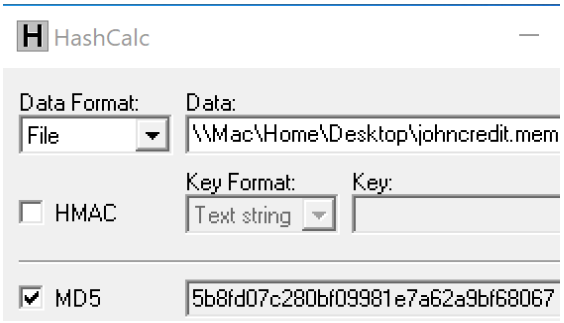

Figure 6. Hash of johncredit.mem

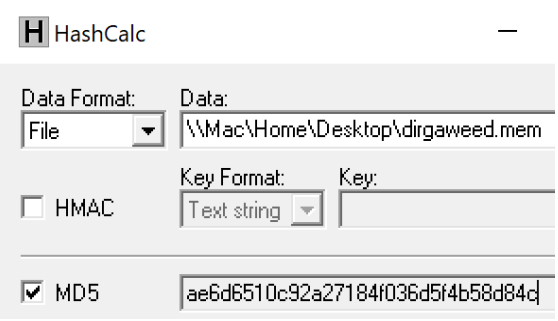

Figure 7. Hash of dirgeweed.mem

With the same results as before moving, the data retrieved with the data to be analyzed is still original and unchanged so that the integrity of the Random Access Memory (RAM) data is still maintained.

C. *Analysis using the WinHex app*

Referring to the Analysis stage, researchers analyzed using the WinHex application to preview data from RAM acquisition data to determine digital evidence. Digital evidence indicators, according to a definition from the International Association of Chiefs of Police Cyber Center website, are any information or data of investigative value that is stored, received, or transmitted via an electronic device. Text messages, emails, images and videos, and internet searches are some of the most common types of digital evidence. By analyzing using WinHex, researchers found evidence of the <PrivateBrowsing> string in the Random Access Memory (RAM) acquisition data results.

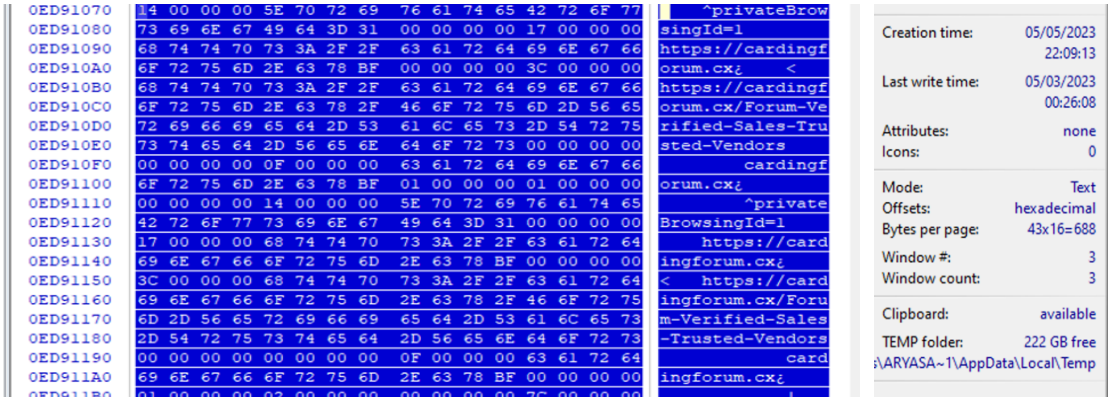

Figure 8. Analysis Result of Carding Forum Scenario

In Figure 8, it is shown that the results of Random Access Memory (RAM) data acquisition in the forum carding scenario can still be read, even though in the forum carding scenario, the Incognito Mode page is closed. This is also proven in the <PrivateBrowsingId=1> string with the cardingforum.cx site. This forum carding scenario shows that even when using Private Web Browsing and then closing the page from Private Web Browsing, the page can still be analyzed through the Live-Forensics method. This carding forum scenario found some evidence, namely using private web browsing mode and also accessing the carding forum site, cardingforum.cx.

Then, in the leafy scenario, I found the evidence shown in Figure 9, with the Private Web Browsing page scenario still open by displaying the leafly.com website, which is a marijuana-buying and selling website. In the Random Access Memory (RAM) data analysis also displays the search history of "website sell weeds" and the history of opening the leafly.com website. This is further confirmed by the clear indication of the string <PrivateBrowsingId=1>, which reveals that the person in question specifically visited the Private Web Browsing page.

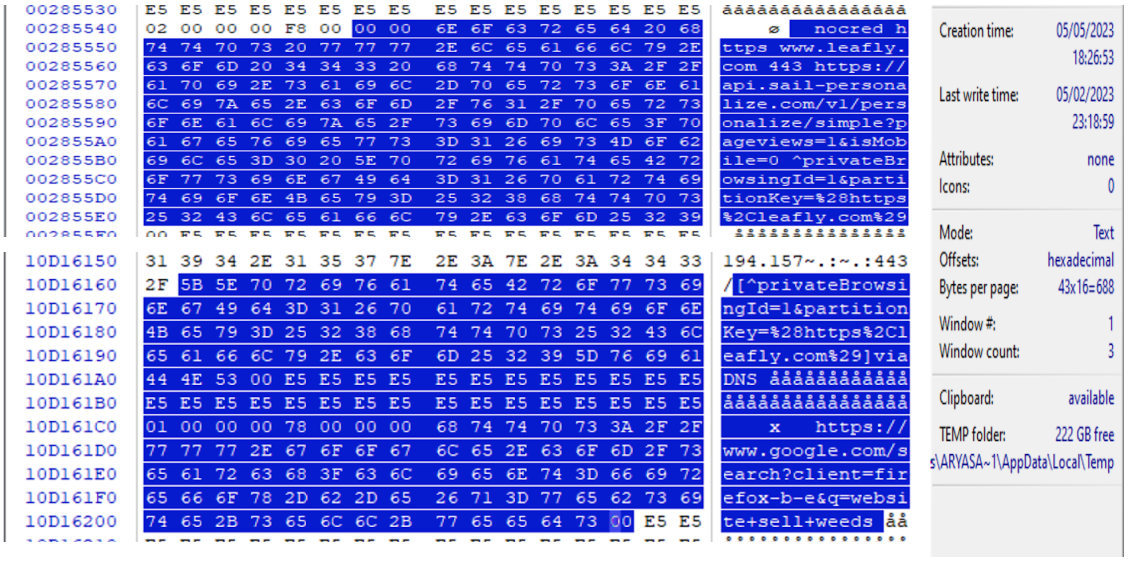

Figure 9. Leafly Scenario Analysis Results

D. Obtaining Valid Evidence

This stage refers to the Reporting stage because, in the two scenarios above, it was proven that the perpetrator used Anti-Forensic techniques because he used private web browsing to commit crimes such as accessing carding forums and accessing marijuana buying and selling sites and closing private web browsing pages. The analysis results still find evidence even though the browser application guarantees that it does not store history. History data is still stored in Random Access Memory (RAM), which stores computer data from the first time it is turned on. Even if the person closes their personal web browsing page on carding forum scenario, some information from their computer memory can still be saved and used as evidence.

IV. CONCLUSION

By doing this research, it can be concluded that the browser application does not really store history because history can still be stored in Random Access Memory (RAM) data. Anti-forensic techniques using private web browsing or incognito mode are proven to be broken. Researchers can still find digital evidence with RAM data acquisition. In the comparison of the two scenarios that have been studied, it is worth noting that researchers can still analyze the scenario where the private web browsing page is closed. Evidence that can be valid evidence in this study is the presence of the <PrivateBrowsing> string, which indicates the perpetrator uses Private Web Browsing, and the presence of a site after the <PrivateBrowsing> string. This research uses the Live-Forensics method because this method handles incidents quickly and makes it possible to get RAM data that is easily lost when the computer is turned off.

REFERENCES

[1] N. Maček, P. Štrbac, D. Čoko, I. Franc, and M. Bogdanoski, "Android Forensic and Anti-Forensic Technicques – a Survey," Oct. 2016.

[2] R. Md Saidi, F. F. Saleh Udin, A. F. Zolkeplay, M. A. Arshad, and F. Sappar, "Analysis of Private Browsing Activities," in *Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016)*, N. A. Yacob, N. A. Mohd Noor, N. Y. Mohd Yunus, R. Lob Yussof, and S. A. K. Y. Zakaria, Eds., Singapore: Springer Singapore, 2018, pp. 217–228. doi: 10.1007/978-981-13-0074-5_20.

[3] V. Rosalina, A. Suhendarsah, and M. Natsir, "ANALISIS DATA RECOVERY MENGGUNAKAN SOFTWARE FORENSIC: WINHEX AND X-WAYS FORENSIC," vol. 3, no. 1, 2016.

[4] V. Sali and H. K. Khanuja, "RAM Forensics: The Analysis and Extraction of Malicious Processes from Memory Image Using GUI Based Memory Forensic Toolkit," Aug. 2018, pp. 1–6. doi: 10.1109/ICCUBEA.2018.8697752.

[5] 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, Apr. 2020, doi: 10.29121/ijetmr.v5.i2.2018.618.

[6] T. Rochmadi, I. Riadi, and Y. Prayudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *Int. J. Comput. Appl.*, vol. 164, no. 8, pp. 31–37, Apr. 2017, doi: 10.5120/ijca2017913717.

[7] R. Umar, A. Yudhana, and M. Nur Faiz, "Experimental Analysis of Web Browser Sessions Using Live Forensics Method," *Int. J. Electr. Comput. Eng. IJECE*, vol. 8, no. 5, p. 2951, Oct. 2018, doi: 10.11591/ijece.v8i5.pp2951-2958.

[8] X. Fernández-Fuentes, T. F. Pena, and J. C. Cabaleiro, "Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux as a case study," *Comput. Secur.*, vol. 115, p. 102626, Apr. 2022, doi: 10.1016/j.cose.2022.102626.

[9] Universitas Hamzanwadi, A. Ahmadi, T. Akbar, and H. Mandala Putra, "PERBANDINGAN HASIL TOOL FORENSIK PADA FILE IMAGE SMARTPHONE ANDROID MENGGUNAKAN METODE NIST," *JIKO J. Inform. Dan Komput.*, vol. 4, no. 2, pp. 92–97, Aug. 2021, doi: 10.33387/jiko.v4i2.2812.

[10] Y. V. Akay, "Computer Forensics and Cyber Crime Handling," vol. 15, 2020.