IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 13, No. 3, June, 2023, pp. 577-585
Journal homepage: http://iieta.org/journals/ijsse

Live Forensic Environment with Parallel Data Acquisition for Investigating Private Mode Browsing

Herman[1*], Anton Yudhana[1], Sarjimin[2]

[1] Department of Informatics, Ahmad Dahlan University, Yogyakarta 55164, Indonesia
[2] Department Electrical Engineering, Ahmad Dahlan University, Yogyakarta 55164, Indonesia

Corresponding Author Email: sarjimin1908048024@webmail.uad.ac.id

https://doi.org/10.18280/ijsse.130320

Received: 15 February 2023
Accepted: 23 May 2023

Keywords:
live forensic, browser, private mode, parallel data acquisition, investigate

ABSTRACT

Web Browser Private mode is a feature hide activities carried out by users, user activities not stored on the hard disk or SSD, so they cannot be analyzed with standard forensic techniques (static forensics). This study aimed to acquire web browser artefacts from Random Access Memory (RAM) and Network Traffic on Windows 10 and Ubuntu Linux operating systems. The problem of this study is how to find evidence of a crime in a web browser that utilizes the private mode feature. The web browser in private mode does not leave any traces on the User's computer, so it becomes an obstacle in the process of searching for digital evidence of a crime. This article proposed parallel data acquisition data through two different sources to obtain digital evidence using private mode web browsers, from RAM and Network Traffic. All website log on Windows 10 and Ubuntu 20.04 are founded with RAM analysis. Analysis network traffic also revealed (1) source IP address, (2) destination IP address, (3) protocol, (4) source port, (5) destination port, (6) timestamp (communication time done), (7) length packet (number of packets transmitted), (8) operating system host client, (9) hostname server and (10) browser client.

1. INTRODUCTION

Private mode is browser's feature that allow user to surf in the Internet and leave minimum traces. Typical web browser provides browsing data and history to facilitate user customization, such as recommendations of websites that have been visited [1, 2]. In contrast, private mode does not provide such features. When cybercrime occurs on social media using browser in private mode, it is less opportunity for investigator to collect evidence due to no browser files or log are available in the device of user/suspect [1, 2]. Investigator even cannot identify site that has been visited by the suspect nor IP of the site. In similar case, investigator usually relies on browser log to obtain evidence and information related to the case [3-5].

The APJII Bulletin published by the Indonesian Internet Service Users Association revealed that in 2019 internet users in Indonesia reached 171.17 million people out of 264.16 million Indonesia population [3]. Due to the extensive use of web browsers, cybercriminals or suspects, commonly, can use browsers to commit any criminal acts or visit different websites to gather information, so this can be considered a good source of electronic evidence for use in lawsuits and other crime-related investigations [1, 4]. The crime is not considered to be finished until the responsible parties are prosecuted before the court [5].

Live Forensics is the process of collecting forensic evidence from an ongoing computer system [6-9]. Live forensic techniques are highly recommended on live systems whose data will be lost when the system is turned off and disconnected from the network. Live forensics on a PC can only be done by running programs on the Suspect's machine, but retrieving files directly from the Suspect's device is contrary to existing forensic procedures, it is feared that it can damage the Suspect's device [10, 11], Live forensic methods are also expected not to intervene and modify the suspect system [12]. According to common forensic principles, investigators should "never have worked on the original system" because working on a suspected machine could damage the existing evidence.

Private browsing has been known in many web browsers. Google Chrome names it Incognito Mode. Chrome [13] will not store browsing history, cookies, site data, or information entered in the form. The files that the user downloads and the bookmarks that the User creates will be saved. User activity is not hidden from websites you visit, companies or user schools, or ISPs. Mozilla Firefox names private browsing [14], i.e., not storing User browsing information, such as history and cookies, without leaving a trace after the User ends the session. Firefox also has Enhanced Tracking Protection, preventing hidden trackers from collecting user data on some websites. Microsoft Edge calls it InPrivate mode [15], i.e., when the User uses the InPrivate tab or window, the User's browsing data (such as User history, temporary internet files, and cookies) is not stored on the User's Personal Computer (PC) once the User is complete. Apple Safari names it Private Browsing [16] that is, when the User uses the private browsing, the User's browsing details are not stored, and the website that the user visits is not shared with other devices [1, 2, 17-20].

Web browser private mode does not leave any trace on primary storage (hard disk). Private browser private mode disables browsing history and web cache [19, 21-23]. The main problem in the live forensic method in private mode web browsers is collecting artefacts on volatile storage media such as CPU Registers, Random Access Memory (RAM), and network connections. The duration of log storage time is also another problem in volatile media [11].

Newer live forensic analysis tools can perform data acquisition on suspects' computer conditions, but these analysis tools may be able to contaminate evidence by leaving traces in memory [11]. The challenges for investigator forensic web browsers are private browsing and portable mode features [10] and retrieving proof of cybercrime through other sources as evidence. The other challenges are how to contaminate the primary evidence of the crime (Suspect's computer). All modern browsers support browsing in private mode; on the other hand, portable mode leaves no trace of Internet activity on the local machine; after the search is complete, all browser files are created on the portable device on which the browser is running.

Live forensic provides the opportunity to access network resources [11] so that the live forensic network can be an alternative source of finding artefacts in cybercrime cases. Forensic browser is expected to provide crucial evidence in cybercrime investigations [10]. Tri Rochmadi research [24] states that suspects can eliminate website browsing data by using anti-forensic tools [24]; that is, by hiding the search data, the capture of data directly also allows for changes to the evidence [11]. So that data acquisition techniques are needed in live forensic methods through other media except for RAM. Every computer used to use a private mode web browser must be connected to the internet network so that data acquisition can be made by live acquisition of internet network activities.

2. LITERATURE REVIEW

Suma, G. S., Dija, S., & Pillai, A.T. Tried to obtain evidence of the crime of using the web browser in the relevant normal mode by leaving minimal evidence on the Suspect's device, analysis of the evidence was conducted on the Investigator's machine. Davies et al. use live forensics to analyze ransomware and recover cryptographic fragments in RAM that may be used to reverse the effects caused by ransomware [25]. Tri Rochmadi, Imam Riadi, Yudi Prayudi's research on forensic anti-forensics revealed that search history, timestamp, and password are still possible if the data in the computer RAM is not deleted (anti-forensic). Still, if the data in RAM has been deleted with tools such as Clean After Me, it isn't easy to find data that can be analyzed [24]. Tri Rochmadi research [26] obtained digital evidence artefacts from Browzar's web browser on the Windows 7 operating system using the DumpIt tool. It analyzed using Forensic Memory Volatility and Winhex to get three potential digital evidence related to criminal cases on the internet; the digital evidence is the URL or address of the website visited by the User's, timestamp, which is the time to access the URL by the perpetrator, and the password that is the perpetrator's account and is used for logging into the Google Mail account. Research written by Junghoon Oh, Seungbong Lee, Sangjin Lee [27] has considered browser log files as a potential source for extracting information. Huwida Said, Noora Al Mutawa, and Ibtesam Al Awadhi [28] extract artefacts using RAM analysis. Rathod [20] uses history, cookies, login data, topsides, shortcuts, user profile, prefetch file, and RAM analysis to collect Google Chrome artefacts. Jadhav [29] have obtained user activity on Mozilla Firefox web browser, opera, internet explorer, and google chrome in normal mode got log history, cookies, searched keywords, website hosts, and download logs. Huwida Said, Noora Al Mutawa, and Ibtesam Al Awadhi [28] extracting private browser artefacts with FTKImager and Winhex found a different result that (1) that Inprivate mode in Internet Explorer stores history on the hard disk but that data will be deleted when Internet Explorer InPrivate Mode is stopped, (2) the test results on Mozilla firefox private mode do not leave history on the hard drive.

Live forensic analysis has disadvantages in the data retrieval part through RAM but live forensics is the process of collecting forensically sound evidence from a running computer system [30]. So, this study aims to find alternative data sources other than RAM in the Live Forensic method. The retrieval of data log network traffic of the Suspect's computer under investigation can be done without contaminating the Suspect's computer. The weakness of live forensic web browser private mode can be overcome by retrieving live forensic data through internet network logs connected to the Suspect's computer. Network traffic logs are a valuable source in digital forensics and data acquisition [31-36]. Parallel data acquisition through RAM and network traffic logs can be an innovative data acquisition method in live forensics. The combination of data acquisition from RAM and network traffic logs carried out with parallel is expected to be able to find more digital artifacts to strengthen evidence. This combination is also expected to provide added value because data from both sources can be compared to each other to confirm the evidence retrieved.

3. METHOD

This paper proposes a parallel data acquisition (Figure 1) to find evidence during browsing in private mode. Parallel data acquisition will take data from two sources, from RAM of the computer's suspect and from the network traffic log. Acquisition data in RAM is carried out when the computer is still running. Data of network traffic log will be collected by recording all network activities pass through the router with a packet analyzer. The combination of data acquisition from RAM and network traffic logs which are carried out in parallel is expected to find more digital artifacts to strengthen evidence. This combination is also useful at the same time because data from both sources can be compared with each other to affirm the evidence obtained. The way that section titles and other headings are displayed in these instructions, is meant to be followed in your paper.

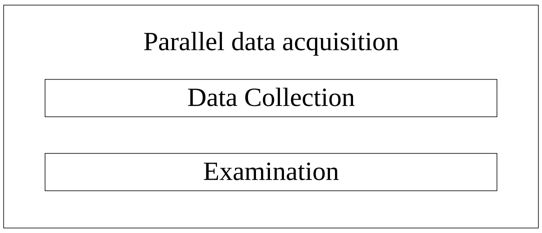


Figure 1. Parallel data acquisition

To perform the proposed parallel data acquisition succeeded in obtaining evidence from private browsing activities, an experimental environment was built to test parallel data acquisition. This experimental environment developed (Figure 2) based on NIST framework. The framework that is widely used in live forensics investigation [6, 9, 25, 37].

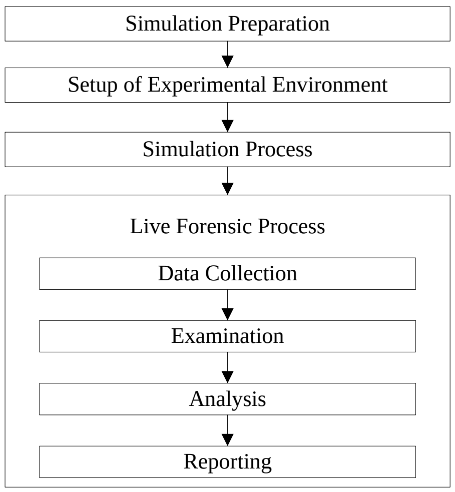


Figure 2. Experimental environment for parallel data acquisition

To build the simulation environment in Figure 2 the author uses few hardware shown in Table 1.

Table 1. Hardware

No	Hardware	Function
1	PC Desktop: Processor Intel(R) Core (TM) i5 CPU 10400F 4 Core(s), Memory RAM 8GB, Windows 10 x64	Computer 1 investigator
2	PC Desktop: Processor Intel(R) Core (TM) i5 CPU 10400F 4 Core(s), Memory RAM 16GB, Ubuntu 20.04 Desktop	Computer 2 Virtualization OS for simulation

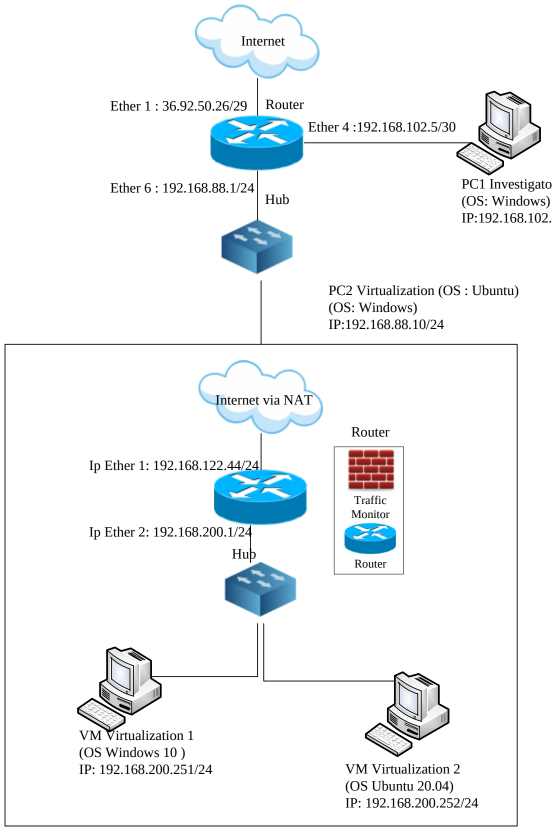


Figure 3. Network topology of a virtual environment built in Computer 2

In order to perform a live forensic environment for parallel data acquisition, it is necessary to build a network topology that support this simulation to be carried out. Figure 3 illustrates the network topology of the built simulation environment.

Environment proposed simulated case scenarios (Figure 3) using the hardware shown on with the equipment in Table 2. This study was conducted with two computers. Computer 1 is used as a Computer Investigator, and Computer 2 is used as a virtual computer running VirtualBox and GNS3. Computer 1 (Investigator) uses Windows 10 and installed forensic autopsy tools, Belkasoft, Magnet Axiom, Wireshark and Networkminer. Computer 1 installed GNS3 and Virtualbox. GNS3 is an open-source that can mimic routers and hardware to create a complex network simulation [38]. VirtualBox is open-source virtualization software to create a virtual environment [39].

To prove whether the proposed parallel data acquisition succeeded in obtaining evidence of private browsing activity, a case study was carried out on the use of private browsing activity.

The scenario in this simulation as follows:

1. Actor 1 and Actor 2 perform private browsing by visiting three websites.
   Actor 1 and Actor 2 accessing three public websites shown on Table 2 with web browser Mozilla Firefox Private Mode. This scenario using operating system Windows and Ubuntu Linux.

Table 2. Public website

No	Website	IP ADDRESS
1	https://www.exploit-db.com	192.124.249.13
2	https://dvwa.co.uk	185.199.108.153 185.199.111.153
3	https://www.w3schools.com	66.29.212.110

2. Actor 1 and Actor 2 were ambushed by Investigators.
3. Investigators perform acquisition of the computer RAM from Actor 1 and Actor 2.
4. Investigator acquisition network traffic logs on the nearest router connected to Actor 1 and Actor 2 computers.

The scenario topology in this simulation shown in Figure 3 and Figure 4.

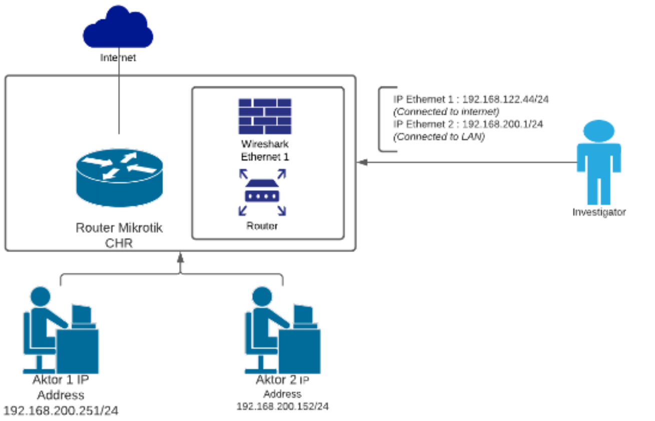


Figure 4. Topology

This simulation requires software and OS virtualization, Table

3 lists the software and OS virtualization.

Table 3. Software and forensic tools

No	Software	Functions
1	VM Ubuntu 1 Linux 20.04, Intel(R) Core(TM) i5 CPU 10400F 4 Core(s), RAM 4GB (VM dibuat pada Virtualbox PC No. 2)	Virtual Machine
2	VM Windows 10 x64, Intel(R) Core(TM) i5 CPU 10400F 4 Core(s), RAM 4GB (VM dibuat pada Virtualbox PC No. 2)	Virtual Machine
3	VM Router Mikrotik Cloud Hosted Router (CHR), Intel(R) Core(TM) i5 CPU 10400F 4 Core(s), RAM 512MB (VM dibuat pada Virtualbox PC No. 1)	Virtual Machine
4	VM Hub 8 Port (make on GNS3)	Virtual Hub
5	Mozilla Firefox	Research Object
6	Sleuth Kit Autopsy	Forensic Tools
7	Magnet Axiom	Forensic Tools
8	Belkasoft	Forensic Tools
9	Wireshark	Forensic Tools
10	Networkminer	Forensic Tools
11	GNS3	Virtualisation Network
12	VirtualBox	Virtualisation Software

Mikrotik Router VM CHR, Windows 10 VM, Ubuntu 20.04 Linux VM created on Desktop PC Number 2. The processor specifications for each VM follow the parent Desktop PC processor. The RAM capacity refers to the minimum standard VM operating system, the minimum standard for Windows 10 is 2 GB, the minimum standard for Ubuntu 20.04 is 4 GB and the minimum standard for Mikrotik CHR is 512MB. The hard disk capacity of each VM is determined dynamically, namely the hard disk capacity adjusts the size of each VM.

Research material of Windows 10 64 bit unlicensed was obtained by trial download form the official website Microsoft.com, Linux Ubuntu 20.04 is an open source which can be downloaded via the official website Ubuntu.com. Mikrotik CHR is a version of the virtualization format provided by mikrotik.com which can be utilized for academic and research purposes.

The RAM logs that have been obtained will be analyzed with Magnet Axiom, Belkasoft and Autopsy. Network traffic logs that have been obtained will be analyzed with Wireshark and Networkminer.

4. RESULTS AND DISCUSSION

4.1 Data collection

Actor 1 and Actor 2 run the data acquisition mechanism on each VM as follows: the mechanism for acquisition private mode web browser logs on Virtual Machine 1 (Windows 10) is by accessing the three websites listed in Table 4 sequentially. After the website access process is complete, proceed retrieving RAM data (memory dump) using the Magnet Axiom RAM Capturer tool and retrieving network traffic logs from the router.

The acquisition of private mode web browser logs on Virtual Machine 2 (Linux Ubuntu) is done by accessing the three websites listed in Table 4 sequentially. After the website access process is complete, it is followed by acquisition RAM data (memory dump) using the Linux Memory Extractor (LIME) tool and retrieving network traffic logs from the router.

Data acquisition on Virtual Machine 1 and Virtual Machine 2 is done at different times so that there is no confusion of Ubuntu 20.04 los or Windows 10 log. Acqusition RAM data from Windows using Belkasoft ram Capturer. Acquisition RAM data on Linux Ubuntu must know the root password; the acquisition performed by executing lime.ko with inserting module insmod lime.ko "path=nama_file.raw format=raw" into the kernel.

Preserving e-evidence and maintaining good documentation of the steps taken during the processing of evidence is critical to success [40]. So we need to make documentation of the evidence retrieved. Documentation about image RAM has been acquisition from Windows 10 and Ubuntu shown in Table 4. Documentation about Network traffic log has been acquisition from Wireshark which records traffic activity from Window and Ubuntu 20.04 shown in Table 5.

Table 4. Image RAM has been acquisitioned from Windows 10 and Ubuntu 20.04

No	Property	Windows 10	Ubuntu 20.04
1	File Name	20210624 ram windows.raw	ramubuntu20210709.raw
2	Type of file	RAW File (.raw)	RAW File (.raw)
3	Created	2021-06-25 00:17	2021-07-09 17:08
4	Modified	-	-
5	Size	1,99 GB (2.147.418.112 bytes)	5.88 GB (6.316.178.842)

Table 5. Network traffic log has been acquisitioned from Wireshark

No	Property	Windows 10 Log	Ubuntu 20.04 Log
1	File Name	CAPTURE WINDOWS 20210624.pcap	CAPTURE UBUNTU 20210709.pcap
2	Type of file	Pcap	Pcap
3	Created	2021-06-24 10:24	2021-07-09 16:52
4	Modified	-	-
5	Size	34,5 MB (36.257.909 bytes)	6,12 MB (6.422.240 bytes)

4.2 Examination

4.2.1 RAM examination

Examination of the RAM image file as a result of electronic evidence aims to find digital evidence of this research.

On this stage, examination RAM using forensic tools Autopsy, Magnet Axiom and Belkasoft. Examination Network Traffic Log using tools Wireshark dan Networkminer.

Data in RAM is not contained in one file but consists of unallocated files, so the search for evidence in RAM in this study uses a search technique. During the acquisition process, the application or tools may have created an index of terms, which are basic units of a search [40]. Researcher finding evidence based on keywords website in Table 1. Defining keywords website base on Table 1 is done directly and does not include the used protocol (http or https).

Examination towards Windows 10 image RAM by Magnet Axiom got 36 logs exploit-db.com, 9 logs dvwa.co.uk, and 71 logs w3schools.com. Examination to Windows 10 by Autopsy gots 179 logs of exploit-db.com, 118 logs of dvwa.co.uk and 318 logs of w3schools.com. Belkasoft gots 2 logs of exploit-db.com, 25 logs of dvwa.co.uk and 1 log of w3schools.com.

Examination towards Ubuntu 20.04 image RAM by Magnet Axiom got 93 logs exploit-db.com, 29 logs dvwa.co.uk, and 227 logs w3schools.com. Examination to Ubuntu 20.04 by Autopsy got 34 logs exploit-db.com, 32 logs dvwa.co.uk, and 83 logs w3schools.com. Examination to Ubuntu 20.04 by Belkasoft got 7 logs exploit-db.com, 15 logs dvwa.co.uk, and 19 logs w3schools.com.

4.2.2 Network traffic examination

Testing exploit-db.com on Windows and Ubuntu got IP server address 192.124.249.13. The dvwa.co.uk testing on Windows and Ubuntu tests leads to IP server address 185.199.110.153. Testing w3schools.com on Windows 10 shows IP address 66.29.212.110, and on testing using Ubuntu leads to IP address 192.229.179.87 as seen in Table 1. Based on that IP address we will examine Windows 10 network traffic and Ubuntu 20.04 network traffic with Wireshark and Networminer.

Examination towards Windows 10 network traffic log by Wireshark got 186 logs exploit-db.com, 212 logs dvwa.co.uk, and 24 logs w3schools.com. Examination to Windows 10 network traffic log by Networkminer got 30 logs exploit-db.com, 33 logs dvwa.co.uk, and 88 logs w3schools.com.

Examination towards Ubuntu 20.04 network traffic log by Wireshark got 589 logs exploit-db.com, 486 logs dvwa.co.uk, and 323 logs w3schools.com. Examination to Ubuntu 20.04 network traffic log by Networkminer got 29 logs exploit-db.com, 30 logs dvwa.co.uk, and 82 logs w3schools.com. For simplicity, the website log evidence is presented in tables. To minimize the amount of these tables, the number website log found for each item of the pre-defined browsing website (Table 1) is not given individually for each location. The result of website log found by each RAM forensics tools and network traffic log shown in Table 6.

Table 6. Number of RAM data extraction log

Website	exploit-db.com		dvwa.co.uk		w3schools.com	
Operating System	⊞	◉	⊞	◉	⊞	◉
Autopsy	179	34	118	32	318	83
Magnet Axiom	95	93	59	29	302	227
Belkasoft	2	7	25	15	1	19
Wireshark	186	589	212	486	24	323
NetworkMiner	30	29	33	30	88	82

4.3 Analyze

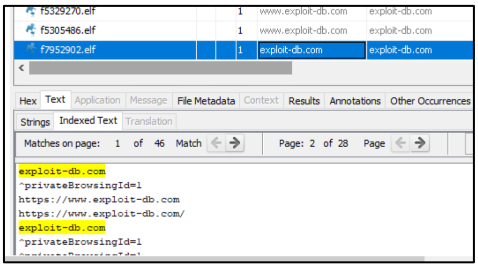
4.3.1 RAM analyze

All logs found at the examination stage must be analyzed in detail. This is to ensure that the log is correct. This analysis stage provides several screenshots of the analysis of the logs retrieved.

Figure 5 shows founded of exploit-db.com by Autopsy tools. The upper half of Figure 5 contained list of unallocated files founded by Autopsy tools and the second half of the figure contains founded evidence for exploit-db.com in an unallocated files. Autopsy founded evidence ^privateBrowsingId=1, this evidence also can be additional information this browsing activity is private browsing [41].

List of unallocated files

Founded evidence for exploit-db.com in an unllocated files

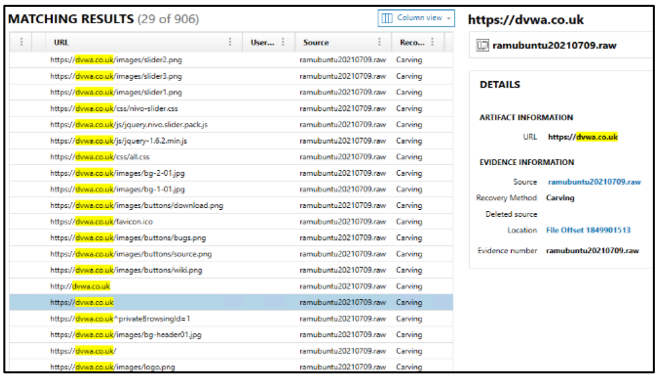


f5329270.elf	1	www.exploit-db.com	exploit-db.com
f5305486.elf	1	www.exploit-db.com	exploit-db.com
f7952902.elf	1	exploit-db.com	exploit-db.com

```
exploit-db.com
^privateBrowsingId=1
https://www.exploit-db.com
https://www.exploit-db.com/
exploit-db.com
^privateBrowsingId=1
```

Figure 5. Exploit-db.com digital evidence by Autopsy in Ubuntu

Magnet Axiom tools got 9 evidence website tested on Windows and also got 29 website tested on Ubuntu (Table 5). Figure 6 shows list of the website dvwa.co.uk found by Ubuntu.



MATCHING RESULTS (29 of 906)

URL	User...	Source	Reco...
https://dvwa.co.uk/images/slider2.png		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/images/slider3.png		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/images/slider1.png		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/css/nivo-slider.css		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/js/jquery.nivo.slider.pack.js		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/js/jquery-1.6.2.min.js		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/css/all.css		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/images/bg-2-01.jpg		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/images/bg-1-01.jpg		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/images/buttons/download.png		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/favicon.ico		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/images/buttons/bugs.png		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/images/buttons/source.png		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/images/buttons/wiki.png		ramubuntu20210709.raw	Carving
http://dvwa.co.uk		ramubuntu20210709.raw	Carving
https://dvwa.co.uk		ramubuntu20210709.raw	Carving
https://dvwa.co.uk^privateBrowsingId=1		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/images/bg-header01.jpg		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/		ramubuntu20210709.raw	Carving
https://dvwa.co.uk/images/logo.png		ramubuntu20210709.raw	Carving

https://dvwa.co.uk

ramubuntu20210709.raw

DETAILS

ARTIFACT INFORMATION

URL https://dvwa.co.uk

EVIDENCE INFORMATION

Source ramubuntu20210709.raw

Recovery Method Carving

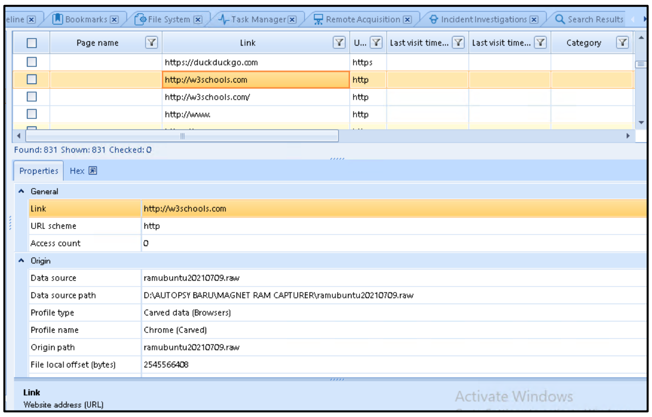
Deleted source

Location File Offset 1849901513

Evidence number ramubuntu20210709.raw

Figure 6. dvwa.co.uk website log by Magnet Axiom in Ubuntu

Belkasoft tools got website log on three websites on the Windows 10 and Ubuntu operating system. Figure 7 shows website log of the w3schools.com website retrieved by Belkasoft on the Ubuntu operating system.



☐	Page name	Link	U...	Last visit time...	Last visit time...	Category
☐		https://duckduckgo.com	https			
☐		http://w3schools.com	http			
☐		http://w3schools.com/	http			
☐		http://www.	http			

Found: 831 Shown: 831 Checked: 0

General

Link	http://w3schools.com
URL scheme	http
Access count	0

Origin

Data source	ramubuntu20210709.raw
Data source path	D:\AUTOPSY BARU\MAGNET RAM CAPTURER\ramubuntu20210709.raw
Profile type	Carved data (Browsers)
Profile name	Chrome (Carved)
Origin path	ramubuntu20210709.raw
File local offset (bytes)	2545566408

Link
Website address (URL)

Figure 7. w3schools.com website log by Belkasoft in Ubuntu

The founded of all website logs in RAM is in line with research by Aggarwal et al. [18] which states that though most of these artifacts are removed from volatile memory after the user exits private mode. This finding is also in line with [40], which states that data in the RAM of a computer that has been used to access an e-mail account several hours earlier can still find e-mail account information even though the web browser has been closed several hours earlier.

Table 7. Network traffic logs on Windows 10

No	Digital Evidence	Wireshark			Networkminer		
		W1	W2	W3	W1	W2	W3
1	Source IP address	Yes	Yes	Yes	Yes	Yes	Yes
2	Destination IP address	Yes	Yes	Yes	Yes	Yes	Yes
3	Protocol	Yes	Yes	Yes	Yes	Yes	Yes
4	Source port	Yes	Yes	Yes	Yes	Yes	Yes
5	Destination port	Yes	Yes	Yes	Yes	Yes	Yes
6	Source MAC address	Yes	Yes	Yes			
7	Destination MAC address	Yes	Yes	Yes	No	Yes	Yes
8	Timestamp	Yes	Yes	Yes	Yes	Yes	Yes
9	Packet length	Yes	Yes	Yes	Yes	Yes	Yes
10	Operating system host client	No	No	No	Yes	Yes	Yes
11	Operating system server	No	No	No	No	No	Yes
12	Hostname server	No	No	No	Yes	Yes	Yes

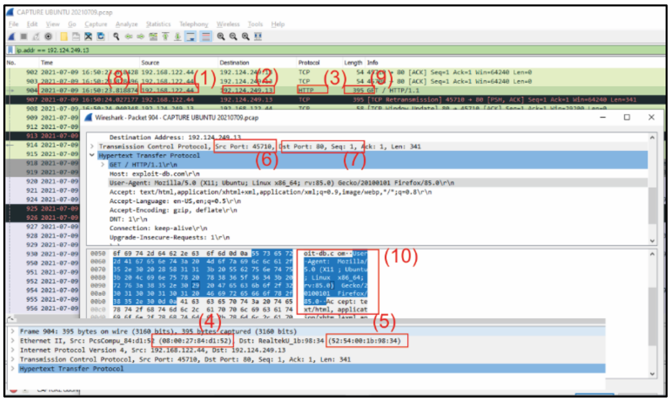
Table 8. Network traffic logs on Ubuntu 20.04

No	Digital Evidence	Wireshark			Networkminer		
		W1	W2	W3	W1	W2	W3
1	Source IP address	Yes	Yes	Yes	Yes	Yes	Yes
2	Destination IP address	Yes	Yes	Yes	Yes	Yes	Yes
3	Protocol	Yes	Yes	Yes	Yes	Yes	Yes
4	Source port	Yes	Yes	Yes	Yes	Yes	Yes
5	Destination port	Yes	Yes	Yes	Yes	Yes	Yes
6	Source MAC address	Yes	Yes	Yes	No	No	No
7	Destination MAC address	Yes	Yes	Yes	Yes	Yes	Yes
8	Timestamp	Yes	Yes	Yes	Yes	Yes	Yes
9	Packet length	Yes	Yes	Yes	Yes	Yes	Yes
10	Operating system host client	Yes	No	No	Yes	Yes	Yes
11	Operating system server	No	No	No	No	No	No
12	Hostname server	No	No	No	Yes	Yes	Yes

4.3.2 Network traffic analyze

Network forensics deals with data that changes from millisecond to millisecond [40]. This research use Wireshark and Networkminer to classify the network traffic log. Wireshark tools and Networkminer tools successfully calssify and got network traffic log on three website tested. Table 7 contains the recapitulation and results of network traffic log from three website on Windows 10 OS. Table 8 contains the recapitulation and results of network traffic log from three website on Ubuntu 20.04 OS.

Figure 8 shows which one of founded network traffic log to exploit-db.com with IP Address 192.124.249.13. Wireshark got entity of, i.e. (1) source IP address, (2) destination IP address, (3) protocol, (4) source port, (5) destination port, (6) timestamp (communication time done), (7) length packet (number of packets transmitted), (8) operating system host client, (9) hostname server and (10) browser client.


CAPTURE UBUNTU 20210709.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 904 · CAPTURE UBUNTU 20210709.pcap
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)

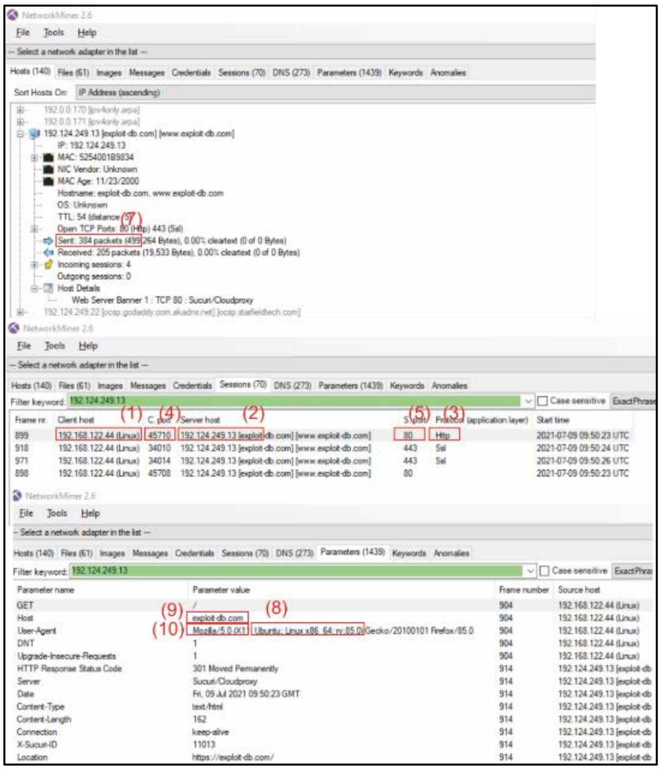
```
ip.addr == 192.124.249.13
No.  Time                           Source          Destination     Protocol Length Info
902 2021-07-09 16:50:23.818428 192.168.122.44  192.124.249.13  TCP      54 45710 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
903 2021-07-09 16:50:23.818496 192.168.122.44  192.124.249.13  TCP      54 45708 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
904 2021-07-09 16:50:23.818874 192.168.122.44  192.124.249.13  HTTP     395 GET / HTTP/1.1
907 2021-07-09 16:50:24.027177 192.168.122.44  192.124.249.13  TCP      395 [TCP Retransmission] 45710 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=341
908 2021-07-09 16:50:24.040348 192.124.249.13  192.168.122.44  TCP      58 [TCP Window Update] 80 → 45710 [ACK] Seq=1 Ack=1 Win=29200 Len=0

  Destination Address: 192.124.249.13
> Transmission Control Protocol, Src Port: 45710, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: exploit-db.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n

0050  6f 69 74 2d 64 62 2e 63  6f 6d 0d 0a 55 73 65 72   oit-db.c om··User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 58 31 31  3b 20 55 62 75 6e 74 75   5.0 (X11 ; Ubuntu
0080  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux  x86_64;
0090  72 76 3a 38 35 2e 30 29  20 47 65 63 6b 6f 2f 32   rv:85.0)  Gecko/2
00a0  30 31 30 30 31 30 31 20  46 69 72 65 66 6f 78 2f   0100101  Firefox/
00b0  38 35 2e 30 0d 0a 41 63  63 65 70 74 3a 20 74 65   85.0··Ac cept: te
00c0  78 74 2f 68 74 6d 6c 2c  61 70 70 6c 69 63 61 74   xt/html, applicat

> Frame 904: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits)
> Ethernet II, Src: PcsCompu_84:d1:52 (08:00:27:84:d1:52), Dst: RealtekU_1b:98:34 (52:54:00:1b:98:34)
> Internet Protocol Version 4, Src: 192.168.122.44, Dst: 192.124.249.13
> Transmission Control Protocol, Src Port: 45710, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
> Hypertext Transfer Protocol
```

Figure 8. Website log exploit-db.co.uk by Wireshark in Ubuntu


NetworkMiner 2.6
File Tools Help
-- Select a network adapter in the list --
Hosts (140) Files (61) Images Messages Credentials Sessions (70) DNS (273) Parameters (1439) Keywords Anomalies
□ Case sensitive
ExactPhrase
(1)
(2)
(3)
(4)
(5)
(7)
(8)
(9)
(10)

```
Sort Hosts On: IP Address (ascending)
192.0.0.170 [ipv4only.arpa]
192.0.0.171 [ipv4only.arpa]
192.124.249.13 [exploit-db.com] [www.exploit-db.com]
    IP: 192.124.249.13
    MAC: 5254001B9834
    NIC Vendor: Unknown
    MAC Age: 11/23/2000
    Hostname: exploit-db.com, www.exploit-db.com
    OS: Unknown
    TTL: 54 (distance: 10)
    Open TCP Ports: 80 (Http) 443 (Ssl)
    Sent: 384 packets (499,264 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 205 packets (19,533 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 4
    Outgoing sessions: 0
    Host Details
        Web Server Banner 1 : TCP 80 : Sucuri/Cloudproxy
192.124.249.22 [ocsp.godaddy.com.akadns.net] [ocsp.starfieldtech.com]
```

Filter keyword: 192.124.249.13

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
899	192.168.122.44 (Linux)	45710	192.124.249.13 [exploit-db.com] [www.exploit-db.com]	80	Http	2021-07-09 09:50:23 UTC
918	192.168.122.44 (Linux)	34010	192.124.249.13 [exploit-db.com] [www.exploit-db.com]	443	Ssl	2021-07-09 09:50:24 UTC
971	192.168.122.44 (Linux)	34014	192.124.249.13 [exploit-db.com] [www.exploit-db.com]	443	Ssl	2021-07-09 09:50:26 UTC
898	192.168.122.44 (Linux)	45708	192.124.249.13 [exploit-db.com] [www.exploit-db.com]	80		2021-07-09 09:50:23 UTC

Filter keyword: 192.124.249.13

Parameter name	Parameter value	Frame number	Source host
GET	/	904	192.168.122.44 (Linux)
Host	exploit-db.com	904	192.168.122.44 (Linux)
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0	904	192.168.122.44 (Linux)
DNT	1	904	192.168.122.44 (Linux)
Upgrade-Insecure-Requests	1	904	192.168.122.44 (Linux)
HTTP Response Status Code	301 Moved Permanently	914	192.124.249.13 [exploit-db
Server	Sucuri/Cloudproxy	914	192.124.249.13 [exploit-db
Date	Fri, 09 Jul 2021 09:50:23 GMT	914	192.124.249.13 [exploit-db
Content-Type	text/html	914	192.124.249.13 [exploit-db
Content-Length	162	914	192.124.249.13 [exploit-db
Connection	keep-alive	914	192.124.249.13 [exploit-db
X-Sucuri-ID	11013	914	192.124.249.13 [exploit-db
Location	https://exploit-db.com/	914	192.124.249.13 [exploit-db

Figure 9. Digital evidence exploit-db.co.uk by Networkminer in Ubuntu

Figure 9 shows which one of founded digital network traffic log retrieved by Network miner to website exploit-db.com. The entity of traffic log found by Networminer is (1) source IP address, (2) destination IP address, (3) protocol, (4) source port, (5) destination port, (6) timestamp, (7) length packet (number of packets transmitted), (8) operating system host client, (9) hostname server and (10) browser client.

4.4 Reporting

Evidence of Information on Table 5, Table 6 and Table 7 shows that there is visitation activity on websites dvwa.co.uk, exploit-db.com, and w3schools.com performed using Windows 10 and Ubuntu 20.04 through network traffic logs analysis. The results of this investigation are used as evidence for a court case. Measurements of investigative success in these experiments were determined based on the ability to find digital evidence data due to misuse of private-mode web browsers.

All test website logs are found in RAM Analysis. Network traffic analysis is also able to obtain (1) source IP address, (2) destination IP address, (3) protocol, (4) source port, (5) destination port, (6) timestamp (communication time done), (7) packet length (number of packets transmitted), (8) operating system host client, (9) server hostname and (10) browser client. This finding is expected to be able to become evidence in the judicial process.

In addition, the authors simulate digital forensic investigations using commonly available tools for law enforcement. Although this research focuses on finding website logs and does not focus on the success percentage of a tool, the parallel data acquisition method is capable of retrieving website log data in RAM and network traffic log entities.

For law enforcement or investigators involved in conducting digital forensic investigations, devices play an important role in investigations. Based on the evidence of this research, on Windows 10 and Ubuntu 20.04 all website logs can be found using the Magnet Axiom, Autopsy and Belkasoft tools.

Based on this paper and the current body of literature, it appears that no browser is highly effective in protecting user privacy and preventing artifacts/logs recovery [28, 42-44].

5. CONCLUSIONS

Investigator Digital forensics is tasked with finding evidence/artefacts left behind by evidence tools to explore a case and looking for other parties involved in a type of crime. At the same time, a private mode web browser seeks to eliminate digital traces left behind from browsing activities carried out by users. Live forensic analysis with parallel data acquisition managed to obtain identic evidence on the use of private browsers. This study analyzes the effectiveness of the "private" mode of Mozilla Firefox which is widely used on Windows 10 and Ubuntu 20.04, yielding many findings in RAM and network traffic. Dedicated computer forensic investigators are able to recover many forensic trace artifacts using effective forensic tools and techniques.

This study uses the private browsing feature in standard browsers, does not involve browsers that have been enhanced in terms of privacy and security. Future research should be able to explore private browsing performance on privacy-enhanced browsers.

REFERENCES

[1] Mahaju, S., Atkison, T. (2017). Evaluation of firefox browser forensics tools. In Proceedings of the SouthEast Conference, pp. 5-12. https://doi.org/10.1145/3077286.3077310

[2] Saverimoutou, A., Mathieu, B., Vaton, S. (2019). A 6-month analysis of factors impacting web browsing quality for QoE prediction. Computer Networks, 164: 106905. https://doi.org/10.1016/j.comnet.2019.106905

[3] APJII, Buletin APJII Edisi-40 2019, Buletin APJII, Jakarta, p. 6, May 2019. https://apjii.or.id/survei.

[4] Shafqat, N. (2016). Forensic investigation of user's web activity on Google Chrome using various forensic tools. IJCSNS International Journal of Computer Science and Network Security, 16(9): 123-132.

[5] Perumal, S., Norwawi, N.M. (2010). Integrated computer forensic investigation model based on Malaysian standards. International Journal of Electronic Security and Digital Forensics, 3(2): 108-119. https://doi.org/10.1504/IJESDF.2010.03378

[6] Umar, R., Yudhana, A., Faiz, M.N. (2018). Experimental analysis of web browser sessions using live forensics method. International Journal of Electrical and Computer Engineering (IJECE), 8(5): 2951-2958. https://doi.org/10.11591/ijece.v8i5.pp.2951-2958

[7] Adelstein, F. (2006). Live forensics: Diagnosing your system without killing it first. Communications of the ACM, 49(2): 63-66. https://doi.org/10.1145/1113034.1113070

[8] Umar, R., Yudhana, A., Faiz, M.N. (2016). Analisis kinerja metode live forensics untuk investigasi random access memory pada sistem proprietary. Prosiding Konferensi Nasional Ke-4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM), 207-211.

[9] Faiz, M.N., Umar, R., Yudhana, A. (2016). Analisis live forensics untuk perbandingan kemananan email pada sistem operasi proprietary. ILKOM Jurnal Ilmiah, 8(3): 242-247. https://doi.org/10.33096/ilkom.v8i3.79.242-247

[10] Suma, G.S., Dija, S., Pillai, A.T. (2017). Forensic analysis of google chrome cache files. In 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, India, pp. 1-5. https://doi.org/10.1109/ICCIC.2017.8524272

[11] Chan, E., Venkataraman, S., David, F., Chaugule, A., Campbell, R. (2010). Forenscope: A framework for live forensics. In Proceedings of the 26th Annual Computer Security Applications Conference, pp. 307-316. https://doi.org/10.1145/1920261.1920307

[12] Cheng, Y., Fu, X., Du, X., Luo, B., Guizani, M. (2017). A lightweight live memory forensic approach based on hardware virtualization. Information Sciences, 379: 23-41. https://doi.org/10.1016/j.ins.2016.07.019

[13] Google, Browse in private, 2020. https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DDesktop&hl=en&oco=0, accessed on Mar. 17, 2020.

[14] Firefox, M. Private Browsing - Use Firefox without saving history, 2020. https://support.mozilla.org/en-

US/kb/private-browsing-use-firefox-without-history, accessed on Mar. 17, 2020.

[15] Microsoft, Browse InPrivate in Microsoft Edge, 2020. https://support.microsoft.com/en-us/help/4026200/microsoft-edge-browse-inprivate, accessed on Mar. 17, 2020.

[16] Apple, Menelusuri secara pribadi di Safari di Mac, 2020. https://support.apple.com/id-id/guide/safari/ibrw1069/mac, accessed on Mar. 17, 2020.

[17] Pereira, M.T. (2009). Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records. Digital Investigation, 5(3-4): 93-103. https://doi.org/10.1016/j.diin.2009.01.003

[18] Aggarwal, G., Bursztein, E., Jackson, C., Boneh, D. (2010). An analysis of private browsing modes in modern browsers. In USENIX Security Symposium, pp. 79-94.

[19] Ohana, D.J., Shashidhar, N. (2013). Do private and portable web browsers leave incriminating evidence? a forensic analysis of residual artifacts from private and portable web browsing sessions. EURASIP Journal on Information Security, 2013: 6. https://doi.org/10.1186/1687-417X-2013-6

[20] Rathod, D. (2017). Web browser forensics: Google chrome. International Journal of Advanced Research in Computer Science, 8(7): 896-899. https://doi.org/10.26483/ijarcs.v8i7.4433

[21] Fernández-Fuentes, X., Pena, T.F., Cabaleiro, J.C. (2022). Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux as a case study. Computers & Security, 115: 102626. https://doi.org/10.1016/j.cose.2022.102626

[22] Nalawade, A., Bharne, S., Mane, V. (2016). Forensic analysis and evidence collection for web browser activity. In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, India, pp. 518-522. https://doi.org/10.1109/ICACDOT.2016.7877639

[23] Yudhana, A., Riadi, I., Zuhriyanto, I. (2019). Analisis live forensics aplikasi media sosial pada browser menggunakan metode digital forensics research workshop (DFRWS). Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto), 20(2): 125-130. http://dx.doi.org/10.30595/techno.v20i2.4594

[24] Rochmadi, T., Riadi, I., Prayudi, Y. (2017). Live forensics for anti-forensics analysis on private portable web browser. International Journal of Computer Applications, 164(8): 31-37. https://doi.org/10.5120/ijca2017913717

[25] Davies, S.R., Macfarlane, R., Buchanan, W.J. (2020). Evaluation of live forensic techniques in ransomware attack mitigation. Forensic Science International: Digital Investigation, 33: 300979. https://doi.org/10.1016/j.fsidi.2020.300979

[26] Rochmadi, T. (2019). Live forensik untuk analisa anti forensik pada web browser studi kasus browzar. Indonesian Journal of Business Intelligence (IJUBI), 1(1): 32-38. http://dx.doi.org/10.21927/ijubi.v1i1.878

[27] Oh, J., Lee, S., Lee, S. (2011). Advanced evidence collection and analysis of web browser activity. Digital Investigation, 8: S62-S70. https://doi.org/10.1016/j.diin.2011.05.008

[28] Said, H., Al Mutawa, N., Al Awadhi, I., Guimaraes, M. (2011). Forensic analysis of private browsing artifacts. In 2011 International Conference on Innovations in Information Technology, Abu Dhabi, United Arab Emirates, pp. 197-202. https://doi.org/10.1109/INNOVATIONS.2011.5893816

[29] Patil, D.N., Meshram, B.B. (2019). Web browser analysis for detecting user activities. In Recent Findings in Intelligent Computing Techniques: Proceedings of the 5th ICACNI 2017, Volume 1 (pp. 279-291). Springer Singapore. https://doi.org/10.1007/978-981-10-8639-7_29

[30] Dija, S., Indu, V., Sajeena, A., Vidhya, J.A. (2017). A framework for browser forensics in live windows systems. In 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, India, pp. 1-5. https://doi.org/10.1109/ICCIC.2017.8524412

[31] Yudhana, A., Riadi, I., Ridho, F. (2018). DDoS classification using neural network and naïve bayes methods for network forensics. International Journal of Advanced Computer Science and Applications, 9(11). https://doi.org/10.14569/ijacsa.2018.091125

[32] Riadi, I., Umar, R., Sugandi, A. (2020). Web forensic on kubernetes cluster services using grr rapid response framework. International Journal of Scientific & Technology Research, 9(1): 3484-3488. https://doi.org/10.15294/sji.v7i1.18299

[33] Yudhana, A., Sulistyo, D., Mufandi, I. (2021). GIS-based and Naïve Bayes for nitrogen soil mapping in Lendah, Indonesia. Sensing and Bio-Sensing Research, 33: 100435. https://doi.org/10.1016/j.sbsr.2021.100435

[34] Yudhana, A., Mukhopadhyay, S., Prima, O.D.A., Akbar, S.A., Nuraisyah, F., Mufandi, I., Fauzi, K.H., Nasyah, N.A. (2021). Multi sensor application-based for measuring the quality of human urine on first-void urine. Sensing and Bio-Sensing Research, 34: 100461. https://doi.org/10.1016/j.sbsr.2021.100461

[35] Yudhana, A., Rahmawan, J., Negara, C.U.P. (2018). Flex sensors and MPU6050 sensors responses on smart glove for sign language translation. In IOP Conference Series: Materials Science and Engineering, 403(1): 012032. https://doi.org/10.1088/1757-899x/403/1/012032

[36] Yudhana, A., Mukhopadhyay, S., Karas, I.R., Azhari, A., Mardhia, M.M., Akbar, S.A., Muslim, A., Ammatulloh, F.I. (2019). Recognizing human emotion patterns by applying Fast Fourier Transform based on brainwave features. In 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia, pp. 249-254. https://doi.org/10.1109/ICIMCIS48181.2019.8985227

[37] Umar, R., Riadi, I., Muthohirin, B.F. (2019). Live forensics of tools on android devices for email forensics. TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(4): 1803-1809. http://doi.org/10.12928/telkomnika.v17i4.11748

[38] Neumann, J.C. (2015). The Book of GNS3: Build Virtual Network Labs Using Cisco, Juniper, and More. No Starch Press.

[39] Agarwal, A., Rao, S.K.S., Mahendra, B.M. (2020). Comprehensive review of virtualization tools. International Research Journal of Engineering and Technology (IRJET), 7(6): 4394-4397.

[40] Volonino, L., Anzaldua, R. (2008). Computer Forensics for Dummies. New Jersey: Wiley Publishing.

[41] Cheta, G. privateBrowsingId is added to the link in Settings - Autoplay in Preferences. Bugzilla, 2019. https://bugzilla.mozilla.org/show_bug.cgi?id=1601256, accessed on Oct. 8, 2022.

[42] Gabet, R.M., Seigfried-Spellar, K.C., Rogers, M.K. (2018). A comparative forensic analysis of privacy enhanced web browsers and private browsing modes of common web browsers. International Journal of Electronic Security and Digital Forensics, 10(4): 356-371. https://doi.org/10.1504/IJESDF.2018.095126

[43] Noorulla, E.S. (2014). Web Browser Private Mode Forensics Analysis. Rochester Institute of Technology.

[44] Marrington, A., Baggili, I., Al Ismail, T., Al Kaf, A. (2012). Portable web browser forensics. In International Conference on Computer Systems and Industrial Informatics, Sharjah, United Arab Emirates, pp. 1-6. https://doi.org/10.1109/ICCSII.2012.6454516