**International Journal of Electrical and Computer Engineering (IJECE)**
Vol. 8, No. 5, October 2018, pp. 2951~2958
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i5.pp2951-2958 

# Experimental Analysis of Web Browser Sessions Using Live Forensics Method

**Rusydi Umar[1], Anton Yudhana[2], Muhammad Nur Faiz[3]**
[1]Department of Informatics Engineering, Universitas Ahmad Dahlan, Indonesia
[2]Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia
[3]Department of Information Technology, Universitas Ahmad Dahlan, Indonesia

**Article Info**

***Article history:***

Received Oct 20, 2017
Revised Jan 29, 2018
Accepted Sep 12, 2018

***Keyword:***

Investigation
Live forensics
RAM
Sessions
Web browser

**ABSTRACT**

In today's digital era almost every aspect of life requires the internet, one way to access the internet is through a web browser. For security reasons, one developed is private mode. Unfortunately, some users using this feature do it for cybercrime. The use of this feature is to minimize the discovery of digital evidence. The standard investigative techniques of NIST need to be developed to uncover an ever-varied cybercrime. Live Forensics is an investigative development model for obtaining evidence of computer usage. This research provides a solution in forensic investigation effectively and efficiently by using live forensics. This paper proposes a framework for web browser analysis. Live Forensics allows investigators to obtain data from RAM that contains computer usage sessions.



***Corresponding Author:***

Muhammad Nur Faiz,
Department of Information Technology,
Universitas Ahmad Dahlan,
Jl. Prof. Dr. Soepomo, Janturan, Yogyakarta, 55164, Indonesia.
Email: hafarafaiz@gmail.com

## 1. INTRODUCTION

At the beginning of the creation Internet, various applications were created including social networks and "worm" programs, as well as Viruses [1]. Web browser is an application to access the Internet. Web browser allows users to search information, do email transactions, to communicate with instant messenger or social network, shop via e-commerce website [2]. Commonly used web browsers, including Mozilla Firefox, Google Chrome, Opera and Apple Safari offer portable browsers that can be launched from removable devices. When removable devices are released, it is believed that traces of browsing activity will be erased, so a personal portable version of the web browser offers better privacy [3]. Use of web browsers worldwide by [4] shown in Figure 1.

Web browser features are always evolving which impact on user privacy including feature options to surf the Internet in-privately. this feature is also tasked with removing the information at the end of the session [2]. The forensics artefacts left by the web browser after the end of this session is not just a list of web visits, cookies, and downloads. These artefacts also contain the sites the user visits, the time and frequency of access, and also the search engine keywords used. When conducting a digital investigation of a system, investigators may collect evidence of the artefacts [5] [6]. Portable web browsers, web browsers tend to store large amounts of data about user surfing activities, username keywords, downloads, temp files, cache, form data and other browser-specific data on the user's hard disk. Based on this, the forensics examiner can collect artefacts to reconstruct the user's web activity time. Forensics tools web browser are the best source for forensics experts to find artefacts from web browsers if there are allegations regarding illegal Internet activity [7]. The role of artefacts (e.g. metadata) in forensics analysis is the loss of artefacts when

data are collected. If metadata (e.g., date of creation/modification of a file, and records of user ownership) is lost during the collection process. This affects the researcher's ability to conduct a forensics investigation of the standards required by the court [8].

Web browser the suspect uses may be used to search for evidence left behind by the suspect including all activities he or she hides. Such digital forensics investigation should be able to search for evidence left behind from web browsing activity as this is an important evidence includes email, Facebook and etc.The average number of email receipts per day is over 20 so email handling is now a hurdle for users including investigators in search of digital evidence [9]. The investigator is worthy of learning the evidence of the web browser used by the suspect including the websites visited, the time and frequency of access, and the search engine keywords used by the suspect after recovering data such as cache, history, cookies, and download lists of suspect computers [10].

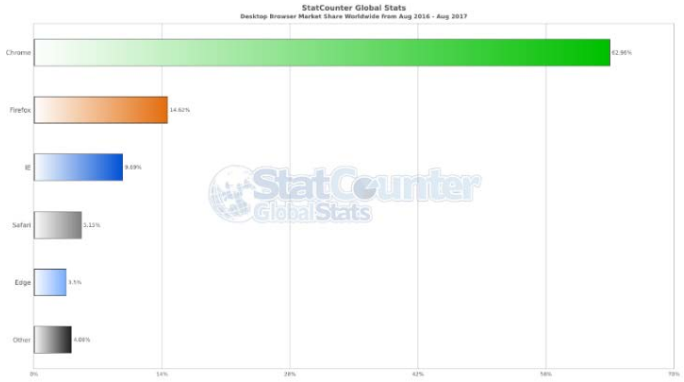


Figure 1. Browsers market share worldwide

Web browsersforensics are widely used in finding digital evidence due to the growing number of crimes on the internet. Analysis on web browsers is helpful in reconstructing user or performer explorations behaviour. an anomalous internet user can be detected from information found during an investigation. An ever-evolving web browser must also be supported by digital forensics investigators to perform forensics analysis. Areas that have been identified in search evidence such as web visits, cache, cookies and the registry.Web browsers are generally used to store data, what information can be recovered or analyzed and how different operating systems store the records. In addition, an application is introduced which can be used by experts to perform analysis in this field. Thus, put forward which data will be obtained and analyzed by digital forensics experts [11] [7]. Web browser such as Safari, Chrome, Mozilla Firefox and Internet Explorer regarding related secret usage activities. Chrome mode in-privateleaves no trace on the local system and is the safest [12].

Investigation on web browser of computer also known digital forensics.Generally, digital forensics is divided into two techniques, live forensics and static forensics. The forensics live method is a method that requires a running state of the computer where all data goes through Random Access Memory (RAM). Data running on the computer is volatile data [13]. The quality of collected data has an impact on the investigation process. The quality of the copied data contains complete information such as access to information and time [14]. Some of the information that can be found in RAM also depends on the operating system it uses [15].

Live forensics can be performed if the system on the computer does not die because almost all of the system usage is stored in RAM, Page files, hibernation files and dump crash files [16] [17]. Information that can be found on RAM such as running processes, information about executable files, Registry Key, information about network activity, drivers used, user logins, passwords and cryptographic keys, hidden processes and data, malware, temporary data, portable applications Application Which is not installed on the computer itself but only runs), DLL and many other important information [18]. The important purpose of data analysis on RAM is to know the location of the data. RAM as traffic All data running, using internet network, copying or moving files, opening files on hard drive or deleting them all recorded on RAM. The difference between RAM and hard disk is that RAM records everything that happens at runtime and certain condition whereas hard disk only provides general information data. This is very important because there is only a large amount of data and never listed on the hard disk is internet data [19]. Data stored in RAM is data that is easy to change because data can not be recovered after the user turns off the computer [20]

.Investigators should distinguish tools that can only collect data and analyse them. There is a toolkit from the market that allows collecting digital evidence from computers such as RAM and DISK [21].

Several researchers have developed and proposed a new framework for identifying activities and improving forensics investigation steps with the aim of finding digital evidence [22]. A structured approach model that aims to identify activities and help improve the process of inquiry. Different models then also have different phases. This new model has also been compared with the Systematic Digital Forensics Investigation Model (SDFIM), Integrated Digital Investigation Process (IDIP), etc. This new model divides the process of inquiry into four levels by phase [23]. Digital forensics process for smartphones can be divided into four distinct, they are collection, preservation, analysis and presentation [24]. According to the NIST, the model of investigation in digital forensics consists of four main stages: Collection, Examination, Analysis, and Reporting [22].

This research examines the web browser of private mode on Google Chrome and Mozilla Firefox usinglive forensics method.The proposed live forensics method is a development of the NIST investigation. This method captures the memory directly after a browsing session and then analyzes the captured memory that searches for forensicsartefacts in memory. The experiments are done in both web browsers, by removing web browser history. The results show that with volatile forensics we can pick up valuable information on private browsing.

## 2. RESEARCH METHOD

This research uses digital forensics investigation basedstep from NIST with live forensics method to obtain data on the state of live media presented in Figure 1. The problems that exist in the process of RAM investigation, especially related to the process of data acquisition on running computer, the method used to perform the data acquisition process, as well as the background of the problem behind live forensics methods, so that it can support ultimate purpose of doing this research.

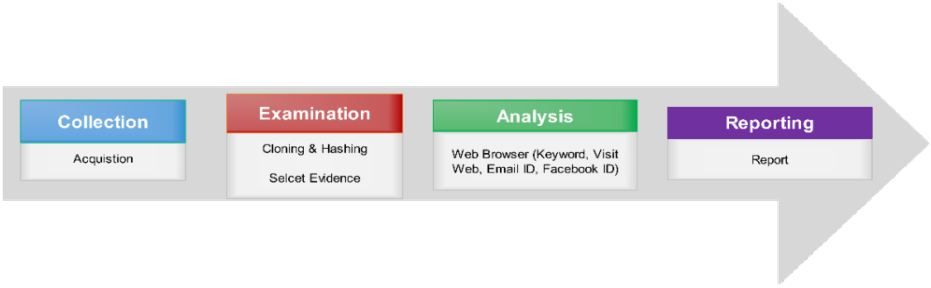


Figure 1. Live forensics method

The prep system is built to simulate the use of web browsers from the offender side using the operating system Windows 10-64bit, VirtualMachine (VMware) version 5.1.28 r117968, RAM 1Gb, Google Chrome version 5.1.28 r117968 and Mozilla Firefox version 56.0.1. The Experiment simulations are made as shown in Figure 2.

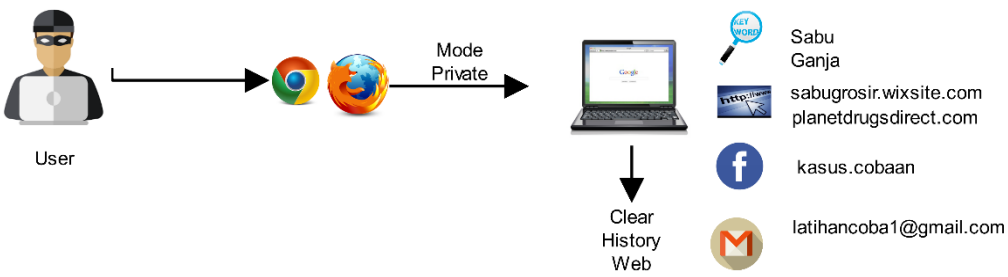


Figure 2. Experiment simulation

This Experiment simulation is an example of a web browser abuse for drug stores. The investigator must obtain potential digital evidence when the media used by the offender is on. The perpetrator trades with the web browser and the police performs a hand-held operation. Investigators find the media used by the perpetrator is still on and done data acquisition on the perpetrator's media. The investigator must find digital evidence relating to search keywords, facebook id, email id and website visits that the perpetrator has done.

An investigation is done after the investigator obtains the acquisition data from RAM on the perpetrator's media then copies the original evidence and hashing to compare the original evidence and the copy evidence that must exactly match each bit. investigators make acquisitions with DumpIt and programs for cloning and hashing of original evidencebased Delphi. The parameters of this investigation that investigators can uncover the search keywords, email id, Facebook id, web visits that have been perpetrators during the media used the offender by developing a digital forensics investigation of NIST which has 4 stages, including:

a. Collection: identification of potential data sources is done to obtain data, acquisition data on running computer.
b. Examination: stage is performed after the data is collected, the examination stage involves the assessment and extracting relevant pieces of information from the data collected. This stage includes the security of original evidence with cloning and hashing for data integrity. After the evidence is equal to the original evidence then the investigator selects the data to be sought as evidence. Text and pattern search can be used to identify relevant data, such as finding web visits based on keywords, email and Facebook ID used.
c. Analysis: process analysis to draw conclusions from predetermined information. The foundation for forensics results uses a methodological approach to reach appropriate conclusions based on data. The analysis should include the identification of user and how are linked so that conclusions can be reached.
d. Reporting: process of preparing and presenting the information resulting from the analysis phase. Factors affecting reporting include alternative explanations, participant considerations, actionable information.

## 3. RESULTS AND ANALYSIS

The live forensics method includes 4 main steps. The first step is the process of acquisition of RAM on laptops used by users, this acquisition is very important because in addition to keeping the laptop used by users will remain clean other than that the user's laptop is also prone to contaminated data. This step can also be called a live acquisition, this step is depicted in Figure 3. The second step is the process of inspection and securing evidence. This process includes selecting what will be analyzed, cloning original evidence and hashing proof of copy also original proof, cloning to duplicate original proof and hashing to prove that the copied evidence and original proof are the same every bit of it. The third step is analysis, this analysis is based on what has been obtained on examination. Things that are studied are keywords, web visits, email account username and facebook. The final step is reporting, reporting everything that has been found. The live process of data acquisition is shown in Figure 3. The process can be done by using software or application. Here are the steps how to get data in RAM.

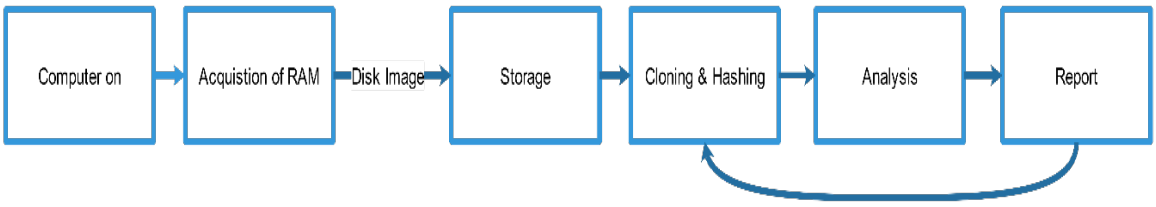


Figure 3. Live acquisition process

Figure 3 is a process of flow for acquisition where the computer still on. Investigators make direct acquisitions on the computer with DumpItand stored on the investigator's storage media. The file generated from the acquisition process in this RAM is *.raw (unprocessed computer data) then the file is copied/cloned because the original evidence should not be analyzed. Investigators do hash to prove that data integrity is the same, then the file is analyzed to look for evidence such as keywords, web visit, email ID and Facebook ID. The last is to report any evidence found in accordance with the incident.

Process of acquisition data on RAM required the best tools for acquisition because when the laptop turns data on RAM will quickly change. The Internet network is disconnected to reduce data on the RAM to be acquired so that it will be exactly the same as the first evidence found. The created image file is saved with the name of the DESKTOP-M57T049-20171010-214020.raw, this process shown in Figure 4.

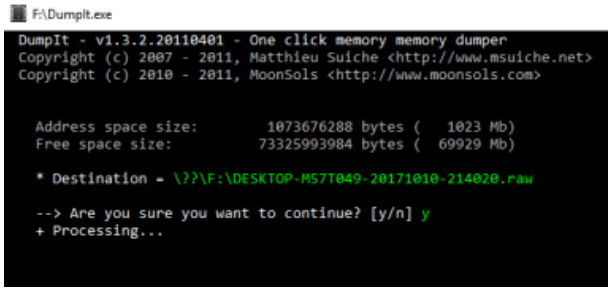


Figure 4. Acquisition ofData on RAM

Research in [25] and [6] The research (Gianni and Solinas 2013) and (Alam, Aziz, and Iqbal 2016) did not discuss how to acquire and secure evidence. In this research, there is a process of how to acquire data with the DumpIt application. Research [11] examines the tools-tools used in search evidence on a web browser.Based on Figure 4, obtained from the acquisition of the suspect laptop, the capacity of the acquisition result is 1023 Mb. This is influenced by the capacity of RAM on a suspect laptop. This DumpIt tool runs on the Command line so it does not leave any artefacts on RAM.The data that has been acquired must be immediately secured by the investigator. Process of cloning and hashing data with Delphi, both of these processes are performed on a single Delphi based application development tool. This application to launch investigators in the investigation processespecially for the clone and hash process, the application there is a source column file and the source of the cloning. Hashing columns contain hashing MD5, SHA1, SHA256 from source and cloned. The investigator must understand the procedure of handling the original evidence because the original evidence should not be used for the analysis process, it must be cloned and hash.

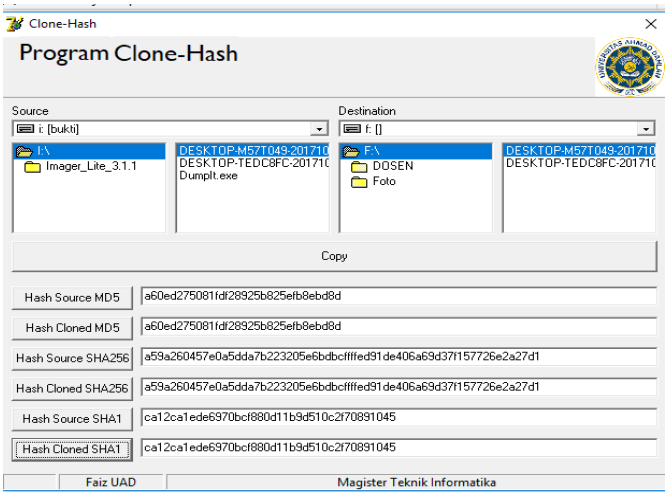


Figure 5. Cloning and hashing evidence

Figure 5 is a process of cloning and hashing. Clone-Hash program based on Delphi for security evidence, shown the result of an acquisition of Ram is DESKTOP-M57T049-20171010-214020 same as a result of cloning. The MD5 hash results for both original and cloned evidence are a60ed275081fdf28925b825efb8ebd8d, the results are matched on SHA256 and SHA1 too so that the original evidence and clone evidence proved to be exactly the same.In the research [25], [2] did not examine clone

and hash processes, this study complements the clone and hash processes as this process is an important stage for verification in the court. Figure 6 shows the use of ganja and sabu keywords in experiments performed, all keywords recorded in RAM. Meanwhile, the web visit found for digital evidence is planetdrugsdirect.com shown in Figure 7. Figure 8 shows the Facebook id and Email id found based on experiments performed, Facebook id used Experiment while for Email id is latihancoba1@gmail.com.

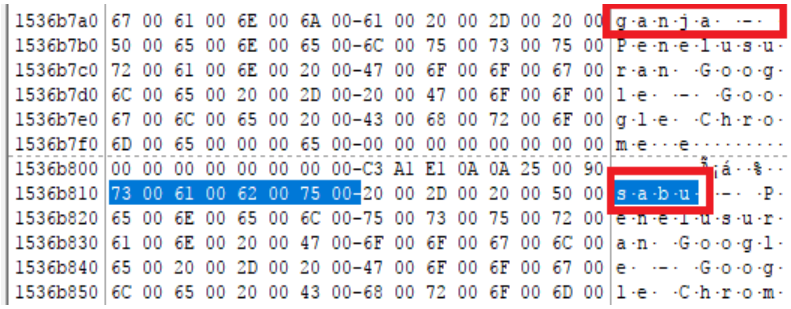


Figure 6. Keyword Evidence Found

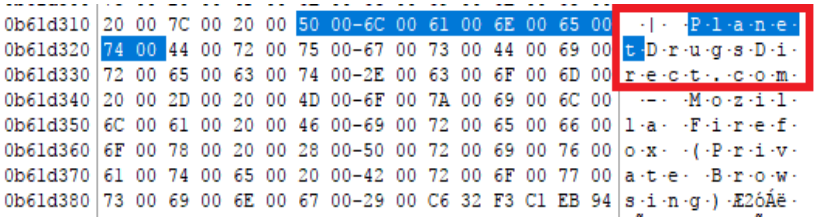


Figure 7. Web Visit Evidence Found

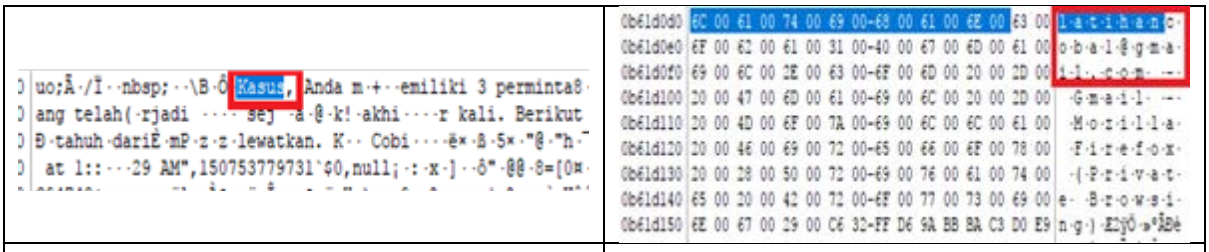


Figure 8. Facebook id and Email ID Evidence Found

The Experiment simulation is done using the web browser of Google Chrome and Mozilla Firefox in private mode, after obtaining the result of acquisition with DumpIt on storage media then cloning and checking the hash value on the original file and the cloning result match. Further analysis of the use of the web browser during the computer is on. The analysis process with live forensics method is done by looking for evidence such as search keywords, web visit, email ID and Facebook ID from both browsers presented in Table 1 as follows:

Table 1. Results of Evidence

| Evidence | Google Chrome | Mozilla Firefox |
|---|---|---|
| Keywords | √ | √ |
| Web Visit | √ | √ |
| Email ID | √ | √ |
| Facebook ID | √ | √ |

The results of the investigation using the live forensics method can be seen in Table 1. The results of this investigation can be demonstrated in court evidence. Facebook ID on both web browsers is hard to find, just first name. Verification of data digital evidence findings in the process of data acquisition directly can be done with the percentage of success in the process of live forensics investigation method is 100%. The success of the investigation in Experiment of abuse of this web browser is able to find the data of digital evidence, keywords, web visit, username Email and Facebook. The evidence can be used to minimize the misuse of web browsers for criminal acts and web browser users become more understanding and careful in using web browsers.

Research [25] which reviewed username email yahoo, Gmail, Hotmail and facebook chat in normal mode and private browsing. Research [7] discusses the cache on web visits, downloads, number of visits during the visit. Research [6] examines keywords, URL visits, email users on Microsoft Edge and private mode. This study examines search keywords, web visits, email ID and Facebook ID used by user using the web browser Google Chrome and Mozilla Firefox

## 4. CONCLUSION

The results of this study contribute to complement previous research in terms of terms reviewed, web browsers and proposed methods. The proposed live forensics framework is used to experimentally test the Firefox and Incognito browser privacy features when used in private mode. It was found that through forensic memory it is possible to retrieve valuable information about suspect activities, such as websites visited, keywords on the Internet, traces of email and facebook id even after the browser is closed and clear history. This artifact is enough to be the link between the data and the suspect. Experiments show that Vendor's claim to privacy can be reversed through live forensics. In other words, the browser vendor's privacy claim is not true. If they want to convey the privacy they need to modify their browser. Among browsers under this experiment, there is no difference between the two browsers. This method is a development of the NIST investigation and was successful in obtaining previously designed evidence. This method is expected to be able to get other digital evidence related to web browsers or it might be developed for mobile forensics.

## REFERENCES

[1] J. Alvarez-Cedillo, E. Acosta-Gonzaga, M. Aguilar-Fernández, and P. Pérez-Romero, "Internet prospective study", *Bull. Electr. Eng. Informatics*, vol. 6, no. 3, pp. 235–240, 2017.
[2] D. Dharan and N. Meeran, "Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser", *IJCA*, vol. 91, no. 4, pp. 32–35, 2014.
[3] A. Ghafarian and S. A. H. Seno, "Forensics Evaluation of Privacy of Portable Web Browsers", *IJCA*, vol. 147, no. 8, pp. 5–11, 2016.
[4] StatCounter Global Stats, "Browser Market Share Worldwide", *Stat Counter Global Stats*, 2017. [Online]. Available: http://gs.statcounter.com.
[5] J. Oh, S. Lee, and S. Lee, "Advanced Evidence Collection and Analysis of Web Browser Activity", *Digit. Investig.*, vol. 8, pp. 63–70, 2011.
[6] S. Alam, M. A. Aziz, and W. Iqbal, "Forensic Analysis of Edge Browser In-Private Mode", *IJCSIS*, vol. 14, no. 9, pp. 256–263, 2016.
[7] N. Shafqat, "Forensic Investigation of User ' s Web Activity on Google Chrome using various Forensic Tools", *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 9, pp. 123–132, 2016.
[8] N. Widiyasono, I. Riadi, and A. Luthfi, "Investigation on the Services of Private Cloud Computing by Using ADAM Method", *Int. J. Electr. Comput. Eng.*, vol. 6, no. 5, pp. 2387–2395, 2016.
[9] T. Suma and S. Y. S. Kumara, "Email Classification Using Adaptive Ontologies Learning", *TELKOMNIKA*, vol. 14, no. 4, pp. 2102–2106, 2017.
[10] A. Nalawade, S. Bharne, and V. Mane, "Forensic Analysis and Evidence Collection for Web Browser Activity", in *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology (I²IT), Pun*, 2016, pp. 518–522.
[11] E. Akbal, G. Fatma, and A. Akbal, "Digital Forensic Analyses of Web Browser Records", *J. Softw.*, vol. 11, no. 7, pp. 631–637, 2016.
[12] R. Montasari and P. Peltola, "Computer Forensic Analysis of Private Browsing Modes", in *In International Conference on Global Security, Safety, and Sustainability*, 2015, vol. 534, pp. 96–109.
[13] M. N. Faiz, R. Umar, and A. Yudhana, "Analisis Live Forensics Untuk Perbandingan Keamanan Email Pada Sistem Operasi Proprietary", *J. Ilm. Ilk.*, vol. 8, no. 3, pp. 242–247, 2016.
[14] R. J. Mcdown, C. Varol, L. Carvajal, and L. Chen, "In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes", *J. Forensic Sci.*, vol. 61, no. January, pp. 110–116, 2016.
[15] M. Kaur, N. Kaur, and S. Khurana, "A Literature Review on Cyber Forensic and its Analysis tools", *IJARCCE*, vol. 5, no. 1, pp. 23–28, 2016.
[16] N. Joseph, S. Sunny, S. Dija, and K. L. Thomas, "Volatile Internet evidence extraction from Windows systems",

*2014 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2014*, 2015.
[17] B. D. Carrier, "Digital forensics works", *IEEE Secur. Priv.*, vol. 7, no. 2, pp. 26–29, 2009.
[18] K. Hausknecht, D. Foit, and J. Burić, "RAM data significance in digital forensics", in *38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2015 - Proceedings*, 2015, pp. 1372–1375.
[19] E. M. Chan, "A Framework for Live Forensics", University of Illinois at Urbana-Champaign, 2011.
[20] S. Thongjul and S. Tritilanunt, "Analyzing and Searching Process of Internet Username and Password Stored in Random Access Memory (RAM)", in *2015 12th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 2015, pp. 257–262.
[21] P. Lallement, "The cybercrime process : an overview of scientific challenges and methods", *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 12, pp. 72–78, 2013.
[22] F. Jafari and R. S. Satti, "Comparative Analysis of Digital Forensic Models", *J. Adv. Comput. Networks*, vol. 3, no. 1, pp. 82–86, 2015.
[23] I. O. Ademu, C. O. Imafidon, and D. S. Preston, "A New Approach of Digital Forensic Model for Digital Forensic Investigation", *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 12, pp. 175–178, 2011.
[24] Ruuhwan;, I. Riadi, and Y. Prayudi, "Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System Methodology", *Int. J. Electr. Comput. Eng.*, vol. 7, no. 5, pp. 2806–2817, 2017.
[25] F. Gianni and F. Solinas, "Live digital forensics: Windows XP vs Windows 7", *2013 2nd Int. Conf. Informatics Appl. ICIA 2013*, pp. 1–6, 2013.