Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser

By Imam Riadi

International Journal of Computer Applications (0975 – 8887)
Volume 164 – No 8, April 2017

Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser

Tri Rochmadi
Department of Informatics
Islamic University of Indonesia
Yogyakarta, Indonesia

Imam Riadi
Department of Information System
Ahmad Dahlan University
Yogyakarta, Indonesia

Yudi Prayudi
Department of Informatics
Islamic University of Indonesia
Yogyakarta, Indonesia

ABSTRACT
Almost all aspects of life already use the internet, to be able to access the Internet one of them using a web browser. For security, some web browser features to develop private mode. Unfortunately, from this feature, by some unscrupulous used for criminal activities by the anti-forensics. An anti-forensics process such as by using a portable web browser and delete registry. Motivation use of anti-forensics is to minimize or inhibit the discovery of digital evidence in criminal cases. So that, be an obstacle for investigators to uncover internet crimes that have been carried out. This paper proposes a framework for analysis phases of the web browser in private mode and anti-forensics. The purpose of this study is to provide solutions in forensic investigations effectively and efficiently using live forensics. This study uses a live forensics to get more detailed 3 evidence information on the computer with the condition is still on. So this method is suitable to be applied to the handling of incidents more quickly and allows getting the data in RAM.

General Terms
Browser Security, Digital Forensic.

Keywords
Web Browser, Live Forensics, Anti-Forensics.

1. INTRODUCTION
The Internet has changed people's lifestyles, either from social, educational, health and even government. It then creates new problems that are a cyber crime, especially in the activity of each transaction or process in the Internet using a web browser software [1]. Ease of access also poses a threat and a crime directly to the web server of an agency so that the loss will be even greater [2]. The web browser designed to store any information such as history uniform resource locator (URL), search keyword, timestamp, password and others who conducted a user when browsing the Internet [3].

However, for user security, so that their information is not stored in the computer system, web browser also competing to make the so that after browsing their information deleted, called the Mode Private Browsing [4].

System security features that made web browser used by the individual to a crime, with anti-forensic others such as using a portable web browser with the private mode that is designed not to leave a trail of digital evidence on the computer [5] and deletion of the registry when it is already surfing. Portable web browser is a web browser that is run without being installed on the computer, so just stored in an external storage medium so as not to leave a file in a computer program [4].

A Registry is a database of information computer which records every activity on a computer is good when there are a new hardware or software running activities. So it becomes a challenge for investigators when doing a forensics or investigates the internet activity of suspects in the case of cybercrime that allows using a web browser.

Previous research on the web browser is limited to the side portable web browser mode private [5] when activity on the internet. The issue poses a great challenge to forensic investigators are trying to reconstruct the recent browsing history, in the event of computer incident [6].

The study took this problem with the addition of anti-forensic process that is the elimination of the registry and a different browser that is Browzar. Overcoming these problems then determined forensic methods do is live forensics. This method is suitable for handling incidents more quickly and allows getting the data in random access memory (RAM) [7] because, as explained earlier, the web browser used is portable and private browsing.

Live forensics is a method to get the data contained in the volatile RAM so that crime can be seen from the volatile data analysis [8]. This research method has benefits as new proposals that could be used in handling the case of web browsers in general and in particular portable.

It becomes crucial because the web browser of many kinds with a variety of engines used in making the web browser, so with this study are expected to increase knowledge and contribute academically and practically. Therefore, research is focused on live forensics for analysis browser.

2. BASIC THEORY
2.1 Forensics Web Browser
The web browser is a software application for the taking, presenting, and traversing information resources on the Internet or World Wide Web (WWW). A source of information is identified by a Uniform Resource Identifier (URI) and may be pages web, images, video, or other pieces of content [9].

A forensic web browser is a forensic activity to find information stored on a web browser. Digital evidence contained in a web browser at least there caches, history, cookies, download file list, and sessions [10]. At least a minimum of digital evidence from a web browser at the top is very important and good used by investigators to analyze in a case of using the internet [11].

2.2 Anti-Forensics

Generally, anti-forensics [12] is a technique or a person's attempt to thwart the investigation included to avoid detection of events, disrupt collection of information needed, spend time on the investigation and casts doubt on the reports.

There are four categories of anti-forensic methods [13] that are data hiding, artifact wiping, trail obfuscation and attacks against the forensics process or tools.

- Data Hiding
  Data hiding [14] claims, hide data so unreadable using techniques such as encryption, steganography, and others.
- Artifact Wiping
  Artefact wiping is a technique used to overwrite the data on the hard drive so it can not be recovered [15].
- Trail Obfuscation
  Trail Obfuscation intended to mislead investigators by hiding or deleting evidence about the source and nature of the attack [13]. This technique can be used to modify the log cleaning log files or modify metadata timestamps.
- Attacks Against Forensics Process or Tool
  Attacks Against Forensics Process or Tools are anti-forensic methods are rare, as it directly working on the investigation procedure to bugs in forensics tools. Attackers require more knowledge and experience of how the tools and work procedures [12].

In this case, the anti-forensic web browser is using a portable web browser, use it in private mode and delete the registry after browsing activity. The registry contains the most information regarding the use of the computer and user configurations, applications and hardware devices on Windows operating systems. This information is categorized based on the order that has been executed, search keyword, last accessed folder, log applications, and others.

2.3 Live Forensics

Live forensics is a forensic investigation is carried out when the system is ON [16]. This is because the data will be lost if the computer is shut down or restarted. Implementation live forensics usually used in the case of volatile memory which is used or stored in RAM [17].

Live Forensics on a computer is through the acquisition and analysis of RAM. The acquisition of RAM here is to perform the capture or imaging of RAM using RAM forensic tool. So live forensic brought some concerns because all life forensic procedure should not affect normal services running on the target system [18].

Although there are some concerns with live forensic when investigating, live forensics is necessary to get more information that will be used as an analysis [7]. After digital evidence obtained from RAM, then followed by analysis using Memory Analysis tool.

3. METHODOLOGY

This paper proposes a methodology that makes it possible to obtain more information from the computer so that digital evidence obtained more match of the case.

Under the proposed methodology in Figure 1, stages of the investigation consist of three main stages that are Pre-Analysis, Analysis and Post Analysis.

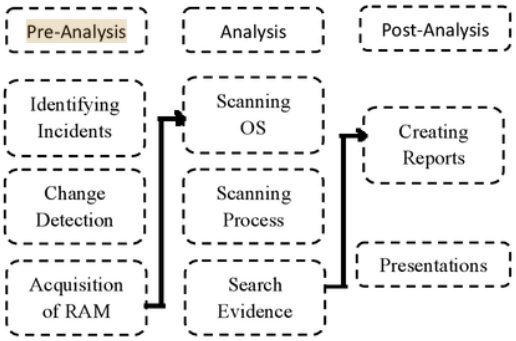

Figure 1. Proposed Methods Live Forensic Web Browser

The methodology proposed case scenario simulated using hardware and software are shown in Table 1.

Table 1. Hardware and Software

Hardware	Software
Laptop Core i5 2GB RAM	Windows 7 SP 2
Flashdrive A-DATA 2 GB	Internet Explorer Portable
Flashdrive TOSHIBA 8 GB	Mozilla Firefox Portable
	Google Chrome Portable
	Browzar Black
	Clean After Me Portable
	ProcMon Portable
	DumpIt
	Winhex
	Volatility Memory Forensic

The study simulated in three stages as shown in Figure 2, the first stage when the web browser is still the way to do acquisition and analysis, the second phase when the web browser is closed do acquisition and analysis, then in the third stage of the acquisition and analysis is done when the web browser is closed and conducted anti-forensics using Clean After Me to delete the registry system on the computer.

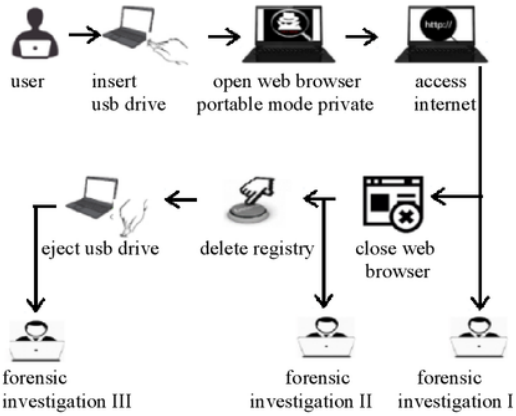

Figure 2. Case Study Simulation

Simulation in each web browser using private mode and by using different keywords in each browser use the internet, as shown in Table 2.

Table 2. Keyword in Web Browser

Web Browser Portable	Activity using web browser portable (Keyword)
Internet Explorer	Google – Batman – Image - Facebook
Mozilla Firefox	Google – Spiderman -Image – Twitter
Google Chrome	Google – Ironman – Image – Mail Yahoo
Browzar Black	Google – Xman – Image – Mail Google

Each browsing activity does a google search with different keywords in every web browser. Likewise for account activity also different in every web browser.

4. ANALYSIS AND RESULTS

Before starting the analysis, preceded by performing incident response by detecting changes in the system followed by the acquisition of computer memory using DumpIt to obtain a copy of the file from the memory RAM. Then began to analyze it to find evidence of a web browser using the Volatility Memory Forensics and WinHex.

This analysis uses the method development of the Generic Model Computer Forensics Investigations (GCFIM). The purpose of this method development is to develop a method that aims to analyze digital evidence efficiently.

4.1 Pre-Analysis

4.1.1 Identification Incident and Change Detection

Incident identification purposes for finding information, collecting data so that it can find a gaffe of the system running.

Detection of changes is found changes to the registry are shown in Table 3. Detection of these changes helps to determine what the appropriate plugin is used to search for digital evidence using volatility memory forensic.

Table 3. Detection of Changes in Registry

Web Browser	Proccess	Location
Internet Explorer.exe	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\okies\CachePrefix
Internet Explorer.exe	RegOpenValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\History
Internet Explorer.exe	RegCloseValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
firefox.exe	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\faultConnectionSettings
firefox.exe	RegCloseValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
firefox.exe	IRP_MJ_READ	C:\pagefile.sys
Web	Proccess	Location
Browser		
chrome.exe	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Time Zones\SE Asia Standart Time\Dynamic DST
chrome.exe	FASTIO_WRITE	C:\Users\User PC\AppData\Local\Temp\GoogleChromePortable\Deafult\Cache\data_1
chrome.exe	IRP_MJ_READ	C:\pagefile.sys
Browzar Black 2000.exe	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Offload
Browzar Black 2000.exe	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\
Browzar Black 2000.exe	RegQueryKey	HKLM\SOFTWARE\Policies\Microsoft\Cryptography\

The detection process is known there is a change in the system registry, and unique is the use Browzar that overwrite data used by Internet Explorer, it is very important to know because as a reference for later analysis.

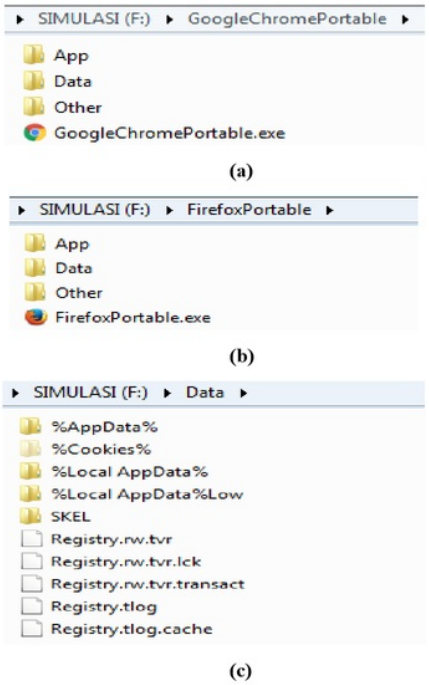

Figure 3. (a) Google Chrome Portable, (b) Mozila Firefox Portable, (c) Internet Explorer Portable

When Internet Explorer, Google Chrome, and Mozilla Firefox Portable executed, There are changes to create new files on the USB drive shown in Figure 3a, 3b and 3c.

BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\WINDOWS\History
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\WINDOWS\History
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\WINDOWS\History
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\WINDOWS\History
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\History\desktop.ini
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\History\History.IE5
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\History\History.IE5
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ind...
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ind...
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Roaming\Microsoft\Windows\Cookies
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Roaming\Microsoft\Windows\Cookies
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\History\History.IE5
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\History\History.IE5
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
BrowzarBlack2000.exe	2008	CreateFile	C:\Users\User PC\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

Figure 4. New File When Browzar is Run

While the use of Browzar does not happen manufacture of new files in the USB drive but occur within the computer system as in Figure 4.

4.1.2 Acquisition of RAM

RAM acquisition to do when a computer is on using DumpIt. From acquisition results obtained the file extension .raw as in Figure 5.

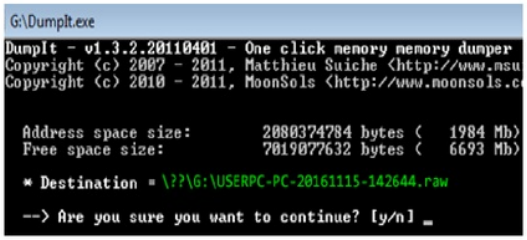

Figure 5. Acquisition of RAM I

On the acquisition of the first ram produces a file imaging named USERPC-PC-20161115-142644.raw are automatically stored in an USB drive where dumpit executed.

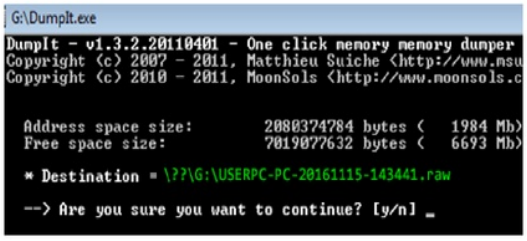

Figure 6. Acquisition of RAM II

As well as on the acquisition of the second ram, produces imaging files in the USB driver which DumpIt run, as shown in Figure 6 produces a file USERPC-PC-20161115-143441.raw.

While the third acquisition in the RAM generates a file named as shown in Figure 7 below when DumpIt executed to retrieve data from the RAM memory.

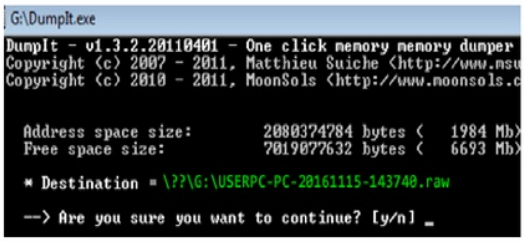

Figure 7. Acquisition of RAM III

Address space size in Figure 5, Figure 6 and Figure 7 shows the size of the RAM to be acquired is equal to 2,080,374,784 bytes (1984 Mb) or rounded up to 2 GB.

4.2 Analysis

4.2.1 Scanning of Operating System

Scanning is intended to know information the operating system used by the computer as shown in Figure 8. Scanning is performed using tool volatility memory forensics with the command imageinfo of imaging files that have been obtained in the acquisition process before.

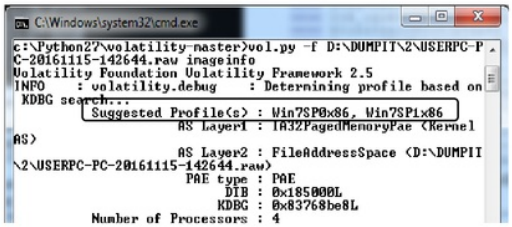

Figure 8. Result Scanning of Operating System

Results scanning system operation obtained information a computer using Win7SP1x86 which mean Windows 7 Service Pack 1 with 32 bits.

4.2.2 Scanning Process

The scanning process is intended to determine the process ID of software used so that the process ID can help facilitate the speed of analysis because it has been filtered during the scanning process ID searches of digital evidence, as shown in Figure 9.

```
Offset(V)  Name                PID   PPID  Thds     Hnds   Sess  Wow64 Start
---------- ------------------- ------ ------ ------ -------- ------ ------ ------------------------------
0x975db408 Internet Explo      1924   1324      8      129      1      0 2016-11-15 14:08:44 UTC+0000
0x85f0a030 Internet Explo      4416   1324     12      445      1      0 2016-11-15 14:09:11 UTC+0000
0x85f4e780 Internet Explo      2108   4416     30      777      1      0 2016-11-15 14:09:25 UTC+0000
0x860be908 FirefoxPortabl      2408   1940      3      148      1      0 2016-11-15 14:11:33 UTC+0000
0x860bf788 firefox.exe         4872   2408     57      701      1      0 2016-11-15 14:11:36 UTC+0000
0x86a70740 GoogleChromePo      1536   1940      1       83      1      0 2016-11-15 14:15:19 UTC+0000
0x894df768 chrome.exe           772   1536     29      788      1      0 2016-11-15 14:15:21 UTC+0000
0x868ef660 chrome.exe           240    772      6       74      1      0 2016-11-15 14:15:25 UTC+0000
0x89609d40 chrome.exe          5748    772      5      165      1      0 2016-11-15 14:15:36 UTC+0000
0x97496628 chrome.exe          4952    772     14      355      1      0 2016-11-15 14:17:44 UTC+0000
0x894a4030 chrome.exe          5692    772      4      170      1      0 2016-11-15 14:17:49 UTC+0000
0x86a95bb8 BrowzarBlack20      2288   1940     28      609      1      0 2016-11-15 14:19:44 UTC+0000
```

Figure 9. Result Scanning Process

4.2.3 Scanning Search Digital Evidence

Digital evidence searches done in 2 ways, that is with Volatility Memory Forensic and Winhex.

a. Internet Explorer
Digital evidence can be found at Volatility Memory Forensics as shown in Table 4.

Table 4. Digital Evidence from Internet Explorer Using Volatility Memory Forensics

Analysis I	Analysis II	Analysis III
Proccess : 4416 Internet Explorer	Proccess : 4416 Internet Explorer	Not Found
Location:Visited User PC@https://www.google.co.id/search?hl=id&source=hp&biw=&bih=&q=xman&gbv=1	Location:Visited User PC@https://www.google.co.id/search?hl=id&source=hp&biw=&bih=&q=xman&gbv=1	
Last accessed: 2016-11-15 14:20:20 UTC+000	Last accessed: 2016-11-15 14:20:20 UTC+000	

The analysis means the process ID 4416 software that runs is Internet Explorer, and there is new information about the history that is accessible and when access occurs.

Digital evidence using WinHex shown in Figure 10.

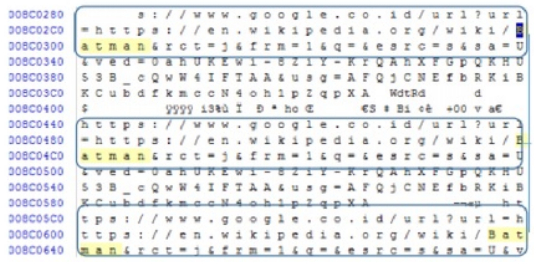

Figure 10. Digital Evidence from Internet Explorer Using Winhex in Simulation I

The Figure 10 shows that the results of the analysis found the history that has been done is to access the google and search for information about Batman.

Digital evidence using WinHex shown in Figure 11 for the second case simulation.

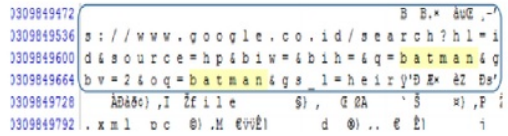

Figure 11. Digital Evidence from Internet Explorer Using Winhex in Simulation II

The results of the analysis in the second simulation shows the difference in the results obtained imaging data RAM bit random and difficult to know the information in the RAM memory data.

Digital evidence using WinHex shown in Figure 12 for the third case simulation.

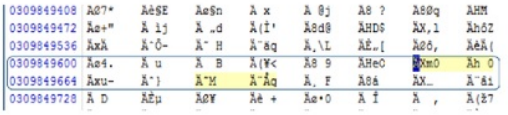

Figure 12. Digital Evidence from Internet Explorer is not Found Using Winhex in Simulation III

The third simulation results when anti-forensics do so history is not found and the data in RAM memory to be very random and difficult to analyze.

History of Internet Explorer is more valid analysis results using WinHex. When using Volatility Memory Forensics found history is the history of scenario simulation using Browzar.

b. Mozilla Firefox
Digital evidence from Mozilla Firefox can be found in RAM as shown in Table 5.

Table 5. Digital Evidence from Mozilla Firefox Using Volatility Memory Forensics

Analysis I	Analysis II	Analysis III
URL : https://www.google.co.id/search?q=spider….ocA6UQ_AUIBigB#6_1ulMGazeiLGM%3A	URL : https://www.google.co.id/search?q=spider….ocA6UQ_AUIBigB#6_1ulMGazeiLGM%3A	URL : https://www.google.co.id/search?q=spider….ocA6UQ_AUIBigB#6_1ulMGazeiLGM%3A

Analysis I	Analysis II	Analysis III
Last Visit Date: 2016-11-15 04:26:23	Last Visit Date: 2016-11-15 04:26:23	Last Visit Date: 2016-11-15 04:26:23

Password account used to log into Twitter can be found, but only found on the first and second simulation before anti-forensic delete the registry.

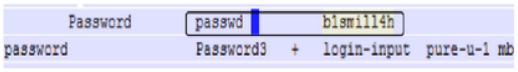

Figure 13. Password in RAM from Mozilla Firefox

Figure 13 shows that the password is found that the password used is b1smill4h.

c. Google Chrome

The results obtained from the analysis of RAM that digital evidence of the use of Google Chrome Portable can also be found as shown in Table 6.

Table 6. Digital Evidence from Google Chrome Using Volatility Memory Forensics

Analysis I	Analysis II	Analysis III
URL : https://www.google.co.id/webhp?ie=UTF-8…cr&ei=upQqWK6qAoT2vASnwbKwbKwBg#q=ironman	URL : https://www.google.co.id/webhp?ie=UTF-8…cr&ei=upQqWK6qAoT2vASnwbKwbKwBg#q=ironman	URL : https://www.google.co.id/webhp?ie=UTF-8…cr&ei=upQqWK6qAoT2vASnwbKwbKwBg#q=ironman
Last Visit Date: 2016-11-15 04:53:47	Last Visit Date: 2016-11-15 04:53:47	Last Visit Date: 2016-11-15 04:53:47

Analysis showed that the history that is found is seeking information about the ironman and done 2016-11-15 04:53:47 like on line Last Visit Date.

d. Browzar

For the analysis of Browzar can be shown in Table 7.

Table 7. Digital Evidence from Browzar Using Volatility Memory Forensics

Analysis I	Analysis II	Analysis III
Proccess : 2288 Browzar Black20	Proccess : 2288 Browzar Black20	Proccess : 2288 Browzar Black20
Location:Visited User PC@https://www.google.co.id/search?hl=id&source=hp&biw=&bih=&q=xman&gbv=1	Location:Visited User PC@https://www.google.co.id/search?hl=id&source=hp&biw=&bih=&q=xman&gbv=1	Location:Visited User PC@https://www.google.co.id/search?hl=id&source=hp&biw=&bih=&q=xman&gbv=1
Last accessed: 2016-11-15 14:20:20 UTC+000	Last accessed: 2016-11-15 14:20:20 UTC+000	Last accessed: 2016-11-15 14:20:20 UTC+000

From the analysis, history url and timestamp can be found, but for passwords used to log into google email can only be found in the first and second simulation, before the anti-forensic process is done, as in Figure 14.

Figure 14. Password in RAM from Browzar

The account used for accessing Google email is the email/username is treesaro@gmail.com and password is bismillah@085642152984.

4.3 Post Analysis

Post-analysis consisted of reports and presentations. The report consists of all the details of the incident cases and all the documentation of the stages before analysis and process analysis. Then this presentation regarding any digital evidence that can be obtained during the investigation and is used to describe in court.

5. ANALYSIS OF RESULT

After doing some simulations and several stages of analysis, the results of the analysis in this study can be seen in Table 8.

Table 8. Summary of Result

Web Browser Portable	History Simulation			Timestamp Simulation			Password Simulation		
	I	II	III	I	II	III	I	II	III
Internet Explorer	√	√	-	√	√	√	-	-	-
Mozilla Firefox	√	√	√	√	√	√	√	√	-
Google Chrome	√	√	√	√	√	√	-	-	-
Browzar Black2000	√	√	√	√	√	√	√	√	-

History URL, timestamp on any browser can be found either with a tool Volatility Memory Forensics and WinHex, except Internet Explorer in simulation III. This is because the engine in Internet Explorer overwritten by Browzar data usage and also because of the anti-forensics.

Simulation of the first and second password can be found at the browsers Mozilla Firefox and Browzar. Simulation third after anti-forensic process conducted, the password can not be found at all web browser.

6. CONCLUSION

The results of the forensic investigation, characteristics of digital evidence can be found in the same RAM with the digital evidence contained on a computer system when using a regular web browser such as url, history, timestamp and password. But there are differences of digital evidence between the browser used, that is on the side of the Internet Explorer history can not be found because the data is affected by the use of Browzar, because Browzar uses engine used by Internet Explorer. After doing some circuit analysis with some of these simulations, digital evidence on Internet Explorer and

Google Chrome Portable Portable there is 2 digital evidence that is history and timestamp. While for Mozilla Firefox Portable and Browzar, there is 3 digital evidence obtained that is history, timestamp, and password. But for the password in all web browsers can not be found when an anti-forensic process is done. The method used for the analysis of portable web browsers mode private with anti-forensics is with Live Forensics in order to obtain more information data from RAM. This research resulted in the proposed framework for the investigation stage of development integrase Generic Computer Forensic Investigation Model, that is pre-analysis phase consists of identifying incidents, change detection and acquisition of RAM. Analysis stage consists of scanning the operating system, scanning ID process and search of digital evidence. Post-analysis stage consists of report creation and presentation of digital evidence.

7. FUTURE WORKS

Conducted a similar study of the web browser that its almost the same with Browzar by applying anti-forensic others such as deleting the data in RAM and how mitigation. It should also develop a plugin of Volatility Memory Forensics for analysis browser from another engine.

8. ACKNOWLEDGMENT

We express gratitude to God Almighty, Parents, Family, PUSFID and friends who helped and support so that this work can be completed.

9. REFERENCES

[1] G. Patel, "Anti-Forensics Techniques for browsing artifacts," 2014.

[2] D. Mualfah and I. Riadi, "Network Forensics For Detecting Flooding Attack On Web Server," IJCSIS, vol. 15, no. 2, pp. 326–331, 2017.

[3] J. Oh, S. Lee, and S. Lee, "Advanced evidence collection and analysis of web browser activity 5," vol. 8, pp. 0–8, 2011.

[4] D. G. Dharan, "Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser," 2014.

[5] G. Aggarwal, E. Burzstein, C. Jackson, and D. Boneh, "An Analysis of Private Browsing Modes in Modern Browsers," California, 2010.

[6] E. D. Adautin, "Forensic Reconstruction and Analysis of Residual Artifacts from Portable Web Browser," vol. 128, no. 18, pp. 19–24, 2015.

[7] S. Rahman and M. N. A. Khan, "Review of Live Forensic Analysis Techniques," vol. 8, no. 2, pp. 379–388, 2015.

[8] Garcia, Gabriela Limon, "Forensic Physical Memory Analysis: An Overview of Tools and Techniques Technical Report," Helsinki University of Technology, 2007.

[9] A. Jain and V. Richariya, "Implementing a Web Browser with Phishing Detection Techniques," World Comput. Sci. Inf. Technol. J., vol. 1, no. 7, pp. 289–291, 2011.

[10] L. Ran and H. Jin, "Analysis Framework to Detect Artifacts of Portable Web Browser," 2012.

[11] B. R. Jones, Internet Forensics, no. October. 2005.

[12] Li, W, "Anti-forensic Digital Investigation for Unauthorized Intrusion on a Wireless Network," Auckland, 2013.

[13] M. K. Rogers, R. Mislan, J. Goldman, T. Wedge, and S. Debrota, "Computer Forensics Field Triage Process Model," Conf. Digit. Forensics, Secur. Law, vol. 1, no. 2, pp. 27–40, 2006.

[14] Rekhis, S., & Boudriga, N., "A System for Formal Digital Forensic Investigation Aware of Anti-Forensic Attacks," Information Forensics and Security, 635-650, 2012.

[15] Sammons, J, "The Basics of Digital Forensics," Waltham: Syngress, 2012.

[16] N. Hermaduanti and I. Riadi, "Automation Framework For Rogue Access Point," vol. 93, no. 2, pp. 287–296, 2016.

[17] M. I. Mazdadi, I. Riadi, and A. Luthfi, "Live Forensics on RouterOS using API Services to Investigate Network Attacks," *IJCSIS*, vol. 15, no.2, pp. 406–410, 2017.

[18] Y. Cheng, X. Fu, X. Du, B. Luo, and M. Guizani, "A Lightweight Live Memory Forensic Approach Based on Hardware Virtualization", Elsevier, 2016, doi: 10.1016/j.ins.2016.07.019

Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser

ORIGINALITY REPORT

5%

SIMILARITY INDEX

PRIMARY SOURCES

1	aut.researchgateway.ac.nz Internet	107 words — 3%
2	lavasoft.com Internet	41 words — 1%
3	l.unsil.ac.id Internet	26 words — 1%
4	www.homokkert.hu Internet	25 words — 1%
5	www.advance7.com Internet	19 words — < 1%
6	Chaoting Xuan. "Toward Revealing Kernel Malware Behavior in Virtual Execution Environments", Lecture Notes in Computer Science, 2009 Crossref	8 words — < 1%

EXCLUDE QUOTES OFF

EXCLUDE MATCHES OFF

EXCLUDE BIBLIOGRAPHY OFF