INTERNATIONAL JOURNAL OF RESEARCHES IN BIOSCIENCES, AGRICULTURE & TECHNOLOGY
© VISHWASHANTI MULTIPURPOSE SOCIETY (Global Peace Multipurpose Society) R. No. MH-659/13(N)
www.vmsindia.org

Computer Forensics for Private Web Browsing of UC Browser

Rahul Neware
P.G. Student, Department of Computer Science and Engineering,
G.H.R.C.E. College, CRPF Gate Hingna Road Nagpur, Maharashtra, India

Abstract:
Private Browsing modes provides the privacy where the surfing activity traces are not present but this Private Browsing is a great task for the Computer Forensics who want to recover the Browser history in the case of any misuse of the web browser. To recover that history the use of volatile memory forensics methodologies and the tools can be used to obtain the traces in main memory after PB(Private Browsing) session. To gain this artefacts left in the foremost reminiscence the proper memory framework will be beneficial for the investigators to successfully retrieve the reminiscence related with the past PB session History. The framework shown in flowchart below is used to overall procedure to collect and analyse the data related to personal browsing using UC Browser.

Keywords: Private Web Browsing, Web Browsers, Computer Forensics, Safe Browsing, Web Browser Artefacts, UC Browser.

I. INTRODUCTION

Many users are continuously using internet to access information or data over internet by using various browsers. Like, Social community, credit card, Online Banking, User email address etc. Therefore, it is very important to ensure privacy of user over the internet. To overcome this problem major browser vendors provide Private Browsing Mode. One of the browser used in India is UC Browser, UC Browser has over 400 million users worldwide; 58% market shares in India. As of now UC browser is the second most popular browser in market shares. The browser claims to have 100 million daily active users, UC Browser provide the Private Browsing Mode(PBM) by the name of "Incognito Browsing". Incognito mode of UC browser claims that when the feature is used all the data is cleared or deleted after browser is closed.

"Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law". A forensic process can be of two kinds, based on how you collect the data. The two kinds are: Live Acquisition and Dead Acquisition.

From a forensic investigation firm point of view, every case would have the following phases:

1. Pre-Investigation Phase
   Request from Clients, Signing Service Level Agreement, Chain of Custody, Hashing Mismatch.
2. Investigation Phase
   Planning, Acquisition, Examination, Analyse.
3. Post Investigation Phase (Reporting, Report Delivery).

II. RELATED WORK

Still the research regarding Private mode of various browsers and its promises given by vendor and its effectiveness, is still limited and in early stages. First Aggarwal et al, 2010 was analyse the private browsing and artifacts of private browsing mode. Aggarwal collect and tested all major browser private browsing artifacts i.e. Chrome, Firefox, Internet Firefox, Safari. Also authors expanded their analysis in both extension and plugging to identify weaknesses of user privacy while using these browsers. They conclude that by using private browsing mode of these browsers exposed the user privacy information.

In 2011, Oh et al focused on analysing the log files created by the browsers like history search, history of deleted data, URL encoding etc. They used WEFA tool for collecting and analysis of data, but the analysis was limited because the browsers used by them are outdated.

In 2013, Ohana and Shashidhar focused on portable web browsers which is quite different technique as compared to private browsing mode in the normal desktop computer. But still by using Portable browsers all data is recoverable.

In 2015, Heule et al provide some important research that mandatory access control and protect sensitive data that may be accessed and used by chrome extension, Many researchers studied about Private Browsing Mode (PBM) in 2015 like Ruize e1 at 2015v focused on technique of recovery for page related dat. Montasari and Peltola 2015, studied at the famous four browsers and concluded that chrome is most secured browser.

In 2016, Ahmad Ghafarian,Sayed Ameen Hosseini Seno studied all famous browser Private Browsing Mode(PBM) and given very good results by using Redline powerful tool but they studied major browsers i.e. already studied by other researchers but get the different and advanced results.

In this research we are also using Redline2. Mandient tool to get good results with UC Browsers which is is not studied earlier by any3. researchers.

III. MATERIAL & METHODS

3.1 Components:

For prove or examine the result we need following components;

- Three computers with Windows OS 32-bir or 64-bit, Two PC used as user machine and the third one used as forensics machine.
- USB adaptor.
- VWware workstation to install Redline in Virtual machine.
- USB flash drive used for forensics machine.
- WinHex tool.
- UC Browser
- External hard drive.
- Mandient Redline forensics software.

3.2 Tool Used:

Mandient Redline is very powerful tool to collecting and evaluating the result generated by Incognito Mode of UC Browser :

1. Redline has a great User Interface.
2. Provide option directly for Private session analysis and all the records by this it is time consuming .
3. Redline allows to import memory analysis result to MS word file for offline processing.
4. The best thing of using Redline is it's easy to use and had great features.

3.3 Method for RAM forensics:

Following are the processes of RAM analysis after Incognito mode;

- Redline has submenu where creating collector is one of the option, which is used to collect from suspect machine.
- .bat is generated, save that file into the removable storage device.
- Run that .bat file collect on suspect machine by connecting removable device into and collect all needed data and Session is generated.
- After collecting data from suspect machine install generated session into forensics machine for evaluation.
- After the report generation click on Hidden Visits to see data access with the help of Private Browsing Mode.

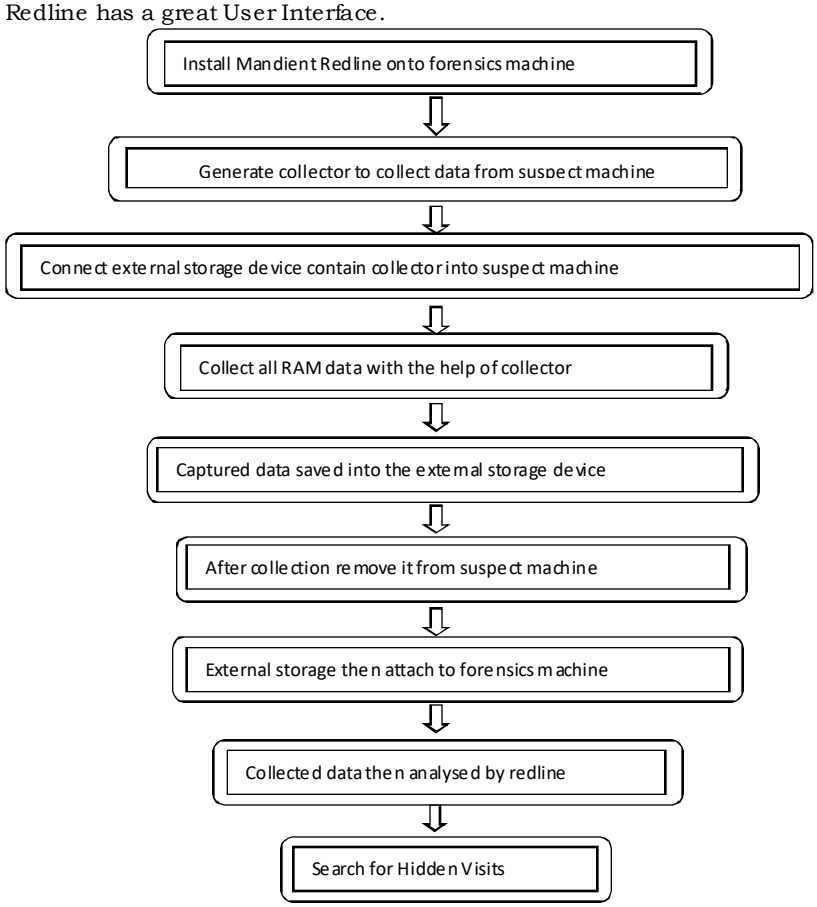

Figure 3.1 RAM Forensics Framework

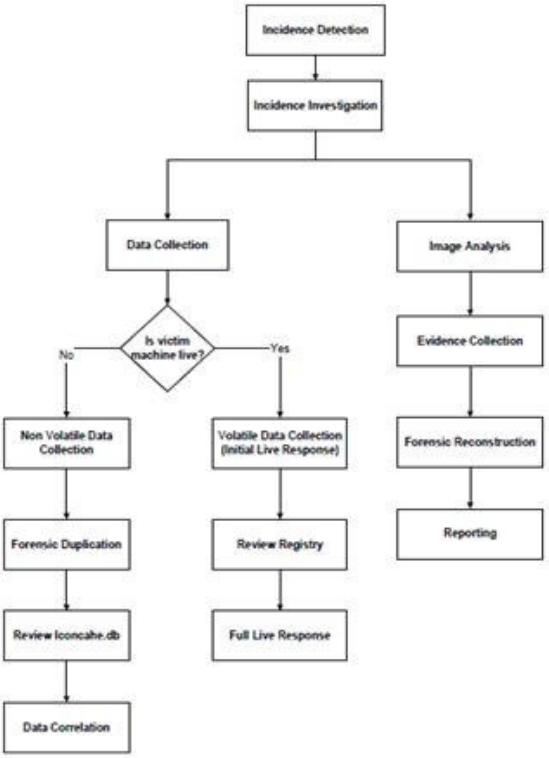

Figure 3.2 Computer forensics overall technique

IV. EXPRIMENT RESULT

Retrieved computer forensics data after "Incognito mode" of UC Browser showed in table.

Table 4.1 Result after analyzing all PWB data

Data Item	UC Browser Closed	UC Browser Open
Browser Processes	No	Yes
Cookies	Yes	Yes
File Download	Yes	Yes
Timelines	Yes	Yes
Browser History	Yes	Yes
Email ID	Yes	Yes
Email Password	No	Yes
Videos	Yes	Yes
Images	Yes	Yes
Search History	Yes	Yes

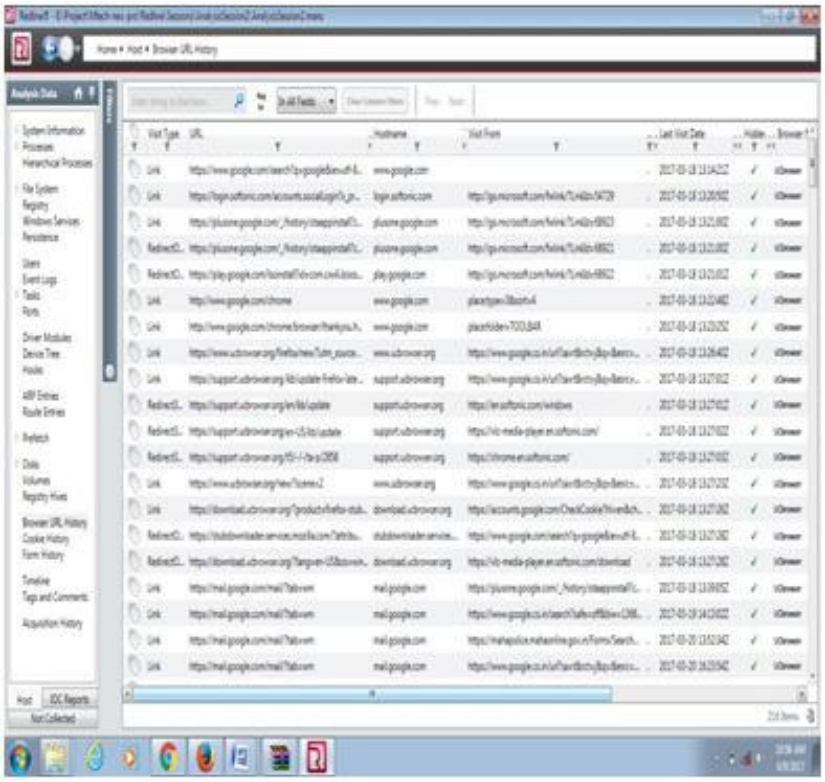

Figure Web History of user after RAM analysis of UC browser.

V. CONCLUSION

When user used Incognito mode of UC Browser then to collect and study the data we used above design framework of volatile memory forensics. It is found that when user used Incognito mode all the data of each event made by user is traced like Login details, Email details, Browsing details etc even after the browser closed or even ope. This details of user while using Incognito mode shows that the normal user and attacking user. The UC Browser vendor says that by using Incognito mode of it user history of events other details will not be traceable but doing this forensics investigation it is discoverable and the private browsing mode is still challenging according to user privacy.

VI. REFRENCES

Aggarwal, G., Bursztein, E., Jackson, C., & Boneh, D. (2010). Analysis of Private Browsing Modes in Modern Browsers. *USENIX Security Symposium* (pp. 79-94).

Al Barghouthy, N., Marrington, A., & Baggili, I. (2013). The forensic investigation of android private browsing sessions using orweb. In *Computer Science and Information Technology (CSIT)*, 2013 5th International Conference on (pp. 33-37). IEEE.

Lerner, B. S., Elberty, L., Poole, N., & Krishnamurthi, S. (2013). Verifying web browser extensions' compliance with private-browsing mode. In *Computer Security–ESORICS 2013* (pp. 57-74). Springer Berlin Heidelberg.

Marrington, A., Baggili, I., Al Ismail, T., & Al Kaf, A. (2012). Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers. In *Computer Systems and Industrial Informatics (ICCSII)*, 2012 International Conference on (pp. 1-6). IEEE.

W3schools, (2016). *Browser Statistics*. [online] Available at: http://www.w3schools.com/browsers/browsers_stats.asp [Accessed 16 Jan. 2015].

W3schools, (2016). *OS Platform Statistics*. [online] Available at: http:// http://www.w3schools.com/browsers/browsers_os.asp [Accessed 16 Jan. 2015].

Montasari, R., & Peltola, P. (2015). Computer Forensic Analysis of Private Browsing Modes. In *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security* (pp. 96-109). Springer International Publishing.

Analysis of Privacy of Private Browsing Mode through Memory Forensics.

International Journal of Computer Applications (0975 – 8887) Volume 132 – No.16, January 2016

Computer Forensic Analysis of Private Browsing Modes.© Springer International Publishing Switzerland 2015H. Jahankhani et al. (Eds.): ICGS3 2015, CCIS 534, pp. 96–109, 2015.

DOI: 10.1007/978-3-319-23276-8_9.

Web security in a windows system as PrivacyDefender in private browsing mode.

Fu-Hau Hsu & Min-Hao Wu & Yi-Wen Chang.

Multimedia Tools Appl (2014) 74:1667–1688

Springer Science+Business Media New York 2014.

Do private and portable web browsers leave incriminating evidence? A forensic analysis of residual artifacts from private and portable web browsing sessions.

Ohana and Shashidhar EURASIP Journal on Information Security 2013, 2013:6

http://jis.eurasipjournals.com/content/2013/1/6.

❖❖❖❖❖