IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. VII (Jul.-Aug. 2017), PP 56-60
www.iosrjournals.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
Corresponding Author: Rahul Neware

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 artifacts 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, Web Browser Artifacts, UC Browser*

Date of Submission: 21-08-2017 Date of acceptance: 05-09-2017

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 el 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 Redline Mandient tool to get good results with UC Browsers which is is not studied earlier by any researchers.

III. Methods & Material

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.
- WinHex

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.

- WinHex tool is used to find out history about ended process in recent by Operating system and gives all details of any ended process.

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.

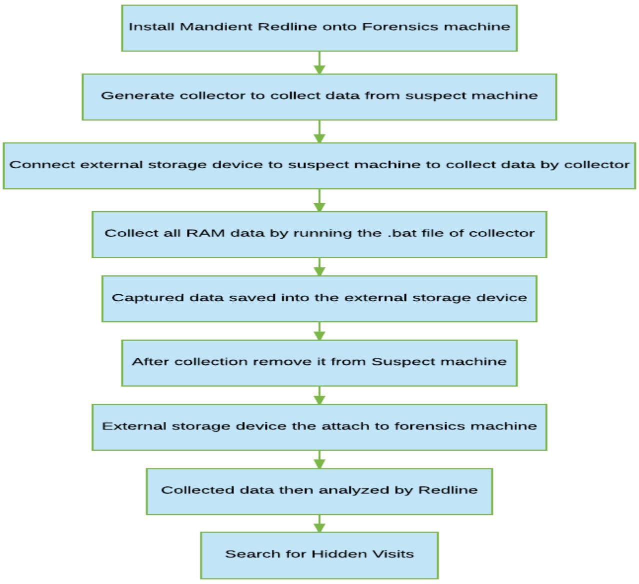

Install Mandient Redline onto Forensics machine
Generate collector to collect data from suspect machine
Connect external storage device to suspect machine to collect data by collector
Collect all RAM data by running the .bat file of collector
Captured data saved into the external storage device
After collection remove it from Suspect machine
External storage device the attach to forensics machine
Collected data then analyzed by Redline
Search for Hidden Visits

Fig 3.1 RAM Forensics Framework

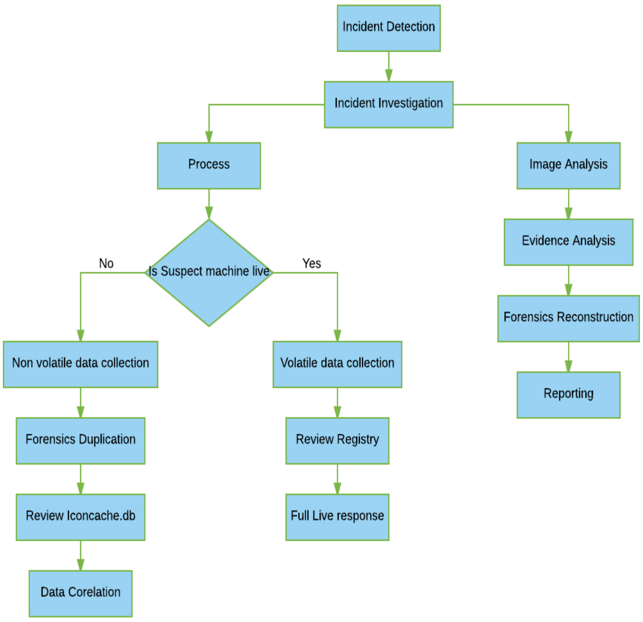


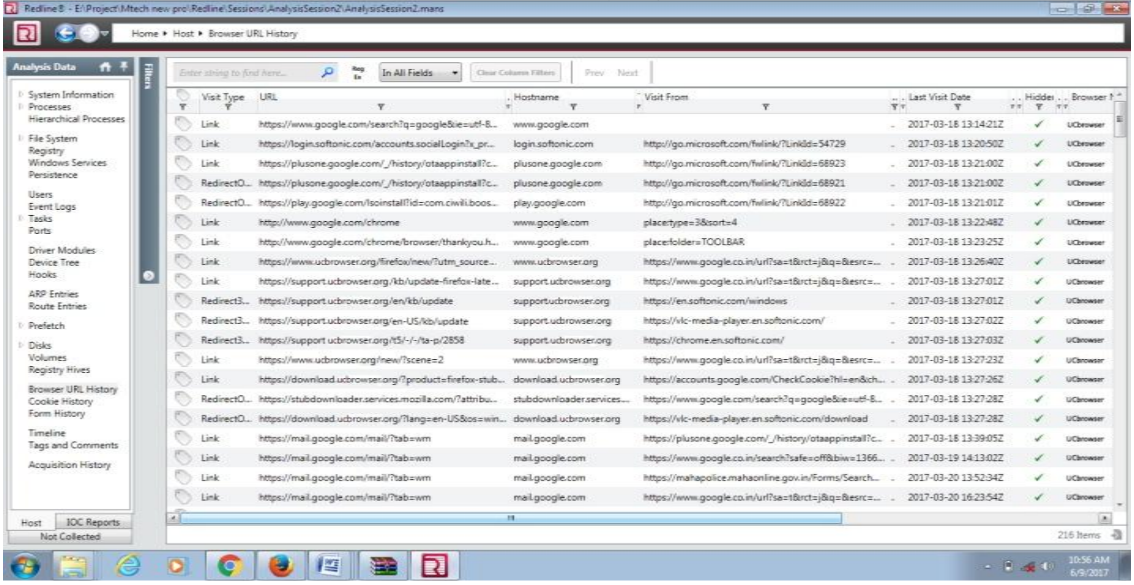
Fig3.2 Computer forensics overall technique

IV. Experimental Result

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

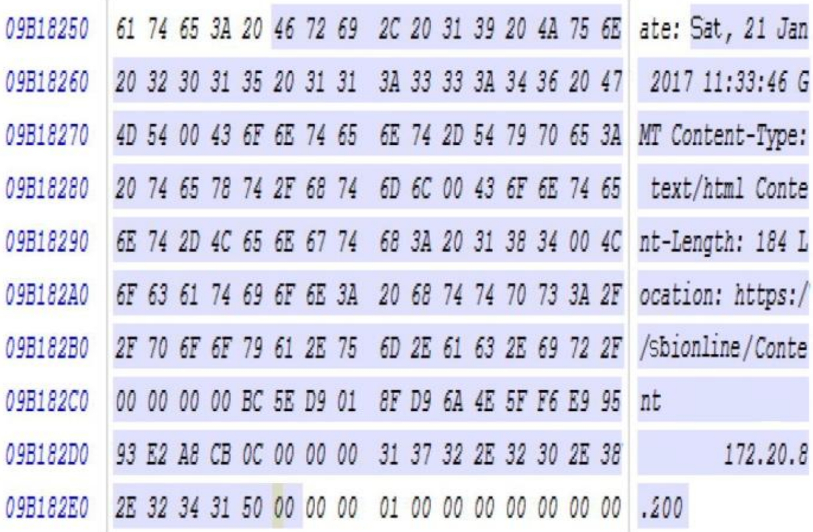
Data Item	UC Browser(Closed)	UC Browser(Open)
Browser Processes	No	Yes
Cookies	Yes	Yes
File Download	Yes	Yes
Timelines	Yes	Yes
Browser History	Yes	Yes
Email ID	Yes	Yes
Email Password	No	Yes
Videos	Yes	Yes
Images	Yes	Yes
Search History	Yes	Yes

Table 4.1 Result after analyzing all PWB data



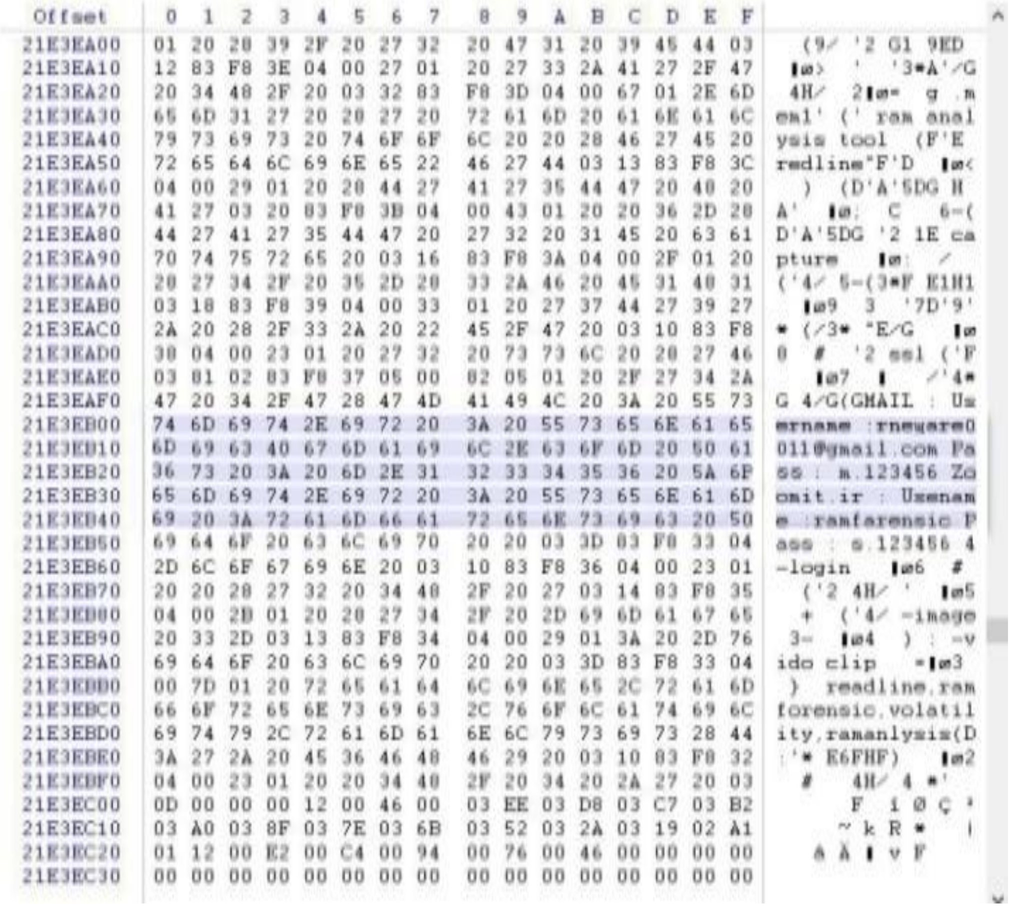
Visit Type	URL	Hostname	Visit From	Last Visit Date	Hidden	Browser N
Link	https://www.google.com/search?q=google&ie=utf-8...	www.google.com		2017-03-18 13:14:21Z	✓	UCbrowser
Link	https://login.softonic.com/accounts.socialLogin?x_pr...	login.softonic.com	http://go.microsoft.com/fwlink/?LinkId=54729	2017-03-18 13:20:50Z	✓	UCbrowser
Link	https://plusone.google.com/_/history/otaappinstall?c...	plusone.google.com	http://go.microsoft.com/fwlink/?LinkId=68923	2017-03-18 13:21:00Z	✓	UCbrowser
RedirectO...	https://plusone.google.com/_/history/otaappinstall?c...	plusone.google.com	http://go.microsoft.com/fwlink/?LinkId=68921	2017-03-18 13:21:00Z	✓	UCbrowser
RedirectO...	https://play.google.com/Isoinstall?id=com.ciwili.boos...	play.google.com	http://go.microsoft.com/fwlink/?LinkId=68922	2017-03-18 13:21:01Z	✓	UCbrowser
Link	http://www.google.com/chrome	www.google.com	placetype=3&sort=4	2017-03-18 13:22:48Z	✓	UCbrowser
Link	http://www.google.com/chrome/browser/thankyou.h...	www.google.com	placefolder=TOOLBAR	2017-03-18 13:23:25Z	✓	UCbrowser
Link	https://www.ucbrowser.org/firefox/new/?utm_source...	www.ucbrowser.org	https://www.google.co.in/url?sa=t&rct=j&q=&esrc=...	2017-03-18 13:26:40Z	✓	UCbrowser
Link	https://support.ucbrowser.org/kb/update-firefox-late...	support.ucbrowser.org	https://www.google.co.in/url?sa=t&rct=j&q=&esrc=...	2017-03-18 13:27:01Z	✓	UCbrowser
Redirect3...	https://support.ucbrowser.org/en/kb/update	supportucbrowser.org	https://en.softonic.com/windows	2017-03-18 13:27:01Z	✓	UCbrowser
Redirect3...	https://support.ucbrowser.org/en-US/kb/update	support.ucbrowser.org	https://vlc-media-player.en.softonic.com/	2017-03-18 13:27:02Z	✓	UCbrowser
Redirect3...	https://support ucbrowser.org/t5/-/-/ta-p/2858	support.ucbrowser.org	https://chrome.en.softonic.com/	2017-03-18 13:27:03Z	✓	UCbrowser
Link	https://www.ucbrowser.org/new/?scene=2	www.ucbrowser.org	https://www.google.co.in/url?sa=t&rct=j&q=&esrc=...	2017-03-18 13:27:23Z	✓	UCbrowser
Link	https://download.ucbrowser.org/?product=firefox-stub...	download.ucbrowser.org	https://accounts.google.com/CheckCookie?hl=en&ch...	2017-03-18 13:27:26Z	✓	UCbrowser
RedirectO...	https://stubdownloader.services.mozilla.com/?attribu...	stubdownloader.services...	https://www.google.com/search?q=google&ie=utf-8...	2017-03-18 13:27:28Z	✓	UCbrowser
RedirectO...	https://download.ucbrowser.org/?lang=en-US&os=win...	download.ucbrowser.org	https://vlc-media-player.en.softonic.com/download	2017-03-18 13:27:28Z	✓	UCbrowser
Link	https://mail.google.com/mail/?tab=wm	mail.google.com	https://plusone.google.com/_/history/otaappinstall?c...	2017-03-18 13:39:05Z	✓	UCbrowser
Link	https://mail.google.com/mail/?tab=wm	mail.google.com	https://www.google.co.in/search?safe=off&biw=1366...	2017-03-19 14:13:02Z	✓	UCbrowser
Link	https://mail.google.com/mail/?tab=wm	mail.google.com	https://mahapolice.mahaonline.gov.in/Forms/Search...	2017-03-20 13:52:34Z	✓	UCbrowser
Link	https://mail.google.com/mail/?tab=wm	mail.google.com	https://www.google.co.in/url?sa=t&rct=j&q=&esrc=...	2017-03-20 16:23:54Z	✓	UCbrowser

Fig. 4.1 Web History of user after RAM analysis of UC browser.



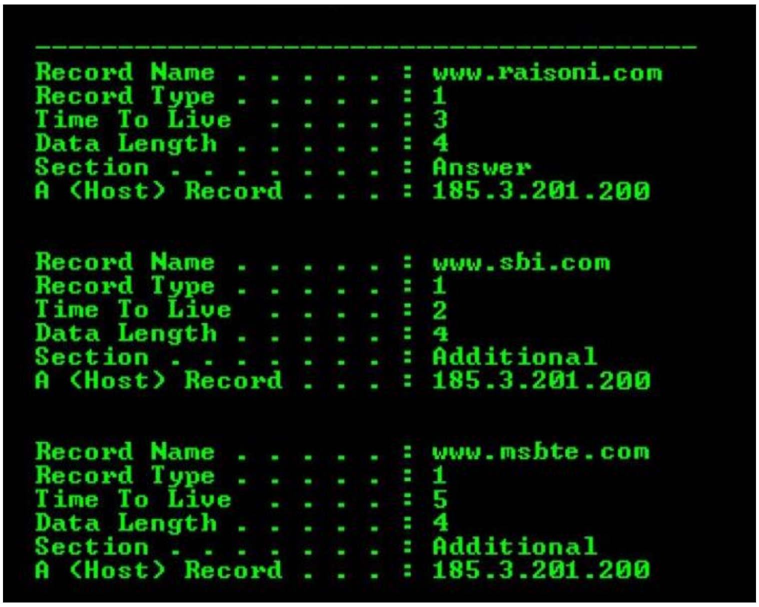
```
09B18250  61 74 65 3A 20 46 72 69  2C 20 31 39 20 4A 75 6E  ate: Sat, 21 Jan
09B18260  20 32 30 31 35 20 31 31  3A 33 33 3A 34 36 20 47   2017 11:33:46 G
09B18270  4D 54 00 43 6F 6E 74 65  6E 74 2D 54 79 70 65 3A  MT Content-Type:
09B18280  20 74 65 78 74 2F 68 74  6D 6C 00 43 6F 6E 74 65   text/html Conte
09B18290  6E 74 2D 4C 65 6E 67 74  68 3A 20 31 38 34 00 4C  nt-Length: 184 L
09B182A0  6F 63 61 74 69 6F 6E 3A  20 68 74 74 70 73 3A 2F  ocation: https:/
09B182B0  2F 70 6F 6F 79 61 2E 75  6D 2E 61 63 2E 69 72 2F  /sbionline/Conte
09B182C0  00 00 00 00 BC 5E D9 01  8F D9 6A 4E 5F F6 E9 95  nt
09B182D0  93 E2 A8 CB 0C 00 00 00  31 37 32 2E 32 30 2E 38          172.20.8
09B182E0  2E 32 34 31 50 00 00 00  01 00 00 00 00 00 00 00  .200
```

Fig. 4.2 Detailed of visited website (Date, Time, Full URL)



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
21E3EA00  01 20 28 39 2F 20 27 32  20 47 31 20 39 45 44 03    (9/ '2 G1 9ED
21E3EA10  12 83 F8 3E 04 00 27 01  20 27 33 2A 41 27 2F 47   ▮ø>  '  '3*A'/G
21E3EA20  20 34 48 2F 20 03 32 83  F8 3D 04 00 67 01 2E 6D   4H/  2▮ø=  g .m
21E3EA30  65 6D 31 27 20 28 27 20  72 61 6D 20 61 6E 61 6C  em1' (' ram anal
21E3EA40  79 73 69 73 20 74 6F 6F  6C 20 20 28 46 27 45 20  ysis tool  (F'E 
21E3EA50  72 65 64 6C 69 6E 65 22  46 27 44 03 13 83 F8 3C  redline"F'D  ▮ø<
21E3EA60  04 00 29 01 20 28 44 27  41 27 35 44 47 20 48 20    )  (D'A'5DG H 
21E3EA70  41 27 03 20 83 F8 3B 04  00 43 01 20 20 36 2D 28  A'  ▮ø;  C   6-(
21E3EA80  44 27 41 27 35 44 47 20  27 32 20 31 45 20 63 61  D'A'5DG '2 1E ca
21E3EA90  70 74 75 72 65 20 03 16  83 F8 3A 04 00 2F 01 20  pture   ▮ø:  /  
21E3EAA0  28 27 34 2F 20 35 2D 28  33 2A 46 20 45 31 48 31  ('4/ 5-(3*F E1H1
21E3EAB0  03 18 83 F8 39 04 00 33  01 20 27 37 44 27 39 27    ▮ø9  3  '7D'9'
21E3EAC0  2A 20 28 2F 33 2A 20 22  45 2F 47 20 03 10 83 F8  * (/3* "E/G   ▮ø
21E3EAD0  38 04 00 23 01 20 27 32  20 73 73 6C 20 28 27 46  8  #  '2 ssl ('F
21E3EAE0  03 81 02 83 F8 37 05 00  82 05 01 20 2F 27 34 2A     ▮ø7  ▮   /'4*
21E3EAF0  47 20 34 2F 47 28 47 4D  41 49 4C 20 3A 20 55 73  G 4/G(GMAIL : Us
21E3EB00  74 6D 69 74 2E 69 72 20  3A 20 55 73 65 6E 61 65  ername :rnewsre0
21E3EB10  6D 69 63 40 67 6D 61 69  6C 2E 63 6F 6D 20 50 61  011@gmail.com Pa
21E3EB20  36 73 20 3A 20 6D 2E 31  32 33 34 35 36 20 5A 6F  ss : m.123456 Zo
21E3EB30  65 6D 69 74 2E 69 72 20  3A 20 55 73 65 6E 61 6D  omit.ir : Usenam
21E3EB40  69 20 3A 72 61 6D 66 61  72 65 6E 73 69 63 20 50  e :ramforensic P
21E3EB50  69 64 6F 20 63 6C 69 70  20 20 03 3D 83 F8 33 04  ass : s.123456 4
21E3EB60  2D 6C 6F 67 69 6E 20 03  10 83 F8 36 04 00 23 01  -login    ▮ø6  #
21E3EB70  20 20 28 27 32 20 34 48  2F 20 27 03 14 83 F8 35    ('2 4H/ '   ▮ø5
21E3EB80  04 00 2B 01 20 28 27 34  2F 20 2D 69 6D 61 67 65    +  ('4/ -image
21E3EB90  20 33 2D 03 13 83 F8 34  04 00 29 01 3A 20 2D 76   3-   ▮ø4  ) : -v
21E3EBA0  69 64 6F 20 63 6C 69 70  20 20 03 3D 83 F8 33 04  ido clip   =▮ø3
21E3EBB0  00 7D 01 20 72 65 61 64  6C 69 6E 65 2C 72 61 6D   }  readline,ram
21E3EBC0  66 6F 72 65 6E 73 69 63  2C 76 6F 6C 61 74 69 6C  forensic,volatil
21E3EBD0  69 74 79 2C 72 61 6D 61  6E 6C 79 73 69 73 28 44  ity,ramanlysis(D
21E3EBE0  3A 27 2A 20 45 36 46 48  46 29 20 03 10 83 F8 32  :'* E6FHF)    ▮ø2
21E3EBF0  04 00 23 01 20 20 34 48  2F 20 34 20 2A 27 20 03    #    4H/ 4 *' 
21E3EC00  0D 00 00 00 12 00 46 00  03 EE 03 D8 03 C7 03 B2        F  î Ø Ç ²
21E3EC10  03 A0 03 8F 03 7E 03 6B  03 52 03 2A 03 19 02 A1       ~ k R *    ¡
21E3EC20  01 12 00 E2 00 C4 00 94  00 76 00 46 00 00 00 00     â Ä ▮ v F    
21E3EC30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Fig 4.3 Email id and password shown by Win Hex when browser is open



```
--------------------------------------------
Record Name . . . . . : www.raisoni.com
Record Type . . . . . : 1
Time To Live  . . . . : 3
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 185.3.201.200


Record Name . . . . . : www.sbi.com
Record Type . . . . . : 1
Time To Live  . . . . : 2
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 185.3.201.200


Record Name . . . . . : www.msbte.com
Record Type . . . . . : 1
Time To Live  . . . . : 5
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 185.3.201.200
```

Fig 4.4 IPConfig/displaydns command in cmd gives the time spend on each website and IP address

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.

References

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

[2]. 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.

[3]. 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.

[4]. 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.

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

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

[7]. 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.

[8]. " Analysis of Privacy of Private Browsing Mode through Memory Forensics". International Journal of Computer Applications (0975 – 8887) Volume 132 – No.16, January 2016

[9]. "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.

[10]. "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.

[11]. "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 Journalon Information Security 2013, 2013:6 http://jis.eurasipjournals.com/content/2013/1/6

Rahul Neware. "Computer Forensics for Private Web Browsing of UC Browser." IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 4, 2017, pp. 56–60.