Web Browser Forensics: A Comparative Integrated Approach on Artefacts Acquisition, Evidence Collections and Analysis of Google Chrome, Firefox and Brave Browser

Hitesh Sanghvi[1], Vismay J. Patel[2], Ramya Shah[2], Parag Shukla[2], and Digvijaysinh Rathod[2](✉)

[1] Directorate of Forensic Science, Gandhinagar, Gujarat, India
[2] School of Cybersecurity and Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India
digvijay.rathod@nfsu.ac.in

Abstract. Web browser is the important application and majority user users use web browsers to access the social media sites, email application, web search engines, ecommerce sites and download the video or photos. Various web browsers are available in the market for this purpose but Google chrome, Mozilla Firefox and Brave are the well-known browser application. These web browsers might be use for normal internet access also use to committee the crime. In such case it is important to use digital forensics techniques to extract evidences which will be produced to court to prove the crime. Literature survey shows that dead forensics were frequently used by researchers but very less work is carried out to use live or RAM forensics to extract the evidences. In this research paper, we created real time scenario with Google Chrome, Mozilla Firefox and Brave browser and use RAM forensics techniques to extract the evidences related to web browser activities.

Keywords: Web browser forensics · RAM forensics · digital forensics · Google chrome · Mozella Firefox · Brave · Autopsy · memory analysis · digital forensics · browser ar-tifacts · browser history

1 Introduction

One of the most common methods of retrieving the Internet is over a web browser, which gives users the ability to carry out traditional crimes or commit crimes online. Computer forensics, a more general area of study, includes web browser forensics. Computer forensics' objective is to locate, gather, protect, and analyze data that contains evidence in a way that keeps the evidence's honesty complete so that it can be used as signal in a law court. In web browser forensics, evidence pertaining to a user's Internet surfing activities is analyzed and extracted. Browser forensics is mostly used to examine a computer's browser log and universal web action in order to look for any doubtful activity or gratified access. In order to obtain precise material about the targeted system, this also relates to

N. Chaubey et al. (Eds.): COMS2 2023, CCIS 1861, pp. 204–218, 2023.
https://doi.org/10.1007/978-3-031-40564-8_15

tracking website traffic and analyzing server-generated LOG files. The goal of computer forensics, a type of forensic investigation, is to describe and analyze the digital signal that remains kept on processers and connected storage broadcasting.

Nearly everybody, including accused under examination, uses the cyberspace. A suspicious person might use a web browser to collect evidence, cover their misconduct, or look for another traditions to obligate criminalities. An important feature of digital forensic investigations is frequently penetrating for web browsing related data. Thus, nearly each action a suspicious took although by means of a web browser would be recorded on a computer. This data can therefore be helpful when a investigator inspects the accused's computer. It is likely to inspect evidence from a accused's computer, counting cookies, cache, log data, and download lists, to control the websites has been checked, when and how frequently they were retrieved, and the examination relations the suspicious used.

The digital forensics analyst either can use dead / hard disk forensics or live/RAM forensics to extract evidences related to activities carried out by the user. RAM is volatile memory but keeps important details related to recent executed programs and application by the user. In this research paper, we used RAM forensics techniques to extract important evidences related to browser activities from Google Chrome, Mozilla Firefox and Brave web browser.

The remaining part of the paper is systematized as follows - the associated research paper assessment is deliberated in Sect. 2, methodology of RAM forensics, Data modeling, Laboratory Set-up and results is discussed in Sect. 3, 4, 5 and 6 respectively. The result is discussed in Sect. 7 and paper is concluded in Sect. 8.

2 Literature Survey

To understand the current status of the research in the domain of browser forensics, we have reviews recent published research paper in this domain, Research on artefact mining of Google Chrome, Mozilla Firefox, Apple Safari, and Internet Explorer in private and moveable browsing mode has been done by Donny J. Ohan, Narasimha, and Shashidhar [1]. The forensics of Google Chrome in both normal and private mode have been discussed by Andrew and Team [2]. Evidence pertaining to internet activity has been recovered from hard disc. Browser log files were taken into consideration by Junghoon Oh and Team [3] as a source of data for potential artefact extraction. Using RAM analysis, Huwida Said and Team [4] collected evidence. D. Rathod [5, 9] has taken RAM dump to gather objects connected to cyberspace actions on windows installed Google Chrome. In their study titled "Digital Forensic Analyses of Web Browser Records," E. Akbal, Futma G., and Ayhan [6] describe how web browsers and operating systems save data. In their research paper titled "Forensics Investigation of Web Application Security Attacks," Amor. L. and Thabet S. [7] deliberated the idea of net application scientific, describing it by way of a subset of nets scientific. They also proposed a procedure that would aid in the successful completion of an examination of net application safety. The following web browser forensic tools have been chosen by J. Oh, S. Lee, and Team [8]: WEFA, Cache Back 3.17, Encase 6.13, FTK 3.2, and Net Analysis 1.52. They concluded that WEFA would be the best tool for browser forensics.

Our review of the literature reveals that the majority of researchers employed browser history, local files, or hard disk examination as their primary bases of data for material extraction linked to online practice. In this research paper we focused on extraction of evidences related to Google search, Facebook, Web WhatsApp, ecommerce sites and movie sites form Google chrome, Mozilla Firefox and Brave web browsers. We focused on RAM forensics digital forensics techniques using volatility 3, Belkasoft Evidence Center X, FTK imager, and python 3.

3 Methodology

In this section we discussed the methodology adopted to carried out web browser forensics experiment.

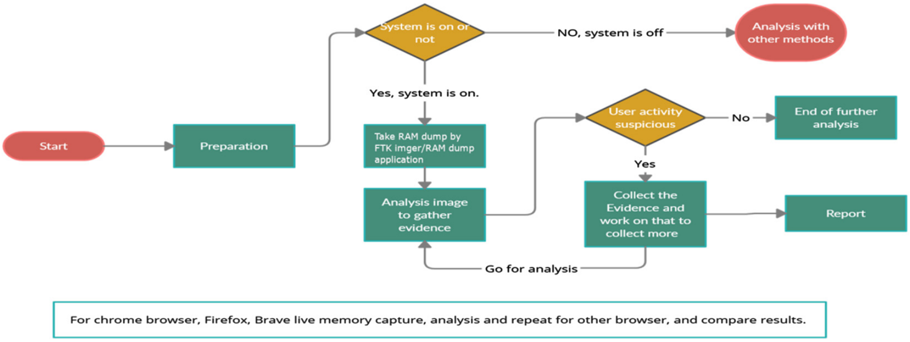

Start
Preparation
System is on or not
NO, system is off
Analysis with other methods
Yes, system is on.
Take RAM dump by FTK imger/RAM dump application
Analysis image to gather evidence
User activity suspicious
No
End of further analysis
Yes
Collect the Evidence and work on that to collect more
Report
Go for analysis
For chrome browser, Firefox, Brave live memory capture, analysis and repeat for other browser, and compare results.

Fig. 1. RAM Forensics Methodology

As shown in the Fig. 1, whenever first responder reaches to the crime scene then he needs to check that system is switched on or off if it is switched on then take the RAM dump using FTK image or any other RAM dump application. If system is switched off then used dead forensics techniques to carried out the forensic. It is important to note down the hash worth of the picture which will be the part of chain of custodian to ensure the integrity of the evidence [10, 11]. The RAM dump is analyzed by the Autopsy and FTK analysis and examination tools. After the analysis, we used keyword search techniques to identify the evidences and this process will be continue until we found the required evidences. Once required evidences found, digital forensic analyst may prepare the report which will be produced in the court.

4 Data Modeling

Table. 1. Data modeling

No	Source	Activity
1	Google.com	The random images related to nature images searched in the Google search engine and nature images downloaded
2	Facebook	Login in to Facebook account, post photos, delete post, send friend request and also chat with friends
3	WhatsApp web	Login in the WhatsApp web, send message “Text1” and receive reply of “Text 2”, made a voice call and video call, send media files and carried out chat also
4	Search for the paid product to download and also tried to find crack or key	lookingfor“adobephotoshopfree download” key word search, downloaded the same and also try to crack the same
5	Searching for free movie	free movie download site to download movies for free
6	Searching for attacks	Searching for tutorial or website which teach how to attack on any site

The goal and objective of this research paper is to represents what kind of artifacts we can get in different situation. To generate the real-world scenario, we have created data model shown in Table 1 in which various activities such as searching keywords in the Google search engine, login, post photos chatting in the Facebook and web WhatsApp etc., are carried out using Google, Facebook, web WhatsApp. Once these activates carried out, we taken RAM dump and analyzed with forensic tools to identify the evidences.

5 Laboratory Set-Up

We carried out the browser forensics with laptop and configure of the laptop is 8 GB RAM, intel i5 processor, 1 TB HDD, AMD Radeon HD 8730M - 2 GB GPU, Dell Inspiron 15R with Windows 10 home and build version 15.19042. The scenario is created with Google chrome version 90.0.4430.93, Mozilla Firefox 86.0.1(x64 en-US), Breve version 90.1.24.812. We have used following additional tools for imaging and analysis purpose,

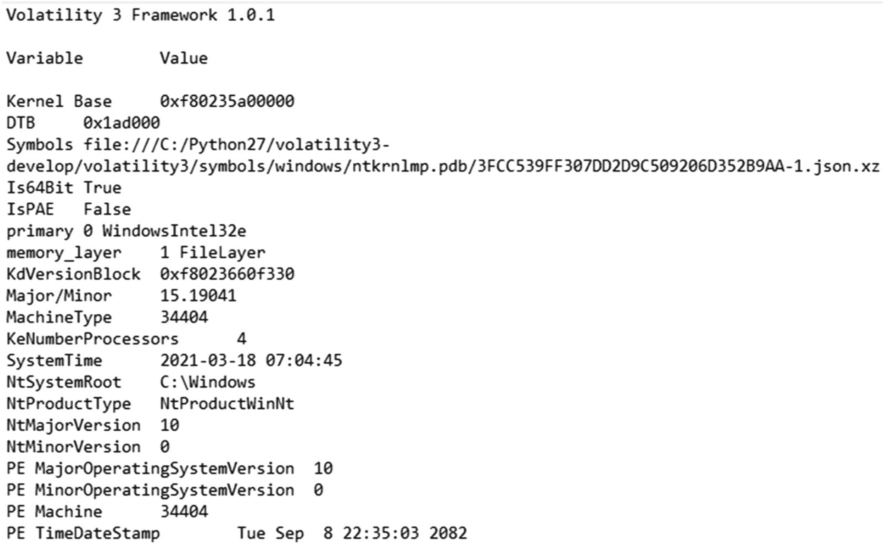
1. FTK imager: FTK imager is used to take the memory dump
2. FTK toolkit: Its computer forensics software and we used to process the memory dump to extract the evidences.
3. Volatility 3 Framework: This is worlds widely used framework to extract digital evidences from volatile memory (RAM).
4. Belkasoft Evidence Center X: This is a digital forensics suite and it will be used to acquires, examines and analyze the evidences form computer, mobile, cloud and RAM.

6 Results

In this section we discussed the evidences extracted for Google Chrome, Mozilla Firefox and Brave web browser forensics.

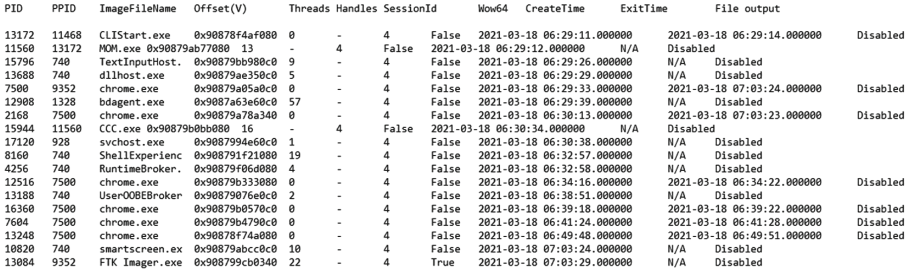
6.1 Google Chrome Browser Forensics

We created various scenario list in the Table 1 and taken RAM dump with Belkasoft. The RAM dump file memChrome.mem is proceed with Volatility 3.0 shown in Fig. 2 and recovered list of process is listed in the Fig. 3. We can see list of process with their name and created time. This will be the important evidences to find the list of programs recently executed by the user.



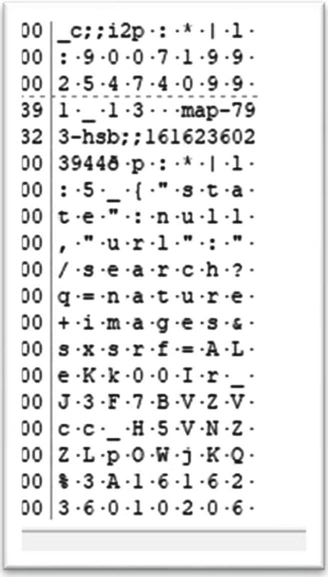
```
Volatility 3 Framework 1.0.1

Variable        Value

Kernel Base     0xf80235a00000
DTB     0x1ad000
Symbols file:///C:/Python27/volatility3-
develop/volatility3/symbols/windows/ntkrnlmp.pdb/3FCC539FF307DD2D9C509206D352B9AA-1.json.xz
Is64Bit True
IsPAE   False
primary 0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf8023660f330
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      4
SystemTime      2021-03-18 07:04:45
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Tue Sep  8 22:35:03 2082
```

Fig. 2. Image Info (Volatility 3)



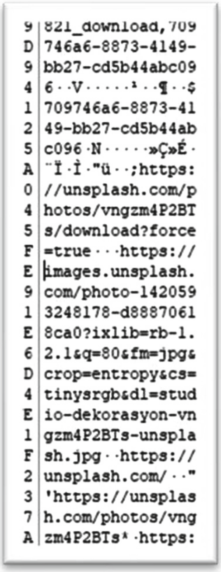
```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

13172   11468   CLIStart.exe    0x90878f4af080  0       -       4       False   2021-03-18 06:29:11.000000      2021-03-18 06:29:14.000000      Disabled
11560   13172   MOM.exe 0x90879ab77080  13      -       4       False   2021-03-18 06:29:12.000000      N/A     Disabled
15796   740     TextInputHost.  0x90879bb980c0  9       -       4       False   2021-03-18 06:29:26.000000      N/A     Disabled
13688   740     dllhost.exe     0x90879ae350c0  5       -       4       False   2021-03-18 06:29:29.000000      N/A     Disabled
7500    9352    chrome.exe      0x90879a05a0c0  0       -       4       False   2021-03-18 06:29:33.000000      2021-03-18 07:03:24.000000      Disabled
12908   1328    bdagent.exe     0x9087a63e60c0  57      -       4       False   2021-03-18 06:29:39.000000      N/A     Disabled
2168    7500    chrome.exe      0x90879a78a340  0       -       4       False   2021-03-18 06:30:13.000000      2021-03-18 07:03:23.000000      Disabled
15944   11560   CCC.exe 0x90879b0bb080  16      -       4       False   2021-03-18 06:30:34.000000      N/A     Disabled
17120   928     svchost.exe     0x9087994e60c0  1       -       4       False   2021-03-18 06:30:38.000000      N/A     Disabled
8160    740     ShellExperienc  0x908791f21080  19      -       4       False   2021-03-18 06:32:57.000000      N/A     Disabled
4256    740     RuntimeBroker.  0x90879f06d080  4       -       4       False   2021-03-18 06:32:58.000000      N/A     Disabled
12516   7500    chrome.exe      0x90879b333080  0       -       4       False   2021-03-18 06:34:16.000000      2021-03-18 06:34:22.000000      Disabled
13188   740     UserOOBEBroker  0x90879076e0c0  2       -       4       False   2021-03-18 06:38:51.000000      N/A     Disabled
16360   7500    chrome.exe      0x90879b0570c0  0       -       4       False   2021-03-18 06:39:18.000000      2021-03-18 06:39:22.000000      Disabled
7604    7500    chrome.exe      0x90879b4790c0  0       -       4       False   2021-03-18 06:41:24.000000      2021-03-18 06:41:28.000000      Disabled
13248   7500    chrome.exe      0x90878f74a080  0       -       4       False   2021-03-18 06:49:48.000000      2021-03-18 06:49:51.000000      Disabled
10820   740     smartscreen.ex  0x90879abcc0c0  10      -       4       False   2021-03-18 07:03:24.000000      N/A     Disabled
13084   9352    FTK Imager.exe  0x908799cb0340  22      -       4       True    2021-03-18 07:03:29.000000      N/A     Disabled
```

Fig. 3. Process List (Volatility 3.0)



```
00 |_c;;i2p·:·*·|·l·
00 |:·9·0·0·7·1·9·9·
00 |2·5·4·7·4·0·9·9·
39 |l·_·l·3···map-79
32 |3-hsb;;161623602
00 |39448·p·:·*·|·l·
00 |:·5·_·{·"·s·t·a·
00 |t·e·"·:·n·u·l·l·
00 |,·"·u·r·l·"·:·"·
00 |/·s·e·a·r·c·h·?·
00 |q·=·n·a·t·u·r·e·
00 |+·i·m·a·g·e·s·&·
00 |s·x·s·r·f·=·A·L·
00 |e·K·k·0·0·I·r·_·
00 |J·3·F·7·B·V·Z·V·
00 |c·c·_·H·5·V·N·Z·
00 |Z·L·p·O·W·j·K·Q·
00 |%·3·A·1·6·1·6·2·
00 |3·6·0·1·0·2·0·6·
```

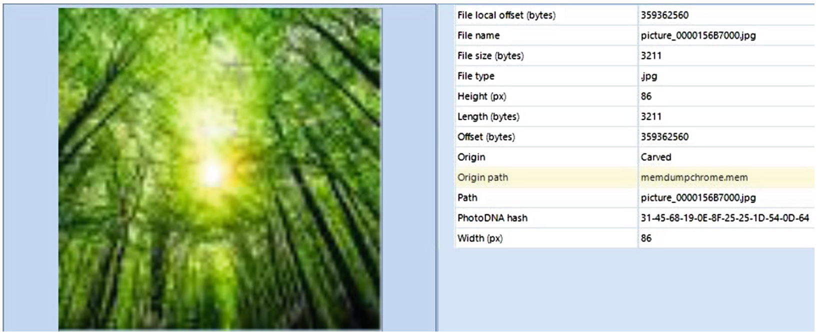
Fig. 4. Searched text in the Google Search Engine



```
9 |821_download,709
D |746a6-8873-4149-
9 |bb27-cd5b44abc09
4 |6··V·····¹··¶··$
1 |709746a6-8873-41
2 |49-bb27-cd5b44ab
5 |c096·N·····»Ç»É·
A |¨Ï·Ì·"ü··;https:
0 |//unsplash.com/p
4 |hotos/vngzm4P2BT
5 |s/download?force
F |=true···https://
E |images.unsplash.
9 |com/photo-142059
1 |3248178-d8887061
E |8ca0?ixlib=rb-1.
6 |2.1&q=80&fm=jpg&
D |crop=entropy&cs=
4 |tinysrgb&dl=stud
E |io-dekorasyon-vn
1 |gzm4P2BTs-unspla
F |sh.jpg··https://
2 |unsplash.com/··"
3 |'https://unsplas
7 |h.com/photos/vng
A |zm4P2BTs*·https:
```

Fig. 5. Visited URL by user

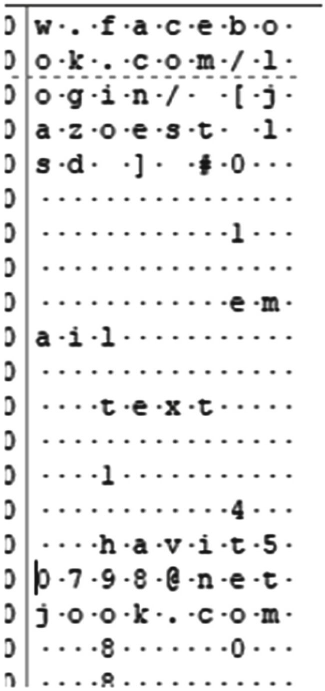
Extracted evidences shows in Fig. 4 depicts that user has searched nature image in the Google search engine and Fig. 5 shows the URL of the site that user has visited. Figure 6 shows image which was download by the user and this evidence is extracted by the Belkasoft.



File local offset (bytes)	359362560
File name	picture_0000156B7000.jpg
File size (bytes)	3211
File type	.jpg
Height (px)	86
Length (bytes)	3211
Offset (bytes)	359362560
Origin	Carved
Origin path	memdumpchrome.mem
Path	picture_0000156B7000.jpg
PhotoDNA hash	31-45-68-19-0E-8F-25-25-1D-54-0D-64
Width (px)	86

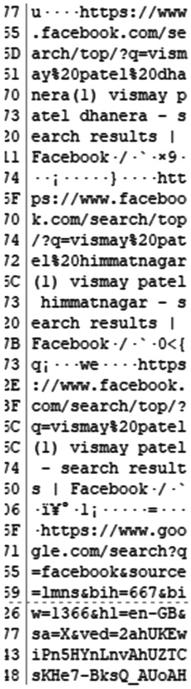
Fig. 6. Image which was download by the user (Belkasoft).

Facebook login evidence is shown in the Fig. 7 and searched people related evidences in the Facebook is shown in Fig. 8.



```
0 |w·.·f·a·c·e·b·o·
0 |o·k·.·c·o·m·/·l·
0 |o·g·i·n·/· ·[·j·
0 |a·z·o·e·s·t· ·l·
0 |s·d· ·]· ·#·0···
0 | ···············
0 | ···········l···
0 | ···············
0 | ···········e·m·
0 |a·i·l···········
0 | ···············
0 | ···t·e·x·t·····
0 | ···············
0 | ···l···········
0 | ···········4···
0 | ···h·a·v·i·t·5·
0 |b·7·9·8·@·n·e·t·
0 |j·o·o·k·.·c·o·m·
0 | ···8·······0···
0 | ···8···········
```

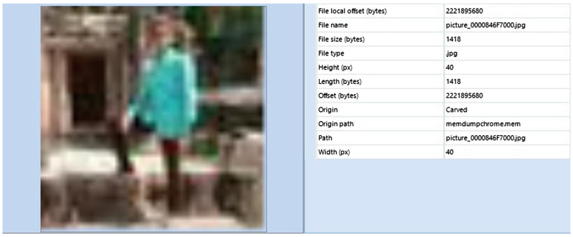
Fig. 7. Facebook login page (FTK)



```
77 |u····https://www
55 |.facebook.com/se
5D |arch/top/?q=vism
51 |ay%20patel%20dha
70 |nera(1) vismay p
73 |atel dhanera - s
20 |earch results |
11 |Facebook·/·`·×9·
74 |··¡·····}····htt
5F |ps://www.faceboo
70 |k.com/search/top
74 |/?q=vismay%20pat
72 |el%20himmatnagar
5C |(1) vismay patel
73 | himmatnagar - s
20 |earch results |
7B |Facebook·/·`·0<{
73 |q¡···we····https
2E |://www.facebook.
3F |com/search/top/?
5C |q=vismay%20patel
5C |(1) vismay patel
74 | - search result
50 |s | Facebook·/·`
06 |·ï¥°·1¡·····=···
5F |·https://www.goo
71 |gle.com/search?q
55 |=facebook&source
59 |=lmns&bih=667&bi
26 |w=1366&hl=en-GB&
77 |sa=X&ved=2ahUKEw
13 |iPn5HYnLnvAhUZTC
18 |sKHe7-BksQ_AUoAH
```

Fig. 8. People search details in Facebook (FTK)

We are able to extract the evidences related to profile picture of the user from RAM shown in the Fig. 9 and original profile picture show in Fig. 10.



File local offset (bytes)	2221895680
File name	picture_0000846F7000.jpg
File size (bytes)	1418
File type	.jpg
Height (px)	40
Length (bytes)	1418
Offset (bytes)	2221895680
Origin	Carved
Origin path	memdumpchrome.mem
Path	picture_0000846F7000.jpg
Width (px)	40

Fig. 9. Extracted profile of the user in the Facebook

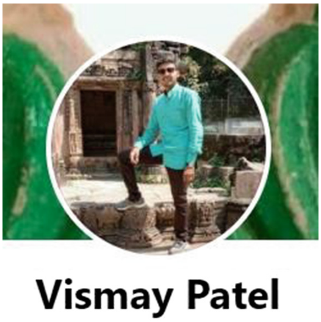
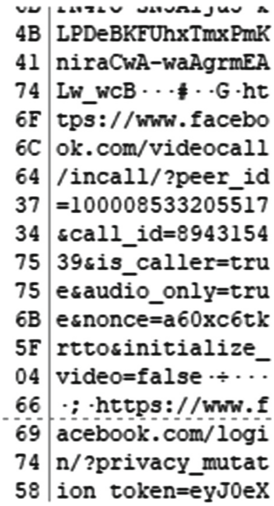


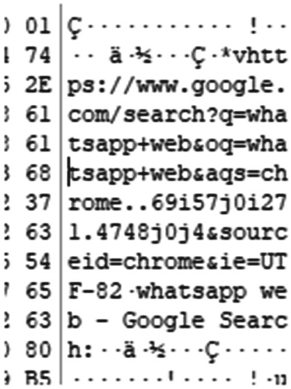
Fig. 10. Original Photo

We are unable to find artifacts related to request send, message send, photo sent but able to find the video call attempt shown in the Fig. 11 using FTK. Figure 12 shows that user has search web whatsapp in the google search engine and Fig. 13 shows mobile number that user has has used to login in the web WhatsApp.



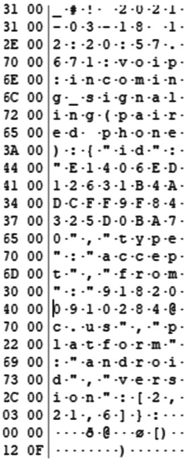
```
4B LPDeBKFUhxTmxPmK
41 niraCwA-waAgrmEA
74 Lw_wcB···#··G·ht
6F tps://www.facebo
6C ok.com/videocall
64 /incall/?peer_id
37 =100008533205517
34 &call_id=8943154
75 39&is_caller=tru
75 e&audio_only=tru
6B e&nonce=a60xc6tk
5F rtto&initialize_
04 video=false·÷···
66 ·;·https://www.f
69 acebook.com/logi
74 n/?privacy_mutat
58 ion token=eyJ0eX
```

Fig. 11. Video call through Facebook (FTK)



```
01 Ç············!··
74 ·· ä·½···Ç·*vhtt
2E ps://www.google.
61 com/search?q=wha
61 tsapp+web&oq=wha
68 tsapp+web&aqs=ch
37 rome..69i57j0i27
63 1.4748j0j4&sourc
54 eid=chrome&ie=UT
65 F-82·whatsapp we
63 b - Google Searc
80 h:··ä·½···Ç·····
B5 ·······!····!·
```

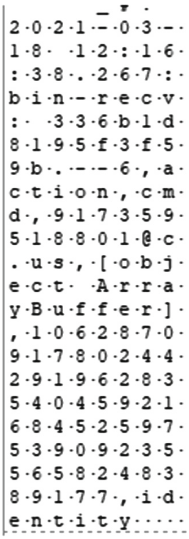
Fig. 12. Web WhatsApp Search Details (FTK)



```
31 00 _·#·!·  ·2·0·2·1·
31 00 –·0·3·–·1·8·  ·1·
2E 00 2·:·2·0·:·5·7·.·
70 00 6·7·1·:·v·o·i·p·
6E 00 :·i·n·c·o·m·i·n·
6C 00 g·_·s·i·g·n·a·l·
72 00 i·n·g·(·p·a·i·r·
65 00 e·d·  ·p·h·o·n·e·
3A 00 )·:·{·"·i·d·"·:·
44 00 "·E·1·4·0·6·E·D·
41 00 1·2·6·3·1·B·4·A·
34 00 D·C·F·F·9·F·8·4·
37 00 3·2·5·D·0·B·A·7·
65 00 0·"·,·"·t·y·p·e·
70 00 "·:·"·a·c·c·e·p·
6D 00 t·"·,·"·f·r·o·m·
30 00 "·:·"·9·1·8·2·0·
40 00 0·9·1·0·2·8·4·@·
70 00 c·.·u·s·"·,·"·p·
22 00 l·a·t·f·o·r·m·"·
69 00 :·"·a·n·d·r·o·i·
73 00 d·"·,·"·v·e·r·s·
2C 00 i·o·n·"·:·[·2·,·
03 00 2·1·,·6·]·}·:···
00 00 ····ð·@···ø·[)··
12 0F ·······)·······
```

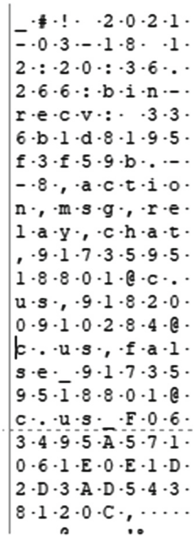
Fig. 13. Web WhatsApp login number retrieved (FTK)

As far as Web WhatsApp calling and chat concern, we are able to recover a artifact of receivers mobile number shown in Fig. 14 and also able to find that with which user (mobile no) user is doing a chat shown in Fig. 15. We are not able to find the evidences related to content of the chat.



```
2·0·2·1·–·0·3·–·
1·8· ·1·2·:·1·6·
:·3·8·.·2·6·7·:·
b·i·n·–·r·e·c·v·
:· ·3·3·6·b·l·d·
8·1·9·5·f·3·f·5·
9·b·.·–·–·6·,·a·
c·t·i·o·n·,·c·m·
d·,·9·1·7·3·5·9·
5·1·8·8·0·1·@·c·
.·u·s·,·[·o·b·j·
e·c·t· ·A·r·r·a·
y·B·u·f·f·e·r·]·
,·1·0·6·2·8·7·0·
9·1·7·8·0·2·4·4·
2·9·1·9·6·2·8·3·
5·4·0·4·5·9·2·1·
6·8·4·5·2·5·9·7·
5·3·9·0·9·2·3·5·
5·6·5·8·2·4·8·3·
8·9·1·7·7·,·i·d·
e·n·t·i·t·y·····
```

Fig. 14. Web WhatsApp Receiver Mobile no. (FTK)



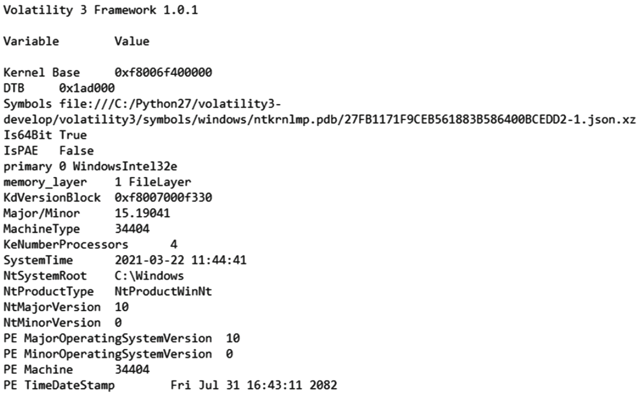
```
_·#·!· ·2·0·2·1·
–·0·3·–·1·8· ·1·
2·:·2·0·:·3·6·.·
2·6·6·:·b·i·n·–·
r·e·c·v·:· ·3·3·
6·b·l·d·8·1·9·5·
f·3·f·5·9·b·.·–·
–·8·,·a·c·t·i·o·
n·,·m·s·g·,·r·e·
l·a·y·,·c·h·a·t·
,·9·1·7·3·5·9·5·
1·8·8·0·1·@·c·.·
u·s·,·9·1·8·2·0·
0·9·1·0·2·8·4·@·
c·.·u·s·,·f·a·l·
s·e·_·9·1·7·3·5·
9·5·1·8·8·0·1·@·
c·.·u·s·_·F·0·6·
3·4·9·5·A·5·7·1·
0·6·1·E·0·E·1·D·
2·D·3·A·D·5·4·3·
8·1·2·0·C·,·····
```

Fig. 15. Web WhatsApp Chat Receiver

6.2 Mozilla Firefox Browser Forensics

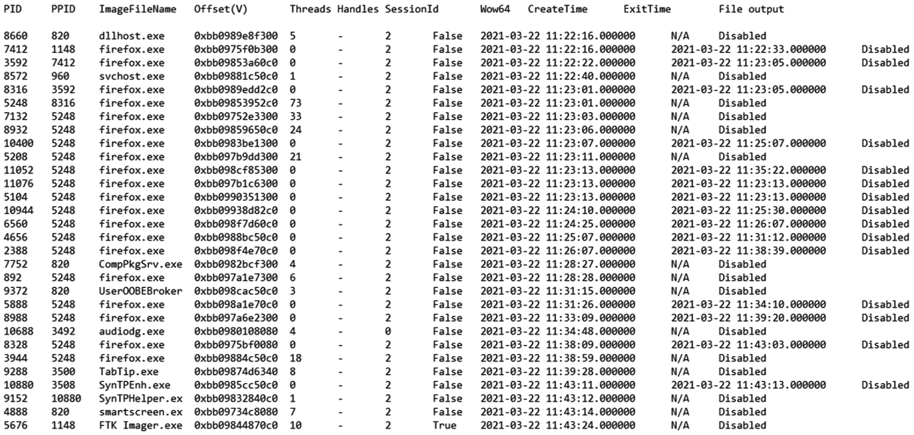
We have crated scenario listed in the Table 1 with Mozilla Firefox and taken the RAM dump using Belkasoft. The RAM dump is processed with FTK and Bulkasoft to identify the evidences related to activities performed by us. In this section, we have discussed the identified evidences for various activities.

The RAM image is processed by the Volatility 3 shown in Fig. 16 and process list is shown in the Fig. 17. We can identify the evidences related to Mozilla Firefox along with creation time.



```
Volatility 3 Framework 1.0.1

Variable        Value

Kernel Base     0xf8006f400000
DTB     0x1ad000
Symbols file:///C:/Python27/volatility3-
develop/volatility3/symbols/windows/ntkrnlmp.pdb/27FB1171F9CEB561883B586400BCEDD2-1.json.xz
Is64Bit True
IsPAE   False
primary 0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf8007000f330
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      4
SystemTime      2021-03-22 11:44:41
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Fri Jul 31 16:43:11 2082
```

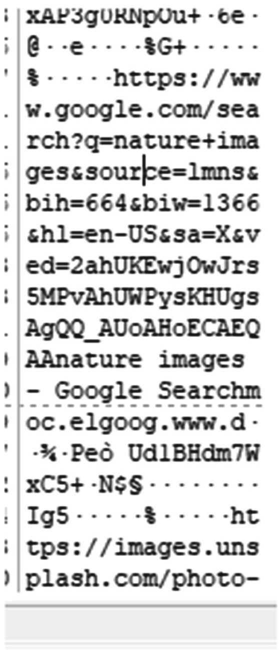
Fig. 16. Image info (Volatility 3)



```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

8660    820     dllhost.exe     0xbb0989e8f300  5       -       2       False   2021-03-22 11:22:16.000000      N/A     Disabled
7412    1148    firefox.exe     0xbb0975f0b300  0       -       2       False   2021-03-22 11:22:16.000000      2021-03-22 11:22:33.000000      Disabled
3592    7412    firefox.exe     0xbb09853a60c0  0       -       2       False   2021-03-22 11:22:22.000000      2021-03-22 11:23:05.000000      Disabled
8572    960     svchost.exe     0xbb09881c50c0  1       -       2       False   2021-03-22 11:22:40.000000      N/A     Disabled
8316    3592    firefox.exe     0xbb0989edd2c0  0       -       2       False   2021-03-22 11:23:01.000000      2021-03-22 11:23:05.000000      Disabled
5248    8316    firefox.exe     0xbb09853952c0  73      -       2       False   2021-03-22 11:23:01.000000      N/A     Disabled
7132    5248    firefox.exe     0xbb09752e3300  33      -       2       False   2021-03-22 11:23:03.000000      N/A     Disabled
8932    5248    firefox.exe     0xbb09859650c0  24      -       2       False   2021-03-22 11:23:06.000000      N/A     Disabled
10400   5248    firefox.exe     0xbb0983be1300  0       -       2       False   2021-03-22 11:23:07.000000      2021-03-22 11:25:07.000000      Disabled
5208    5248    firefox.exe     0xbb097b9dd300  21      -       2       False   2021-03-22 11:23:11.000000      N/A     Disabled
11052   5248    firefox.exe     0xbb098cf85300  0       -       2       False   2021-03-22 11:23:13.000000      2021-03-22 11:35:22.000000      Disabled
11076   5248    firefox.exe     0xbb097b1c6300  0       -       2       False   2021-03-22 11:23:13.000000      2021-03-22 11:23:13.000000      Disabled
5104    5248    firefox.exe     0xbb0990351300  0       -       2       False   2021-03-22 11:23:13.000000      2021-03-22 11:23:13.000000      Disabled
10944   5248    firefox.exe     0xbb09938d82c0  0       -       2       False   2021-03-22 11:24:10.000000      2021-03-22 11:25:30.000000      Disabled
6560    5248    firefox.exe     0xbb098f7d60c0  0       -       2       False   2021-03-22 11:24:25.000000      2021-03-22 11:26:07.000000      Disabled
4656    5248    firefox.exe     0xbb0988bc50c0  0       -       2       False   2021-03-22 11:25:07.000000      2021-03-22 11:31:12.000000      Disabled
2388    5248    firefox.exe     0xbb098f4e70c0  0       -       2       False   2021-03-22 11:26:07.000000      2021-03-22 11:38:39.000000      Disabled
7752    820     CompPkgSrv.exe  0xbb0982bcf300  4       -       2       False   2021-03-22 11:28:27.000000      N/A     Disabled
892     5248    firefox.exe     0xbb097a1e7300  6       -       2       False   2021-03-22 11:28:28.000000      N/A     Disabled
9372    820     UserOOBEBroker  0xbb098cac50c0  3       -       2       False   2021-03-22 11:31:15.000000      N/A     Disabled
5888    5248    firefox.exe     0xbb098a1e70c0  0       -       2       False   2021-03-22 11:31:26.000000      2021-03-22 11:34:10.000000      Disabled
8988    5248    firefox.exe     0xbb097a6e2300  0       -       2       False   2021-03-22 11:33:09.000000      2021-03-22 11:39:20.000000      Disabled
10688   3492    audiodg.exe     0xbb0980108080  4       -       0       False   2021-03-22 11:34:48.000000      N/A     Disabled
8328    5248    firefox.exe     0xbb0975bf0080  0       -       2       False   2021-03-22 11:38:09.000000      2021-03-22 11:43:03.000000      Disabled
3944    5248    firefox.exe     0xbb09884c50c0  18      -       2       False   2021-03-22 11:38:59.000000      N/A     Disabled
9288    3500    TabTip.exe      0xbb09874d6340  8       -       2       False   2021-03-22 11:39:28.000000      N/A     Disabled
10880   3508    SynTPEnh.exe    0xbb0985cc50c0  0       -       2       False   2021-03-22 11:43:11.000000      2021-03-22 11:43:13.000000      Disabled
9152    10880   SynTPHelper.ex  0xbb09832840c0  1       -       2       False   2021-03-22 11:43:12.000000      N/A     Disabled
4888    820     smartscreen.ex  0xbb09734c8080  7       -       2       False   2021-03-22 11:43:14.000000      N/A     Disabled
5676    1148    FTK Imager.exe  0xbb09844870c0  10      -       2       True    2021-03-22 11:43:24.000000      N/A     Disabled
```

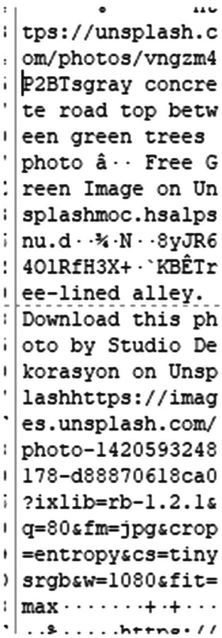
Fig. 17. Profess List (Volatility 3)

The user has searched for the in the Google search engine for the nature images and we are able to find the evidences related to search item from the RAM shown in Fig. 18. We are able to find the URL of the site from which nature image is downloaded as shown in the Fig. 19.



```
xAP3gURNpUu+·6e·
@··e····$G+·····
$·····https://ww
w.google.com/sea
rch?q=nature+ima
ges&source=lmns&
bih=664&biw=1366
&hl=en-US&sa=X&v
ed=2ahUKEwjOwJrs
5MPvAhUWPysKHUgs
AgQQ_AUoAHoECAEQ
AAnature images
- Google Searchm
oc.elgoog.www.d·
·¾·Peò Ud1BHdm7W
xC5+·N$§········
Ig5·····$·····ht
tps://images.uns
plash.com/photo-
```

Fig. 18. Google Search results (FTK)



```
tps://unsplash.c
om/photos/vngzm4
P2BTsgray concre
te road top betw
een green trees
photo â·· Free G
reen Image on Un
splashmoc.hsalps
nu.d··¾·N··8yJR6
401RfH3X+·`KBÊTr
ee-lined alley.
Download this ph
oto by Studio De
korasyon on Unsp
lashhttps://imag
es.unsplash.com/
photo-1420593248
178-d88870618ca0
?ixlib=rb-1.2.1&
q=80&fm=jpg&crop
=entropy&cs=tiny
srgb&w=1080&fit=
max·······+·+···
··$·····https://
```

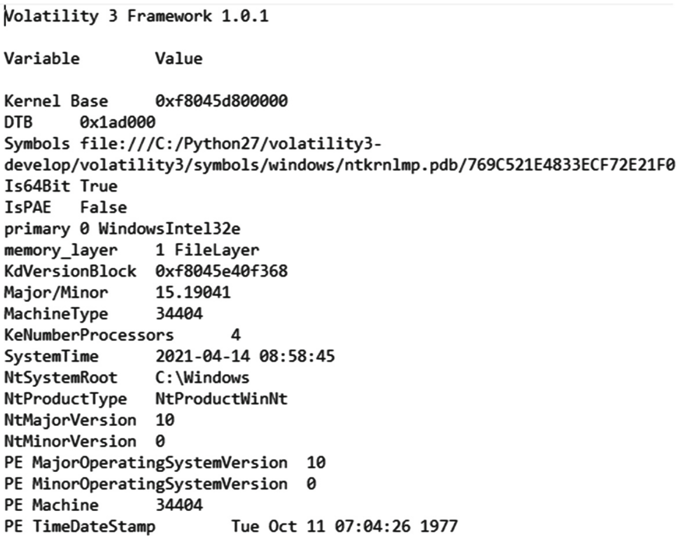
Fig. 19. URI of site to download the image (FTK)

6.3 Brave Browser Forensics

The Brave Browser is constructed on the open-source Chromium Web core and client code is released under the Mozilla Public License 2.0 [13]. Brave, a browser which conceits the situation in the safety and confidentiality it offers and it has more than 13 million active handlers per month [16] or 0.05% of Global Desktop Browser Market Share [17]. As Brave browser is open sources and considering the percentage share in the global desktop browser market, it is important to know that what kind of evidence a digital forensic analysis can found in case Brave browser is used to committee the crime.

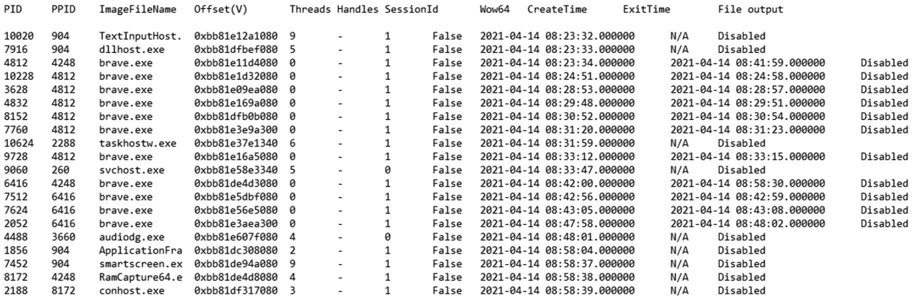
We have carried out the activities list in the data model Table 1 using Brave browser and taken the RAM dump. The following evidences were obtained for the activities list in the Table 1.

The image of RAM dump created for the Brave browser is process by the volatility 3.0 framework shown in Fig. 20 and process list listed by the volatility 3.0 is shown in the Fig. 38. We observed the evidences related to Brave browser along with created date (Fig. 21).



```
Volatility 3 Framework 1.0.1

Variable        Value

Kernel Base     0xf8045d800000
DTB     0x1ad000
Symbols file:///C:/Python27/volatility3-
develop/volatility3/symbols/windows/ntkrnlmp.pdb/769C521E4833ECF72E21F0
Is64Bit True
IsPAE   False
primary 0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf8045e40f368
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      4
SystemTime      2021-04-14 08:58:45
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Tue Oct 11 07:04:26 1977
```

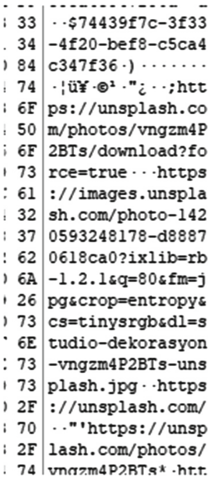
Fig. 20. Image info of Brave browser [Volatility 3]



```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

10020   904     TextInputHost.  0xbb81e12a1080  9       -       1       False   2021-04-14 08:23:32.000000      N/A     Disabled
7916    904     dllhost.exe     0xbb81dfbef080  5       -       1       False   2021-04-14 08:23:33.000000      N/A     Disabled
4812    4248    brave.exe       0xbb81e11d4080  0       -       1       False   2021-04-14 08:23:34.000000      2021-04-14 08:41:59.000000      Disabled
10228   4812    brave.exe       0xbb81e1d32080  0       -       1       False   2021-04-14 08:24:51.000000      2021-04-14 08:24:58.000000      Disabled
3628    4812    brave.exe       0xbb81e09ea080  0       -       1       False   2021-04-14 08:28:53.000000      2021-04-14 08:28:57.000000      Disabled
4832    4812    brave.exe       0xbb81e169a080  0       -       1       False   2021-04-14 08:29:48.000000      2021-04-14 08:29:51.000000      Disabled
8152    4812    brave.exe       0xbb81dfb0b080  0       -       1       False   2021-04-14 08:30:52.000000      2021-04-14 08:30:54.000000      Disabled
7760    4812    brave.exe       0xbb81e3e9a300  0       -       1       False   2021-04-14 08:31:20.000000      2021-04-14 08:31:23.000000      Disabled
10624   2288    taskhostw.exe   0xbb81e37e1340  6       -       1       False   2021-04-14 08:31:59.000000      N/A     Disabled
9728    4812    brave.exe       0xbb81e16a5080  0       -       1       False   2021-04-14 08:33:12.000000      2021-04-14 08:33:15.000000      Disabled
9060    260     svchost.exe     0xbb81e58e3340  5       -       0       False   2021-04-14 08:33:47.000000      N/A     Disabled
6416    4248    brave.exe       0xbb81de4d3080  0       -       1       False   2021-04-14 08:42:00.000000      2021-04-14 08:58:30.000000      Disabled
7512    6416    brave.exe       0xbb81e5dbf080  0       -       1       False   2021-04-14 08:42:56.000000      2021-04-14 08:42:59.000000      Disabled
7624    6416    brave.exe       0xbb81e56e5080  0       -       1       False   2021-04-14 08:43:05.000000      2021-04-14 08:43:08.000000      Disabled
2052    6416    brave.exe       0xbb81e3aea300  0       -       1       False   2021-04-14 08:47:58.000000      2021-04-14 08:48:02.000000      Disabled
4488    3660    audiodg.exe     0xbb81e607f080  4       -       0       False   2021-04-14 08:48:01.000000      N/A     Disabled
1856    904     ApplicationFra  0xbb81dc308080  2       -       1       False   2021-04-14 08:58:04.000000      N/A     Disabled
7452    904     smartscreen.ex  0xbb81de94a080  9       -       1       False   2021-04-14 08:58:37.000000      N/A     Disabled
8172    4248    RamCapture64.e  0xbb81de4d8080  4       -       1       False   2021-04-14 08:58:38.000000      N/A     Disabled
2188    8172    conhost.exe     0xbb81df317080  3       -       1       False   2021-04-14 08:58:39.000000      N/A     Disabled
```

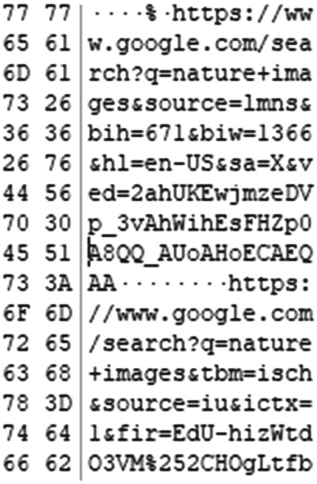
Fig. 21. Process list [Volatility 3]

The user has searched for the nature images in the Google search engine and we recovered evidences for the same in the Fig. 22. We are also able to find the URL of the web site form which user downloaded the nature images (Fig. 23) .



```
33 | ··$74439f7c-3f33
34 | -4f20-bef8-c5ca4
84 | c347f36·)·······
74 | ·¦ü¥·©¹·"¿··;htt
6F | ps://unsplash.co
50 | m/photos/vngzm4P
6F | 2BTs/download?fo
73 | rce=true···https
61 | ://images.unspla
32 | sh.com/photo-142
37 | 0593248178-d8887
62 | 0618ca0?ixlib=rb
6A | -1.2.1&q=80&fm=j
26 | pg&crop=entropy&
73 | cs=tinysrgb&dl=s
6E | tudio-dekorasyon
73 | -vngzm4P2BTs-uns
73 | plash.jpg··https
2F | ://unsplash.com/
70 | ··"'https://unsp
2F | lash.com/photos/
74 | vngzm4P2BTs*·htt
```

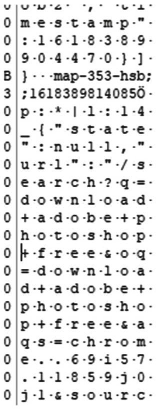
Fig. 22. Search text in the Google search engine



```
77 77 | ····$·https://ww
65 61 | w.google.com/sea
6D 61 | rch?q=nature+ima
73 26 | ges&source=lmns&
36 36 | bih=671&biw=1366
26 76 | &hl=en-US&sa=X&v
44 56 | ed=2ahUKEwjmzeDV
70 30 | p_3vAhWihEsFHZp0
45 51 | A8QQ_AUoAHoECAEQ
73 3A | AA·········https:
6F 6D | //www.google.com
72 65 | /search?q=nature
63 68 | +images&tbm=isch
78 3D | &source=iu&ictx=
74 64 | 1&fir=EdU-hizWtd
66 62 | O3VM%252CHOgLtfb
```

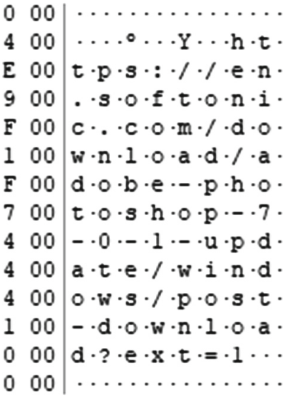
Fig. 23. URL of the site to download image

The evidence related to keywork search "Adobe" and URL of the site from which Adobe is download is recovered from RAM and same is shown is Fig. 24 and Fig. 25 respectively.



```
0 m·e·s·t·a·m·p·"·
0 :·1·6·1·8·3·8·9·
0 9·0·4·4·7·0·}·]·
B }···map-353-hsb;
3 ;1618389814085Ö·
0 p·:·*·|·1·:·1·4·
0 _·{·"·s·t·a·t·e·
0 "·:·n·u·l·l·,·"·
0 u·r·l·"·:·"·/·s·
0 e·a·r·c·h·?·q·=·
0 d·o·w·n·l·o·a·d·
0 +·a·d·o·b·e·+·p·
0 h·o·t·o·s·h·o·p·
0 +·f·r·e·e·&·o·q·
0 =·d·o·w·n·l·o·a·
0 d·+·a·d·o·b·e·+·
0 p·h·o·t·o·s·h·o·
0 p·+·f·r·e·e·&·a·
0 q·s·=·c·h·r·o·m·
0 e·.·.·6·9·i·5·7·
0 .·1·1·8·5·9·j·0·
0 j·l·&·s·o·u·r·c·
```

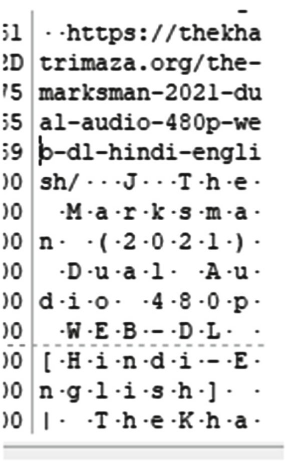
Fig. 24. Adobe keywork search in the Google search engine



```
0 00 ················
4 00 ····°···Y···h·t·
E 00 t·p·s·:·/·/·e·n·
9 00 .·s·o·f·t·o·n·i·
F 00 c·.·c·o·m·/·d·o·
1 00 w·n·l·o·a·d·/·a·
F 00 d·o·b·e·-·p·h·o·
7 00 t·o·s·h·o·p·-·7·
4 00 -·0·-·1·-·u·p·d·
4 00 a·t·e·/·w·i·n·d·
4 00 o·w·s·/·p·o·s·t·
1 00 -·d·o·w·n·l·o·a·
0 00 d·?·e·x·t·=·1···
0 00 ················
```

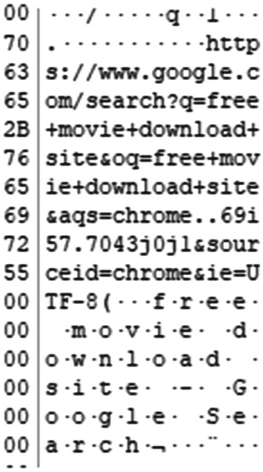
Fig. 25. URL of the site to download Adobe

The evidence related to free movie search, URL of the site from which movie is downloaded and URL of the YouTube video which user has watched is shown in Fig. 26, Fig. 27 and Fig. 28 respectively.



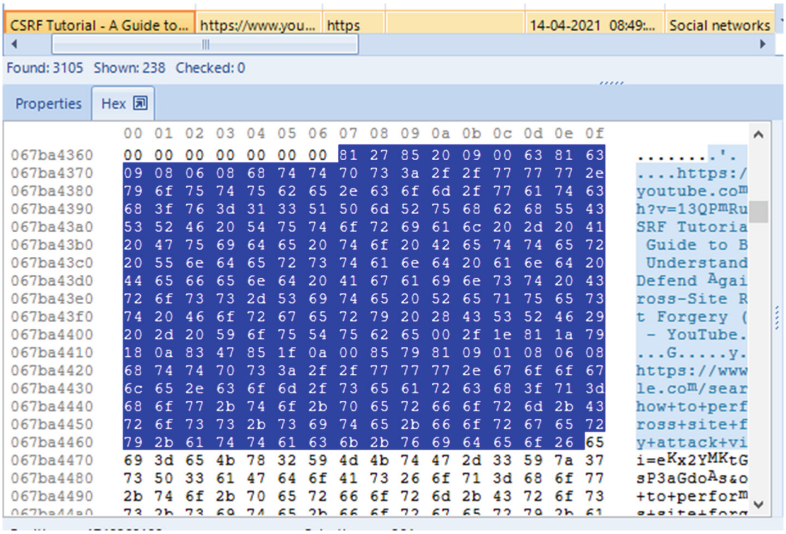
```
51 ··https://thekha
2D trimaza.org/the-
75 marksman-2021-du
55 al-audio-480p-we
59 b-dl-hindi-engli
00 sh/···J···T·h·e·
00  ·M·a·r·k·s·m·a·
00 n· ·(·2·0·2·1·)·
00  ·D·u·a·l· ·A·u·
00 d·i·o· ·4·8·0·p·
00  ·W·E·B·-·D·L· ·
00 [·H·i·n·d·i·-·E·
00 n·g·l·i·s·h·]· ·
00 |· ·T·h·e·K·h·a·
```

Fig. 26. Movie search in the Google Search Engine (FTK)



```
00 ···/·····q··1···
70 .···········http
63 s://www.google.c
65 om/search?q=free
2B +movie+download+
76 site&oq=free+mov
65 ie+download+site
69 &aqs=chrome..69i
72 57.7043j0j1&sour
55 ceid=chrome&ie=U
00 TF-8(···f·r·e·e·
00  ·m·o·v·i·e· ·d·
00 o·w·n·l·o·a·d· ·
00 s·i·t·e· ·-· ·G·
00 o·o·g·l·e· ·S·e·
00 a·r·c·h·¬···¨···
```

Fig. 27. URL of site to download movie (FTK)



CSRF Tutorial - A Guide to... | https://www.you... | https | | 14-04-2021 08:49:... | Social networks
Found: 3105 Shown: 238 Checked: 0
Properties
Hex

```
          00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
067ba4360 00 00 00 00 00 00 00 81 27 85 20 09 00 63 81 63   ........'.
067ba4370 09 08 06 08 68 74 74 70 73 3a 2f 2f 77 77 77 2e   ....https:/
067ba4380 79 6f 75 74 75 62 65 2e 63 6f 6d 2f 77 61 74 63   youtube.com
067ba4390 68 3f 76 3d 31 33 51 50 6d 52 75 68 62 68 55 43   h?v=13QPmRu
067ba43a0 53 52 46 20 54 75 74 6f 72 69 61 6c 20 2d 20 41   SRF Tutoria
067ba43b0 20 47 75 69 64 65 20 74 6f 20 42 65 74 74 65 72    Guide to B
067ba43c0 20 55 6e 64 65 72 73 74 61 6e 64 20 61 6e 64 20    Understand
067ba43d0 44 65 66 65 6e 64 20 41 67 61 69 6e 73 74 20 43   Defend Agai
067ba43e0 72 6f 73 73 2d 53 69 74 65 20 52 65 71 75 65 73   ross-Site R
067ba43f0 74 20 46 6f 72 67 65 72 79 20 28 43 53 52 46 29   t Forgery (
067ba4400 20 2d 20 59 6f 75 54 75 62 65 00 2f 1e 81 1a 79    - YouTube.
067ba4410 18 0a 83 47 85 1f 0a 00 85 79 81 09 01 08 06 08   ...G.....y.
067ba4420 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67   https://www
067ba4430 6c 65 2e 63 6f 6d 2f 73 65 61 72 63 68 3f 71 3d   le.com/sear
067ba4440 68 6f 77 2b 74 6f 2b 70 65 72 66 6f 72 6d 2b 43   how+to+perf
067ba4450 72 6f 73 73 2b 73 69 74 65 2b 66 6f 72 67 65 72   ross+site+f
067ba4460 79 2b 61 74 74 61 63 6b 2b 76 69 64 65 6f 26 65   y+attack+vi
067ba4470 69 3d 65 4b 78 32 59 4d 4b 74 47 2d 33 59 7a 37   i=eKx2YMKtG
067ba4480 73 50 33 61 47 64 6f 41 73 26 6f 71 3d 68 6f 77   sP3aGdoAs&o
067ba4490 2b 74 6f 2b 70 65 72 66 6f 72 6d 2b 43 72 6f 73   +to+perform
067ba44a0 73 2b 73 69 74 65 2b 66 6f 72 67 65 72 79 2b 61   s+site+forg
```

Fig. 28. YouTube URL of Video (Belkasoft)

7 Result Discussion

The results shows that in the case of Google Chrome, Mozilla Firefox and Brave web browser forensics, we are able to extract the evidences related to recent process list, Google search items along with URL of sited recently visited, images downloaded along with site and downloaded images, people search in the Facebook, Facebook profile, Facebook video call related information, web WhatsApp login details with mobile number, URL of site from which user has downloaded the movies or software. It is observed from the result that artifacts related to web WhatsApp chat found in the case of Google chrome, Facebook ID and password found in the case of Mozilla Firefox and Facebook ID in the case of Brave web browser recovered from the RAM.

8 Conclusion

A web browser remains a software program or device used to navigate the internet. Lots of persons today using web browsers to examine on Google search engine, access the social media sites and email application, view videos in the YouTube etc., Digital forensics is the branch of the forensic science which deals through acquisition, collection, analysis then reporting of the digital evidences. Today, criminals use web browser to committee the misconduct and it is significant for the digital scientific analyst know digital forensic techniques to recover the evidences form the browser. In this research paper we focused well-known browser Google chrome, Mozilla Firefox and Brave web browsers and also discussed that RAM forensics will be important techniques to recover the evidences related to recent activities carried out by the user.

References

1. Ohana, D.J., Shashidhar, N.: Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions. EURASIP J. Inf. Secur. **2013**, 6 (2013)
2. Marrington, A., Baggili, I., Al Ismail, T., Al Kaf, A.: Portable web browser forensics: a forensic examination of the privacy benefits of portable web browsers. In: 2012 International Conference on Computer Systems and Industrial Informatics, pp. 18–20 (2012)
3. Oh, J., Lee, S., Lee, S.: Advanced evidence collection and analysis of web browser activity. Digit. Invest. **8**, S62–S70 (2011)
4. Said, H., Al Mutawa, N., Al Awadhi, I., Guimaraes, M.: Forensic analysis of private browsing artifacts. In: 2011 International Conference on Innovations in Information Technology, pp.25–27 (2011)
5. Rathod, D.: Web browser forensics: google chrome. Int. J. Adv. Res. Comput. Sci. **8**(7), 896–899 (2017)
6. Akbal, E., Günes, F., Akbal, A.: Digital forensic analyses of web browser records. J. Softw. 11(7), 631–637 (2016). Accessed 10 Mar 2020. https://doi.org/10.17706/jsw.11.7.631-637
7. Amor. L, Thabet S.: Forensics investigation of web application security attacks. Int. J. Comput. Netw. Inf. Secur. **7**, 10–17 (2015). https://doi.org/10.5815/ijcnis.2015.03.02. Accessed 10 Mar 2020
8. Oh, J., Lee, S., Lee, S.: Advanced evidence collection and analysis of web browser activity. In: The Digital Forensic Research Conference, 2001 USA (2020). Accessed 17 Mar 2020. https://doi.org/10.1016/j.diin.2011.05.008
9. "Basis Technology Corporation: Autopsy and The Sleuth", Accessed 14 Mar 2020. http://www.autopsy.com/wpcontent/uploads/sites/8/2016/02/Autopsy-4.0-EN-optimized.pdf
10. Mohammmed, S., Sridevi, R.: A survey on digital forensics phases, tools and challenges. In: Raju, K., Govardhan, A., Rani, B., Sridevi, R., Murty, M. (eds) Proceedings of the Third International Conference on Computational Intelligence and Informatics. Advances in Intelligent Systems and Computing, vol. 1090, pp. 237–248. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-1480-7_20
11. Aminnezhad, A., Dehghantanha, A., Abdullah, M.T.: A survey on privacy issues in digital forensics. Int. J. Cyber-Secur. Digit. Forensics **1**(4), 311–324 (2012)
12. https://kinsta.com/browser-market-share/. Accessed 5 Dec 2022
13. https://www.forbes.com/sites/billybambrough/2020/04/09/billions-of-google-chrome-usersnow-have-another-surprising-option/?sh=58f2bdd45956. Accessed 5 Dec 2022