IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 4 (Nov. - Dec. 2013), PP 76-80
www.iosrjournals.org

Study on Live analysis of Windows Physical Memory

Divyang Rahevar
Institute of Forensic Science, Gujarat Forensic Sciences University, Gujarat, India

Abstract: *Memory forensics and data carving methods are usually used during volatile investigation and is nowadays a big area of interest. Volatile memory dump is used for offline analysis of live data. Live analysis of the running system gives the information of which events are going on. Volatile memory analysis can give the sensitive information such as User Ids, Passwords, Hidden Processes, Root kits, Sockets etc. which are not stored on the physical drive. This Paper represents various approaches and tools used to capture and analyse data from computer memory.*

Keywords*: Memory forensics, RAM, sensitive information.*

I. Introduction

The volatile data is referred to as stateful information from the subject system while it is remain powered on [1]. Memory forensics can be done by two approaches mainly Hardware based and Software based. For Analysing the Live Memory we have to first create the dump of the live system. There are so many
Tools are available for dumping the memory. Why the investigator has to dump the live memory?

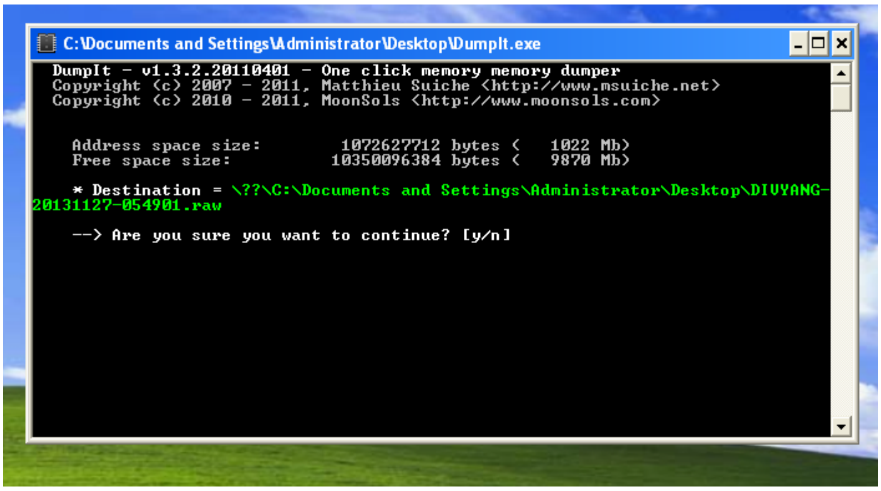
When an investigator interacts with the live system there may be chances of the altering data which may cause loss of evidence. Digital evidence is very sensitive and can be easily altered. With live analysis data is collected from a running system [2].

II. Memory Dump

There are mainly two approaches for acquire physical memory images:
Hardware based tools and Software based tools. In this paper the focus is on the software based tools.

There are so many tools available for capturing the live memory. These tools can give the image of the live RAM. Here I have explained two different tools for imaging the live memory.

DumpIt is a compact portable tool which makes it easy to save the content of the physical memory [3]. The DumpIt tool is a very user-friendly just you have to double click on it and the below screen appear.



```
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


    Address space size:        1072627712 bytes (   1022 Mb)
    Free space size:          10350096384 bytes (   9870 Mb)

    * Destination = \??\C:\Documents and Settings\Administrator\Desktop\DIVYANG-
20131127-054901.raw

    --> Are you sure you want to continue? [y/n]
```

Figure 1: Creating memory dump using DumpIt.

When you run the DumpIt it will ask for the imaging .and shows the destination path to where the image has been created. After pressing ‘y’ it will proceed for memory dump and creates the memory image at the destination path and shows the status ‘success’. The file type is the .raw file.

By using this dump file the investigator has to analyse the data which are stored in the RAM. There are some analysis tools which are discussed in next section.

The second software which I have used for memory dump is the FTK Imager from Access Data[4].

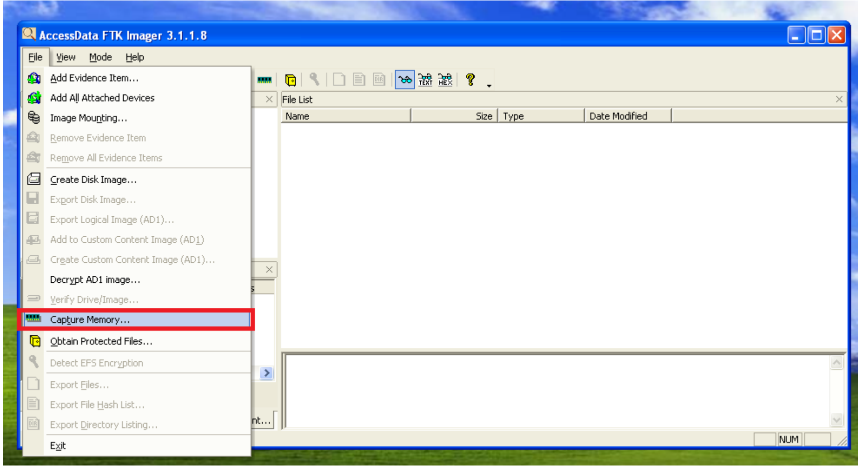
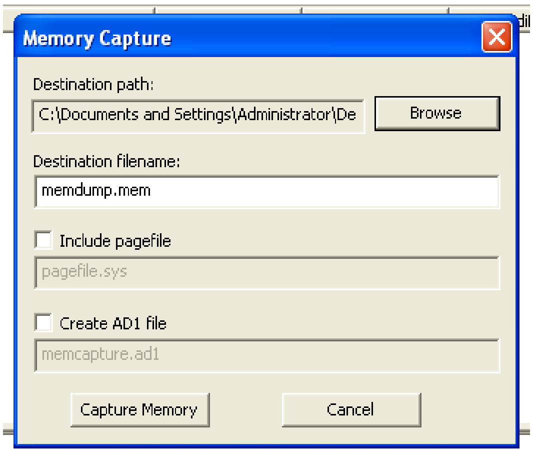


Figure 2: Memory capture using FTK Imager.

By clicking on a capture Memory option the new window opens which asks about the destination path of the imaged memory.


Memory Capture

Destination path: C:\Documents and Settings\Administrator\De

Destination filename: memdump.mem

□ Include pagefile

pagefile.sys

□ Create AD1 file

memcapture.ad1

Figure 3: capture memory option using FTK Imager.

The image file which is created by the FTK Imager is having .mem extension.
This will capture the all the processes which are running at the time of imaging and also the dll files which are used by the processes.

The live memory acquisition is very helpful in the forensic investigation. It will give the sensitive information which is not stored in the physical memory. It gives the information of the open ports, malwares and the unusual things happen to the machine.

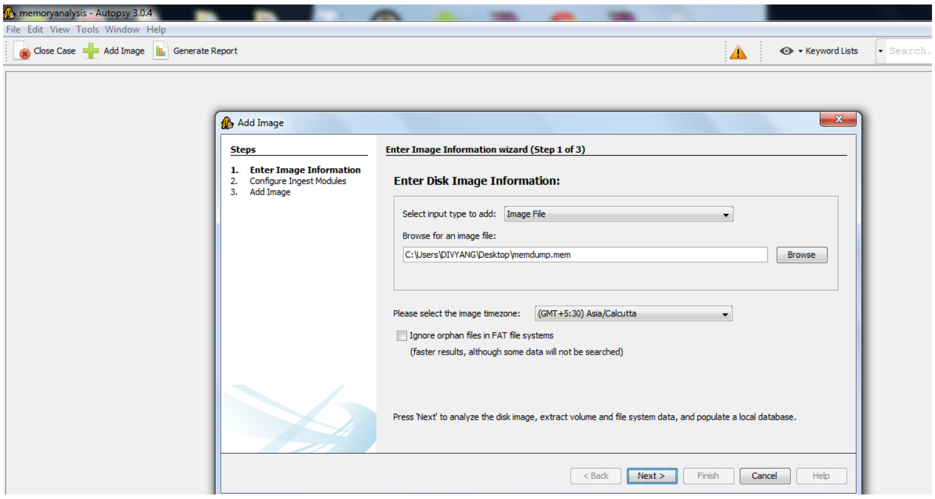
III. Memory Analysis

After creating the dump of the live memory the next and important step is to analyse the memory. In this step the investigator has to analyse carefully because he/she can find the potential evidence from the memory image.

By analysing the memory we can get the running processes, list of dlls which are running at a time, open ports, network connections. This information is commonly concerned by a forensic investigator [3].

There are different tools used for memory analysis also. Here I have explained some of them. For the best result of the memory analysis the tool is WinHex [5]. By using the searching ability from the image the Autopsy [6] is a very good tool for finding the sensitive data in a string format.

Using Autopsy there are some interesting and sensitive data I found. First open the Autopsy and load the image to which we want to analyse.



Steps

1. Enter Image Information
2. Configure Ingest Modules
3. Add Image

Enter Image Information wizard (Step 1 of 3)

Enter Disk Image Information:

Select input type to add: Image File

Browse for an image file: C:\Users\DIVYANG\Desktop\memdump.mem [Browse]

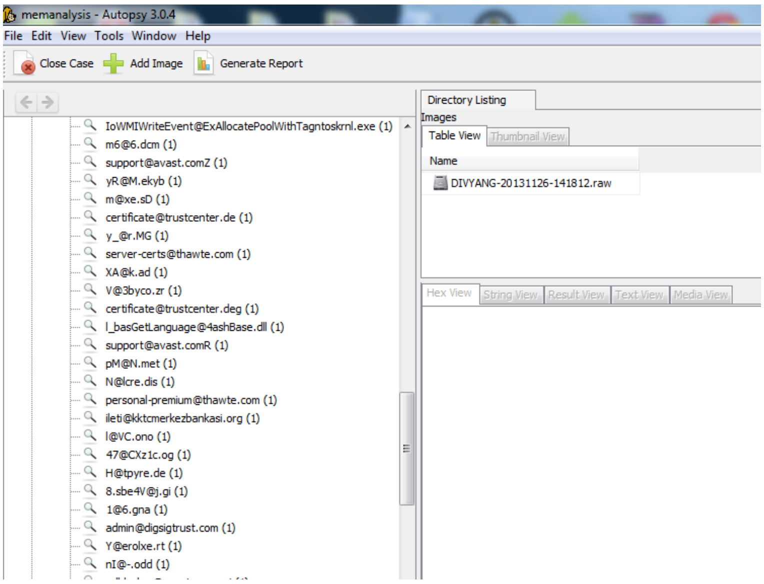
Please select the image timezone: (GMT+5:30) Asia/Calcutta

□ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

Press 'Next' to analyze the disk image, extract volume and file system data, and populate a local database.

Figure 4 : Memory analysis using Autopsy

By loading the memory image it will gives the list of Email Addresses which are stored in the address book of email or captured from the websites visited.

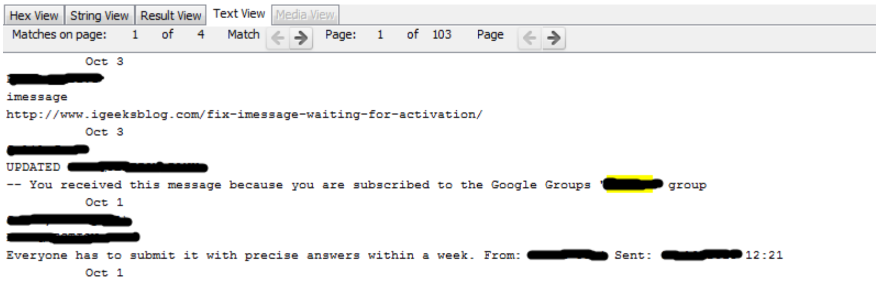


```
IoWMIWriteEvent@ExAllocatePoolWithTagntoskrnl.exe (1)
m6@6.dcm (1)
support@avast.comZ (1)
yR@M.ekyb (1)
m@xe.sD (1)
certificate@trustcenter.de (1)
y_@r.MG (1)
server-certs@thawte.com (1)
XA@k.ad (1)
V@3byco.zr (1)
certificate@trustcenter.deg (1)
l_basGetLanguage@4ashBase.dll (1)
support@avast.comR (1)
pM@N.met (1)
N@lcre.dis (1)
personal-premium@thawte.com (1)
ileti@kktcmerkezbankasi.org (1)
l@VC.ono (1)
47@CXz1c.og (1)
H@tpyre.de (1)
8.sbe4V@j.gi (1)
1@6.gna (1)
admin@digsigtrust.com (1)
Y@erolxe.rt (1)
nI@-.odd (1)
```

Name
DIVYANG-20131126-141812.raw

Figure 5: Email Ids stored in memory using Autopsy

Analysing memory using Autopsy it will shows the Email messages which are store in the RAM. This may become the potential evidence.



Matches on page: 1 of 4 Match Page: 1 of 103 Page

```
          Oct 3
[redacted]
imessage
http://www.igeeksblog.com/fix-imessage-waiting-for-activation/
          Oct 3
[redacted]
UPDATED [redacted]
-- You received this message because you are subscribed to the Google Groups '[redacted] group
          Oct 1
[redacted]
Everyone has to submit it with precise answers within a week. From: [redacted] Sent: [redacted] 12:21
          Oct 1
```

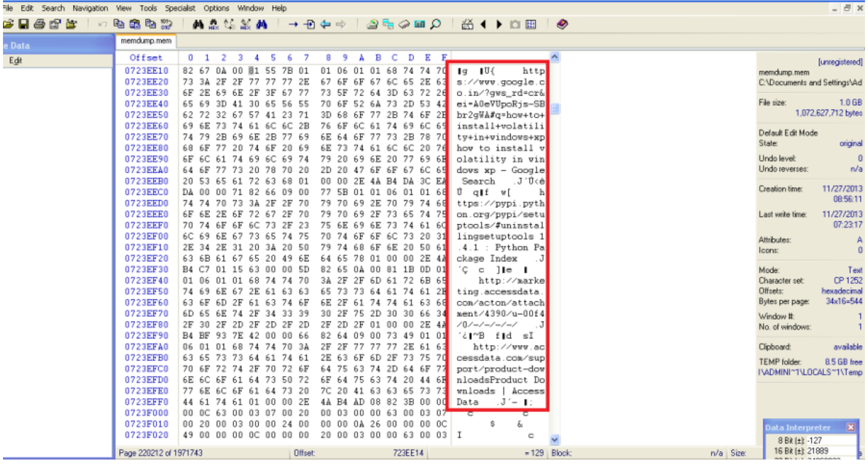
Figure 6: Email messages stored in memory dump Using Autopsy

The keyword search is very important for analysing the live memory dump. By using key word searching it will become the faster to search the evidences.

The Next tool which is used for memory analysis is the WinHex.

The tool WinHex is in its core a universal hexadecimal editor, particularly helpful in computer forensics, data recovery, low-level data processing, IT security [7].

The WinHex has showed the visited websites from the memory dump.



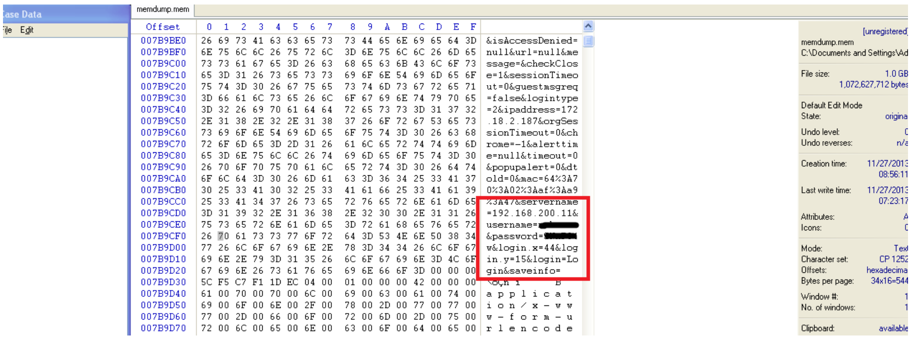
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
Edit
memdump.mem
Data Interpreter

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0723EE10  82 67 0A 00 81 55 7B 01  01 06 01 01 68 74 74 70   g  U{      http
0723EE20  73 3A 2F 2F 77 77 77 2E  67 6F 6F 67 6C 65 2E 63  s://www.google.c
0723EE30  6F 2E 69 6E 2F 3F 67 77  73 5F 72 64 3D 63 72 26  o.in/?gws_rd=cr&
0723EE40  65 69 3D 41 30 65 56 55  70 6F 52 6A 73 2D 53 42  ei=A0eVUpoRjs-SB
0723EE50  62 72 32 67 57 41 23 71  3D 68 6F 77 2B 74 6F 2B  br2gWA#q=how+to+
0723EE60  69 6E 73 74 61 6C 6C 2B  76 6F 6C 61 74 69 6C 69  install+volatili
0723EE70  74 79 2B 69 6E 2B 77 69  6E 64 6F 77 73 2B 78 70  ty+in+windows+xp
0723EE80  68 6F 77 20 74 6F 20 69  6E 73 74 61 6C 6C 20 76  how to install v
0723EE90  6F 6C 61 74 69 6C 69 74  79 20 69 6E 20 77 69 6E  olatility in win
0723EEA0  64 6F 77 73 20 78 70 20  2D 20 47 6F 6F 67 6C 65  dows xp - Google
0723EEB0  20 53 65 61 72 63 68 01  00 00 2E 4A B4 DA 3C EA   Search   .J´Ú<ê
0723EEC0  DA 00 00 71 82 66 09 00  77 5B 01 01 06 01 01 68  Ú  q f  w[     h
0723EED0  74 74 70 73 3A 2F 2F 70  79 70 69 2E 70 79 74 68  ttps://pypi.pyth
0723EEE0  6F 6E 2E 6F 72 67 2F 70  79 70 69 2F 73 65 74 75  on.org/pypi/setu
0723EEF0  70 74 6F 6F 6C 73 2F 23  75 6E 69 6E 73 74 61 6C  ptools/#uninstal
0723EF00  6C 69 6E 67 73 65 74 75  70 74 6F 6F 6C 73 20 31  lingsetuptools 1
0723EF10  2E 34 2E 31 20 3A 20 50  79 74 68 6F 6E 20 50 61  .4.1 : Python Pa
0723EF20  63 6B 61 67 65 20 49 6E  64 65 78 01 00 00 2E 4A  ckage Index   .J
0723EF30  B4 C7 01 15 63 00 00 5D  82 65 0A 00 81 1B 0D 01  ´Ç  c  ] e
0723EF40  01 06 01 01 68 74 74 70  3A 2F 2F 6D 61 72 6B 65      http://marke
0723EF50  74 69 6E 67 2E 61 63 63  65 73 73 64 61 74 61 2E  ting.accessdata.
0723EF60  63 6F 6D 2F 61 63 74 6F  6E 2F 61 74 74 61 63 68  com/acton/attach
0723EF70  6D 65 6E 74 2F 34 33 39  30 2F 75 2D 30 30 66 34  ment/4390/u-00f4
0723EF80  2F 30 2F 2D 2F 2D 2F 2D  2F 2D 2F 01 00 00 2E 4A  /0/-/-/-/-/   .J
0723EF90  B4 BF 93 7E 42 00 00 66  82 64 09 00 73 49 01 01  ´¿ ~B  f d  sI
0723EFA0  06 01 01 68 74 74 70 3A  2F 2F 77 77 77 2E 61 63     http://www.ac
0723EFB0  63 65 73 73 64 61 74 61  2E 63 6F 6D 2F 73 75 70  cessdata.com/sup
0723EFC0  70 6F 72 74 2F 70 72 6F  64 75 63 74 2D 64 6F 77  port/product-dow
0723EFD0  6E 6C 6F 61 64 73 50 72  6F 64 75 63 74 20 44 6F  nloadsProduct Do
0723EFE0  77 6E 6C 6F 61 64 73 20  7C 20 41 63 63 65 73 73  wnloads | Access
0723EFF0  44 61 74 61 01 00 00 2E  4A B4 AD 08 82 3B 00 00  Data   .J´-  ;
0723F000  00 0C 63 00 03 07 00 20  00 03 00 00 63 00 03 07    c          c
0723F010  00 20 00 03 00 00 24 00  00 00 0A 26 00 00 00 0C        $    &
0723F020  49 00 00 00 0C 00 00 00  20 00 03 00 00 63 00 03  I            c
Page 220212 of 1971743        Offset:        723EE14        = 129  Block:        n/a  Size:
```

[unregistered]
memdump.mem
C:\Documents and Settings\Ad
File size: 1.0 GB
1,072,627,712 bytes
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 11/27/2013 08:56:11
Last write time: 11/27/2013 07:23:17
Attributes: A
Icons: 0
Mode: Text
Character set: CP 1252
Offsets: hexadecimal
Bytes per page: 34x16=544
Window #: 1
No. of windows: 1
Clipboard: available
TEMP folder: 8.5 GB free
\ADMINI~1\LOCALS~1\Temp
8 Bit (±): -127
16 Bit (±): 21889

Figure 7: Visited websites using WinHex.

Using this tool we can find lots of sensitive information. In this memory dump I have found the login in to some account which shows the username and password.

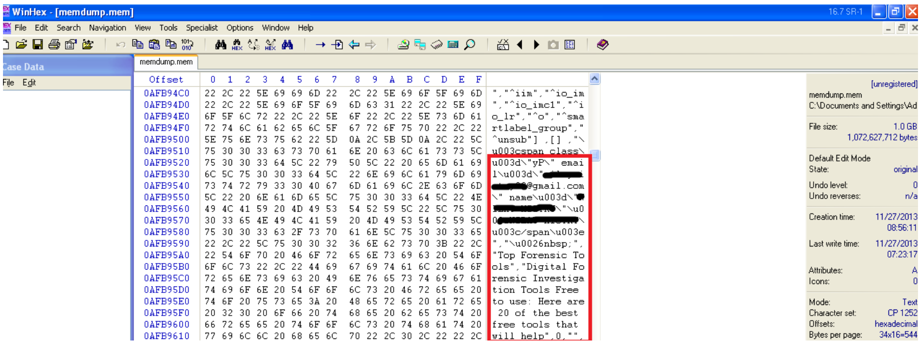


```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
007B9BE0  26 69 73 41 63 63 65 73  73 44 65 6E 69 65 64 3D  &isAccessDenied=
007B9BF0  6E 75 6C 6C 26 75 72 6C  3D 6E 75 6C 6C 26 6D 65  null&url=null&me
007B9C00  73 73 61 67 65 3D 26 63  68 65 63 6B 43 6C 6F 73  ssage=&checkClos
007B9C10  65 3D 31 26 73 65 73 73  69 6F 6E 54 69 6D 65 6F  e=1&sessionTimeo
007B9C20  75 74 3D 30 26 67 75 65  73 74 6D 73 67 72 65 71  ut=0&guestmsgreq
007B9C30  3D 66 61 6C 73 65 26 6C  6F 67 69 6E 74 79 70 65  =false&logintype
007B9C40  3D 32 26 69 70 61 64 64  72 65 73 73 3D 31 37 32  =2&ipaddress=172
007B9C50  2E 31 38 2E 32 2E 31 38  37 26 6F 72 67 53 65 73  .18.2.187&orgSes
007B9C60  73 69 6F 6E 54 69 6D 65  6F 75 74 3D 30 26 63 68  sionTimeout=0&ch
007B9C70  72 6F 6D 65 3D 2D 31 26  61 6C 65 72 74 74 69 6D  rome=-1&alerttim
007B9C80  65 3D 6E 75 6C 6C 26 74  69 6D 65 6F 75 74 3D 30  e=null&timeout=0
007B9C90  26 70 6F 70 75 70 61 6C  65 72 74 3D 30 26 64 74  &popupalert=0&dt
007B9CA0  6F 6C 64 3D 30 26 6D 61  63 3D 36 34 25 33 41 37  old=0&mac=64%3A7
007B9CB0  30 25 33 41 30 32 25 33  41 61 66 25 33 41 61 39  0%3A02%3Aaf%3Aa9
007B9CC0  25 33 41 34 37 26 73 65  72 76 65 72 6E 61 6D 65  %3A47&servername
007B9CD0  3D 31 39 32 2E 31 36 38  2E 32 30 30 2E 31 31 26  =192.168.200.11&
007B9CE0  75 73 65 72 6E 61 6D 65  3D 72 61 68 65 76 65 72  username=[redacted]
007B9CF0  26 70 61 73 73 77 6F 72  64 3D 53 4E 6E 50 38 34  &password=[redacted]
007B9D00  77 26 6C 6F 67 69 6E 2E  78 3D 34 34 26 6C 6F 67  w&login.x=44&log
007B9D10  69 6E 2E 79 3D 31 35 26  6C 6F 67 69 6E 3D 4C 6F  in.y=15&login=Lo
007B9D20  67 69 6E 26 73 61 76 65  69 6E 66 6F 3D 00 00 00  gin&saveinfo=
007B9D30  5C F5 C7 F1 1D EC 04 00  01 00 00 00 42 00 00 00  \õÇñ ì      B
007B9D40  61 00 70 00 70 00 6C 00  69 00 63 00 61 00 74 00  a p p l i c a t
007B9D50  69 00 6F 00 6E 00 2F 00  78 00 2D 00 77 00 77 00  i o n / x - w w
007B9D60  77 00 2D 00 66 00 6F 00  72 00 6D 00 2D 00 75 00  w - f o r m - u
007B9D70  72 00 6C 00 65 00 6E 00  63 00 6F 00 64 00 65 00  r l e n c o d e
```

[unregistered]
memdump.mem
C:\Documents and Settings\Ad
File size: 1.0 GB
1,072,627,712 bytes
Default Edit Mode
State: origina
Undo level: (
Undo reverses: n/a
Creation time: 11/27/2013 08:56:11
Last write time: 11/27/2013 07:23:17
Attributes: A
Icons: (
Mode: Text
Character set: CP 1252
Offsets: hexadecima
Bytes per page: 34x16=544
Window #: 1
No. of windows: 1
Clipboard: available

Figure 8: Username and password using WinHex.

As shown in the Autopsy, Here also we can get the information of email message. Here the user got an email message which is stored in the memory.



WinHex - [memdump.mem]
16.7 SR-1
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
memdump.mem

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0AFB94C0  22 2C 22 5E 69 69 6D 22  2C 22 5E 69 6F 5F 69 6D  ","^iim","^io_im
0AFB94D0  22 2C 22 5E 69 6F 5F 69  6D 63 31 22 2C 22 5E 69  ","^io_imc1","^i
0AFB94E0  6F 5F 6C 72 22 2C 22 5E  6F 22 2C 22 5E 73 6D 61  o_lr","^o","^sma
0AFB94F0  72 74 6C 61 62 65 6C 5F  67 72 6F 75 70 22 2C 22  rtlabel_group","
0AFB9500  5E 75 6E 73 75 62 22 5D  0A 2C 5B 5D 0A 2C 22 5C  ^unsub"] ,[] ,"\
0AFB9510  75 30 30 33 63 73 70 61  6E 20 63 6C 61 73 73 5C  u003cspan class\
0AFB9520  75 30 30 33 64 5C 22 79  50 5C 22 20 65 6D 61 69  u003d\"yP\" emai
0AFB9530  6C 5C 75 30 30 33 64 5C  22 6E 69 6C 61 79 6D 69  l\u003d\"[redacted]
0AFB9540  73 74 72 79 33 30 40 67  6D 61 69 6C 2E 63 6F 6D  [redacted]@gmail.com
0AFB9550  5C 22 20 6E 61 6D 65 5C  75 30 30 33 64 5C 22 4E  \" name\u003d\"[redacted]
0AFB9560  49 4C 41 59 20 4D 49 53  54 52 59 5C 22 5C 75 30  [redacted]\"\u0
0AFB9570  30 33 65 4E 49 4C 41 59  20 4D 49 53 54 52 59 5C  0[redacted]\
0AFB9580  75 30 30 33 63 2F 73 70  61 6E 5C 75 30 30 33 65  u003c/span\u003e
0AFB9590  22 2C 22 5C 75 30 30 32  36 6E 62 73 70 3B 22 2C  ","\u0026nbsp;",
0AFB95A0  22 54 6F 70 20 46 6F 72  65 6E 73 69 63 20 54 6F  "Top Forensic To
0AFB95B0  6F 6C 73 22 2C 22 44 69  67 69 74 61 6C 20 46 6F  ols","Digital Fo
0AFB95C0  72 65 6E 73 69 63 20 49  6E 76 65 73 74 69 67 61  rensic Investiga
0AFB95D0  74 69 6F 6E 20 54 6F 6F  6C 73 20 46 72 65 65 20  tion Tools Free
0AFB95E0  74 6F 20 75 73 65 3A 20  48 65 72 65 20 61 72 65  to use: Here are
0AFB95F0  20 32 30 20 6F 66 20 74  68 65 20 62 65 73 74 20   20 of the best
0AFB9600  66 72 65 65 20 74 6F 6F  6C 73 20 74 68 61 74 20  free tools that
0AFB9610  77 69 6C 6C 20 68 65 6C  70 22 2C 30 2C 22 22 2C  will help",0,"",
```

[unregistered]
memdump.mem
C:\Documents and Settings\Ad
File size: 1.0 GB
1,072,627,712 bytes
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 11/27/2013 08:56:11
Last write time: 11/27/2013 07:23:17
Attributes: A
Icons: 0
Mode: Text
Character set: CP 1252
Offsets: hexadecimal
Bytes per page: 34x16=544

Figure 9 : Email message showing in WinHex.

These all are the information which we can get through different tools. The tools which are used for the analysing the memory have their different approach. The above tools are the graphical tools, there are some other tools which also do the memory analysis.

The volatility framework is also used for the memory analysis. There are so many papers available for the volatility. The volatility is powerful and gives the information about the hidden processes, dll lists, open ports, malwares, and registry information [3].

The PTFinder is a perl script that can use for finding out processes and threads. This script searches for EPROCESS structures and perform a series of comparisons against rules to ensure the authenticity [8][9].

IV. Conclusion

There are so many tools and techniques are available for memory acquisition and analysis. They all have different methods and different approaches. It is very good to find out the sensitive information from the memory. This is helpful for solving the cyber crimes. The data which is stored in the RAM are changes repeatedly. The data are overwritten every time. The tools which are used for analysis and capturing the memory have to be develop more powerful with coming years.

References

[1] Cutifa Safitri , "A Study: Volatility Forensic on Hidden Files", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

[2] Sasa Mrdovic, Alvin Huseinovic, Ernedin Zajko, "Combining Static and Live Digital Forensic Analysis in Virtual Environment"

[3] Liming Cai, Jing Sha ,Wei Qian," Study on Forensic Analysis of Physical Memory"

[4] FTKImager download , http://www.accessdata.com/support/product-downloads

[5] X-ways software Technology AG, WinHex Editor http://winhex.com/winhex/

[6] Autopsy download , http://www.sleuthkit.org/autopsy/

[7] Qian Zhao, Tianjie Cao, "Collecting Sensitive Information from Windows Physical Memory", JOURNAL OF COMPUTERS, VOL. 4, NO. 1, JANUARY 2009

[8] Gabriela Limon Garcia," Forensic physical memory analysis:an overview of tools and techniques "

[9] Andrea Schuster, Searching for processes and threads in Microsoft Windows memory dumps. Digital forensic research workgroup, 2007.