Master of Information Security

MIS4203 – Independent Studies in Information Security

Index Number – 16770217 | Reg. Number – 2016MIS021

Study Number - 06 - Digital Forensic – I

January 12, 2019

University of Colombo School of Computing

Table of Contents

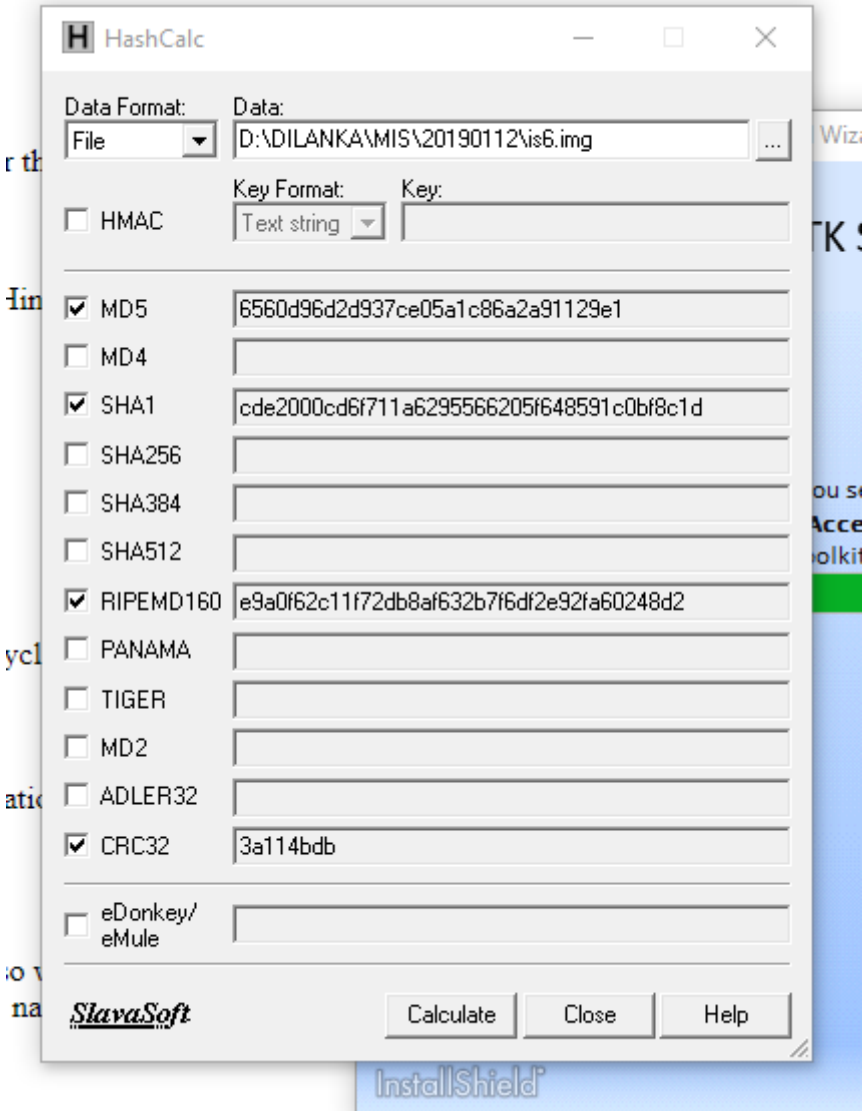
Problem

Perform a forensics analysis of the given disk image “is6.img” and gather the following evidence:

Validating image Hash Value:

- Disk Image “is6.img”

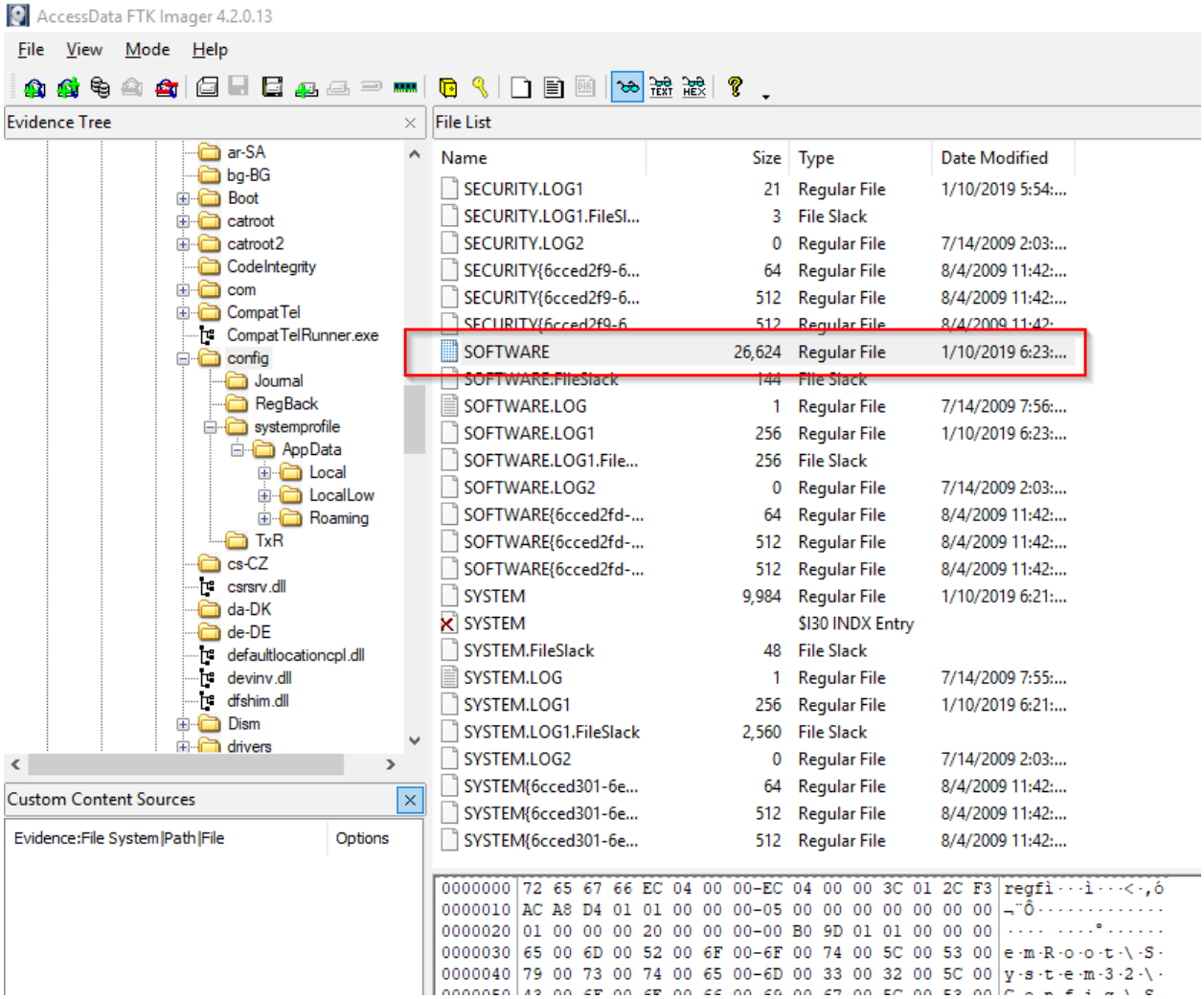
  SHA1 Hash value: “cde2000cd6f711a6295566205f648591c0bf8c1d”



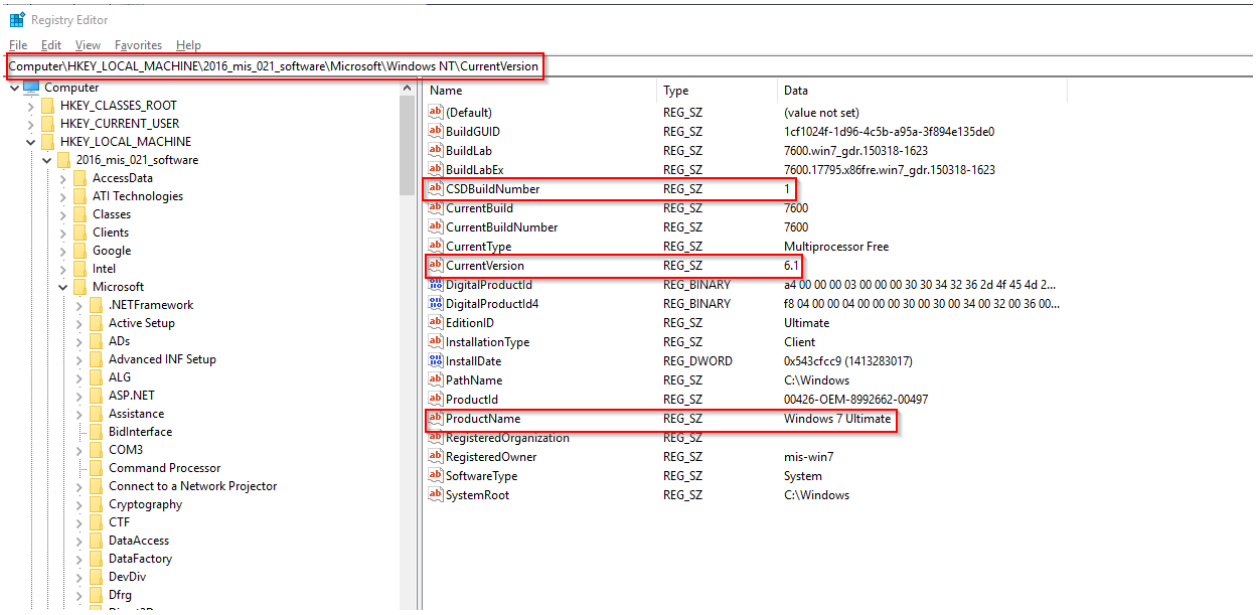
1. System Information

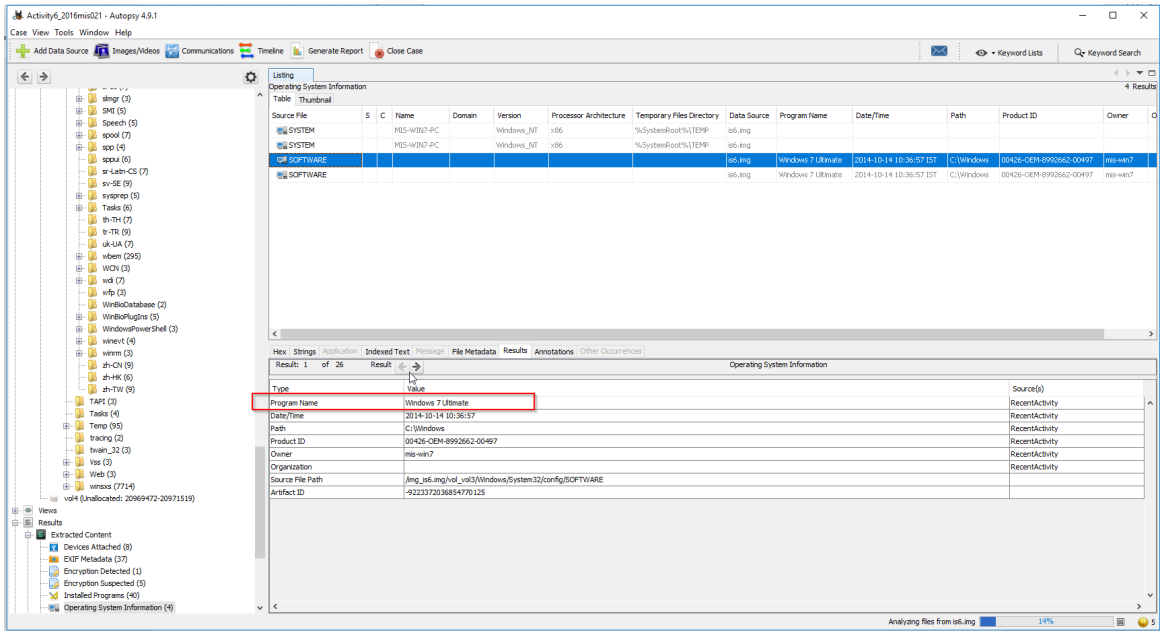
    1. Operating System name and version

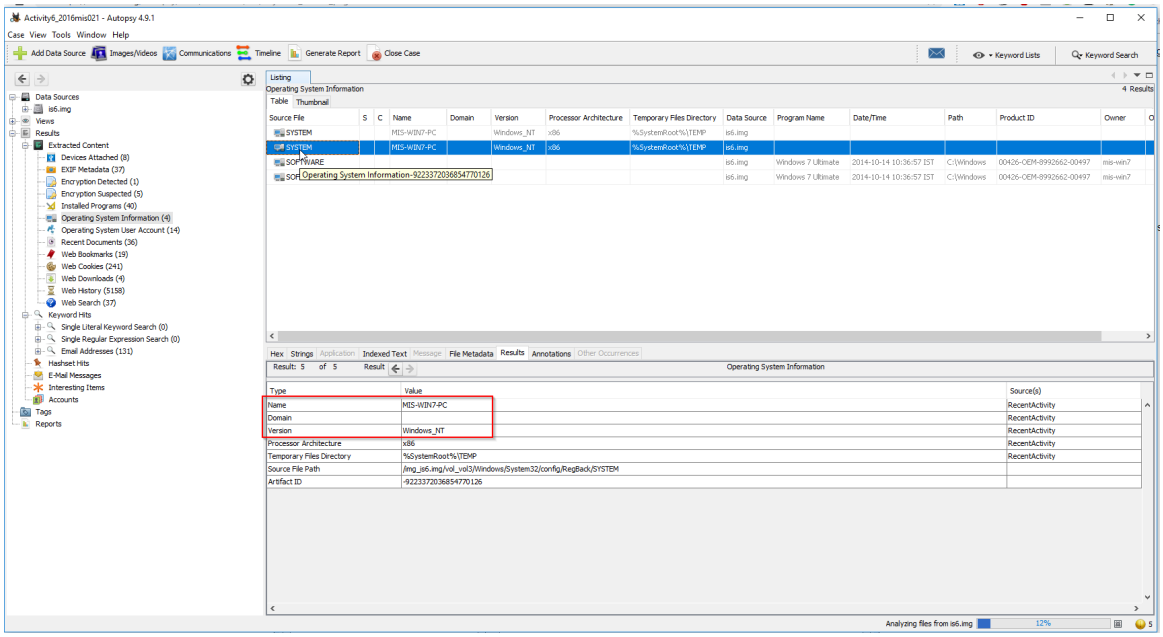
        Extracted the registry hive (SOFTWARE)



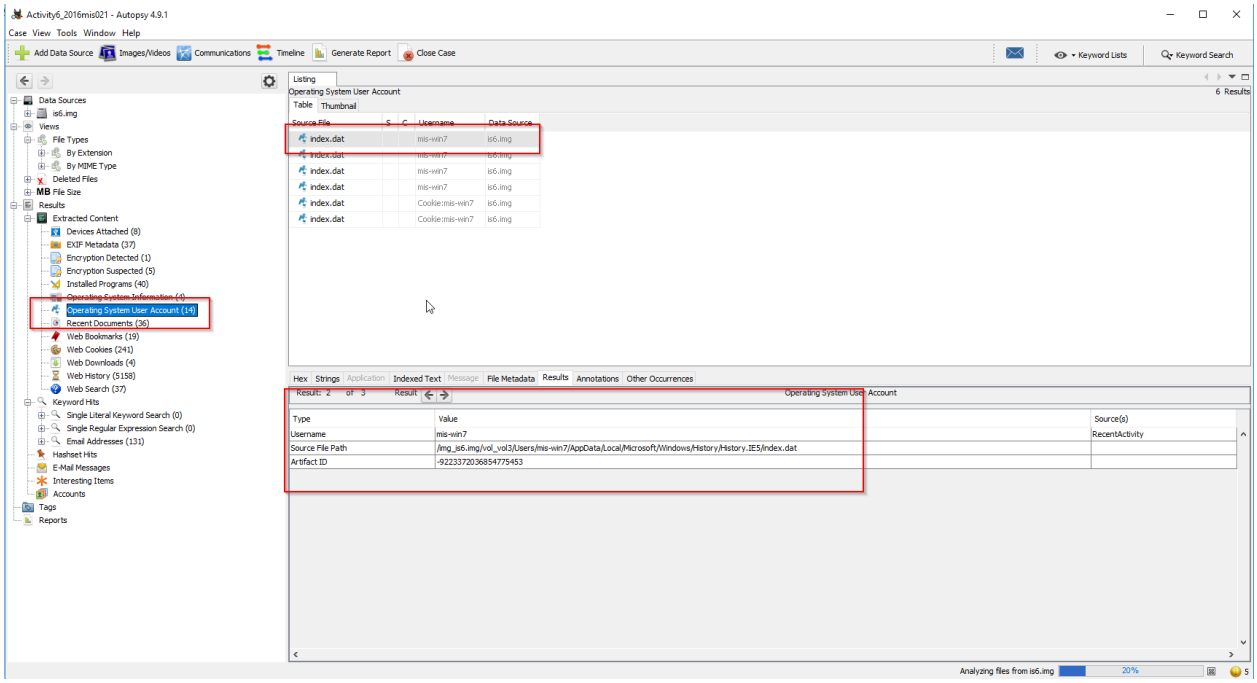
Load registry hive to registry editor and find the information as below:







2. User account information (Usernames, Passwords and Hints, Create time, Login time and etc.)



Using RegRipper extracted the SAM hive

```
User Information
------------------------
Username        : Administrator [500]
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Tue Oct 14 23:05:19 2014 Z
Name            :
Last Login Date : Tue Jul 14 04:53:58 2009 Z
Pwd Reset Date  : Tue Jul 14 04:55:45 2009 Z
Pwd Fail Date   : Never
Login Count     : 1
  --> Password does not expire
  --> Account Disabled
  --> Normal user account
```

```
Username        : Guest [501]
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Tue Oct 14 23:05:19 2014 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Account Disabled
  --> Password not required
  --> Normal user account
```

```
Username        : mis-win7 [1001]
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Tue Oct 14 10:35:59 2014 Z
Name            :
Last Login Date : Thu Jan 10 05:42:56 2019 Z
Pwd Reset Date  : Tue Oct 14 10:35:59 2014 Z
Pwd Fail Date   : Never
Login Count     : 22
  --> Password does not expire
  --> Password not required
  --> Normal user account
```

```
Username        : HomeGroupUser$ [1002]
Full Name       : HomeGroupUser$
User Comment    : Built-in account for homegroup access to the computer
Account Type    : Custom Limited Acct
Account Created : Tue Oct 14 10:35:59 2014 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Tue Oct 14 10:35:59 2014 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account
```

```
-------------------------
Group Membership Information
-------------------------
Group Name     : Users [2]
LastWrite      : Tue Oct 14 10:35:59 2014 Z
Group Comment : Users are prevented from making accidental or intentional system-wide changes and can run most applications
Users :
  S-1-5-4
  S-1-5-11

Group Name     : Event Log Readers [0]
LastWrite      : Tue Jul 14 04:34:12 2009 Z
Group Comment : Members of this group can read event logs from local machine
Users          : None

Group Name     : Guests [1]
LastWrite      : Tue Oct 14 22:39:30 2014 Z
Group Comment : Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
Users :
  S-1-5-21-2696881825-1152443378-3678611488-501

Group Name     : Distributed COM Users [0]
LastWrite      : Tue Jul 14 04:34:12 2009 Z
Group Comment : Members are allowed to launch, activate and use Distributed COM objects on this machine.
Users          : None

Group Name     : Administrators [2]
LastWrite      : Tue Oct 14 10:35:59 2014 Z
Group Comment : Administrators have complete and unrestricted access to the computer/domain
Users :
  S-1-5-21-2696881825-1152443378-3678611488-1001
  S-1-5-21-2696881825-1152443378-3678611488-500

Group Name     : Network Configuration Operators [0]
LastWrite      : Tue Oct 14 22:39:57 2014 Z
Group Comment : Members in this group can have some administrative privileges to manage configuration of networking features
Users          : None

Group Name     : Cryptographic Operators [0]
LastWrite      : Tue Oct 14 22:39:57 2014 Z
Group Comment : Members are authorized to perform cryptographic operations.
Users          : None

Group Name     : Power Users [0]
LastWrite      : Tue Oct 14 22:39:57 2014 Z
Group Comment : Power Users are included for backwards compatibility and possess limited administrative powers
Users          : None
```

```
Group Name     : Performance Log Users [0]
LastWrite      : Tue Jul 14 04:34:12 2009 Z
Group Comment : Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer
Users          : None

Group Name     : Replicator [0]
LastWrite      : Tue Oct 14 22:39:57 2014 Z
Group Comment : Supports file replication in a domain
Users          : None

Group Name     : Performance Monitor Users [0]
LastWrite      : Tue Jul 14 04:34:12 2009 Z
Group Comment : Members of this group can access performance counter data locally and remotely
Users          : None

Group Name     : Remote Desktop Users [0]
LastWrite      : Tue Oct 14 22:39:57 2014 Z
Group Comment : Members in this group are granted the right to logon remotely
Users          : None

Group Name     : IIS_IUSRS [1]
LastWrite      : Tue Jul 14 04:34:12 2009 Z
Group Comment : Built-in group used by Internet Information Services.
Users :
  S-1-5-17

Group Name     : Backup Operators [0]
LastWrite      : Tue Oct 14 22:39:57 2014 Z
Group Comment : Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Users          : None

Analysis Tips:
 - For well-known SIDs, see http://support.microsoft.com/kb/243330
    - S-1-5-4  = Interactive
    - S-1-5-11 = Authenticated Users
 - Correlate the user SIDs to the output of the ProfileList plugin

----------------------------------------
```

3. Start time and End time

```
----------------------------------------
shutdown v.20080324
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
ControlSet001\Control\Windows
LastWrite Time Thu Jan 10 05:42:42 2019 (UTC)
  ShutdownTime = Thu Jan 10 05:42:42 2019 (UTC)
----------------------------------------
shutdowncount v.20080709
```

4. Application used

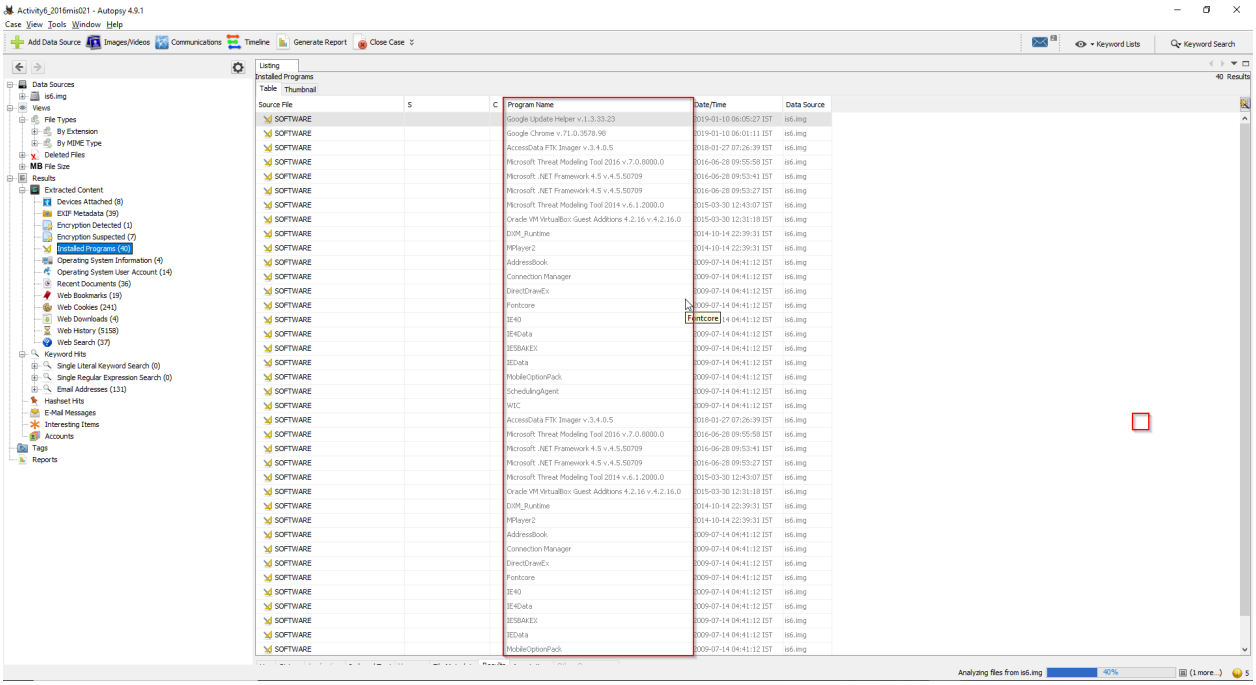
Used applications from registry extracted using RegRipper

```
App Paths
Microsoft\Windows\CurrentVersion\App Paths

Thu Jan 10 06:01:11 2019 (UTC)
  chrome.exe - C:\Program Files\Google\Chrome\Application\chrome.exe
Tue Oct 14 23:38:40 2014 (UTC)
  cmmgr32.exe -
  IEXPLORE.EXE - C:\Program Files\Internet Explorer\IEXPLORE.EXE
Tue Jul 14 07:51:40 2009 (UTC)
  dvdmaker.exe - %ProgramFiles%\DVD Maker\dvdmaker.exe
  Journal.exe - %ProgramFiles%\Windows Journal\Journal.exe
  mip.exe - %CommonProgramFiles%\Microsoft Shared\Ink\mip.exe
  SnippingTool.exe - %SystemRoot%\system32\SnippingTool.exe
  TabTip.exe - %CommonProgramFiles%\microsoft shared\ink\TabTip.exe
Tue Jul 14 04:41:12 2009 (UTC)
  install.exe -
  migwiz.exe -
  mplayer2.exe - %ProgramFiles%\Windows Media Player\wmplayer.exe
  pbrush.exe - %SystemRoot%\System32\mspaint.exe
  PowerShell.exe - %SystemRoot%\system32\WindowsPowerShell\v1.0\PowerShell.exe
  setup.exe -
  sidebar.exe - "%ProgramFiles%\Windows Sidebar\sidebar.exe"
  table30.exe -
  wab.exe - %ProgramFiles%\Windows Mail\wab.exe
  wabmig.exe - %ProgramFiles%\Windows Mail\wabmig.exe
  wmplayer.exe - %ProgramFiles%\Windows Media Player\wmplayer.exe
  WORDPAD.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
  WRITE.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
Wow6432Node\Microsoft\Windows\CurrentVersion\App Paths not found.
--------------------------------------
App Paths
Microsoft\Windows\CurrentVersion\App Paths

1547100071|REG|||App Paths - chrome.exe - C:\Program Files\Google\Chrome\Application\chrome.exe
1413329920|REG|||App Paths - cmmgr32.exe -
1413329920|REG|||App Paths - IEXPLORE.EXE - C:\Program Files\Internet Explorer\IEXPLORE.EXE
1247557900|REG|||App Paths - dvdmaker.exe - %ProgramFiles%\DVD Maker\dvdmaker.exe
1247557900|REG|||App Paths - Journal.exe - %ProgramFiles%\Windows Journal\Journal.exe
1247557900|REG|||App Paths - mip.exe - %CommonProgramFiles%\Microsoft Shared\Ink\mip.exe
1247557900|REG|||App Paths - SnippingTool.exe - %SystemRoot%\system32\SnippingTool.exe
1247557900|REG|||App Paths - TabTip.exe - %CommonProgramFiles%\microsoft shared\ink\TabTip.exe
1247546472|REG|||App Paths - install.exe -
1247546472|REG|||App Paths - migwiz.exe -
1247546472|REG|||App Paths - mplayer2.exe - %ProgramFiles%\Windows Media Player\wmplayer.exe
1247546472|REG|||App Paths - pbrush.exe - %SystemRoot%\System32\mspaint.exe
1247546472|REG|||App Paths - PowerShell.exe - %SystemRoot%\system32\WindowsPowerShell\v1.0\PowerShell.exe
1247546472|REG|||App Paths - setup.exe -
1247546472|REG|||App Paths - sidebar.exe - "%ProgramFiles%\Windows Sidebar\sidebar.exe"
1247546472|REG|||App Paths - table30.exe -
1247546472|REG|||App Paths - wab.exe - %ProgramFiles%\Windows Mail\wab.exe
1247546472|REG|||App Paths - wabmig.exe - %ProgramFiles%\Windows Mail\wabmig.exe
1247546472|REG|||App Paths - wmplayer.exe - %ProgramFiles%\Windows Media Player\wmplayer.exe
1247546472|REG|||App Paths - WORDPAD.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
1247546472|REG|||App Paths - WRITE.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
--------------------------------------
```

Last visited apps can found here:

```
LastVisitedPidlMRU
LastWrite: Thu Jan 10 06:13:53 2019
Note: All value names are listed in MRUListEx order.

  chrome.exe - Users
  rr.exe - Users\mis
  iexplore.exe - Users
  FTK Imager.exe - My Computer\E:
  TMT7.exe - Users
  TMT4.exe - My Computer\E:\MIS\3102\Lab
```

All installed apps



2. File Analysis

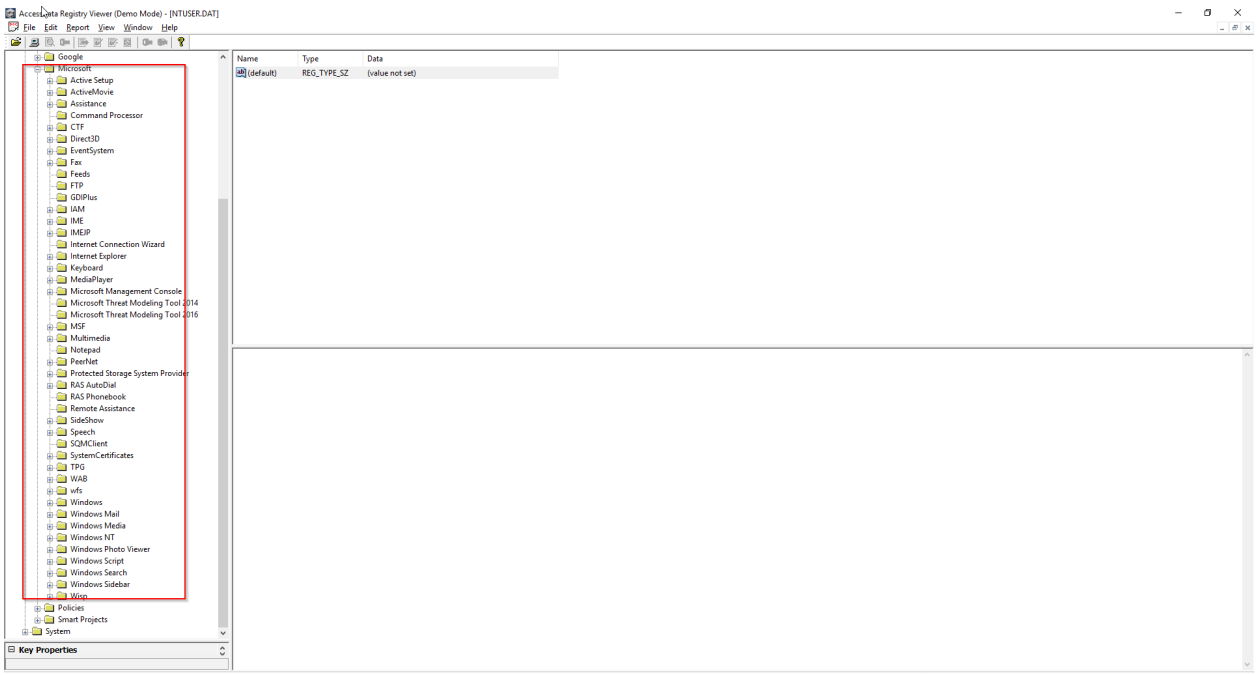
    1. List of most recent used files

        Extracted NTUSER.DAT file and exported registry via RegRipper. Generated report contain MRUs items.

```
----------------------------------------
recentdocs_timeline v.20161112
(NTUSER.DAT) Gets contents of user's RecentDocs key and place last write times into timeline based on MRUListEx

RecentDocs
Sat Jan 27 09:53:09 2018        :   NTUSER.DAT.copy0
Sat Jan 27 09:25:42 2018        :   NTUSER (2).DAT
Sat Jan 27 08:13:13 2018        :   TechBank_User_Machine.dd
Tue Jun 28 14:02:30 2016        :   LoggingModelReport-2014mis001.htm
Thu Jan 10 06:16:34 2019        :   fixedw_large_4x.jpg
Sat Jan 27 09:45:22 2018        :   NTUSER1.log
Tue Jun 28 12:38:20 2016        :   MIS3102SecureSoftwareSystems-TreatModelingwithMicrosoftSDLThreatModelingTool.pdf
Mon Mar 30 13:13:31 2015        :   Lab1.tm4
Tue Jun 28 14:03:52 2016        :   InClassActivity-2014mis001.tm7
Thu Jan 10 06:23:41 2019        :   pass.txt
Sat Jan 27 09:17:59 2018        :   RegRipper2.8-master.zip
Thu Jan 10 06:23:41 2019        :   Downloads
```

    2. List of searched files

        Information about searched file supposed to save ACMru file in registry. Software\Microsoft\Search Assistant\ Here using Registry Viewer application, you can import NTUSER.dat file and see the registry file as it is.



Cannot find the folder here. Suspect that ACMru used to store search history has been removed. According to this, user may delete the registry file which use to store the searched files information.

Using RegRipper:

```
acmru v.20080324
- Gets contents of user's ACMru key

Software\Microsoft\Search Assistant\ACMru not found.
-------------------------------------
```

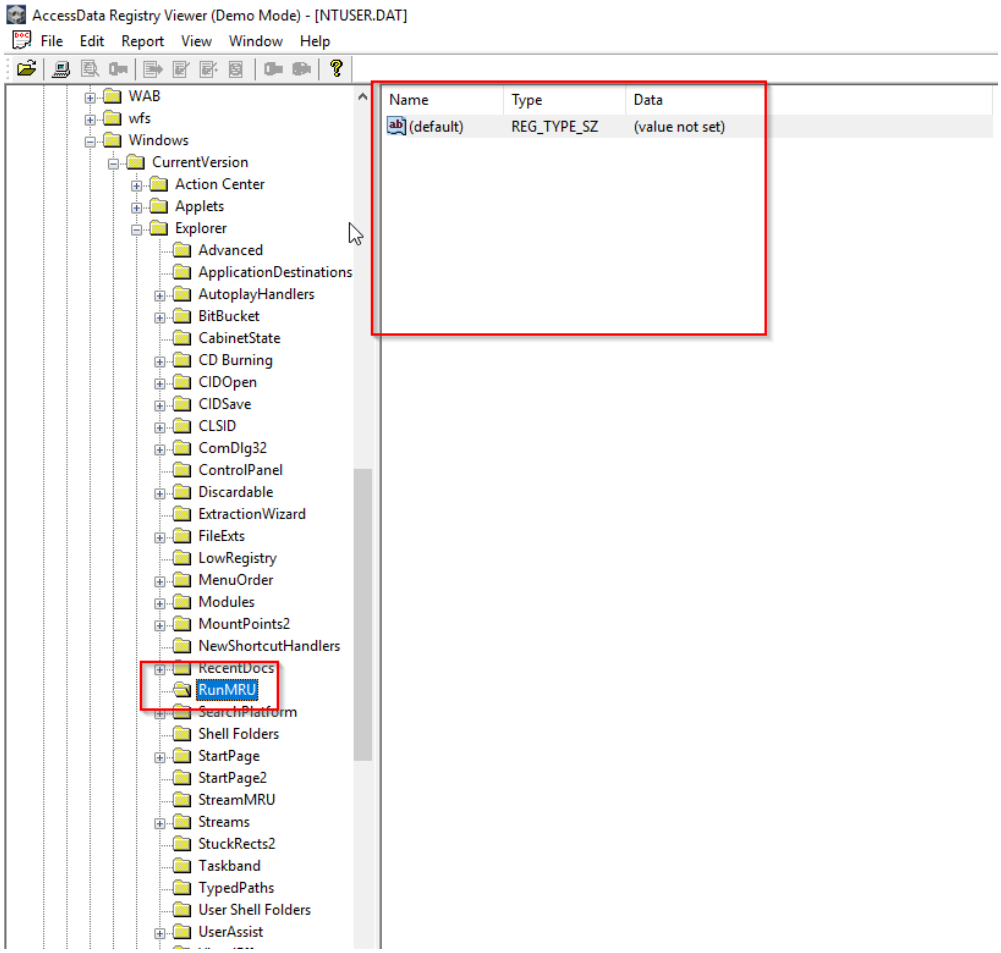
3. Last command executed

This registry key contains the list of commands user entered using the Start>Run commands. According to the investigation, there is not commands executed

HKCU\SOFTWARE\Microsoft\Windows\CurrentVers ion\Explorer\RunMRU

```
44
45  -------------------------------------
46  runmru v.20080324
47  (NTUSER.DAT) Gets contents of user's RunMRU key
48
49  RunMru
50  Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
51  LastWrite Time Mon Mar 30 12:29:51 2015 (UTC)
52  Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU has no values.
53  -------------------------------------
```

Via registry viewer



4. Last Files saved

OpenSaveMRU registry used to store the information about saved files using windows save file dialog box. Following are the information gathered from NTUSER.dat registry file.

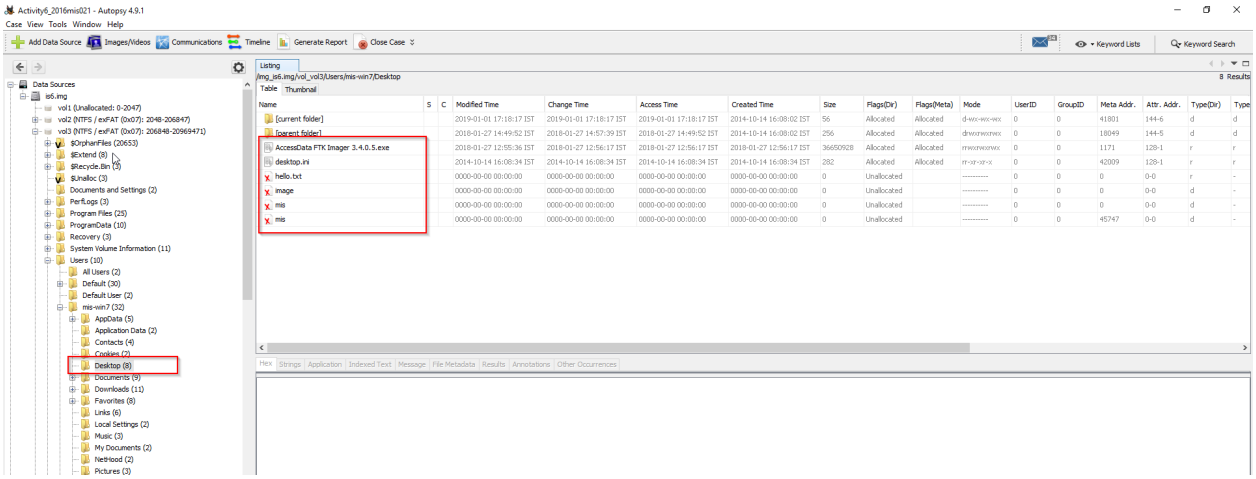
HKCU\SOFTWARE\Microsoft\Windows\CurrentVers ion\Explorer\ComDlg32
- OpenSaveMRU => Windows XP
- OpenSavePIDLMRU => Windows 7/ 8/ 10

Extracted using RegRipper

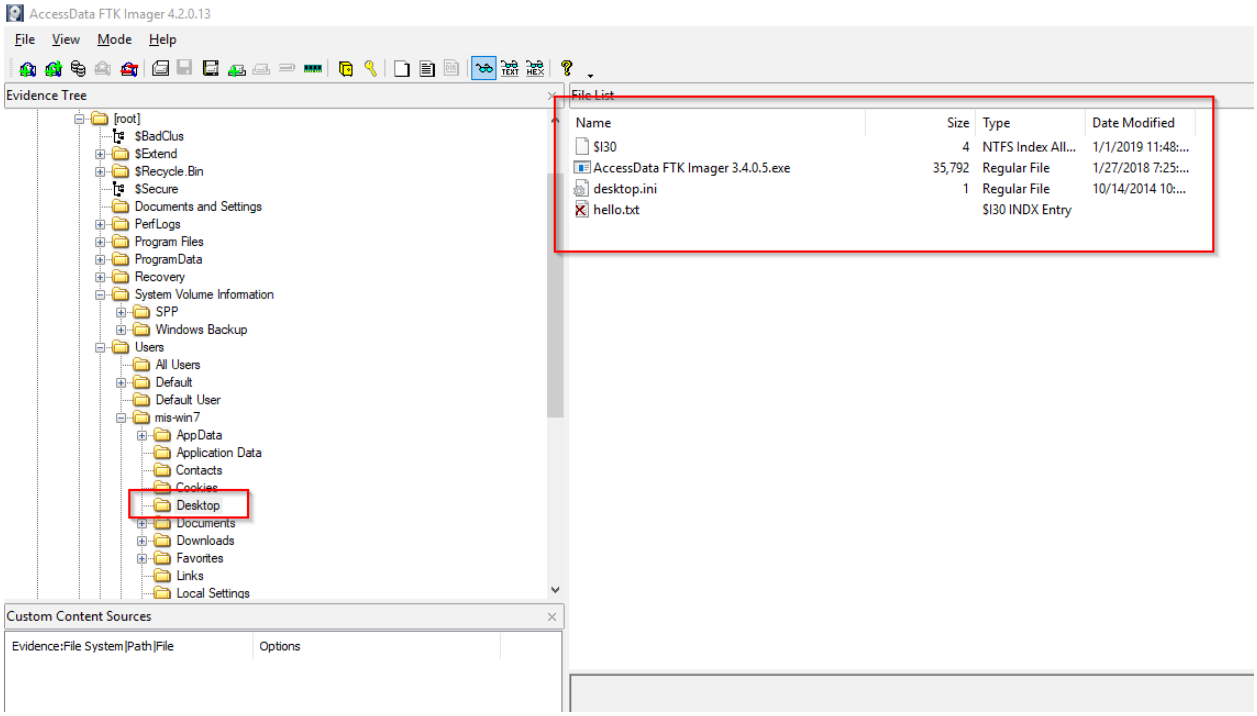
```
OpenSavePidlMRU
LastWrite: Thu Jan 10 06:11:01 2019
OpenSavePidlMRU\*
LastWrite Time: Thu Jan 10 06:13:53 2019
Note: All value names are listed in MRUListEx order.

  Users\fixedw_large_4x.jpg
  Users\img-20160614-wa0013-largejpg.jpg
  Users\mis\NTUSER
  Users\mis\NTUSER.DAT.copy0
  Users\mis\NTUSER.txt
  Users\NTUSER.DAT.copy0
  hello
  mis\NTUSER
  mis\NTUSER (2).DAT
  Users\RegRipper2.8-master.zip
  My Computer\E:\TechBank_User_Machine.dd
  Users\InClassActivity-2014mis001.tm7
  Users\LoggingModelReport-2014mis001.htm
  Libraries
  Libraries
  Users\InClassActivity.tm7
  Libraries
  Users\MIS3102SecureSoftwareSystems-TreatModelingwithMicrosoftSDLThreatModelingTool.pdf
  Users\ThreatModelingTool2016.msi
  My Computer\E:\MIS\3102\Lab\Lab1.tm4
```

5. Which files are on the user Desktop?

Using Autopsy

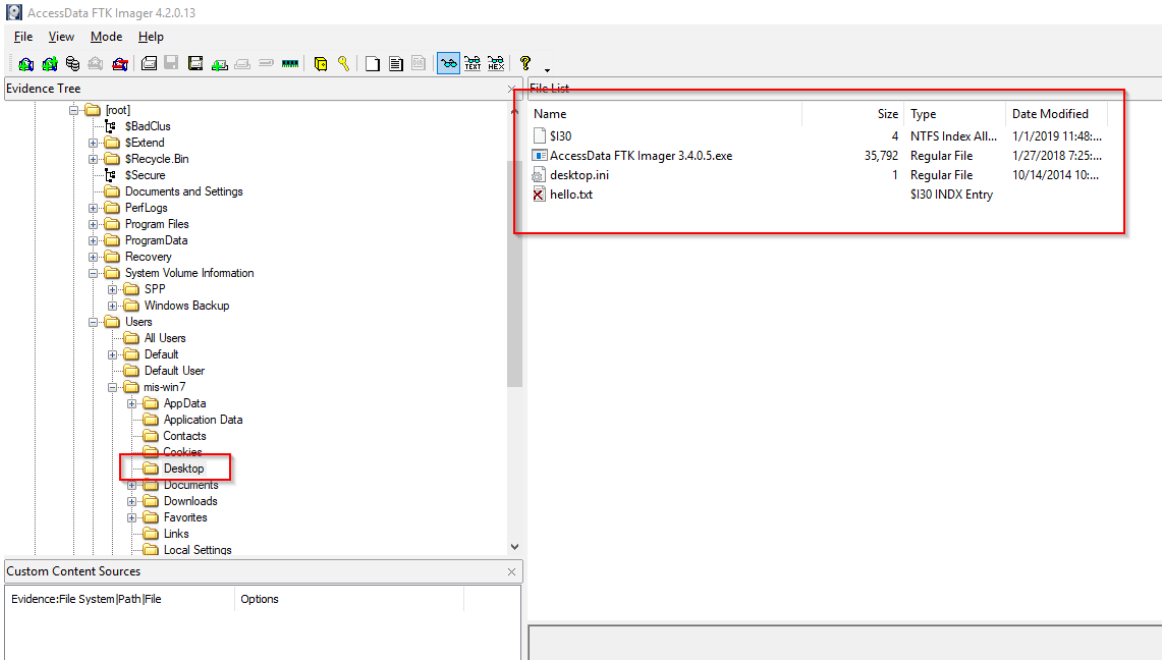


Using FTK Imager



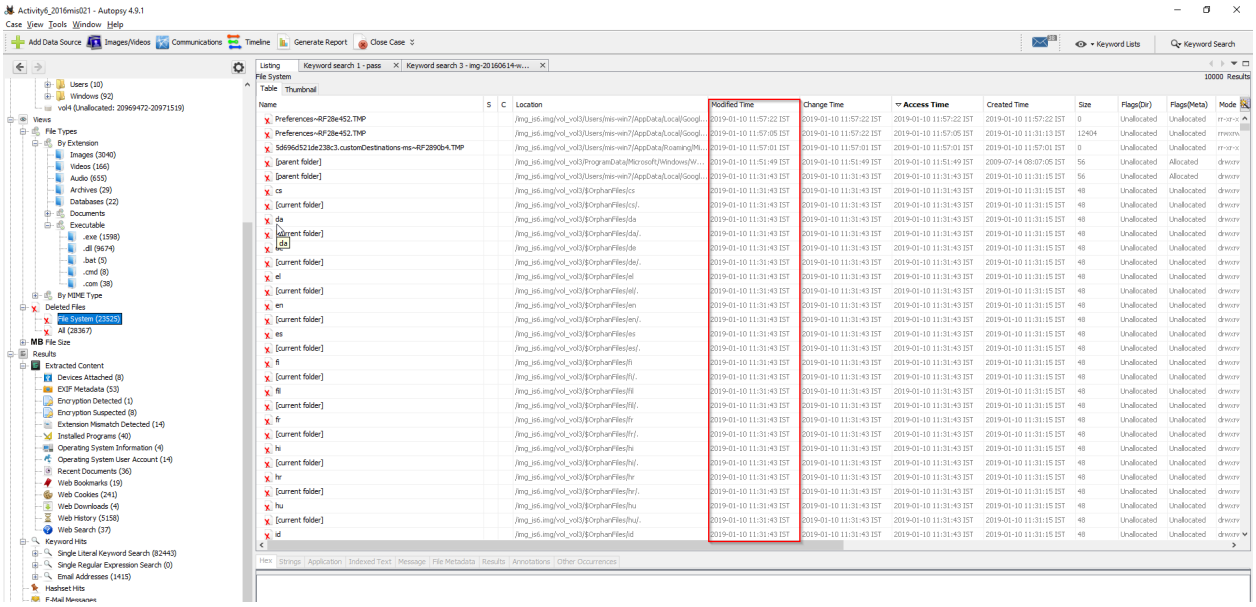
6. Identify which files were deleted and are still in the Recycle bin

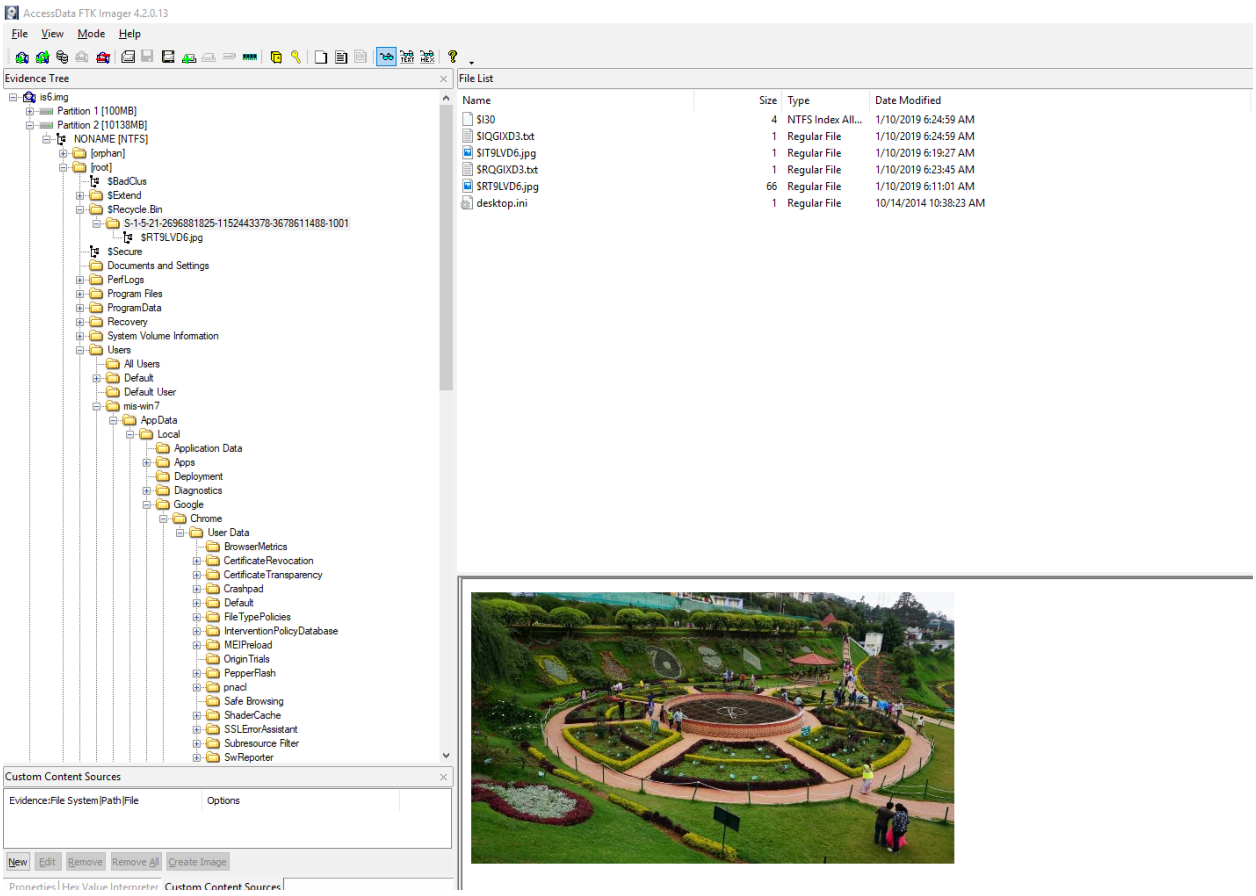
Using Autopsy



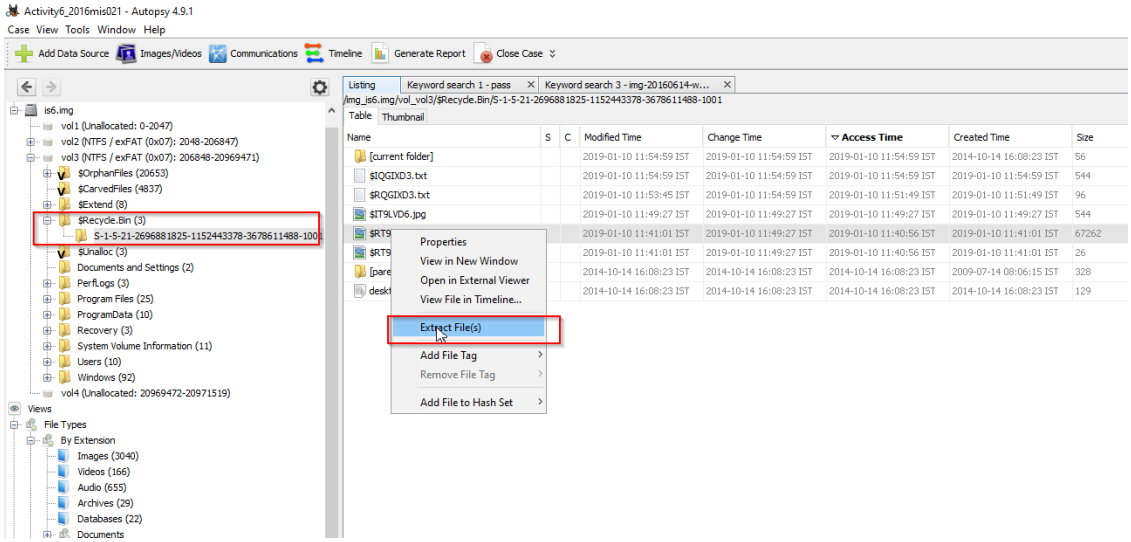
7. List of deleted files

According to Autopsy, there are lot of files deleted. Count is 23525

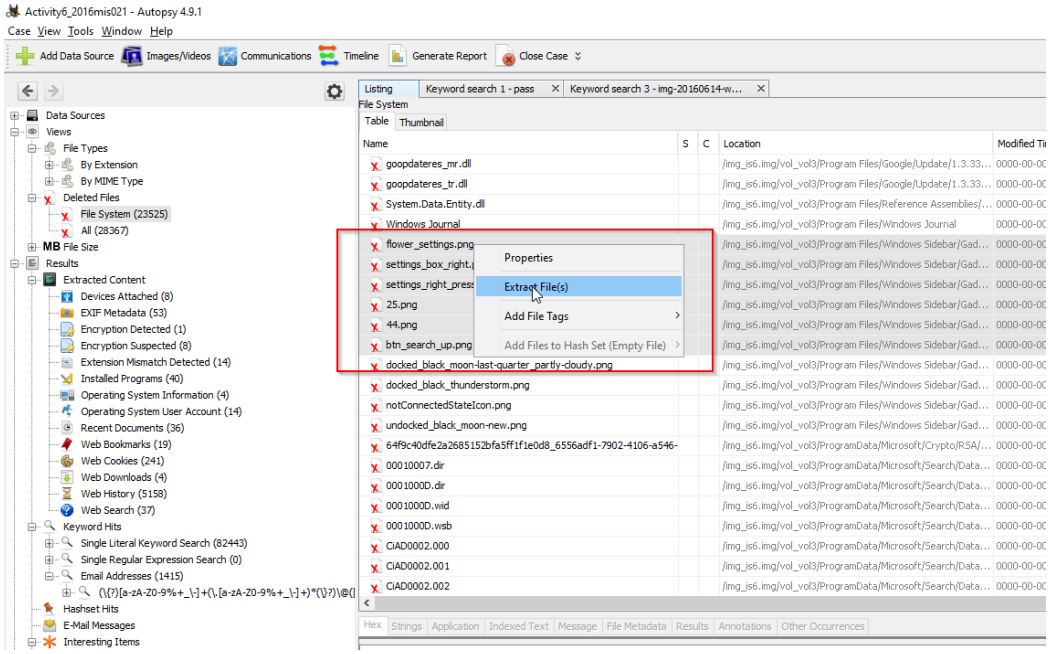




8. Recover any deleted files

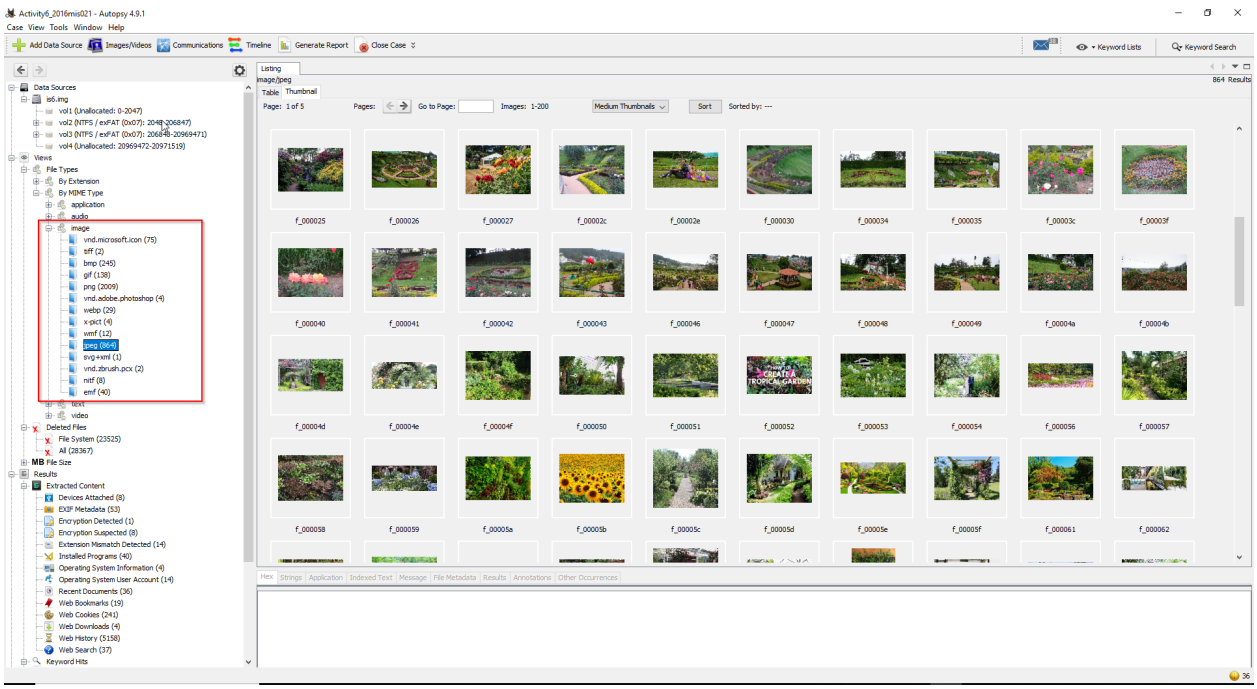


Via Autopsy



9. Open image files

Using Autopsy, we can see all the images and filtered by the image type as well.



Recently opened image files list can be found via registry as well.

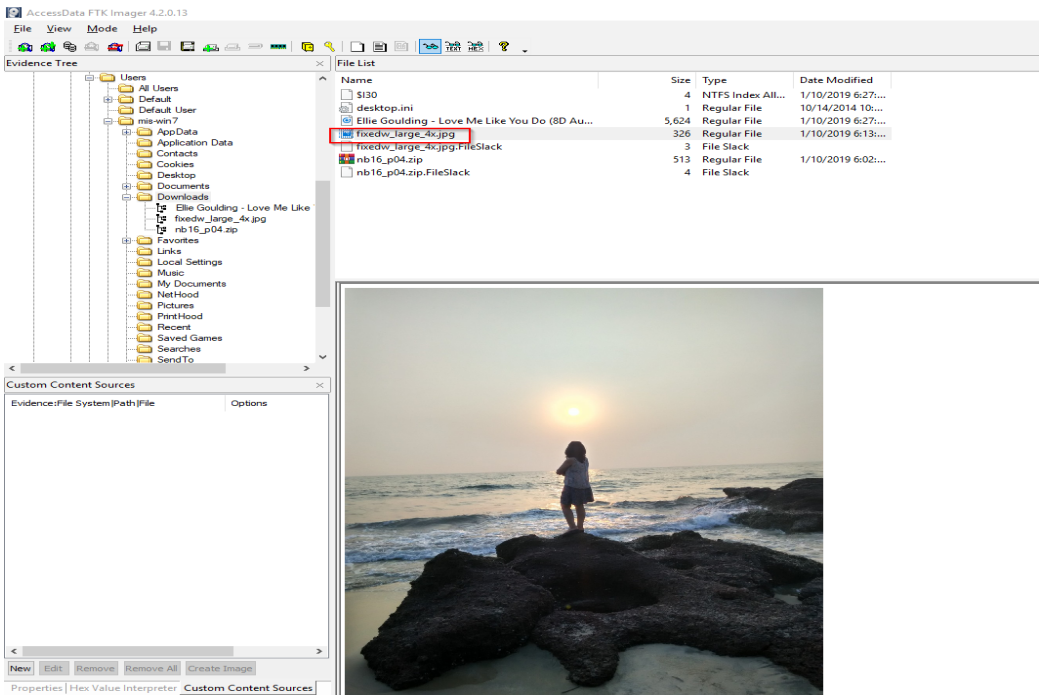
```
40
41  OpenSavePidlMRU\jpg
42  LastWrite Time: Thu Jan 10 06:13:53 2019
43  Note: All value names are listed in MRUListEx order.
44
45    Users\fixedw_large_4x.jpg
46    Users\img-20160614-wa0013-largejpg.jpg
47
```

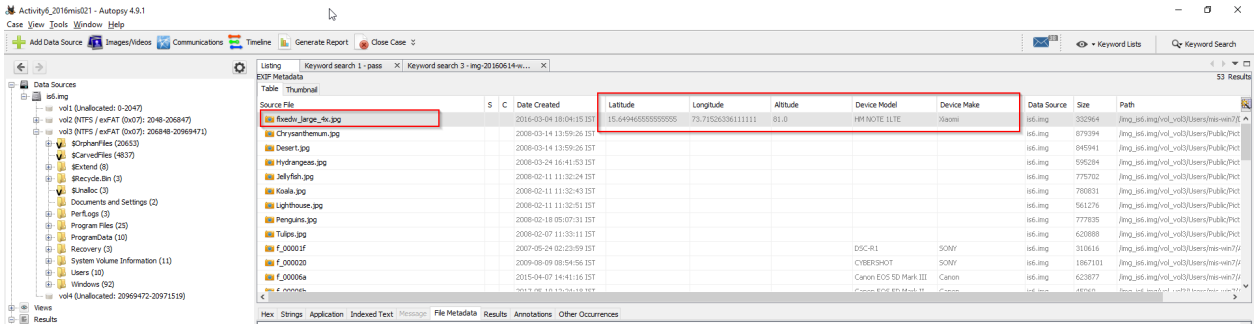
10. Does any of the opened images contain sensitive information? If so what is that information?

    Using RegRipper, can find out the recent opened files. According to that there are two image files.

```
40
41  OpenSavePidlMRU\jpg
42  LastWrite Time: Thu Jan 10 06:13:53 2019
43  Note: All value names are listed in MRUListEx order.
44
45    Users\fixedw_large_4x.jpg
46    Users\img-20160614-wa0013-largejpg.jpg
47
```

1st image:

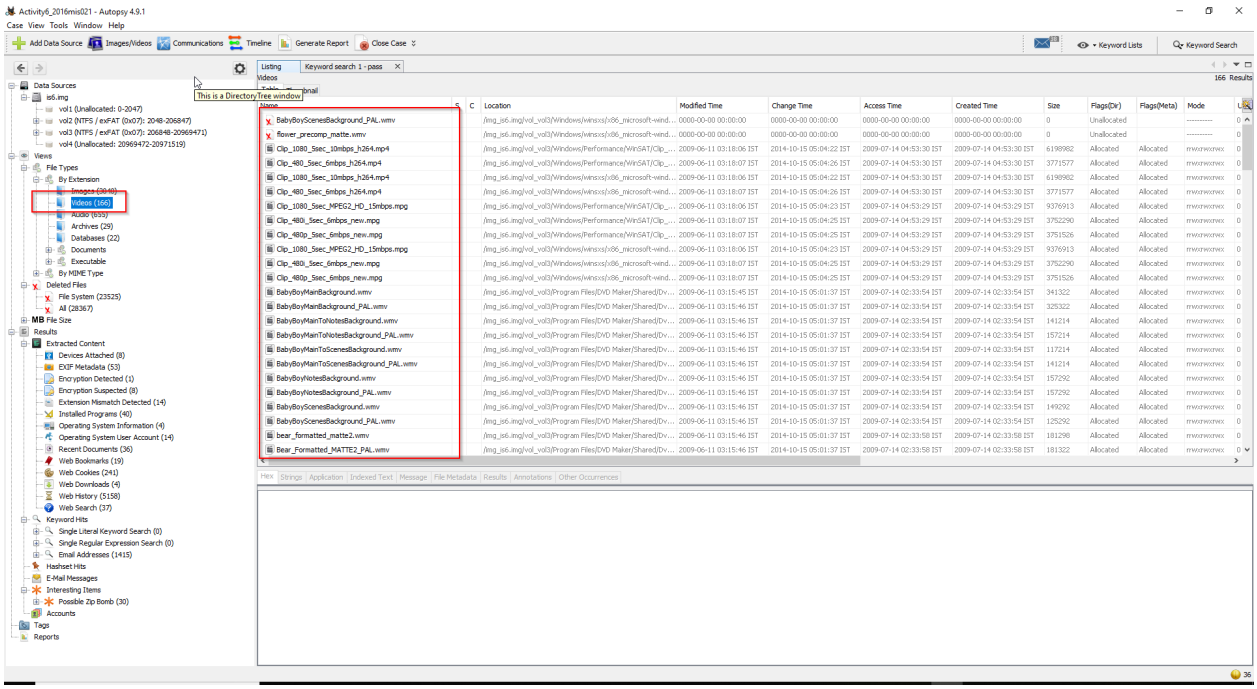


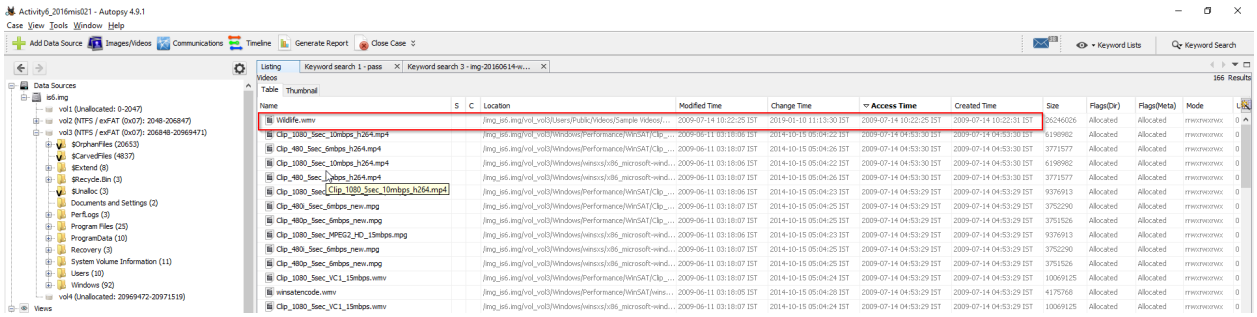


11. List played audio and video files

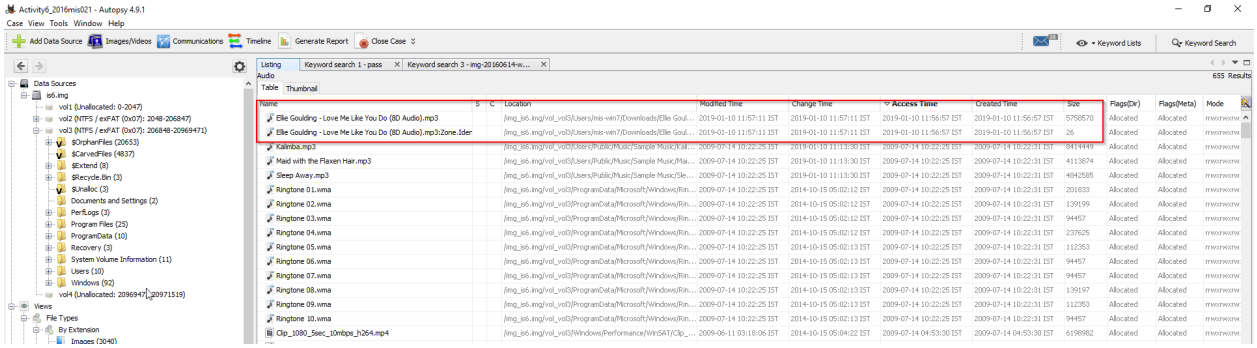
Using Autopsy

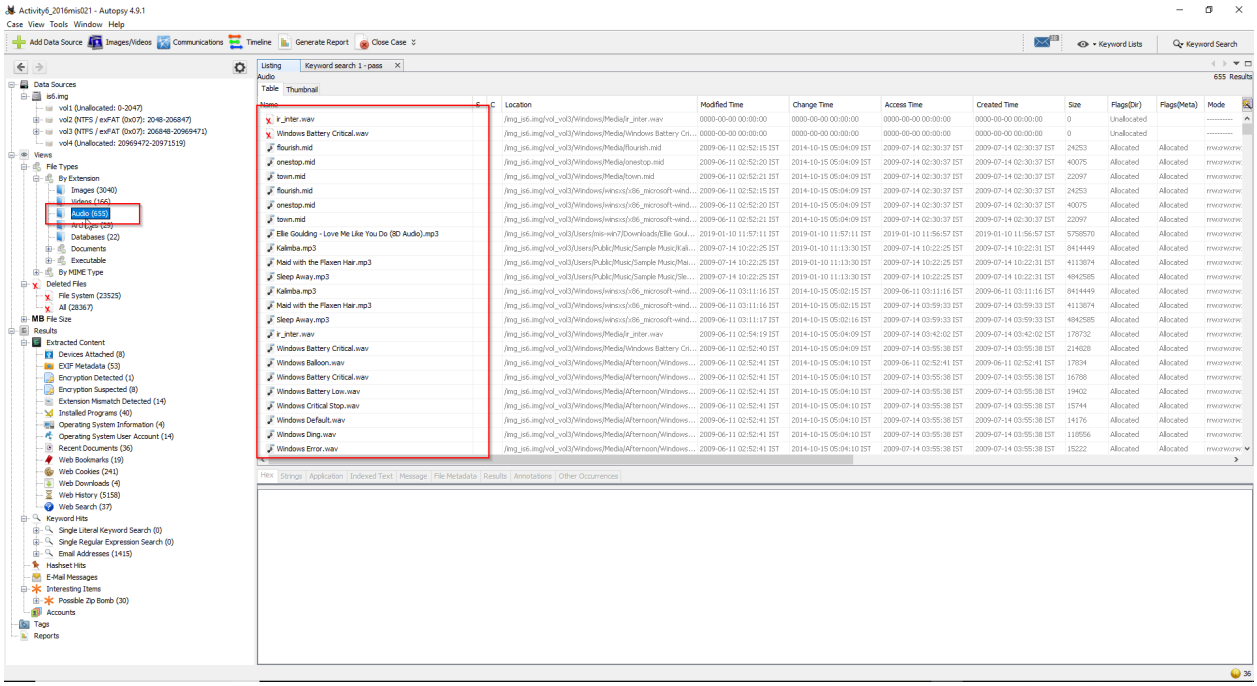
Video files:





Audio files:





3. Applications Analysis

1. Last time the password was changed

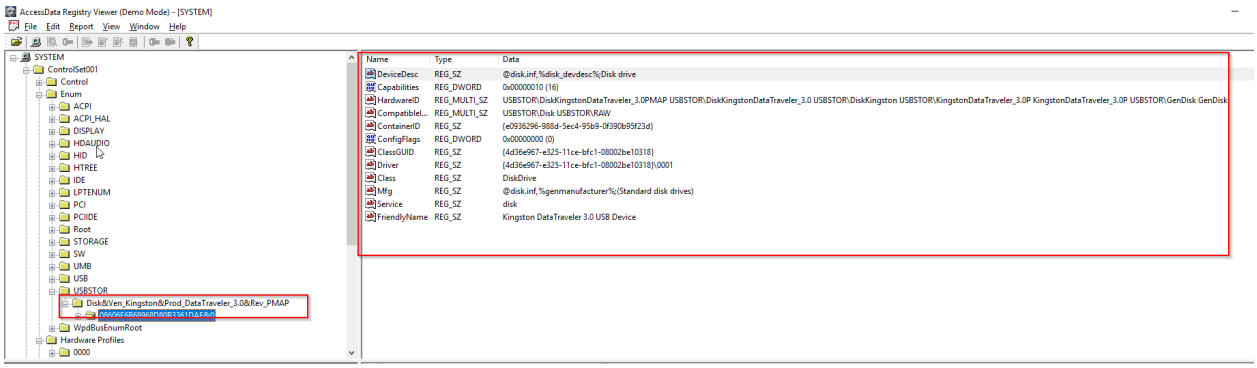
```
-------------------------
Username         : Administrator [500]
Full Name        :
User Comment     : Built-in account for administering the computer/domain
Account Type     : Default Admin User
Account Created : Tue Oct 14 23:05:19 2014 Z
Name             :
Last Login Date : Tue Jul 14 04:53:58 2009 Z
Pwd Reset Date   : Tue Jul 14 04:55:45 2009 Z
Pwd Fail Date    : Never
Login Count      : 1
  --> Password does not expire
  --> Account Disabled
  --> Normal user account
```

```
Username         : mis-win7 [1001]
Full Name        :
User Comment     :
Account Type     : Default Admin User
Account Created  : Tue Oct 14 10:35:59 2014 Z
Name             :
Last Login Date  : Thu Jan 10 05:42:56 2019 Z
Pwd Reset Date   : Tue Oct 14 10:35:59 2014 Z
Pwd Fail Date    : Never
Login Count      : 22
   --> Password does not expire
   --> Password not required
   --> Normal user account
```

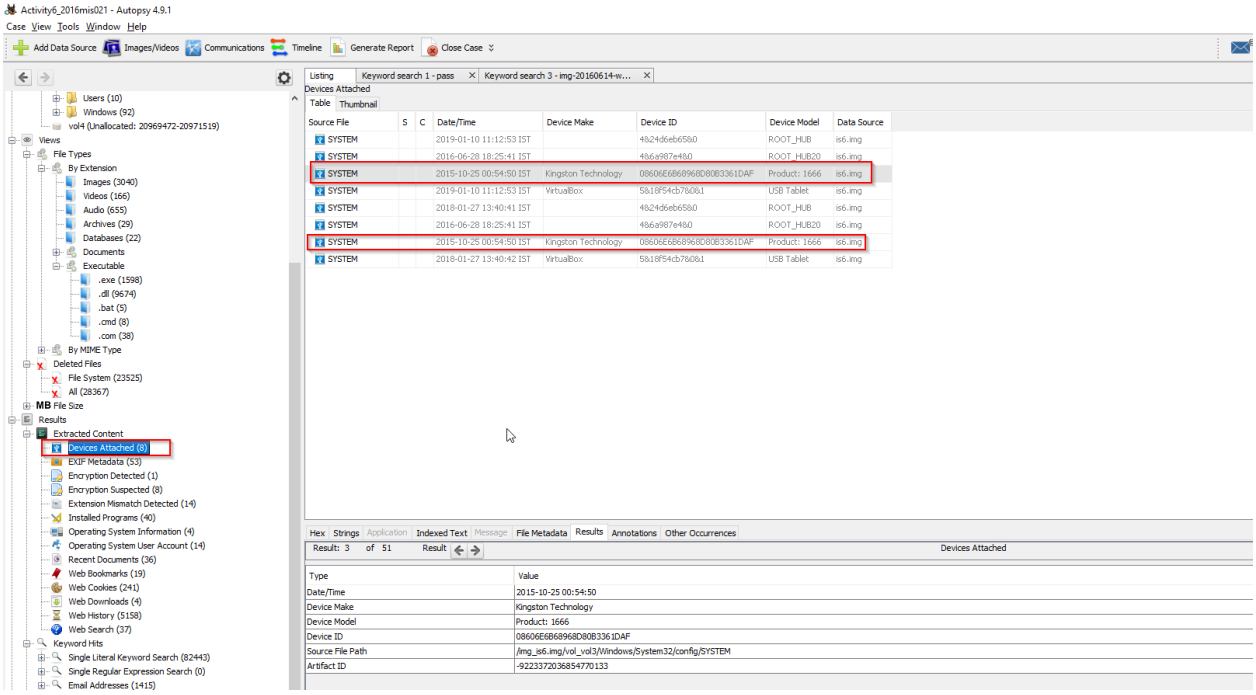
2. Was a USB stick ever connected to the machine and if so what information can you gather about that USB?

    - HKLM\SYSTEM\CurrentControl Set\Enum
        - USB
        - USBSTOR
    - CurrentControlSet – only in live system
    - ControlSet001 / ControlSet002 – in offline images

```
----------------------------------------
usbstor2 v.20080825
MIS-WIN7-PC,Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP,08606E6B68968D80B3361DAF&0,1445714690,Kingston DataTraveler 3.0 USB Device
----------------------------------------
Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP,Sat Oct 24 19:24:50 2015,08606E6B68968D80B3361DAF&0,Sat Oct 24 19:24:50 2015,Kingston DataTraveler 3.0 USB Device,
----------------------------------------
wpdbusenum v.20141111
(System) Get WpdBusEnumRoot subkey info

DISK&VEN_KINGSTON&PROD_DATATRAVELER_3.0&REV_PMAP (08606E6B68968D80B3361DAF&0)
  LastWrite: Sat Oct 24 19:24:50 2015
  DeviceDesc: DataTraveler 3.0
  Friendly: Shanil3
  Mfg: Kingston
  Device Parameters LastWrite: [Sat Oct 24 19:24:50 2015]
  LogConf LastWrite          : [Sat Oct 24 19:24:50 2015]
  Properties LastWrite       : [Sat Oct 24 19:24:50 2015]
  InstallDate     : Mon Mar 30 13:13:00 2015 UTC
  FirstInstallDate: Mon Mar 30 13:13:00 2015 UTC

ControlSet001\Control\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}
DISK&VEN_KINGSTON&PROD_DATATRAVELER_3.0&REV_PMAP\08606E6B68968D80B3361DAF&0
LastWrite: Mon Mar 30 13:13:00 2015

----------------------------------------
xpedition v.20120722
(System) Queries System hive for XP Edition info

xpedition v.20120722
----------------------------------------
ALERT: svcdll: wbem found in path: Winmgmt -> %SystemRoot%\system32\wbem\WMIsvc.dll
ALERT: svcdll: Relative path detected: WinHttpAutoProxySvc -> winhttp.dll
1247546229|ALERT|||svc_tln: Poss. ADS in path: %SystemRoot%\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
```



From Autopsy:

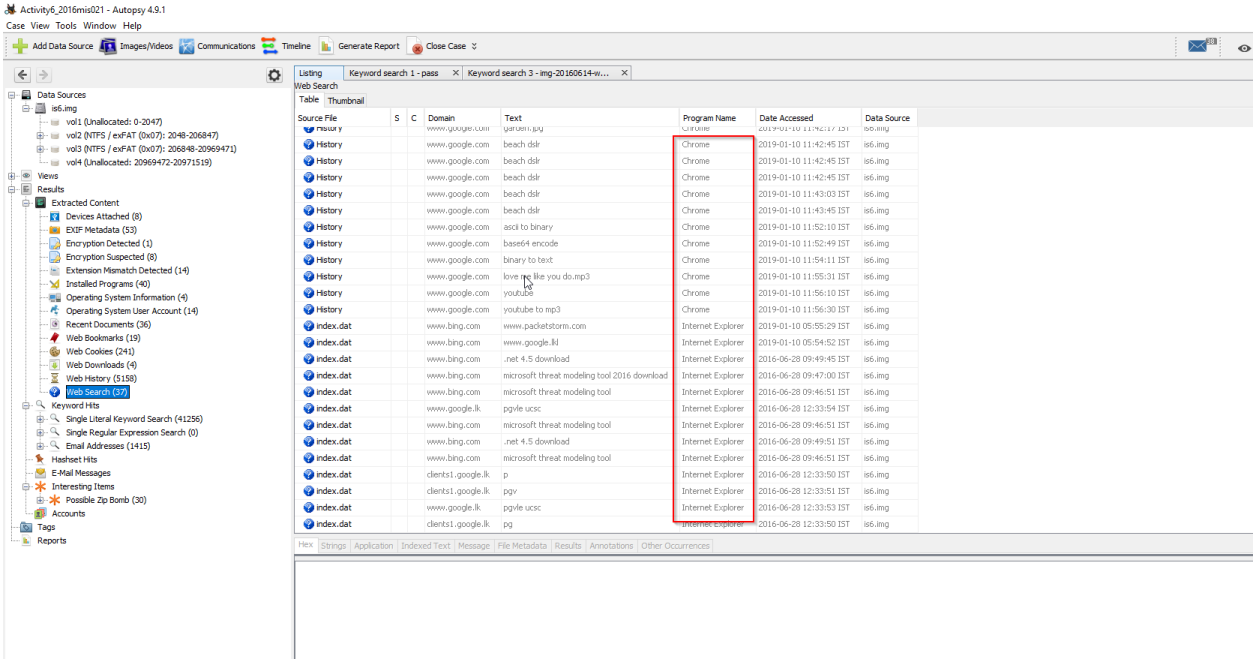


3. If user copied any files from the USB, What are the file names? File destination? Which applications open that files?

4. Browsing Information

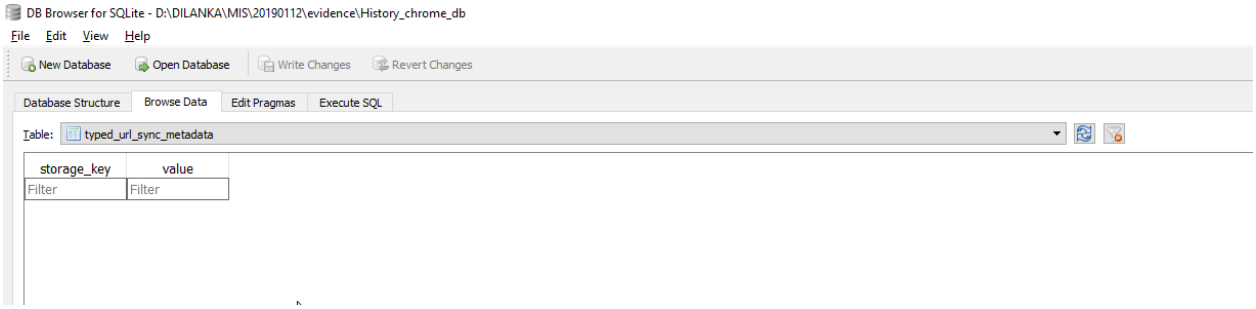
1. Which browser does the user use?

Using Autopsy, can easily identify browsing information. User has used both internet explorer and Google Chrome for browsing.

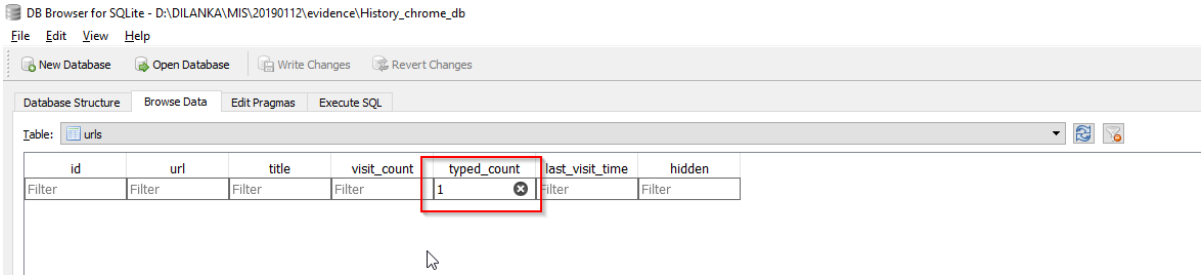


2. List of typed URL

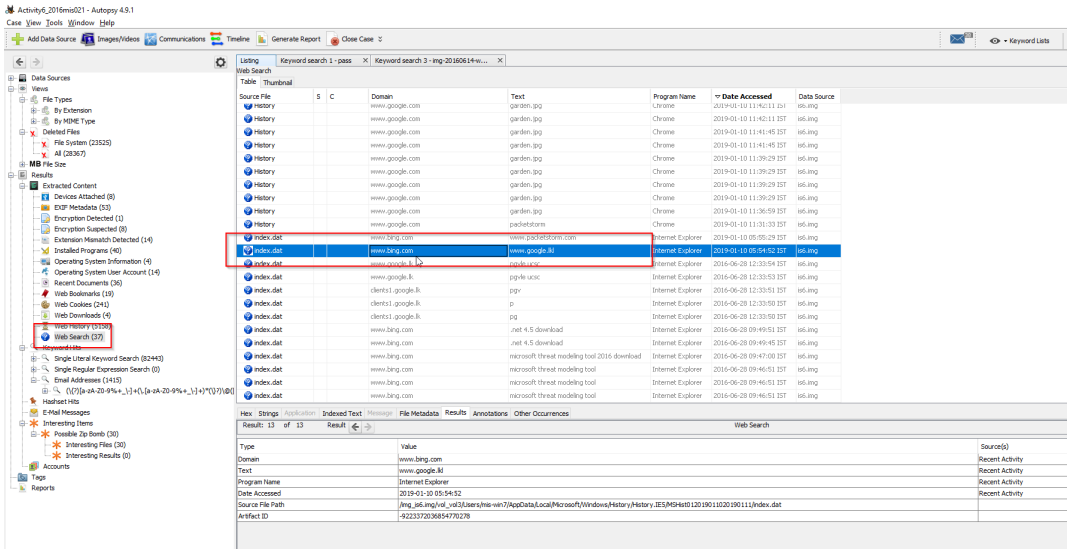
Imported the Chrome database to Sqlite. No typed url.



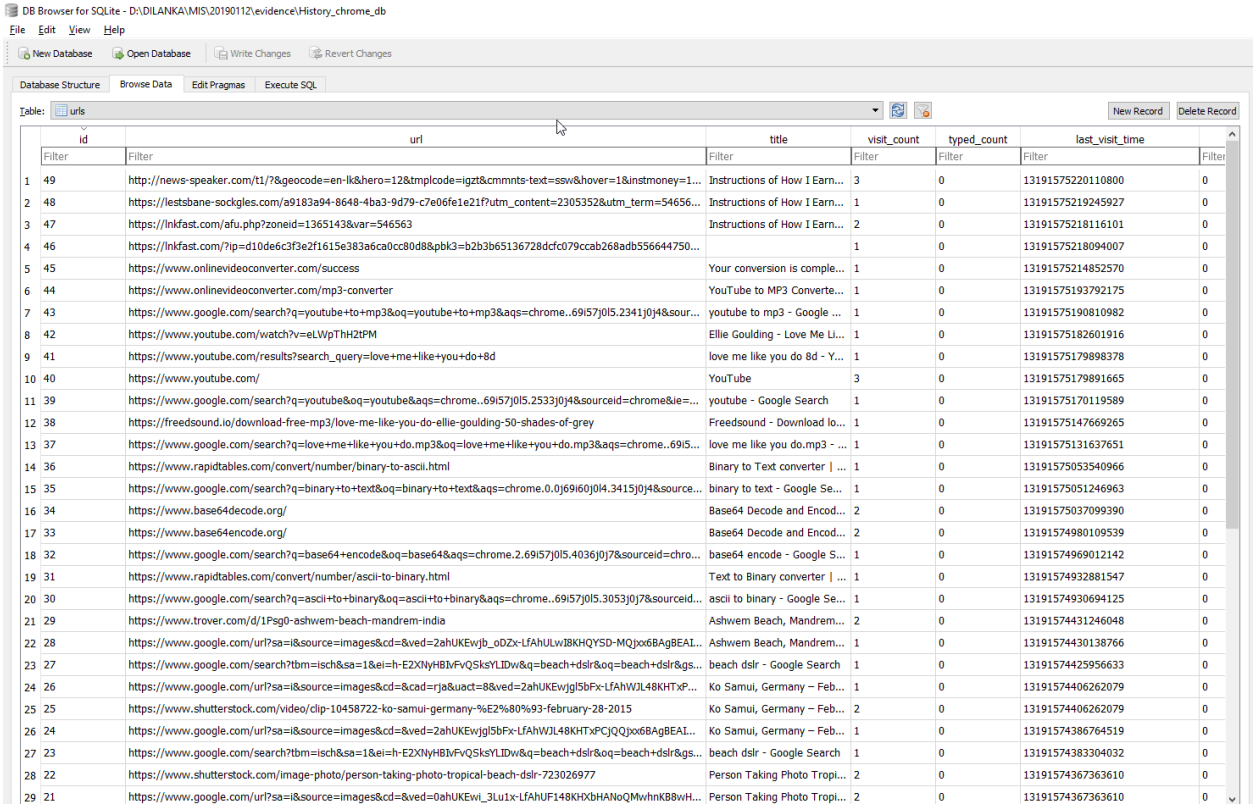
No filtering results:



But According to Autopsy, when examine domains, could see type error url:



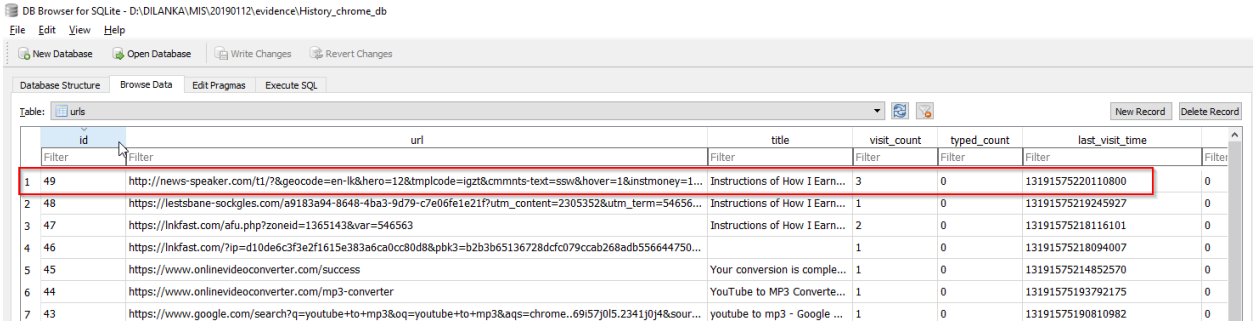
3. List of the URL visited by the user



	id	url	title	visit_count	typed_count	last_visit_time	
1	49	http://news-speaker.com/t1/?&geocode=en-lk&hero=12&tmplcode=igzt&cmmnts-text=ssw&hover=1&instmoney=1...	Instructions of How I Earn...	3	0	13191575220110800	0
2	48	https://lestsbane-sockgles.com/a9183a94-8648-4ba3-9d79-c7e06fe1e21f?utm_content=2305352&utm_term=54656...	Instructions of How I Earn...	1	0	13191575219245927	0
3	47	https://lnkfast.com/afu.php?zoneid=1365143&var=546563	Instructions of How I Earn...	2	0	13191575218116101	0
4	46	https://lnkfast.com/?ip=d10de6c3f3e2f1615e383a6ca0cc80d8&pbk3=b2b3b65136728dcfc079ccab268adb556644750...		1	0	13191575218094007	0
5	45	https://www.onlinevideoconverter.com/success	Your conversion is comple...	1	0	13191575214852570	0
6	44	https://www.onlinevideoconverter.com/mp3-converter	YouTube to MP3 Converte...	1	0	13191575193792175	0
7	43	https://www.google.com/search?q=youtube+to+mp3&oq=youtube+to+mp3&aqs=chrome..69i57j0l5.2341j0j4&sour...	youtube to mp3 - Google ...	1	0	13191575190810982	0
8	42	https://www.youtube.com/watch?v=eLWpThH2tPM	Ellie Goulding - Love Me Li...	1	0	13191575182601916	0
9	41	https://www.youtube.com/results?search_query=love+me+like+you+do+8d	love me like you do 8d - Y...	1	0	13191575179898378	0
10	40	https://www.youtube.com/	YouTube	3	0	13191575179891665	0
11	39	https://www.google.com/search?q=youtube&oq=youtube&aqs=chrome..69i57j0l5.2533j0j4&sourceid=chrome&ie=...	youtube - Google Search	1	0	13191575170119589	0
12	38	https://freesound.io/download-free-mp3/love-me-like-you-do-ellie-goulding-50-shades-of-grey	Freesound - Download lo...	1	0	13191575147669265	0
13	37	https://www.google.com/search?q=love+me+like+you+do.mp3&oq=love+me+like+you+do.mp3&aqs=chrome..69i5...	love me like you do.mp3 - ...	1	0	13191575131637651	0
14	36	https://www.rapidtables.com/convert/number/binary-to-ascii.html	Binary to Text converter | ...	1	0	13191575053540966	0
15	35	https://www.google.com/search?q=binary+to+text&oq=binary+to+text&aqs=chrome.0.0j69i60j0l4.3415j0j4&source...	binary to text - Google Se...	1	0	13191575051246963	0
16	34	https://www.base64decode.org/	Base64 Decode and Encod...	2	0	13191575037099390	0
17	33	https://www.base64encode.org/	Base64 Decode and Encod...	2	0	13191574980109539	0
18	32	https://www.google.com/search?q=base64+encode&oq=base64&aqs=chrome.2.69i57j0l5.4036j0j7&sourceid=chro...	base64 encode - Google S...	1	0	13191574969012142	0
19	31	https://www.rapidtables.com/convert/number/ascii-to-binary.html	Text to Binary converter | ...	1	0	13191574932881547	0
20	30	https://www.google.com/search?q=ascii+to+binary&oq=ascii+to+binary&aqs=chrome..69i57j0l5.3053j0j7&sourceid...	ascii to binary - Google Se...	1	0	13191574930694125	0
21	29	https://www.trover.com/d/1Psg0-ashwem-beach-mandrem-india	Ashwem Beach, Mandrem...	2	0	13191574431246048	0
22	28	https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwjb_oDZx-LfAhULwI8KHQYSD-MQjxx6BAgBEAI...	Ashwem Beach, Mandrem...	1	0	13191574430138766	0
23	27	https://www.google.com/search?tbm=isch&sa=1&ei=h-E2XNyHBIvFvQSksYLIDw&q=beach+dslr&oq=beach+dslr&gs...	beach dslr - Google Search	1	0	13191574425956633	0
24	26	https://www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjgl5bFx-LfAhWJL48KHTxP...	Ko Samui, Germany – Feb...	1	0	13191574406262079	0
25	25	https://www.shutterstock.com/video/clip-10458722-ko-samui-germany-%E2%80%93-february-28-2015	Ko Samui, Germany – Feb...	2	0	13191574406262079	0
26	24	https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwjgl5bFx-LfAhWJL48KHTxPCjQQjJxx6BAgBEAI...	Ko Samui, Germany – Feb...	1	0	13191574386764519	0
27	23	https://www.google.com/search?tbm=isch&sa=1&ei=h-E2XNyHBIvFvQSksYLIDw&q=beach+dslr&oq=beach+dslr&gs...	beach dslr - Google Search	1	0	13191574383304032	0
28	22	https://www.shutterstock.com/image-photo/person-taking-photo-tropical-beach-dslr-723026977	Person Taking Photo Tropi...	2	0	13191574367363610	0
29	21	https://www.google.com/url?sa=i&source=images&cd=&ved=0ahUKEwi_3Lu1x-LfAhUF148KHXbHANoQMwhnKB8wH...	Person Taking Photo Tropi...	2	0	13191574367363610	0

4. What was the last page visited by the user?

Ordered by descending order by Id or visit time:



	id	url	title	visit_count	typed_count	last_visit_time	
1	49	http://news-speaker.com/t1/?&geocode=en-lk&hero=12&tmplcode=igzt&cmmnts-text=ssw&hover=1&instmoney=1...	Instructions of How I Earn...	3	0	13191575220110800	0
2	48	https://lestsbane-sockgles.com/a9183a94-8648-4ba3-9d79-c7e06fe1e21f?utm_content=2305352&utm_term=54656...	Instructions of How I Earn...	1	0	13191575219245927	0
3	47	https://lnkfast.com/afu.php?zoneid=1365143&var=546563	Instructions of How I Earn...	2	0	13191575218116101	0
4	46	https://lnkfast.com/?ip=d10de6c3f3e2f1615e383a6ca0cc80d8&pbk3=b2b3b65136728dcfc079ccab268adb556644750...		1	0	13191575218094007	0
5	45	https://www.onlinevideoconverter.com/success	Your conversion is comple...	1	0	13191575214852570	0
6	44	https://www.onlinevideoconverter.com/mp3-converter	YouTube to MP3 Converte...	1	0	13191575193792175	0
7	43	https://www.google.com/search?q=youtube+to+mp3&oq=youtube+to+mp3&aqs=chrome..69i57j0l5.2341j0j4&sour...	youtube to mp3 - Google ...	1	0	13191575190810982	0

http://news-speaker.com/t1/?&geocode=en-lk&hero=12&tmplcode=igzt&cmmnts-text=ssw&hover=1&instmoney=1&instsmall=1&bbb=1&multioffer=1&isback=1&back=aHR0cHM6Ly9sZXN0c2JhbmUtc29ja2dsZXMuY29tL2RiZTMwNWI4LTQ0NzItNDQxNi1hZTA3LTc1YmZmNDEwZmU0Nz91dG1fdGVybT17em9uZWlkfSZ1dG1fc291cmNlPWJhY2smdXRtX21lZGl1bT1wJnJlZj1wX0JBQ0tfYmFja19CQUNLX2Rlc2s=&cep=4KoI6M6neWmE1gNaCykK0VcBIbvJBM_u5eBkgd4R5QSRLXoD_gKFFx6DTrYIda_6rihb-FdCzDNpyCYR4dMkOEJ10iwlH4i2P-K1mp2OZeB09TZoMuvmwT3ekoR-n-Q8zJFniqhT_FKJZFUDMSarDusAQM3uM_NMiqnMVeeF8429QaGdstQdiEHBRKOIN2bzGFcEBQd11WPeJq3WvRPgOnTXnMS5BWZ8C-kKfHklfNdmmxg9Bo9LGWrpj4j1Nb1cJXh2Nn7MZ0BmYD6NhJpWxV6yTqyWlFuiafxat3Hn4IEyeN6zM0buZDdeAbeDmGMmXkq8EcxY9lPgDdGTLrXeW1H1AvJoS_NJvluiB7LIVZc&utm_content=2305352&utm_term=546563&utm_source=propeller&utm_campaign=1589119&utm_medium=p&ref=p_prop_ia_t104-lk&eid=107114548531568642

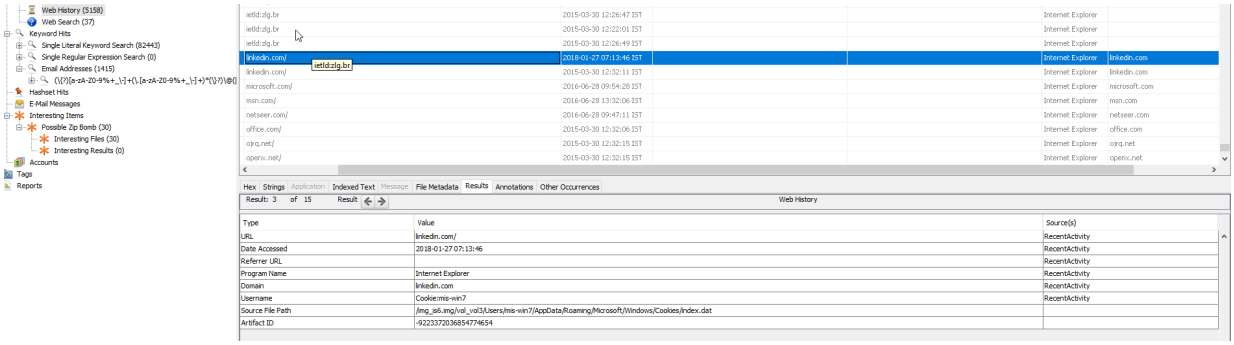
5. Did the user visit any chat room? If so, state which ones and who are the people chat with this user? And content of those conversations?

   If there are chat history, it is recorded in “Chats” table of browser related database. But there is no such table found. So assumed that there is no chat history.

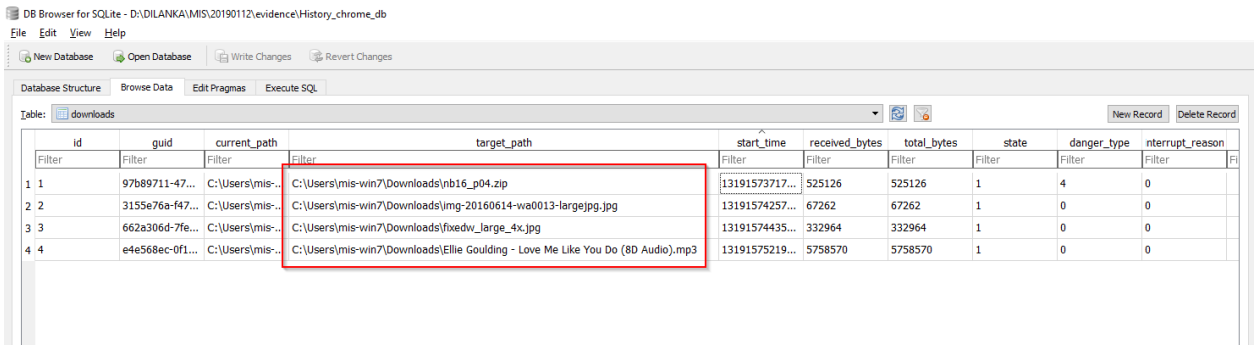
   But according to the web history, user has accessed the some google.com, msn, bing sites, but those chats we cannot monitor if user accessed chat via chat client that we cannot monitor.

6. Did the user joined with any social networking community websites? If so identify what are those websites, Information about the user profile and what kind of activities the user was doing?

   According to the web history, couldn’t find any social media network domain by filter with Autopsy except linkedIn.



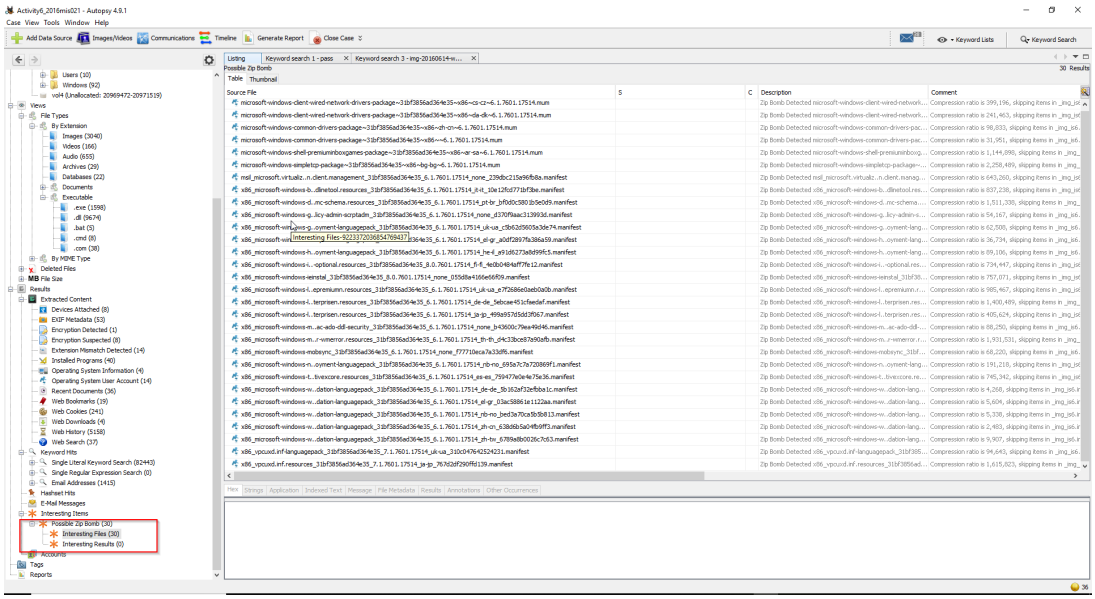
7. List downloaded files



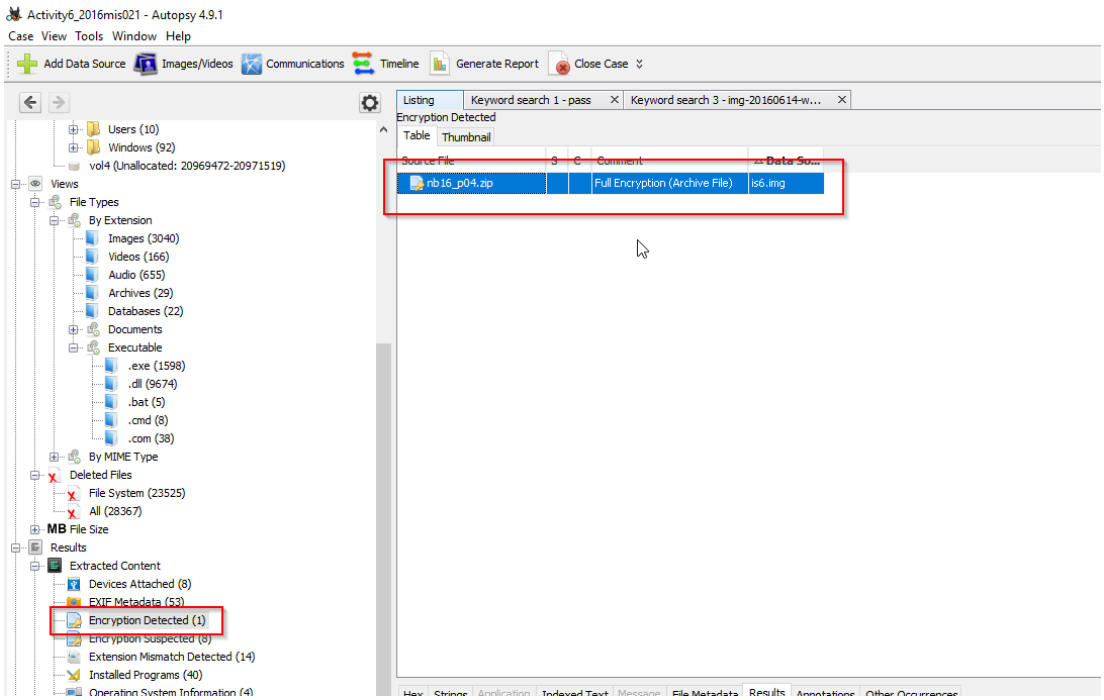
5. Malicious activities

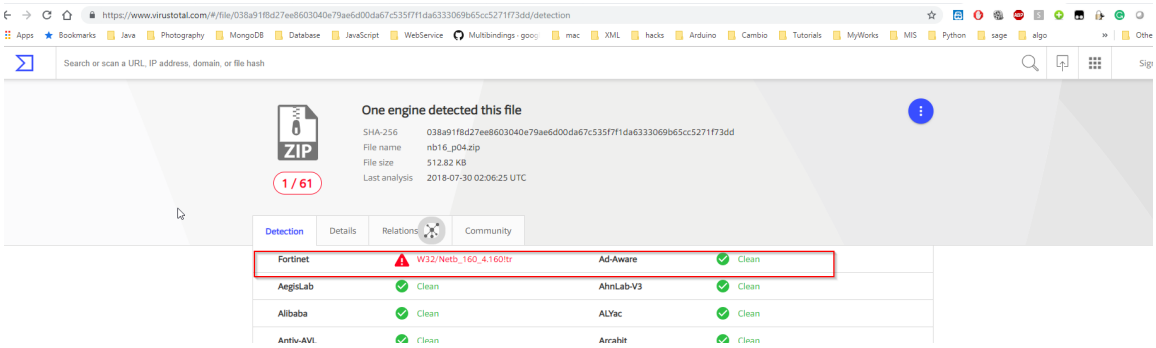
    1. List malicious applications.
        1. Their types?

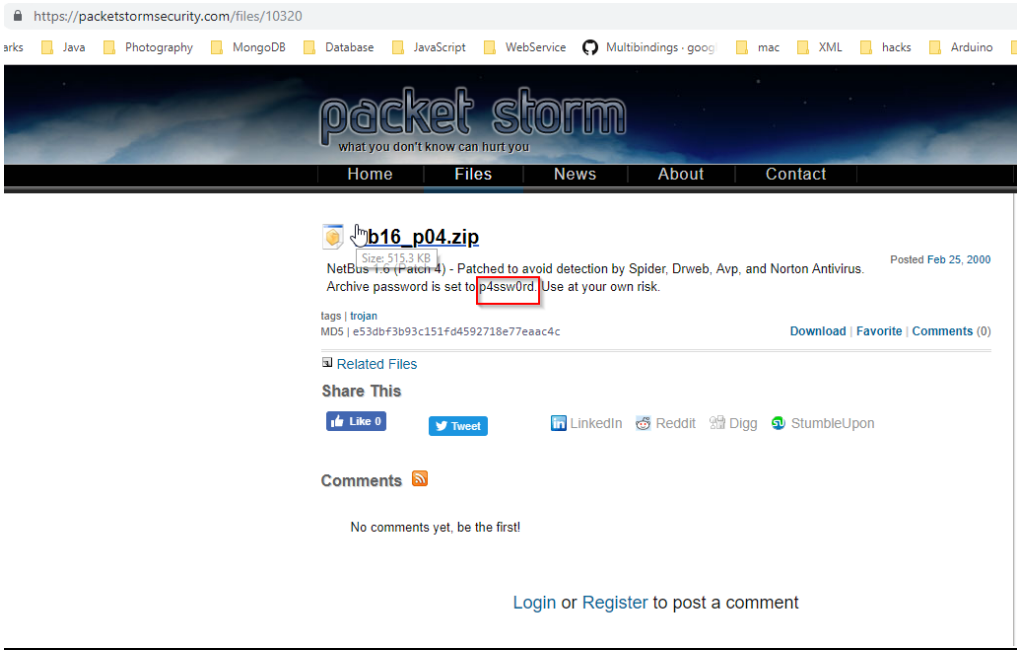
Zip bombs



Backdoors







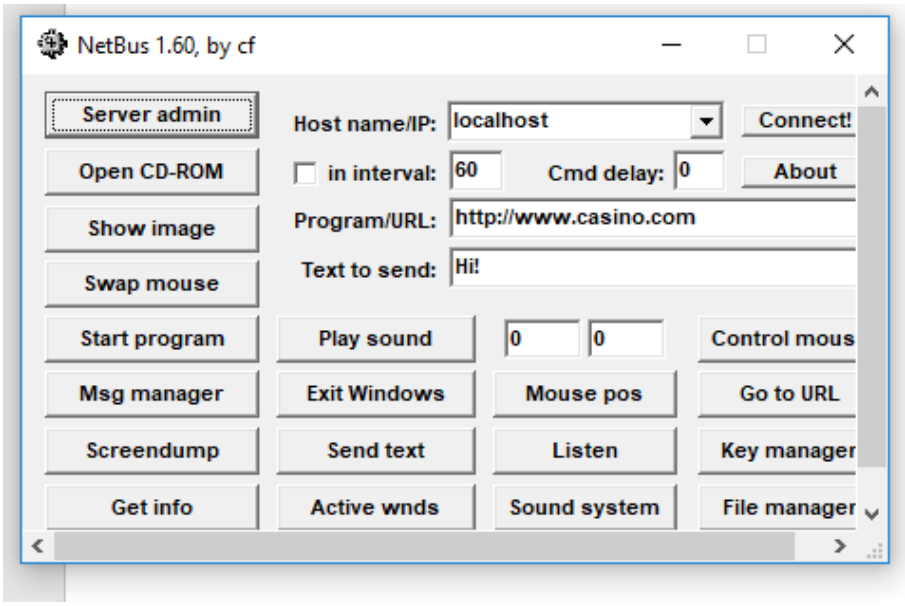
2. How they infected machine?

Zip bombs

When extracting zip files, may cause of resource starvation of the server and make servers or some services unavailable.

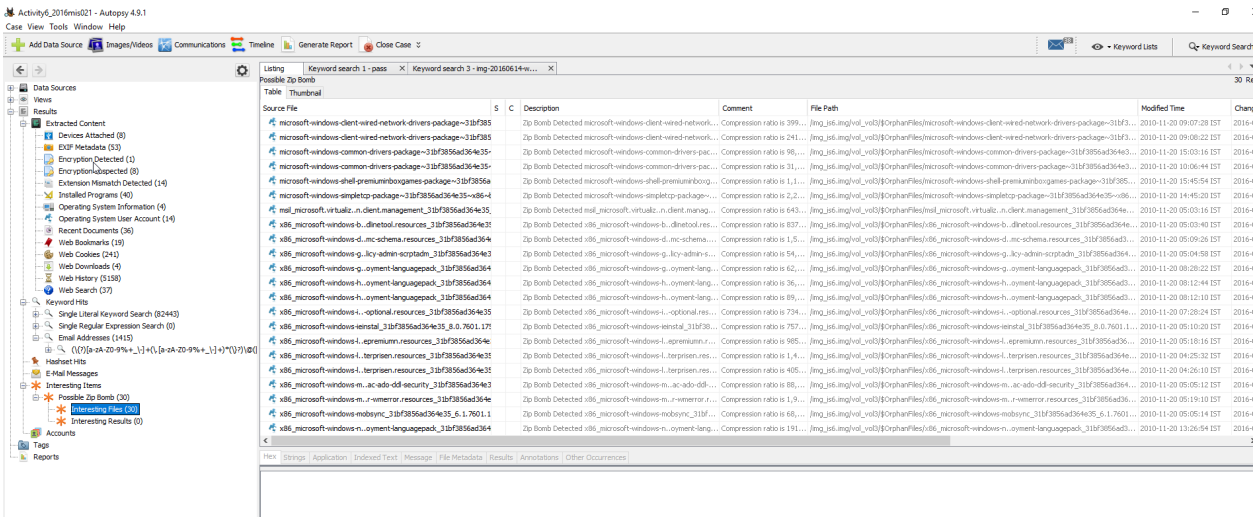
Backdoor

Attacker can install backdoors and get access to some services of victims PC or servers to do some malicious activities or stole sensitive data.



3. Their activities?

Can see zip bombs are spread multiple places



Other findings

```
----------------------------------------
ahaha v.20131009
(Software,NTUSER.DAT) Detect possible presence of ahaha malware
```

```
Microsoft\ESENT\Process not found.
----------------------------------------
etos v.20150325
(Software) Checks Software hive for indicators of Etos malware
```

```
LoadAppInit_DLLs
----------------------------------------
inprocserver v.20141126
(Software) Checks CLSID InProcServer32 values for indications of malware

Classes\CLSID

Possible Lurk infection found!
  c:\windows\system32\pngfilt.dll
----------------------------------------
```

```
----------------------------------------
renocide v.20130425
(Software) Check for Renocide malware
```

```
----------------------------------------
mmo v.20130217
(NTUSER.DAT) Checks NTUSER for Multimedia\Other values [malware]

Software\Microsoft\Multimedia\Other not found.
Software\Microsoft\CTF\LangBarAddIn not found.
----------------------------------------
```

2. Windows registry changes

   Can find some audit policy logs from the registry extracted from RegRipper

```
----------------------------------------
auditfail v.20081212
(System) Get CrashOnAuditFail value

CrashOnAuditFail = 0
Feature is off; the system will not halt
----------------------------------------
backuprestore v.20130904
(System) Gets the contents of the FilesNotToSnapshot, KeysNotToRestore, and FilesNotToBackup keys

ControlSet001\Control\BackupRestore\FilesNotToSnapshot
LastWrite Time Tue Jul 14 04:37:09 2009 (UTC)
The listed directories/files are not backed up in Volume Shadow Copies

  WUA : %windir%\softwaredistribution\*.* /s
  OutlookOST : $UserProfile$\AppData\Local\Microsoft\Outlook\*.ost
  FVE : $AllVolumes$\System Volume Information\FVE.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}
  RAC : %ProgramData%\Microsoft\RAC\* %ProgramData%\Microsoft\RAC\StateData\* %ProgramData%\Microsoft\RAC\Outbound\* %ProgramData%\Microsoft\RAC\PublishedData\* %ProgramData%\Microsoft\RAC\

FilesNotToBackup key
ControlSet001\Control\BackupRestore\FilesNotToBackup
LastWrite Time Tue Oct 14 22:40:12 2014 (UTC)
Specifies the directories and files that backup applications should not backup or restore

  Temporary Files : %TEMP%\* /s
  Power Management : \hiberfil.sys
  Memory Page File : \Pagefile.sys
  Offline Files Cache : C:\Windows\CSC\* /s
  Netlogon : %SystemRoot%\netlogon.chg
  Internet Explorer : %UserProfile%\index.dat /s
  BITS_LOG : C:\Windows\System32\Bits.log
  BITS_BAK : C:\Windows\System32\Bits.bak
  WUA : %windir%\softwaredistribution\*.* /s
  WER : %ProgramData%\Microsoft\Windows\WER\* /s
  BITS_metadata : C:\ProgramData\Microsoft\Network\Downloader\*
  ETW : %SystemRoot%\system32\LogFiles\WMI\RtBackup\*.*
  Kernel Dumps : %systemroot%\Minidump\* /s %systemroot%\memory.dmp
  Mount Manager : \System Volume Information\MountPointManagerRemoteDatabase
  VSS Default Provider : \System Volume Information\*{3808876B-C176-4e48-B7AE-04046E6CC752} /s
  VSS Service DB : \System Volume Information\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}DB
  FVE_Log : \System Volume Information\FVE.{c9ca54a3-6983-46b7-8684-a7e5e23499e3}
  FVE_Wipe : \System Volume Information\FVE.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}
  VSS Service Alternate DB : \System Volume Information\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}ALT
  FVE_Control : \System Volume Information\FVE.{e40ad34d-dae9-4bc7-95bd-b16218c10f72}.*
  MS Distributed Transaction Coordinator : C:\Windows\system32\MSDtc\MSDTC.LOG C:\Windows\system32\MSDtc\trace\dtctrace.log
  RAC : %ProgramData%\Microsoft\RAC\* %ProgramData%\Microsoft\RAC\StateData\* %ProgramData%\Microsoft\RAC\Outbound\* %ProgramData%\Microsoft\RAC\PublishedData\* %ProgramData%\Microsoft\RAC\

KeysNotToRestore key
ControlSet001\Control\BackupRestore\KeysNotToRestore
LastWrite Time Tue Jul 14 04:37:09 2009 (UTC)

Specifies the names of the registry subkeys and values that backup applications should not restore
```

Approach

1. With the artefact provided and as it is disk dump, decided to choose appropriate tools which help to analyse and examine disk dump.
2. Initially started the analysis with the tool called Autopsy.
3. Able to find information related to the infrastructure related information with the analysis by the Volatility.
   a. System/OS information
   b. Hardware compatibility
   c. Deleted files.
   d. Files by type.
   e. Zip bombs identified.
   f. Files by size.
   g. Encrypted files.
   h. Attached device information.
   i. And other many information…
4. Once analyse the disk dump, identified suspicious files which are large files and encrypted files.
5. Encrypted files must be user encrypted files or some malicious files.
6. So suspected that encrypted files is malicious and had a look file information in common virus databases.
7. Then tried to find it via common virus databases.
   a. https://packetstormsecurity.com
   b. https://www.virustotal.com

8. Founded that encrypted file is a backdoor file which attacker can perform unauthorized activities on victim's computer.

Conclusion

1. Victim user has downloaded this backdoor zip file. (can identify when examine downloaded files).
2. There are lot of large zip files can found inside disk image. By analysing them, they are some OS related updates and drivers. But this kind of files may lead to resource starvation problems of the computer and it will be impacted to the availability of the information. (violation of main information security key point which is **Availability**)

********** End **********