



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

| | |
|--|----|
| Study Number - 06 - Digital Forensic – I | 1 |
| Problem..... | 3 |
| Approach | 30 |
| Conclusion | 31 |

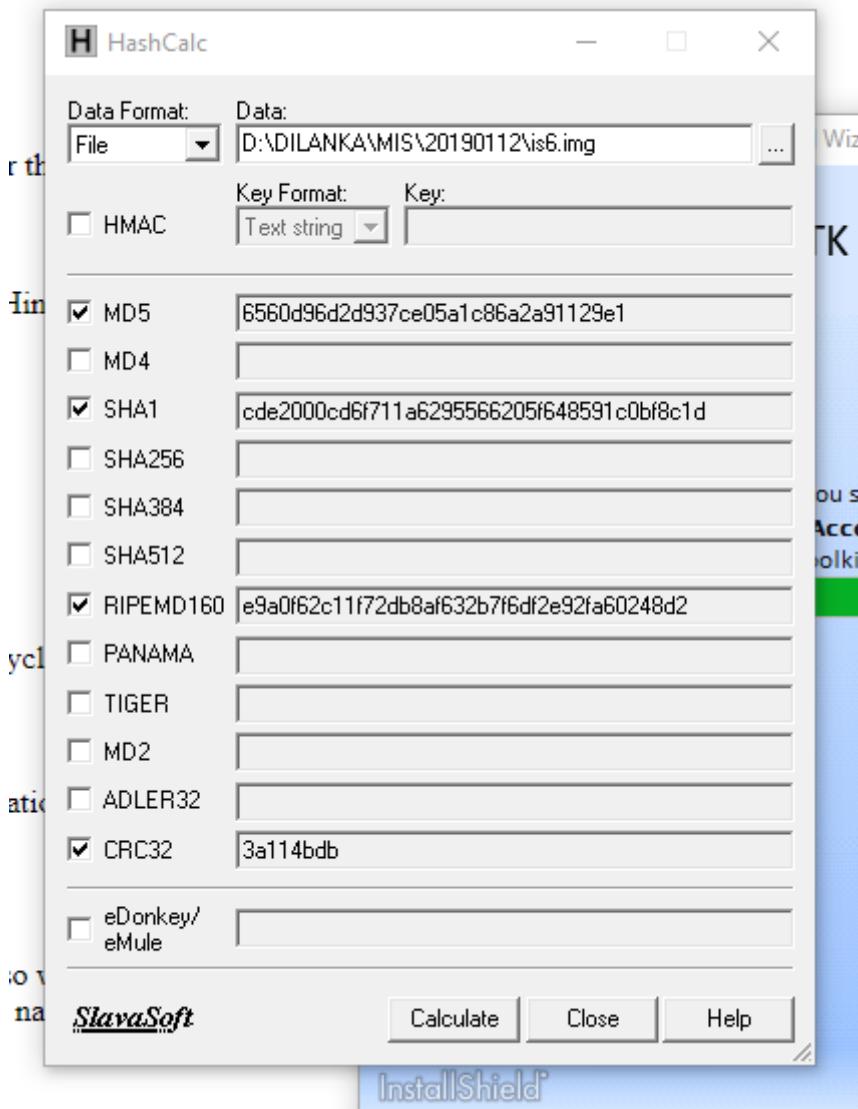
Problem

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)

The screenshot shows the AccessData FTK Imager interface. The Evidence Tree pane on the left displays a hierarchical file structure of a Windows system, including folders like ar-SA, bg-BG, Boot, catroot, catroot2, CodeIntegrity, com, CompatTel, CompatTelRunner.exe, config, Journal, RegBack, systemprofile, AppData, Local, LocalLow, Roaming, TxR, cs-CZ, csrssv.dll, da-DK, de-DE, defaultlocationcpl.dll, devinv.dll, dfshim.dll, Dism, and drivers. The SOFTWARE file is located under the config\Journal\RegBack\systemprofile\appdata folder. The File List pane on the right shows a detailed list of files with columns for Name, Size, Type, and Date Modified. The SOFTWARE file is listed with a size of 26,624 bytes, type Regular File, and date modified 1/10/2019 6:23:... It is highlighted with a red box. Below the File List is a hex dump of the file's contents.

| Name | Size | Type | Date Modified |
|-------------------------|---------------|---------------------|---------------------------|
| SECURITY.LOG1 | 21 | Regular File | 1/10/2019 5:54:... |
| SECURITY.LOG1.FileSl... | 3 | File Slack | |
| SECURITY.LOG2 | 0 | Regular File | 7/14/2009 2:03:... |
| SECURITY(6cced2f9-6... | 64 | Regular File | 8/4/2009 11:42:... |
| SECURITY(6cced2f9-6... | 512 | Regular File | 8/4/2009 11:42:... |
| SECURITY(6cced2f9-6... | 512 | Regular File | 8/4/2009 11:42:... |
| SOFTWARE | 26,624 | Regular File | 1/10/2019 6:23:... |
| SOFTWARE.FileSlack | 144 | File Slack | |
| SOFTWARE.LOG | 1 | Regular File | 7/14/2009 7:56:... |
| SOFTWARE.LOG1 | 256 | Regular File | 1/10/2019 6:23:... |
| SOFTWARE.LOG1.File... | 256 | File Slack | |
| SOFTWARE.LOG2 | 0 | Regular File | 7/14/2009 2:03:... |
| SOFTWARE(6cced2fd-... | 64 | Regular File | 8/4/2009 11:42:... |
| SOFTWARE(6cced2fd-... | 512 | Regular File | 8/4/2009 11:42:... |
| SOFTWARE(6cced2fd-... | 512 | Regular File | 8/4/2009 11:42:... |
| SYSTEM | 9,984 | Regular File | 1/10/2019 6:21:... |
| SYSTEM | | \$130 INDX Entry | |
| SYSTEM.FileSlack | 48 | File Slack | |
| SYSTEM.LOG | 1 | Regular File | 7/14/2009 7:55:... |
| SYSTEM.LOG1 | 256 | Regular File | 1/10/2019 6:21:... |
| SYSTEM.LOG1.FileSlack | 2,560 | File Slack | |
| SYSTEM.LOG2 | 0 | Regular File | 7/14/2009 2:03:... |
| SYSTEM(6cced301-6e... | 64 | Regular File | 8/4/2009 11:42:... |
| SYSTEM(6cced301-6e... | 512 | Regular File | 8/4/2009 11:42:... |
| SYSTEM(6cced301-6e... | 512 | Regular File | 8/4/2009 11:42:... |

Custom Content Sources:

Evidence:File System|Path|File Options

Hex Dump:

| | | |
|----------|--|-------------------------|
| 00000000 | 72 65 67 66 EC 04 00 00-EC 04 00 00 3C 01 2C F3 | regfi...i...<.,ö |
| 00000010 | AC A8 D4 01 01 00 00 00-05 00 00 00 00 00 00 00 | ~"Ö..... |
| 00000020 | 01 00 00 00 20 00 00 00-00 B0 9D 01 01 00 00 00 | |
| 00000030 | 65 00 6D 00 52 00 6F 00-6F 00 74 00 5C 00 53 00 | e-m-R-o-o-t\·S- |
| 00000040 | 79 00 73 00 74 00 65 00-6D 00 33 00 32 00 5C 00 | y-s-t-e-m-3-2\· |
| 00000050 | 42 00 FF | C o n f i d e n t i a l |

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

The screenshot shows the Windows Registry Editor with the path `Computer\HKEY_LOCAL_MACHINE\2016_mis_021_software\Microsoft\Windows NT\CurrentVersion` selected. Several registry entries are highlighted with red boxes:

- `ab|CSDBuildNumber`: REG_SZ, Value: 1
- `ab|CurrentBuild`: REG_SZ, Value: 7600
- `ab|CurrentBuildNumber`: REG_SZ, Value: 7600
- `ab|CurrentType`: REG_SZ, Value: Multiprocessor Free
- `ab|CurrentVersion`: REG_SZ, Value: 6.1
- `ab|DigitalProductId`: REG_BINARY, Value: a4 00 00 03 00 00 30 30 34 32 36 2d 4f 45 4d 2...
- `ab|DigitalProductId4`: REG_BINARY, Value: f8 04 00 00 04 00 00 30 00 30 00 34 00 32 00 36 00...
- `ab|EditionID`: REG_SZ, Value: Ultimate
- `ab|InstallationType`: REG_SZ, Value: Client
- `ab|InstallDate`: REG_DWORD, Value: 0x543fcfc9 (1413283017)
- `ab|PathName`: REG_SZ, Value: C:\Windows
- `ab|ProductId`: REG_SZ, Value: 00426-OEM-8992662-00497
- `ab|ProductName`: REG_SZ, Value: Windows 7 Ultimate
- `ab|RegisteredOrganization`: REG_SZ, Value: mis-win7
- `ab|RegisteredOwner`: REG_SZ, Value: mis-win7
- `ab|SoftwareType`: REG_SZ, Value: System
- `ab|SystemRoot`: REG_SZ, Value: C:\Windows

The screenshot shows the Autopsy 4.9.1 interface. In the center, there is a table titled "Operating System Information" showing details of the operating system. One row for "SOFTWARE" is selected and expanded, showing the following details:

| Source File | S | C | Name | Domain | Version | Processor Architecture | Temporary Files Directory | Data Source | Program Name | Date/Time | Path | Product ID | Owner |
|-------------|---|---|-------------|--------|------------|------------------------|---------------------------|-------------|--------------------|-------------------------|------------|-------------------------|----------|
| SYSTEM | | | MSI-WIN7-IC | | Windows_NT | x86 | %SystemRoot%\TEMP | is6.img | | | | | |
| SYSTM | | | MSI-WIN7-IC | | Windows_NT | x86 | %SystemRoot%\TEMP | is6.img | | | | | |
| OR SOFTWARE | | | | | | | | is6.img | Windows 7 Ultimate | 2014-10-14 10:36:57 IST | C:\Windows | 00426-OEM-8992662-00497 | mis-win7 |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

In the bottom right panel, a detailed view of the "SOFTWARE" entry is shown, with the "Program Name" field highlighted:

| Type | Value |
|------------------|--|
| Program Name | Windows 7 Ultimate |
| Open time | 2014-10-14 10:36:57 |
| Path | C:\Windows |
| Product ID | 00426-OEM-8992662-00497 |
| Owner | mis-win7 |
| Organization | |
| Source File Path | Img_is6.img\vol_0\3\Windows\System32\config\SOFTWARE |
| Artifact ID | 9223372036854770125 |

Operating System User Account

| Type | Value | Source(s) |
|---------------------------|---|----------------|
| Name | ms-WIN7-PC | RecentActivity |
| Domain | Windows_NT | RecentActivity |
| Version | Windows_NT | RecentActivity |
| Processor Architecture | x86 | RecentActivity |
| Temporary Files Directory | %SystemRoot%\TEMP | RecentActivity |
| Source File Path | \img_is6.img\vol_1\Windows\System32\config\RegBack\SYSTEM | RecentActivity |
| Artifact ID | 9223372036854770126 | |

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

Operating System User Account

| Type | Value | Source(s) |
|------------------|--|----------------|
| Username | ms-win7 | RecentActivity |
| Source File Path | \img_is6.img\vol_1\Users\ms-win7\AppData\Local\Microsoft\Windows\History\History.IE5\Index.dat | RecentActivity |
| Artifact ID | 9223372036854775453 | |

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 [/]
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
    msp.exe - %CommonProgramFiles%Microsoft Shared\Ink\msp.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
    pbbrush.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

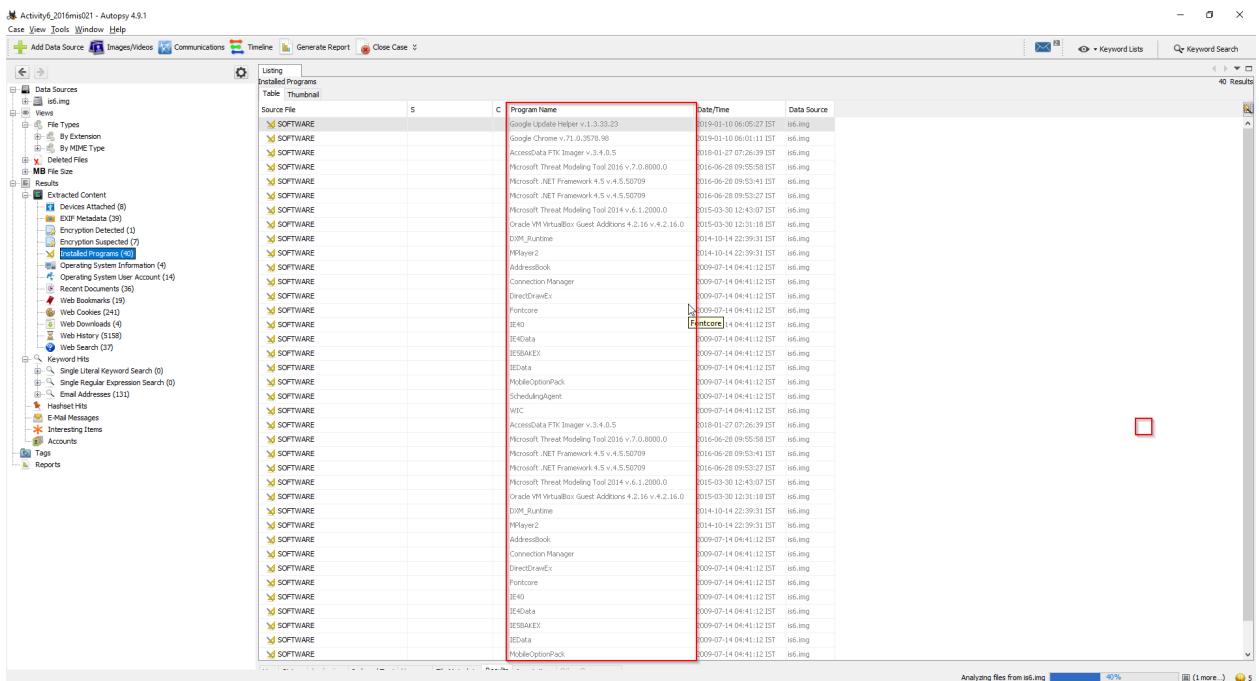
1547100071|REG|||App Paths - chrome.exe - C:\Program Files\Google\Chrome\Application\chrome.exe
1413329920|REG|||App Paths - cmmgr32.exe -
1413329920|REG|||App Paths - IEXPLORE.EXE - C:\Program Files\Internet Explorer\IEXPLORE.EXE
1247557900|REG|||App Paths - dvdmaker.exe - %ProgramFiles%DVD Maker\dvdmaker.exe
1247557900|REG|||App Paths - Journal.exe - %ProgramFiles%Windows Journal\Journal.exe
1247557900|REG|||App Paths - msp.exe - %CommonProgramFiles%Microsoft Shared\Ink\msp.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 - pbbrush.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:

```
LastVisitedPid1MRU
LastWrite: Thu Jan 10 06:13:53 2019
Note: All value names are listed in MRUListEx order.

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

All installed apps



| Source File | S | C | Program Name | Date/Time | Data Source |
|-------------|---|---|--|-------------------------|-------------|
| | | | Google Update Helper v.1.33.33.23 | 2019-01-10 06:05:27 IST | is6.img |
| | | | Google Chrome v.71.0.3678.96 | 2019-01-10 06:01:11 IST | is6.img |
| | | | AccessData FTK Imager v.3.4.0.5 | 2018-01-20 07:26:39 IST | is6.img |
| | | | Microsoft Threat Modeling Tool 2016 v.7.0.8000.0 | 2016-06-28 09:55:58 IST | is6.img |
| | | | Microsoft .NET Framework 4.5 v.4.5.50709 | 2016-06-28 09:53:41 IST | is6.img |
| | | | Microsoft .NET Framework 4.5 v.4.5.50709 | 2016-06-28 09:53:27 IST | is6.img |
| | | | Microsoft Threat Modeling Tool 2014 v.6.1.2000.0 | 2015-03-01 02:43:07 IST | is6.img |
| | | | Oracle VM VirtualBox Guest Additions 4.2.16 v.4.2.16.0 | 2015-03-01 12:31:18 IST | is6.img |
| | | | D3D_RunTime | 2014-10-14 22:39:31 IST | is6.img |
| | | | INFAYER2 | 2014-10-14 22:39:31 IST | is6.img |
| | | | AddressBook | 2009-07-14 04:41:12 IST | is6.img |
| | | | ConnectionManager | 2009-07-14 04:41:12 IST | is6.img |
| | | | DirectDriveEx | 2009-07-14 04:41:12 IST | is6.img |
| | | | Fantcore | 2009-07-14 04:41:12 IST | is6.img |
| | | | IEAO | 2009-07-14 04:41:12 IST | is6.img |
| | | | IE504fa | 2009-07-14 04:41:12 IST | is6.img |
| | | | IESBAAEX | 2009-07-14 04:41:12 IST | is6.img |
| | | | IEDATA | 2009-07-14 04:41:12 IST | is6.img |
| | | | MobileOptionPack | 2009-07-14 04:41:12 IST | is6.img |
| | | | SchedulingAgent | 2009-07-14 04:41:12 IST | is6.img |
| | | | NIC | 2009-07-14 04:41:12 IST | is6.img |
| | | | AccessData FTK Imager v.3.4.0.5 | 2018-01-20 07:26:39 IST | is6.img |
| | | | Microsoft Threat Modeling Tool 2016 v.7.0.8000.0 | 2016-06-28 09:55:58 IST | is6.img |
| | | | Microsoft .NET Framework 4.5 v.4.5.50709 | 2016-06-28 09:53:41 IST | is6.img |
| | | | Microsoft .NET Framework 4.5 v.4.5.50709 | 2016-06-28 09:53:27 IST | is6.img |
| | | | Microsoft Threat Modeling Tool 2014 v.6.1.2000.0 | 2015-03-01 02:43:07 IST | is6.img |
| | | | Oracle VM VirtualBox Guest Additions 4.2.16 v.4.2.16.0 | 2015-03-01 12:31:18 IST | is6.img |
| | | | D3D_RunTime | 2014-10-14 22:39:31 IST | is6.img |
| | | | INFAYER2 | 2014-10-14 22:39:31 IST | is6.img |
| | | | AddressBook | 2009-07-14 04:41:12 IST | is6.img |
| | | | ConnectionManager | 2009-07-14 04:41:12 IST | is6.img |
| | | | DirectDriveEx | 2009-07-14 04:41:12 IST | is6.img |
| | | | Fantcore | 2009-07-14 04:41:12 IST | is6.img |
| | | | IEAO | 2009-07-14 04:41:12 IST | is6.img |
| | | | IE504fa | 2009-07-14 04:41:12 IST | is6.img |
| | | | IESBAAEX | 2009-07-14 04:41:12 IST | is6.img |
| | | | IEDATA | 2009-07-14 04:41:12 IST | is6.img |
| | | | MobileOptionPack | 2009-07-14 04:41:12 IST | is6.img |

2. File Analysis

1. List of most recent used files

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

```

5
6
7 recentdocs_timeline v.20161112
8 (NTUSER.DAT) Gets contents of user's RecentDocs key and place last write times into timeline based on MRUListEx
9
10 RecentDocs
11 Sat Jan 27 09:53:09 2018 : NTUSER.DAT.copy0
12 Sat Jan 27 09:25:42 2018 : NTUSER (2).DAT
13 Sat Jan 27 08:13:13 2018 : TechBank_User_Machine.dd
14 Tue Jun 26 14:02:30 2016 : LoggingModelReport-2014mis001.htm
15 Thu Jan 10 06:16:34 2019 : fixeddw_large_4x.jpg
16 Sat Jan 27 09:45:22 2018 : NTUSER1.log
17 Tue Jun 26 12:38:20 2016 : MIS3102SecureSoftwareSystems-TreatModelingwithMicrosoftSDLThreatModelingTool.pdf
18 Mon Mar 30 13:13:31 2015 : Lab1.tmd
19 Tue Jun 28 14:03:52 2016 : InClassActivity-2014mis001.tm7
20 Thu Jan 10 06:23:41 2019 : pass.txt
21 Sat Jan 27 09:17:59 2018 : RegRipper2.8-master.zip
22 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.
```

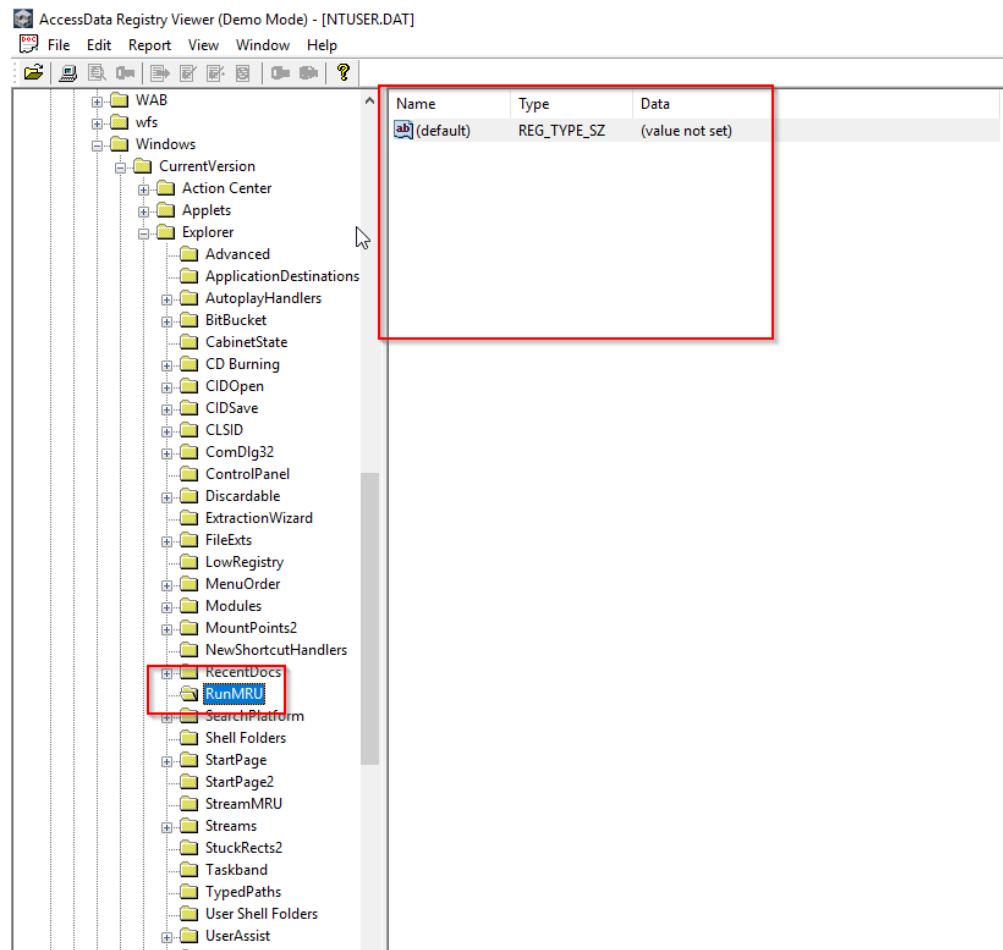
3. Last command executed

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\CurrentVersion\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\CurrentVersion\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-large.jpg.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

The screenshot shows the Autopsy 4.9.1 interface with the case 'Activity_2016mis021'. The left sidebar shows the 'Data Sources' tree, which includes 's6.mng' and 'User (1)'. Under 'User (1)', there are several sub-folders: 'All Users (2)', 'Default (20)', 'Default User (2)', 'mis-win7 (32)', and 'Desktop (8)'. The 'Desktop (8)' folder is highlighted with a red box. The main pane displays a table of files found on the desktop. The table has columns: Name, S, C, Modified Time, Change Time, Access Time, Created Time, Size, Flag(Dr), Flag(Meta), Mode, UserID, GroupID, Meta Addr., Attr. Addr., Type(Dir), and Type. A second red box highlights the file 'AccessData FTK Imager 3.4.0.5.exe' in the list.

| Name | S | C | Modified Time | Change Time | Access Time | Created Time | Size | Flag(Dr) | Flag(Meta) | Mode | UserID | GroupID | Meta Addr. | Attr. Addr. | Type(Dir) | Type | |
|-----------------------------------|---|---|-------------------------|-------------------------|-------------------------|-------------------------|----------|-------------|------------|------|--------|---------|------------|-------------|-----------|------|--|
| [Current folder] | | | 2019-01-01 17:18:17 IST | 2019-01-01 17:18:17 IST | 2019-01-01 17:18:17 IST | 2014-10-14 16:09:02 IST | 56 | Allocated | d-mis-win7 | 0 | 0 | 41001 | 144-6 | r | d | | |
| [Parent folder] | | | 2018-01-27 14:49:52 IST | 2018-01-27 14:49:52 IST | 2018-01-27 14:49:52 IST | 2014-10-14 16:09:02 IST | 256 | Allocated | d-mis-win7 | 0 | 0 | 18049 | 144-5 | d | d | | |
| AccessData FTK Imager 3.4.0.5.exe | | | 2018-01-27 12:55:36 IST | 2018-01-27 12:55:36 IST | 2018-01-27 12:55:36 IST | 2010-01-27 12:56:17 IST | 36650928 | Allocated | m-mis-win7 | 0 | 0 | 1771 | 128-1 | r | r | | |
| desktop.htm | | | 2014-10-14 16:08:34 IST | 2014-10-14 16:08:34 IST | 2014-10-14 16:08:34 IST | 2014-10-14 16:08:34 IST | 282 | Allocated | m-mis-win7 | 0 | 0 | 42009 | 128-1 | r | r | | |
| hello.txt | X | | | | | | 0 | Unallocated | | | 0 | 0 | 0 | 0-0 | r | - | |
| image | X | | | | | | 0 | Unallocated | | | 0 | 0 | 0 | 0-0 | d | - | |
| mis | X | | | | | | 0 | Unallocated | | | 0 | 0 | 0 | 0-0 | d | - | |
| | | | | | | | 0 | Unallocated | | | 0 | 0 | 45747 | 0-0 | d | - | |

Using FTK Imager

The screenshot shows the FTK Imager interface. The Evidence Tree pane on the left displays a hierarchical file system structure. A red box highlights the 'Desktop' folder under the 'mis-win7\AppData\Roaming' path. The File List pane on the right shows a list of files with columns for Name, Size, Type, and Date Modified. A red box highlights the file 'hello.txt' in the list.

| Name | Size | Type | Date Modified |
|-----------------------------------|--------|-------------------|-------------------|
| \$130 | 4 | NTFS Index All... | 1/1/2019 11:48... |
| AccessData FTK Imager 3.4.0.5.exe | 35,792 | Regular File | 1/27/2018 7:25... |
| desktop.ini | 1 | Regular File | 10/14/2014 10... |
| hello.txt | | \$130 INDX Entry | |

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

Using Autopsy

The screenshot shows the FTK Imager interface. The Evidence Tree pane on the left displays a hierarchical file system structure. A red box highlights the 'Desktop' folder under the 'mis-win7\AppData\Roaming' path. The File List pane on the right shows a list of files with columns for Name, Size, Type, and Date Modified. A red box highlights the file 'hello.txt' in the list.

| Name | Size | Type | Date Modified |
|-----------------------------------|--------|-------------------|-------------------|
| \$130 | 4 | NTFS Index All... | 1/1/2019 11:48... |
| AccessData FTK Imager 3.4.0.5.exe | 35,792 | Regular File | 1/27/2018 7:25... |
| desktop.ini | 1 | Regular File | 10/14/2014 10... |
| hello.txt | | \$130 INDX Entry | |

7. List of deleted files

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

The screenshot shows the AccessData FTK Imager interface. The Evidence Tree pane on the left displays a hierarchical view of disk partitions and their contents. Partition 1 (100MB) contains a \$130 file. Partition 2 (10138MB) contains a \$130 file, \$IQGIXD3.txt, \$T9LV6.jpg, \$RQGIXD3.txt, \$RT9LV6.jpg, and desktop.ini. The System Volume Information folder contains \$Secure, Documents and Settings, PerfLogs, Program Files, ProgramData, Recovery, and System Volume Information. The Users folder contains All Users, Default, Default User, and mis-wm7. mis-wm7's AppData folder contains Local, Application Data, Apps, Deployment, Diagnostics, and Google. Google's Chrome folder contains User Data, BrowserMetrics, CertificateRevocation, CertificateTransparency, Crashpad, Default, FileTypePolicies, InterventionPolicyDatabase, MEFReload, OriginTrials, PepperFlash, pnacl, Safe Browsing, ShareCache, SSLErrorAssistant, Subresource Filter, and SvReporter.

The File List pane on the right shows a table of files with columns for Name, Size, Type, and Date Modified. The table includes:

| Name | Size | Type | Date Modified |
|---------------|------|-------------------|------------------------|
| \$130 | 4 | NTFS Index All... | 1/10/2019 6:24:59 AM |
| \$IQGIXD3.txt | 1 | Regular File | 1/10/2019 6:24:59 AM |
| \$T9LV6.jpg | 1 | Regular File | 1/10/2019 6:19:27 AM |
| \$RQGIXD3.txt | 1 | Regular File | 1/10/2019 6:23:45 AM |
| \$RT9LV6.jpg | 66 | Regular File | 1/10/2019 6:11:01 AM |
| desktop.ini | 1 | Regular File | 10/14/2014 10:38:23 AM |

The preview pane at the bottom right displays a photograph of a circular garden with a fountain, surrounded by green lawns and trees, with people walking around.

8. Recover any deleted files

The screenshot shows the Autopsy 4.9.1 interface. The left sidebar displays a file tree for 'i6f.img' containing various volumes and their contents. A red box highlights a file named 'S-1-5-21-2696881825-1152443378-3678611488-100'. A context menu is open over this file, with the 'Extract File(s)' option highlighted by a red box.

| Name | S | C | Modified Time | Change Time | Access Time | Created Time | Size |
|------------------|---|---|-------------------------|-------------------------|-------------------------|-------------------------|-------|
| [current folder] | | | 2019-01-10 11:54:59 IST | 2019-01-10 11:54:59 IST | 2019-01-10 11:54:59 IST | 2014-10-14 16:08:23 IST | 56 |
| \$IQGND3.txt | | | 2019-01-10 11:54:59 IST | 2019-01-10 11:54:59 IST | 2019-01-10 11:54:59 IST | 2019-01-10 11:54:59 IST | 544 |
| \$RQGIXD3.txt | | | 2019-01-10 11:53:45 IST | 2019-01-10 11:54:59 IST | 2019-01-10 11:51:49 IST | 2019-01-10 11:51:49 IST | 96 |
| \$T9.VD6.jpg | | | 2019-01-10 11:49:27 IST | 2019-01-10 11:49:27 IST | 2019-01-10 11:49:27 IST | 2019-01-10 11:49:27 IST | 544 |
| \$RT9 | | | 2019-01-10 11:41:01 IST | 2019-01-10 11:49:27 IST | 2019-01-10 11:40:56 IST | 2019-01-10 11:41:01 IST | 67262 |
| \$RT9 | | | 2019-01-10 11:41:01 IST | 2019-01-10 11:49:27 IST | 2019-01-10 11:40:56 IST | 2019-01-10 11:41:01 IST | 26 |
| [parent] | | | 2014-10-14 16:08:23 IST | 2014-10-14 16:08:23 IST | 2014-10-14 16:08:23 IST | 2009-07-14 08:06:15 IST | 328 |
| [desk] | | | 2014-10-14 16:08:23 IST | 2014-10-14 16:08:23 IST | 2014-10-14 16:08:23 IST | 2014-10-14 16:08:23 IST | 129 |



Via Autopsy

The screenshot shows the Autopsy 4.9.1 interface with the 'File System' tab selected. On the left, the 'Data Sources' tree shows several volumes and their contents. The 'File Types' section is expanded, showing categories like 'Image/Video' which contains 'image' (75 items). In the center, a table lists files with columns for Name, S, C, Location, and Modified Time. A context menu is open over a row of image files, with 'Extract File(s)' highlighted. The bottom navigation bar includes tabs for Hex, Strings, Application, Indexed Text, Message, File Metadata, Results, Annotations, and Other Occurrences.

9. Open image files

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

This screenshot shows the same Autopsy interface as above, but with a specific filter applied. The 'File Types' section on the left has 'image' selected, and the main pane displays a grid of image thumbnails. The thumbnails represent various outdoor scenes, including gardens and landscapes. The bottom navigation bar remains the same.

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

```
40
41 OpenSavePid1MRU\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-large.jpg.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 OpenSavePid1MRU\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-large.jpg.jpg
47
```

1st image:

| Name | Size | Type | Date Modified |
|--|-------|-------------------|--------------------|
| \$130 | 4 | NTFS Index All... | 1/10/2019 6:27:... |
| desktop.ini | 1 | Regular File | 10/14/2014 10:... |
| Ellie Goulding - Love Me Like You Do (8D Au... | 5,624 | Regular File | 1/10/2019 6:27:... |
| fixedw_large_4x.jpg | 326 | Regular File | 1/10/2019 6:13:... |
| fixedw_large_4x.jpg.FileSlack | 3 | File Slack | |
| nb16_p04.zip | 513 | Regular File | 1/10/2019 6:02:... |
| nb16_p04.zip.FileSlack | 4 | File Slack | |

Activity_6_2016mid021 - Autopsy 4.9.1

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Generate Report Close Case

Using Keyword search 1 - pass Keyword search 3 - img-20160614w...

Data Sources

- vol1 (Unallocated: 0-3047)
- vol2 (NTFS / exFAT (0x07): 2048-206847)
- vol3 (NTFS / exFAT (0x07): 206848-20969471)
- vol4 (Unallocated: 20969472-20971519)
- Views
- Results

Table: Thumbnail

Source File

| S | C | Date Created | Latitude | Longitude | Altitude | Device Model | Device Make | DataSource | Size | Path |
|---|---|-------------------------|-----------------|-------------------|----------|--------------------|-------------|------------|---------|--|
| | | 2016-03-14 18:04:15 IST | 15.649465530305 | 75.71536398111111 | 81.0 | HUAWEI NOTE 10 LTE | HUAWEI | .iso | 332964 | /img_16.iso/vol1/vol3/Users/Public/Desktop/Sample_Video... |
| | | 2008-03-14 13:59:26 IST | | | | | | .iso | 67394 | /img_16.iso/vol1/vol3/Users/Public/Pic... |
| | | 2008-03-14 13:59:26 IST | | | | | | .iso | 645941 | /img_16.iso/vol1/vol3/Users/Public/Pic... |
| | | 2008-03-24 16:45:53 IST | | | | | | .iso | 595284 | /img_16.iso/vol1/vol3/Users/Public/Pic... |
| | | 2008-02-11 11:32:44 IST | | | | | | .iso | 775702 | /img_16.iso/vol1/vol3/Users/Public/Pic... |
| | | 2008-02-11 11:32:43 IST | | | | | | .iso | 788031 | /img_16.iso/vol1/vol3/Users/Public/Pic... |
| | | 2008-02-11 11:32:51 IST | | | | | | .iso | 561276 | /img_16.iso/vol1/vol3/Users/Public/Pic... |
| | | 2008-02-18 05:07:31 IST | | | | | | .iso | 777035 | /img_16.iso/vol1/vol3/Users/Public/Pic... |
| | | 2008-02-07 11:15:11 IST | | | | | | .iso | 620688 | /img_16.iso/vol1/vol3/Users/Public/Pic... |
| | | 2007-05-24 02:22:59 IST | | | | DSC-R1 | SONY | .iso | 310616 | /img_16.iso/vol1/vol3/Users/Public/Pic... |
| | | 2009-08-09 08:54:56 IST | | | | | | .iso | 1867101 | /img_16.iso/vol1/vol3/Users/Public/Pic... |
| | | 2015-04-07 14:41:16 IST | | | | | | .iso | 628877 | /img_16.iso/vol1/vol3/Users/Public/Pic... |

Hex Strings Application IndexedText Message File Metadata Results Annotations Other Occurrences

11. List played audio and video files

Using Autopsy

Video files:

Activity_6_2016mid021 - Autopsy 4.9.1

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Generate Report Close Case

Using Keyword search 1 - pass Keyword Search

Data Sources

- vol1 (Unallocated: 0-3047)
- vol2 (NTFS / exFAT (0x07): 2048-206847)
- vol3 (NTFS / exFAT (0x07): 206848-20969471)
- vol4 (Unallocated: 20969472-20971519)
- Views
- Results

Table: Videos

Name

| C | Location | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dr) | Flags(Meta) | Mode |
|---|--|-------------------------|-------------------------|-------------------------|-------------------------|---------|-------------|-------------|-----------|
| | /BabyBoySceneBackground_PAL.wmv | 2000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | ----- | |
| | /fewer_recom_hatte.wmv | 2000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | ----- | |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-01-11 03:18:06 IST | 2014-10-15 05:04:22 IST | 2009-07-14 04:53:30 IST | 2009-07-14 04:53:30 IST | 6190982 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_6mbps_h264.mp4 | 2009-01-11 03:18:07 IST | 2014-10-15 05:04:26 IST | 2009-07-14 04:53:30 IST | 2009-07-14 04:53:30 IST | 3771577 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_6mbps_h264.mp4 | 2009-01-11 03:18:06 IST | 2014-10-15 05:04:22 IST | 2009-07-14 04:53:30 IST | 2009-07-14 04:53:30 IST | 6190982 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_6mbps_h264.mp4 | 2009-01-11 03:18:07 IST | 2014-10-15 05:04:26 IST | 2009-07-14 04:53:30 IST | 2009-07-14 04:53:30 IST | 3771577 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_MPEG2_HD_15mbps.wmv | 2009-01-11 03:18:06 IST | 2014-10-15 05:04:23 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 9376913 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-01-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-01-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-01-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /BabyBoyBackground_gm.wmv | 2009-01-11 03:15:45 IST | 2014-10-15 05:04:30 IST | 2009-07-14 04:33:54 IST | 2009-07-14 04:33:54 IST | 341322 | Allocated | Allocated | rw-rw-rw- |
| | /BabyBoyBackground_PAL.wmv | 2009-01-11 03:15:45 IST | 2014-10-15 05:04:30 IST | 2009-07-14 04:33:54 IST | 2009-07-14 04:33:54 IST | 325322 | Allocated | Allocated | rw-rw-rw- |
| | /BabyBoyBackground_TelefonixSkype.wmv | 2009-01-11 03:15:46 IST | 2014-10-15 05:04:37 IST | 2009-07-14 04:33:54 IST | 2009-07-14 04:33:54 IST | 141214 | Allocated | Allocated | rw-rw-rw- |
| | /BabyBoyHandTelefonixSkype.wmv | 2009-01-11 03:15:46 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:33:54 IST | 2009-07-14 04:33:54 IST | 157214 | Allocated | Allocated | rw-rw-rw- |
| | /BabyBoyHandTelefonixBackground_PAL.wmv | 2009-01-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:33:54 IST | 2009-07-14 04:33:54 IST | 117214 | Allocated | Allocated | rw-rw-rw- |
| | /BabyBoyHandTelefonixBackground.wmv | 2009-01-11 03:15:46 IST | 2014-10-15 05:04:27 IST | 2009-07-14 04:33:54 IST | 2009-07-14 04:33:54 IST | 141214 | Allocated | Allocated | rw-rw-rw- |
| | /BabyBoyNotesBackground.wmv | 2009-01-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:33:54 IST | 2009-07-14 04:33:54 IST | 157292 | Allocated | Allocated | rw-rw-rw- |
| | /BabyBoyNotesBackground_PAL.wmv | 2009-01-11 03:15:46 IST | 2014-10-15 05:04:37 IST | 2009-07-14 04:33:54 IST | 2009-07-14 04:33:54 IST | 149092 | Allocated | Allocated | rw-rw-rw- |
| | /BabyBoyNotesBackground_TelefonixSkype.wmv | 2009-01-11 03:15:46 IST | 2014-10-15 05:04:37 IST | 2009-07-14 04:33:54 IST | 2009-07-14 04:33:54 IST | 125292 | Allocated | Allocated | rw-rw-rw- |
| | /bear_formatted_mattie2.wmv | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:37 IST | 2009-07-14 02:33:58 IST | 2009-07-14 02:33:58 IST | 181122 | Allocated | Allocated | rw-rw-rw- |
| | /bear_formatted_MATTIE2_PAL.wmv | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:37 IST | 2009-07-14 02:33:58 IST | 2009-07-14 02:33:58 IST | 181122 | Allocated | Allocated | rw-rw-rw- |

Hex Strings Application IndexedText Message File Metadata Results Annotations Other Occurrences

Activity_6_2016mid021 - Autopsy 4.9.1

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Generate Report Close Case

Using Keyword search 1 - pass Keyword Search

Data Sources

- vol1 (Unallocated: 0-3047)
- vol2 (NTFS / exFAT (0x07): 2048-206847)
- vol3 (NTFS / exFAT (0x07): 206848-20969471)
- vol4 (Unallocated: 20969472-20971519)
- Views
- Results

Table: Videos

Name

| C | Location | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dr) | Flags(Meta) | Mode |
|---|--------------------------------|-------------------------|-------------------------|-------------------------|-------------------------|---------|-------------|-------------|-----------|
| | /Wildlife.wmv | 2009-07-14 10:22:25 IST | 2009-07-14 10:22:31 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 2624606 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:22 IST | 2009-07-14 04:53:30 IST | 2009-07-14 04:53:30 IST | 6190982 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_6mbps_h264.mp4 | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:26 IST | 2009-07-14 04:53:30 IST | 2009-07-14 04:53:30 IST | 3771577 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_6mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:22 IST | 2009-07-14 04:53:30 IST | 2009-07-14 04:53:30 IST | 6190982 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_h264.mp4 | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:20 IST | 2009-07-14 04:53:30 IST | 2009-07-14 04:53:30 IST | 3771577 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:23 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:23 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:23 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:23 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:23 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:23 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:23 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:23 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_1080_Sec_10mbps_h264.mp4 | 2009-06-11 03:18:06 IST | 2014-10-15 05:04:23 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated | Allocated | rw-rw-rw- |
| | /Clip_480_Sec_6mbps_new.mpq | 2009-06-11 03:18:07 IST | 2014-10-15 05:04:25 IST | 2009-07-14 04:53:29 IST | 2009-07-14 04:53:29 IST | 3752290 | Allocated</ | | |

Audio files:

The screenshots show two separate forensic analysis sessions. Both are titled 'Activity_2016mid021 - Autopsy 4.9.1'. The left screenshot displays a list of audio files under the 'Data Sources' section, specifically within the 'v01 (Unallocated: 0-2047)' volume. The right screenshot shows a similar list from a different session or volume. Both tables include columns for file metadata such as name, location, modification time, and access time. Red boxes highlight specific files in both tables, likely indicating they are of interest for further investigation.

3. Applications Analysis

1. Last time the password was changed

```

-----[redacted]-----
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
-----[redacted]-----

```

```

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

```

102 -----
103 usbstor2 v.20080825
104 MIS-WIN7-PC,Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP,08606E6B689680B3361DAF&0,1445714690,Kingston DataTraveler 3.0 USB Device
105 Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP,Sat Oct 24 19:24:50 2015,08606E6B689680B3361DAF&0,Sat Oct 24 19:24:50 2015,Kingston DataTraveler 3.0 USB Device,
106 (System) Get WpdBusEnumRoot subkey info
107
108 wpdbusenum v.20141111
109 (System) Get WpdBusEnumRoot subkey info
110
111 DISK&VEN_KINGSTON&PROD_DATATRAVELER_3.0&REV_PMAP (08606E6B689680B3361DAF&0)
112 LastWrite: Sat Oct 24 19:24:50 2015
113 DeviceDesc: DataTraveler 3.0
114 Friendly: Shan13
115 Mfg: Kingston
116 Device Parameters LastWrite: [Sat Oct 24 19:24:50 2015]
117 LogConf LastWrite : [Sat Oct 24 19:24:50 2015]
118 Properties LastWrite : [Sat Oct 24 19:24:50 2015]
119 InstallDate : Mon Mar 30 13:13:00 2015 UTC
120 FirstInstallDate: Mon Mar 30 13:13:00 2015 UTC
121
122 ControlSet001\Control\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}
123 DISK&VEN_KINGSTON&PROD_DATATRAVELER_3.0&REV_PMAP\08606E6B689680B3361DAF&0
124 LastWrite: Mon Mar 30 13:13:00 2015
125
126 -----
127 xpedition v.20120722
128 (System) Queries System hive for XP Edition info
129
130 xpedition v.20120722
131
132 ALERT: winsvc: when found in path: WinInet -> %SystemRoot%\system32\when\WMIsvc.dll
133 ALERT: winsvc: Relative path detected: WinhttpAutoProxySvc -> winhttp.dll
134 1247546229[ALERT]|||svc_tin: Poss. ADS in path: %SystemRoot%\system32\dllhost.exe /ProcessId:(02D4B3F1-FD88-11D1-960D-00805FC79235)
135

```

| Name | Type | Data |
|--------------|--------------|--|
| DeviceDesc | REG_SZ | @disk.inf,%disk_devdesc%Disk drive |
| Capabilities | REG_DWORD | 0x00000010 (16) |
| HardwareID | REG_MULTI_SZ | USBSTOR\DiskKingstonDataTraveler_3.0\PMAP USBSTOR\DiskKingstonDataTraveler_3.0 USBSTOR\KingstonDataTraveler_3.0 KingstonDataTraveler_3.0 USBSTOR\GenDisk GenDisk |
| Compatible.. | REG_MULTI_SZ | USBSTOR\DiskKingstonDataTraveler_3.0\PMAP USBSTOR\RAW |
| ConfigFlags | REG_DWORD | 0x00000000 (0) |
| ClassGUID | REG_SZ | {4d3fe697-e323-11ce-bfc1-08002be10318} |
| Driver | REG_SZ | {4d3fe697-e323-11ce-bfc1-08002be10318}0001 |
| Class | REG_SZ | DiskDrive |
| Mfg | REG_SZ | @disk.inf,%Manufacturer%\\(Standard disk drives) |
| Service | REG_SZ | disk |
| FriendlyName | REG_SZ | Kingston DataTraveler 3.0 USB Device |

From Autopsy:

| Source File | S | C | Date/Time | Device Make | Device ID | Device Model | Data Source |
|-------------|---|---|-------------------------|---------------------|--------------------------|---------------|-------------|
| SYSTEM | | | 2019-01-10 11:12:53 IST | | 4824d6b6580 | ROOT_HUB | is6.img |
| SYSTEM | | | 2016-06-20 10:25:41 IST | | 496a997e490 | ROOT_HUB02 | is6.img |
| SYSTEM | | | 2015-10-25 00:54:50 IST | Kingston Technology | 086065686968D800B3361DAF | Product: 1666 | is6.img |
| SYSTEM | | | 2019-01-10 11:12:53 IST | VirtualBox | 5818f54cb76081 | USB Tablet | is6.img |
| SYSTEM | | | 2018-01-27 13:40:41 IST | | 4824d6b6580 | ROOT_HUB | is6.img |
| SYSTEM | | | 2016-06-28 18:25:41 IST | | 496a997e490 | ROOT_HUB02 | is6.img |
| SYSTEM | | | 2015-10-25 00:54:50 IST | Kingston Technology | 086065686968D800B3361DAF | Product: 1666 | is6.img |
| SYSTEM | | | 2018-01-27 13:40:42 IST | VirtualBox | 5818f54cb76081 | USB Tablet | is6.img |

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

4. Browsing Information

- Which browser does the user use?

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

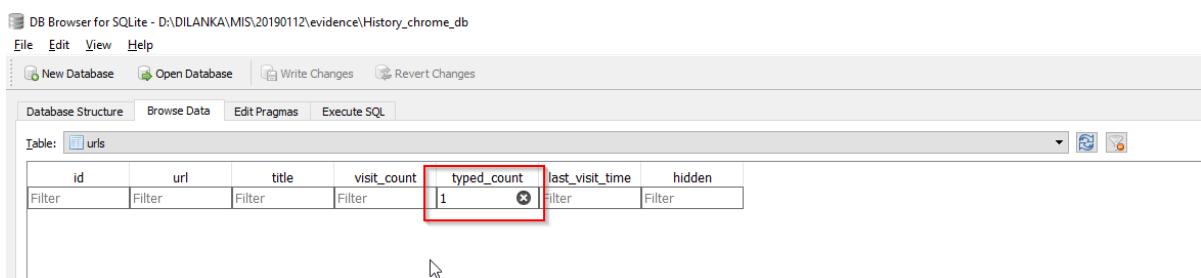
| Source File | S | C | Domain | Text | Program Name | Date Accessed | Data Source |
|-------------|---|---|--------------------|--|-------------------|----------------------------|-------------|
| History | | | www.google.com | yarunay | Chrome | 2019-01-10 11:42:17 IST | is6.img |
| History | | | www.google.com | beach dsl | Chrome | 2019-01-10 11:42:45 IST | is6.img |
| History | | | www.google.com | beach dsl | Chrome | 2019-01-10 11:42:45 IST | is6.img |
| History | | | www.google.com | beach dsl | Chrome | 2019-01-10 11:43:03 IST | is6.img |
| History | | | www.google.com | beach dsl | Chrome | 2019-01-10 11:43:45 IST | is6.img |
| History | | | www.google.com | asd to binary | Chrome | 2019-01-10 11:52:10 IST | is6.img |
| History | | | www.google.com | base64 encode | Chrome | 2019-01-10 11:52:49 IST | is6.img |
| History | | | www.google.com | binary to text | Chrome | 2019-01-10 11:54:11 IST | is6.img |
| History | | | www.google.com | love me like you do.mp3 | Chrome | 2019-01-10 11:55:31 IST | is6.img |
| History | | | www.google.com | youtube | Chrome | 2019-01-10 11:56:10 IST | is6.img |
| History | | | www.google.com | youtube to mp3 | Chrome | 2019-01-10 11:56:30 IST | is6.img |
| index.dat | | | www.bing.com | www.packetstorm.com | Internet Explorer | 2019-01-10 05:55:29 IST | is6.img |
| index.dat | | | www.bing.com | www.google.lk | Internet Explorer | 2019-01-10 05:54:52 IST | is6.img |
| index.dat | | | www.bing.com | .net 4.5 download | Internet Explorer | 2016-06-28 09:49:45 IST | is6.img |
| index.dat | | | www.bing.com | microsoft threat modeling tool 2016 download | Internet Explorer | 2016-06-28 09:49:47:00 IST | is6.img |
| index.dat | | | www.bing.com | microsoft threat modeling tool | Internet Explorer | 2016-06-28 09:46:51 IST | is6.img |
| index.dat | | | www.google.lk | pgv | Internet Explorer | 2016-06-28 12:33:50 IST | is6.img |
| index.dat | | | www.google.lk | pgv | Internet Explorer | 2016-06-28 12:33:53 IST | is6.img |
| index.dat | | | clients1.google.lk | pg | Internet Explorer | 2016-06-28 12:33:50 IST | is6.img |

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

DB Browser for SQLite - D:\DILANKA\MIS\20190112\ evidence\History_chrome_db

| urls | | | | | | |
|------|----|--|--------------------------------|-------------|-------------|-------------------|
| | 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 |
| 2 | 48 | https://testbane-sockgles.com/a9183a94-8648-4ba3-9d79-c7e0fe1e21?utm_content=230532&utm_term=54656... | Instructions of How I Earn... | 1 | 0 | 13191575219245927 |
| 3 | 47 | https://lnkfast.com/afu.php?zoneid=1365143&var=546563 | Instructions of How I Earn... | 2 | 0 | 13191575218116101 |
| 4 | 46 | https://lnkfast.com/?p=d10decf3e2f1615e38a6ca0cc80d8pbk3=b2b3b65136728dcf079ccab268adb556644750... | Instructions of How I Earn... | 1 | 0 | 13191575218094007 |
| 5 | 45 | https://www.onlinevideoconverter.com/success | Your conversion is comple... | 1 | 0 | 13191575214852570 |
| 6 | 44 | https://www.onlinevideoconverter.com/mp3-converter | YouTube to MP3 Converte... | 1 | 0 | 13191575193792175 |
| 7 | 43 | https://www.google.com/search?q=youtube+to+mp3&oq=youtube+to+mp3&aqs=chrome..69i5j0l5.2341j0j4&sour... | youtube to mp3 - Google ... | 1 | 0 | 13191575190810982 |
| 8 | 42 | https://www.youtube.com/watch?v=eLWpThzH2PM | Elle Goulding - Love Me Li... | 1 | 0 | 13191575182601916 |
| 9 | 41 | https://www.youtube.com/results?search_query=love+me+like+you+do+8d | love me like you do 8d - Y... | 1 | 0 | 1319157517988378 |
| 10 | 40 | https://www.youtube.com/ | YouTube | 3 | 0 | 13191575179881665 |
| 11 | 39 | https://www.google.com/search?q=youtube&oq=youtube&aqs=chrome..69i5j0l5.2533j0j4&sourceid=chrome&ie=... | youtube - Google Search | 1 | 0 | 13191575170115989 |
| 12 | 38 | https://freesound.io/download-free-mp3/love-me-like-you-do-elle-goulding-50-shades-of-grey | Freesound - Download lo... | 1 | 0 | 13191575147669265 |
| 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 |
| 14 | 36 | https://www.rapidtables.com/convert/number/binary-to-ascii.html | Binary to Text converter ... | 1 | 0 | 13191575053540966 |
| 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 |
| 16 | 34 | https://www.base64decode.org/ | Base64 Decode and Encod... | 2 | 0 | 13191575037099390 |
| 17 | 33 | https://www.base64encode.org/ | Base64 Decode and Encod... | 2 | 0 | 13191574980109539 |
| 18 | 32 | https://www.google.com/search?q=base64+encode&oq=base64&aqs=chrome.2.69i5j0l5.4036j0j7&sourceid=chrom... | base64 encode - Google S... | 1 | 0 | 13191574969012142 |
| 19 | 31 | https://www.rapidtables.com/convert/number/ascii-to-binary.html | Text to Binary converter ... | 1 | 0 | 13191574932881547 |
| 20 | 30 | https://www.google.com/search?q=ascii+to+binary&oq=ascii+to+binary&aqs=chrome..69i5j0l5.3035j0j7&sourceid... | ascii to binary - Google Se... | 1 | 0 | 13191574930694125 |
| 21 | 29 | https://www.trover.com/d/1Fsg0-ashwem-beach-mandrem-india | Ashwem Beach, Mandrem... | 2 | 0 | 13191574431246048 |
| 22 | 28 | https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwjbl_oDZcLfAhULwIBKHQYSMDQjox6BAgBEAI... | Ashwem Beach, Mandrem... | 1 | 0 | 13191574430138766 |
| 23 | 27 | https://www.google.com/search?tbm=isch&sas=1&ei=h-E2XNHBIVtQSkSYLDw&q=beach+dslr&q=beach+dslr&gs... | beach dslr - Google Search | 1 | 0 | 1319157425956633 |
| 24 | 26 | https://www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjgl5bFx-LfAhWJL48KHTxP... | Ko Samui, Germany - Febr... | 1 | 0 | 13191574406262079 |
| 25 | 25 | https://www.shutterstock.com/video/clip-10458722-k-o-samui-germany-%E2%80%93-february-28-2015 | Ko Samui, Germany - Febr... | 2 | 0 | 13191574406262079 |
| 26 | 24 | https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwjgl5bFx-LfAhWJL48KHTxPCjQQjox6BAgBEAI... | Ko Samui, Germany - Febr... | 1 | 0 | 13191574386764519 |
| 27 | 23 | https://www.google.com/search?tbm=isch&sas=1&ei=h-E2XNHBIVtQSkSYLDw&q=beach+dslr&q=beach+dslr&gs... | beach dslr - Google Search | 1 | 0 | 13191574383304032 |
| 28 | 22 | https://www.shutterstock.com/image-photo/person-taking-photo-tropical-beach-dslr-723026977 | Person Taking Photo Tropi... | 2 | 0 | 13191574367363610 |
| 29 | 21 | https://www.google.com/url?sa=i&source=images&cd=&ved=0ahUKEwi_3Lu1x-LfAhUF148KHbHAnoQMwhnKB8wH... | Person Taking Photo Tropi... | 2 | 0 | 13191574367363610 |

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

Ordered by descending order by Id or visit time:

DB Browser for SQLite - D:\DILANKA\MIS\20190112\ evidence\History_chrome_db

| urls | | | | | | |
|------|----|--|-------------------------------|-------------|-------------|-------------------|
| | 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 |
| 2 | 48 | https://testbane-sockgles.com/a9183a94-8648-4ba3-9d79-c7e0fe1e21?utm_content=230532&utm_term=54656... | Instructions of How I Earn... | 1 | 0 | 13191575219245927 |
| 3 | 47 | https://lnkfast.com/afu.php?zoneid=1365143&var=546563 | Instructions of How I Earn... | 2 | 0 | 13191575218116101 |
| 4 | 46 | https://lnkfast.com/?p=d10decf3e2f1615e38a6ca0cc80d8pbk3=b2b3b65136728dcf079ccab268adb556644750... | Instructions of How I Earn... | 1 | 0 | 13191575218094007 |
| 5 | 45 | https://www.onlinevideoconverter.com/success | Your conversion is comple... | 1 | 0 | 13191575214852570 |
| 6 | 44 | https://www.onlinevideoconverter.com/mp3-converter | YouTube to MP3 Converte... | 1 | 0 | 13191575193792175 |
| 7 | 43 | https://www.google.com/search?q=youtube+to+mp3&oq=youtube+to+mp3&aqs=chrome..69i5j0l5.2341j0j4&sour... | youtube to mp3 - Google ... | 1 | 0 | 13191575190810982 |

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=aHR0cHM6Ly9sZXN0c2JhbmtUc29ja2dsZXMuY29tL2RiZTMwNW14LTQ0NzItNDQxNi1hZTA3LTc1YmZmNDEwZmU0Nz91dG1fdGvbtT17em9uZWlkfSZ1dG1fc291cmNIPWJhY2smdXRtX21lZGl1bT1wJnJlZj1wX0JBQ0tfYmFja19CQUNLX2Rlc2s=&cep=4KoI6M6neWmE1gNaCyK0VcB1bvJBM_u5eBkgd4R5QSRLXoD_gKFFx6DTrYIda_6rihb-FdCzDNpyCYR4dMkOEJ10iwIh4i2P-K1mp2OZeB09TZOmuvmwT3ekoR-n-Q8zJFnighT_FKJZFUDMSarDusAQm3uM_NMiqnMveeF8429QaGdstQdiEHBRKOIN2bzGFcEBQd11WP_eJq3WvRPgOnTXnMS5BWZ8C-kKfHkfNdmmxg9Bo9LGWrpi4j1Nb1cJXh2Nn7MZ0BmYD6NhJpWxV6yTqyWIFufiafxat3Hn4IEyeN6zM0buZDdeAbeDmGMmXkq8Ecxy9lPgDdGTLrXeW1H1AvJoS_NJvuiB7LIVZc&utm_content=230532&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.

| Type | Value | Source(s) |
|------------------|---|-------------------|
| URL | linkedin.com/ | ReconnectActivity |
| Date Accessed | 2018-01-27 07:13:46 | ReconnectActivity |
| Referrer URL | | ReconnectActivity |
| Program Name | Internet Explorer | ReconnectActivity |
| Domain | linkedin.com | ReconnectActivity |
| Username | CodeRed-007 | ReconnectActivity |
| Source File Path | \img\js\img_id_1d73Users\mis-win7\AppData\Roaming\Microsoft\Windows\Cookies\index.dat | |
| Artifact ID | 922337239854774654 | |

7. List downloaded files

| id | guid | current_path | target_path | start_time | received_bytes | total_bytes | state | danger_type | interrupt_reason |
|----|-----------------|-----------------|---|----------------|----------------|-------------|-------|-------------|------------------|
| 1 | 97b89711-47... | C:\Users\mis... | C:\Users\mis-win7\Downloads\rb16_p04.zip | 13191573717... | 525126 | 525126 | 1 | 4 | 0 |
| 2 | 315e76a-f47... | C:\Users\mis... | C:\Users\mis-win7\Downloads\mp-20160614-wa0013-large.jpg.jpg | 13191574257... | 67262 | 67262 | 1 | 0 | 0 |
| 3 | 662a306d-7fe... | C:\Users\mis... | C:\Users\mis-win7\Downloads\fixeddw_large_4x.jpg | 13191574435... | 332964 | 332964 | 1 | 0 | 0 |
| 4 | e4e568ec-0f1... | C:\Users\mis... | C:\Users\mis-win7\Downloads\Ellie Goulding - Love Me Like You Do (8D Audio).mp3 | 13191575219... | 5758570 | 5758570 | 1 | 0 | 0 |

5. Malicious activities

1. List malicious applications.
1. Their types?

Zip bombs

The screenshot shows the Autopsy 4.9.1 interface with a search results table titled 'Zip bombs'. The table has columns for Source File, S, C, Comment, and Data Sum. One entry is highlighted: 'rb16_p04.zip' with 'Full Encryption (Archive File)' in the Comment column and 'is6.img' in the Data Sum column. A red box highlights the 'Encryption Detected' section in the sidebar under 'Results'.

| Source File | S | C | Comment | Data Sum |
|--------------|---|---|--------------------------------|----------|
| rb16_p04.zip | | | Full Encryption (Archive File) | is6.img |

Backdoors

The screenshot shows the Autopsy 4.9.1 interface with a search results table titled 'Backdoors'. A red box highlights the 'Encryption Detected' section in the sidebar under 'Results'.

| Source File | S | C | Comment | Data Sum |
|--------------|---|---|--------------------------------|----------|
| rb16_p04.zip | | | Full Encryption (Archive File) | is6.img |

One engine detected this file

SHA-256: 038a01fd27ee8603040e79ae6d00da67c535f7f1da6333069b65cc5271f73dd
 File name: nb16_p04.zip
 File size: 512.82 KB
 Last analysis: 2018-07-30 02:06:25 UTC

| | Detection | Details | Relations | Community |
|-----------|--|-----------|--|-----------|
| Fortinet | ⚠ W32/Netb_160_4.160!tr | Ad-Aware | Clean | |
| AegisLab | Clean | AhnLab-V3 | Clean | |
| Alibaba | Clean | ALYac | Clean | |
| Antiv-AVI | Clean | ArcaBit | Clean | |

[nb16_p04.zip](https://packetstormsecurity.com/files/10320/nb16_p04.zip)
 Size: 515.3 KB
 NetBus 1.0 (Patch 4) - Patched to avoid detection by Spider, Drweb, Avp, and Norton Antivirus.
 Archive password is set to p4ssw0rd. Use at your own risk.

Posted Feb 25, 2000

tags | trojan
 MD5 | e53dbf3b93c151fd4592718e77eaac4c

[Download](#) | [Favorite](#) | [Comments \(0\)](#)

[Related Files](#)

[Share This](#)

[Like 0](#) [Tweet](#) [LinkedIn](#) [Reddit](#) [Digg](#) [StumbleUpon](#)

[Comments](#) [RSS](#)

No comments yet, be the first!

Login or Register to post a comment

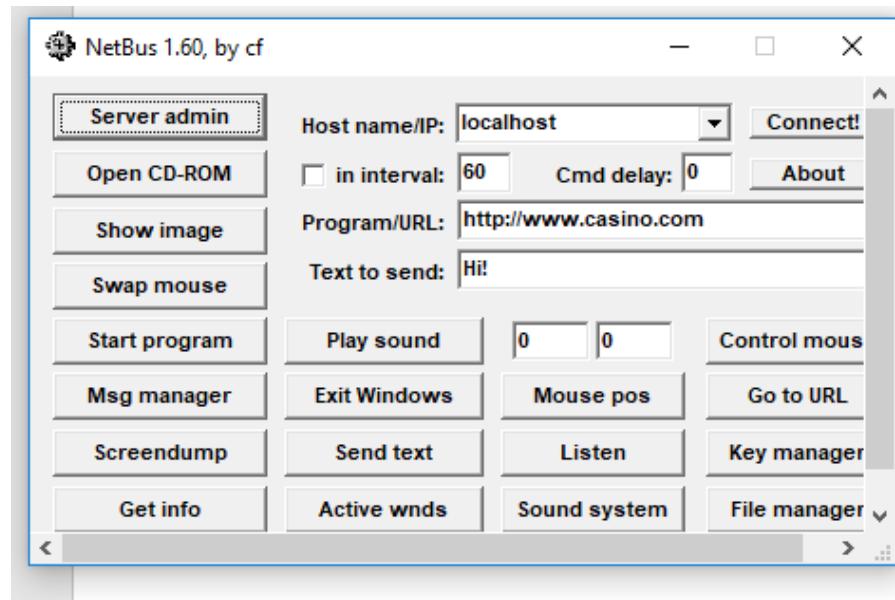
2. How they infected machine?

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

| Activity6_2016mid21 - Autopsy 4.9.1 | | | | | | |
|---|----------|----------|---|---------|-----------|-------------------------|
| Case View Tools Window Help | | | | | | |
| Keywords | | | | | | |
| Keywords | | | | | | |
| Source File | S | C | Description | Comment | File Path | Modified Time |
| x86_microsoft-windows-client-wired-network-drivers-package->31bf385 | Zip Bomb | Detected | microsoft-windows-client-wired-network..._Compression ratio is 399... [img] | [img] | [img] | 2010-11-20 09:07:28 IST |
| x86_microsoft-windows-client-wired-network-drivers-package->31bf385 | Zip Bomb | Detected | microsoft-windows-client-wired-network..._Compression ratio is 241... [img] | [img] | [img] | 2010-11-20 09:08:22 IST |
| x86_microsoft-windows-common-drivers-package->31bf385&id=345 | Zip Bomb | Detected | microsoft-windows-common-drivers-pac..._Compression ratio is 98... [img] | [img] | [img] | 2010-11-20 15:05:16 IST |
| x86_microsoft-windows-common-drivers-package->31bf385&id=35 | Zip Bomb | Detected | microsoft-windows-common-drivers-pac..._Compression ratio is 31... [img] | [img] | [img] | 2010-11-20 10:06:44 IST |
| x86_microsoft-windows-shell-premiumgames-package->31bf385a | Zip Bomb | Detected | microsoft-windows-shell-premiumg..._Compression ratio is 11... [img] | [img] | [img] | 2010-11-20 15:45:54 IST |
| x86_microsoft-windows-snapclip-package->31bf385&id=388-4 | Zip Bomb | Detected | microsoft-windows-snapcli..._Compression ratio is 212... [img] | [img] | [img] | 2010-11-20 14:46:20 IST |
| msf_microsoft_windows_n_client_management_31bf385&id=345 | Zip Bomb | Detected | msf_microsoft_windows_n_c..._Compression ratio is 64... [img] | [img] | [img] | 2010-11-20 09:15:15 IST |
| x86_microsoft-windows_b_directory_resources_31bf385&id=4e3 | Zip Bomb | Detected | x86_microsoft-windows_b_d..._Compression ratio is 63... [img] | [img] | [img] | 2010-11-20 09:05:40 IST |
| x86_microsoft-windows_d_mc-schema_resources_31bf385&id=364 | Zip Bomb | Detected | x86_microsoft-windows_d_mc..._Compression ratio is 15... [img] | [img] | [img] | 2010-11-20 09:09:26 IST |
| x86_microsoft-windows_g_lcid_adm_31bf385&id=3e3 | Zip Bomb | Detected | x86_microsoft-windows_g_lc..._Compression ratio is 54... [img] | [img] | [img] | 2010-11-20 09:04:58 IST |
| x86_microsoft-windows_g_oemnt-languagepack_31bf385&id=364 | Zip Bomb | Detected | x86_microsoft-windows_g_oem..._Compression ratio is 62... [img] | [img] | [img] | 2010-11-20 09:08:26 IST |
| x86_microsoft-windows_h_oemnt-languagepack_31bf385&id=364 | Zip Bomb | Detected | x86_microsoft-windows_h_oem..._Compression ratio is 36... [img] | [img] | [img] | 2010-11-20 09:12:44 IST |
| x86_microsoft-windows_i_optional_resources_31bf385&id=3e35 | Zip Bomb | Detected | x86_microsoft-windows_i_o..._Compression ratio is 794... [img] | [img] | [img] | 2010-11-20 07:28:24 IST |
| x86_microsoft-windows_iestab_31bf385&id=3e35_0_76011_171 | Zip Bomb | Detected | x86_microsoft-windows_iestab..._Compression ratio is 757... [img] | [img] | [img] | 2010-11-20 09:10:20 IST |
| x86_microsoft-windows_i_premium_resources_31bf385&id=364 | Zip Bomb | Detected | x86_microsoft-windows_i_p..._Compression ratio is 965... [img] | [img] | [img] | 2010-11-20 09:16:16 IST |
| x86_microsoft-windows_i_teprisen_resources_31bf385&id=3e35 | Zip Bomb | Detected | x86_microsoft-windows_i_te..._Compression ratio is 14... [img] | [img] | [img] | 2010-11-20 09:25:32 IST |
| x86_microsoft-windows_m_ac-addd-security_31bf385&id=364 | Zip Bomb | Detected | x86_microsoft-windows_m_ac..._Compression ratio is 88... [img] | [img] | [img] | 2010-11-20 09:05:12 IST |
| x86_microsoft-windows_m_r-heimer.resources_31bf385&id=364 | Zip Bomb | Detected | x86_microsoft-windows_m_r..._Compression ratio is 13... [img] | [img] | [img] | 2010-11-20 09:19:10 IST |
| x86_microsoft-windows-moblyn_31bf385&id=3e35_0_1_7601_1 | Zip Bomb | Detected | x86_microsoft-windows-mob..._Compression ratio is 68... [img] | [img] | [img] | 2010-11-20 09:05:14 IST |
| x86_microsoft-windows_n_oemnt-languagepack_31bf385&id=364 | Zip Bomb | Detected | x86_microsoft-windows_n_oem..._Compression ratio is 191... [img] | [img] | [img] | 2010-11-20 13:26:54 IST |

Other findings

```
1 -----
2 ahaha v.20131009
3 (Software,NTUSER.DAT) Detect possible presence of ahaha malware
4 -----
```

```
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 : %UserProfiles%\AppData\Local\Microsoft\Outlook\*.ost  
FVE : $AllVolumes\System Volume Information\FVE.(Seef82dfa-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 File 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\/*  
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\MountPointManager\RemoteDatabase  
VSS Default Provider : \System\Volume\Information\{3900876B-C176-4e48-B7AE-0404E6CC752\} /*  
VSS Service DB : \System\Volume\Information\{7c00876f-1efc-6865-5d00-0017fd1bc1DB\}  
FVE_Log : \System\Volume\Information\FVE.(Seef82dfa-1239-4a30-83e6-3b3e9b8fed08)  
FVE_Win : \System\Volume\Information\FVE.(Seef82dfa-1239-4a30-83e6-3b3e9b8fed08)  
VSS_Service Alternate DB : \System\Volume\Information\{7cc467ef-6865-4831-853f-2a4017fd1bc1\}ALT  
FVE_Control : \System\Volume\Information\FVE.(e40ad34d-dae9-4b7c-79bd-b16218c10f72).  
MS Distributed Transaction Coordinator : C:\Windows\system32\MSDTC\MSDTC.LOG C:\Windows\system32\MSDTC\trace\dsgtrace.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 *****