

University of Piraeus

**Department of Digital Systems
Postgraduate Programme “ Security of Digital Systems”**



Master Thesis

Forensic Methodology for Windows 7 and Windows 8

Marios Soulas

February 2014

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Supervisor

Sokratis Katsikas, Professor
University of Piraeus

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Examination Board

Sokratis Katsikas, Professor
University of Piraeus

Christos Xenakis, Assistant Professor
University of Piraeus

Constantinos Lambrinoudakis, Associate Professor
University of Piraeus

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Table of Contents

Preface – Acknowledgements	pg 6
Chapter 1 – Introduction	pg 8
1.1 Scope and Methodology Plan	pg 8
1.2 Windows 7 Methodology	pg 8
1.3 Windows 8 Methodology	pg 8
1.4 Tools Choise	pg 9
1.5 Lab Environment.....	pg 9
Chapter 2 - Forensics Analysis of a Windows 7 Host	
2.1 Machine Details	pg 10
2.2 Live response using mir-ror	pg 10
2.3 Memory Analysis	pg 27
2.4 Disk Imaging and Registry copy	pg 33
2.5 SANS SIFT ANALYSIS	pg 37
2.6 Registry Analysis	pg 43
Chapter 3 Forensics Analysis of a Windows 8 Host	
3.1 Machine Details	pg 55
3.2 Live response using mir-ror	pg 55
3.3 Memory Analysis	pg 68
3.4 SAN SIFT ANALYSIS	pg 76
3.5 Registry Analysis	pg 77
Chapter 4 - Conclusions	
4.1 Final Verification	pg 79
4.2 File Downloads	pg 79
4.3 Program Execution	pg 79
4.4 File Opening/Creation	pg 79
4.5 Deleted Information	pg 80
4.6 Information About Physical Location	pg 80
4.7 USB Drive Usage	pg 80
4.8 Account Usage	pg 80
4.9 Memory Forensics	pg 80
4.10 Disk Forensics	pg 80
4.11 Live Response	pg 80
4.12 Summary	pg 80
References	pg 82

Preface - Acknowledgements

My research interest in digital security systems was triggered by my engagement with the implementation and maintenance of networks and telecommunications technologies. In my daily work I had to face a variety of security issues. This is why I decided to study in this specific postgraduate program.

The experience I gained through these studies of mine is immense. In combination with my capacity as a network engineer, I will henceforth be able to propose and elaborate also solutions in the field of network security. Through my study in the specific postgraduate program, I gained enough experience to have now a more comprehensive and integrated view of telecommunications and networks in general and of the security-related issues. Upon completion of my postgraduate studies, I would like to thank Prof. Sokratis Katsikas, the supervisor of this thesis, as well as my mentor throughout the MSc course. He inspired me and taught me how to get a global view on each problem and then try to solve it in a particular framework. The roles of Prof. Christos Xenakis and Prof. Konstantinos Lambrinouidakis were also important. Prof. Xenakis helped me understand the technical and engineering level of security issues that arise in wired and wireless telecom environments. I could say without any reservation that he is one of the most technically knowledgeable professors I have ever met. Prof. Lambrinouidakis taught me the way of discovering alternative solutions in each problem. He is a multidimensional teacher with excellent knowledge on his subject of tackling each problem and each variant in an excellent manner and with a particular approach. I must also mention here Dr Ntantogian, Prof. Mitrou and Prof. Rizomyliotis for their specific and specialized knowledge that they managed to pass on to me throughout my study. Special thanks are offered to Mr. Spyros Papageorgiou who specifically guided me through the technical aspects of this project and also tried to improve my project in each step through helpful remarks. He is an excellent security engineer and a special man too.

I offer my biggest thanks to the people closest to me, who contributed to my efforts. Specifically I want to thank my wife, and my family who gave me the initial encouragement to engage in academic research. They supported me through my study for the specific postgraduate program. I thank them and dedicate to them this thesis.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Chapter 1 – Introduction

1.1 Scope and Methodology Plan

In this thesis we propose a methodology for digital data analysis in Windows 7 and Windows 8 environments. The aim of this research is to map out how the analyst should be thinking and how he should modify the available tools in order to make them fit fully in his operational needs. When a new version of an operating system is released, the adaptation of the analyst is usually difficult. Through this work we try to emulate a proper way of thinking, in order to allow the analyst to have a full and smooth transition into the new version.

In order to follow a specific forensics plan, one must first break the methodology into small independent processes. After that, one must come up with the tools that one is going to use in each process.

The forensics methodology follows a basic rule, namely that we should make as few changes as possible to the system under review. The first step is to make sure that we have an incident. We achieve that with the process of incident handling (response). After we ascertain that we have an incident, we move on the next steps which is making copies of the memory, the registry and the hard disk. By using the mirror tool, we take a copy of the memory in order to make as few changes to the system (memory) as possible. We use some other tools for the registry and the hard disk copy. The work finishes with the analysis of the memory, the registry and the hard disk.

This thesis is structured as follows: firstly we discuss the tools and the working environment chosen for this particular research. Second the methodology is applied to the windows 7 operating system. After that, the tools we use are modified and applied again in the windows 8 operating system. In conclusion we make a comparison of our results between these two operating systems.

1.2 Windows 7 Methodology

The Independent processes we choose for windows 7 forensics are:

- Incident response (registry, memory copy)
- Memory analysis
- Disk copy
- File analysis
- Registry Analysis

The tools that we are going to use in each step are:

- MIR-ROR (Is a security incident response tool, command-line script that calls specific Windows Sysinternals tools. It provides live capture data for investigation.) / We add winpmem (Open source windows memory imager. It has the ability to analyze live memory on a running computer) for memory copying also to this tool.
- Volatility (Framework with open collection of tools, implemented in python. It used for extraction of digital artifacts from RAM)
- SIFT (Vmware Appliance with forensic tools preconfigure and cross compatibility between Linux and Windows).
- Regripper (Written in perl, is a data extraction tool for windows registry).

1.3 Windows 8 Methodology

The Independent processes we choose for windows 8 forensics are:

- Incident response (registry, memory copy)
- Memory analysis
- Disk copy
- File analysis
- Registry Analysis

The tools that we will use in each step are:

- MIR-ROR (suite of tools for incident response) / We add winpmem for memory copying also to this tool.
- Memoryze (Free memory forensic software which can acquire and analyze memory images on a live system)
- SIFT (for disk copy and file analysis)
- Regripper (for registry analysis)

1.4 Tools Choise

In order to spot the differences between the two operating systems, we chose to use the same tools (except volatility which was not available for windows 8 yet) for the two operating systems.

The Mirror suite is also not available for windows 8. However, after creating a signature (identify OS) and making some changes in the batch file (extra tools added) we managed to make it compatible with windows 8 as well.

Care has been taken to be as compatible as possible with the SANS Digital Forensics and Incident Response Poster of 2012. [1]

1.5 Lab Environment

The analysis was carried out on two Virtual Machines, running in Oracle VirtualBox platform.

Windows 7	Windows 8
Ultimate (32 bit, ver. 6.1.7600)	Pro(32 bit, ver. 6.2.9200)
1GB RAM	1GB RAM
20GB Hard Disk	20GB Hard Disk

The details of the Virtual Machines are given before our analysis at the beginning of each chapter.

Chapter 2 - Forensics Analysis of a Windows 7 Host

2.1 Machine Details

The analysis was carried out on a Virtual Machine running in Oracle Virtualbox with 1 GB RAM and 20 GB Hard disk. Windows 7 Ultimate (32 bit) with version 6.1.7600 was analyzed for forensics evidence.

2.2 Live response using mir-ror

Mir-ror V2.0 was used to carry out live response evidence collection from the host to gather the state of the live system as present at the time of incident report. Default script for Mir-ror was adapted to work under Windows 7 environment as it is originally designed for Windows XP and Windows 2003. The modifications made included commenting out the calls to now.exe as they were valid for Windows 2003 only. [2, 3]

```
REM now.exe [Copying the registry files for offline analysis] >> %LOGS%\Livecap_%COMPUTERNAME%\MIR-ROR.log
```

Image 2.2.1: Modification

Then there were few tools called in the script which were not available in the Sysinternal suite installation for Mir-ror and included in fetch.txt. They needed to be downloaded and included in the Mir-ror installation directory.[4]

MIR-ROR v.2.0 as of 3/21/12

fetch.txt v.2.0.1 as of 4/11/12

- 1) Download the Sysinternals Suite: <http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>
- 2) Download **NTFScopy**: http://www.tzworks.net/prototype_page.php?proto_id=9
- 3) Download **The SleuthKit (TSK)**: <http://www.sleuthkit.org/sleuthkit/download.php>
- 4) Download **the Windows Server 2003 Resource Kit Tools**: <http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en>
- 5) Download **seccheck.exe** from Holisticinfosec.org: <http://holisticinfosec.org/toolsmith/files/seccheck/seccheck.exe>
- 6) Download **openports.exe** from Holisticinfosec.org: <http://holisticinfosec.org/toolsmith/files/openports/openports.exe>

Image 2.2.2: Extra tools

The files that were downloaded and included in the tools are shown below.

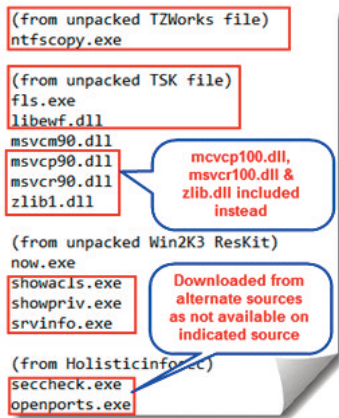


Image 2.2.3: Files Included

Additionally memory dump was created using winpmem v1.4.1 and for that purpose following command was added to the script.

```
ECHO Running winpmem of %COMPUTERNAME%.
winpmem_1.4.exe %LOGS%\Livecap_%COMPUTERNAME%\phymem.raw
winpmem 1.4.exe -d %LOGS%\Livecap_%COMPUTERNAME%\phymemdump.dmp
ECHO.
```

Image 2.2.4: Winpmem

All the tools were copied to a USB flash drive under \\tools\mir-ror directory and this drive was plugged in a host on the same network as the target system and this directory was mapped as a network drive 'M'. Therefore no tools were needed to be copied to the target host. After mir-ror was run it generated output in a directory with a suffix of the host name as the host-name was 'T-PC, the directory was named Livecap_T-PC.

A look at the mirror output reveals:-

Recycle Bin:

There were three pdf files found in recycle bin. They were Oracle tutorials.

Name	Date modified	Type	Size
SIIEJ2LM.PDF	1/18/2013 11:23 PM	PDF File	1 KB
SIL9CGL5.pdf	1/18/2013 11:22 PM	PDF File	1 KB
SIOO46GX.pdf	1/18/2013 11:23 PM	PDF File	1 KB

Image2.2.5: Recycle Bin

A list of cookies found:

Name	Date modified	Type	Size
index.dat	10/24/2013 4:30 PM	DAT File	48 KB
t@ad.yieldmanager[1].txt	1/18/2013 10:38 PM	Text Document	1 KB
t@atdmt[1].txt	1/18/2013 11:25 PM	Text Document	1 KB
t@atdmt[2].txt	10/24/2013 4:28 PM	Text Document	1 KB
t@bing[1].txt	1/18/2013 10:44 PM	Text Document	1 KB
t@bing[2].txt	10/24/2013 4:29 PM	Text Document	1 KB
t@bluekai[2].txt	10/24/2013 4:16 PM	Text Document	1 KB
t@c.atdmt[2].txt	1/18/2013 10:37 PM	Text Document	1 KB
t@c.atdmt[3].txt	10/24/2013 4:28 PM	Text Document	1 KB
t@c.bing[1].txt	1/18/2013 10:37 PM	Text Document	1 KB
t@c.bing[3].txt	10/24/2013 4:29 PM	Text Document	1 KB
t@c1.atdmt[1].txt	1/18/2013 11:25 PM	Text Document	1 KB
t@c1.microsoft[1].txt	1/18/2013 11:25 PM	Text Document	1 KB
t@debugger.immunityinc[1].txt	10/24/2013 4:14 PM	Text Document	1 KB
t@debugger.immunityinc[2].txt	1/18/2013 10:40 PM	Text Document	1 KB
t@demdex[2].txt	10/24/2013 4:15 PM	Text Document	1 KB
t@doubleclick[1].txt	1/18/2013 10:38 PM	Text Document	1 KB
t@fastclick[1].txt	1/18/2013 10:37 PM	Text Document	1 KB
t@google[1].txt	1/18/2013 10:38 PM	Text Document	1 KB
t@google[3].txt	1/18/2013 11:25 PM	Text Document	1 KB
t@google[4].txt	1/18/2013 11:25 PM	Text Document	1 KB
t@interclick[1].txt	1/18/2013 10:37 PM	Text Document	1 KB
t@invitemedia[2].txt	1/18/2013 10:38 PM	Text Document	1 KB
t@live[2].txt	10/24/2013 4:15 PM	Text Document	1 KB
t@m.webtrends[2].txt	1/18/2013 11:25 PM	Text Document	1 KB
t@m.webtrends[3].txt	10/24/2013 4:14 PM	Text Document	1 KB
t@microsoft[1].txt	10/24/2013 4:14 PM	Text Document	1 KB
t@microsoft[2].txt	1/18/2013 11:25 PM	Text Document	2 KB
t@microsoftsto.112.2o7[1].txt	1/18/2013 11:25 PM	Text Document	1 KB

Image 2.2.6: Cookies

Three administrator accounts were found to be present on the target host.

```

admin_accounts.log - Notepad
File Edit Format View Help
Alias name administrators
Comment Administrators have complete and unrestricted access to
the computer/domain

Members

-----
Administrator
backdoor
t
The command completed successfully.

```

Image 2.2.7: Admin Accounts

There were total four accounts on the host including the Guest account.

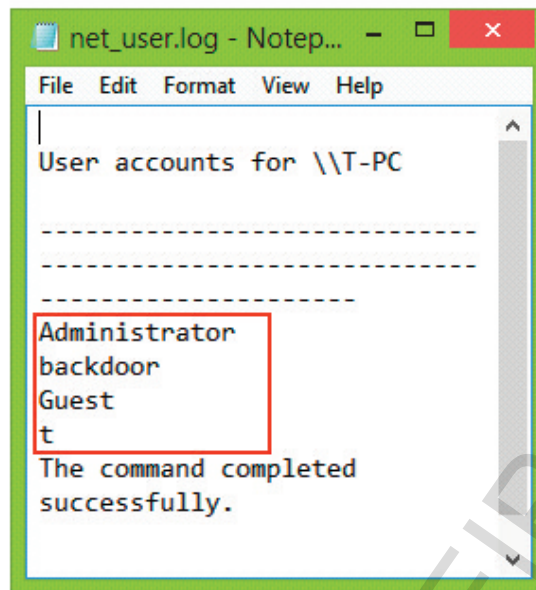


Image 2.2.8: Users Accounts

The network mapped drive found was the one containing the tools directory for mir-ror.

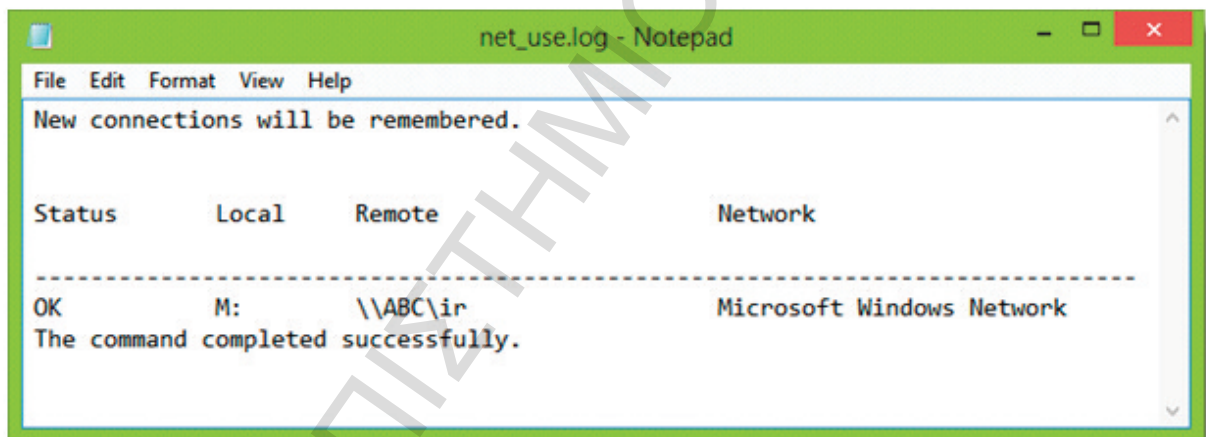


Image 2.2.9: Network Mapped Drive

Ftype utility is used to list all registry keys contained in HKEY_CLASSES_ROOT carrying the shell\open\command sub Key and shows the all the registered file types along with the application used to open these including any arguments and switches etc. This key is sometimes used by Malware as a persistence mechanism to execute the malware each time a particular file type is opened. No traces of such activity were found on this host.

```

SPCFile=%SystemRoot%\system32\rundll32.exe cryptext.dll,CryptExtOpenPKCS7 %1
STLFile=%SystemRoot%\system32\rundll32.exe cryptext.dll,CryptExtOpenCTL %1
stssync="C:\PROGRA~1\MICROS~2\Office12\OUTLOOK.EXE" /share "%1"
telnet="C:\Windows\System32\rundll32.exe" "C:\Windows\System32\url.dll",TelnetProtocolHandler %1
textfile="%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE" "%1"
themefile=%SystemRoot%\system32\rundll32.exe %SystemRoot%\system32\shell32.dll,Control_RunDLL %SystemRoot%\system32\desk.cpl desk,@Themes /Action:OpenTheme /file:"%1"
themepackfile=%SystemRoot%\system32\rundll32.exe %SystemRoot%\system32\shell32.dll,Control_RunDLL %SystemRoot%\system32\desk.cpl desk,@Themes /Action:OpenTheme /file:"%1"
TIFFImage.Document=%SystemRoot%\System32\rundll32.exe "%ProgramFiles%\Windows Photo Viewer\PhotoViewer.dll",ImageView_Fullscreen %1
tn3270="C:\Windows\System32\rundll32.exe" "C:\Windows\System32\url.dll",TelnetProtocolHandler %1
txtfile=%SystemRoot%\system32\notepad.exe %1
VBFile="%SystemRoot%\System32\WScript.exe" "%1" %*
VBSFile="%SystemRoot%\System32\WScript.exe" "%1" %*
vcard_wab_auto_file="%ProgramFiles%\Windows Mail\wab.exe" /vcard "%1"
VisioViewer.Viewer="C:\Program Files\Internet Explorer\iexplore.exe" -nohome
VSTA.config.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.cs.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.csproj.8.0="C:\Program Files\Microsoft Shared\MSEnv\VSLauncher.exe" "%1"
VSTA.datasource.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.disco.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.dtd.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.sdl.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.snippet.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.vb.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.vbproj.8.0="C:\Program Files\Microsoft Shared\MSEnv\VSLauncher.exe" "%1"
VSTA.vstemplate.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.wsd.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.xdr.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.xml.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.xsl.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
VSTA.xslt.8.0="C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\vsta.exe" /dde
wab_auto_file="%ProgramFiles%\Windows Mail\wab.exe" /Import "%1"
wbcatfile=%SystemRoot%\system32\sdclt.exe /restorepage
WCN.AutoPlayHandler=%systemroot%\system32\rundll32.exe %systemroot%\system32\wzcdlg.dll,ImportFlashProfile %L

```

Image 2.2.10: Registry Keys

Hosts file is sometimes used by malware to corrupt the DNS query mechanism of the compromised hosts. No such traces were found on this host.

```

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com               # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost

```

Image 2.2.11: Hosts File

Administrative shares found on the target host are shown below.

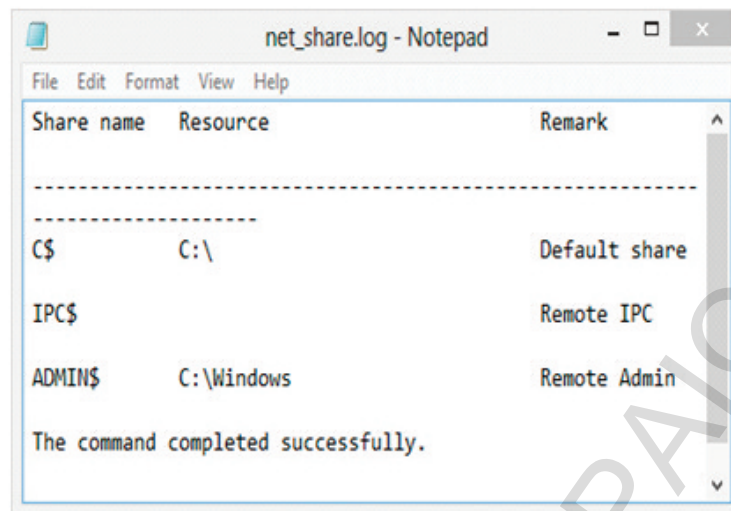


Image 2.2.12: Admin Shares

ARP table is analyzed to see whether ARP poisoning has been used to carryout MITM attacks. No indications of such activity were found.

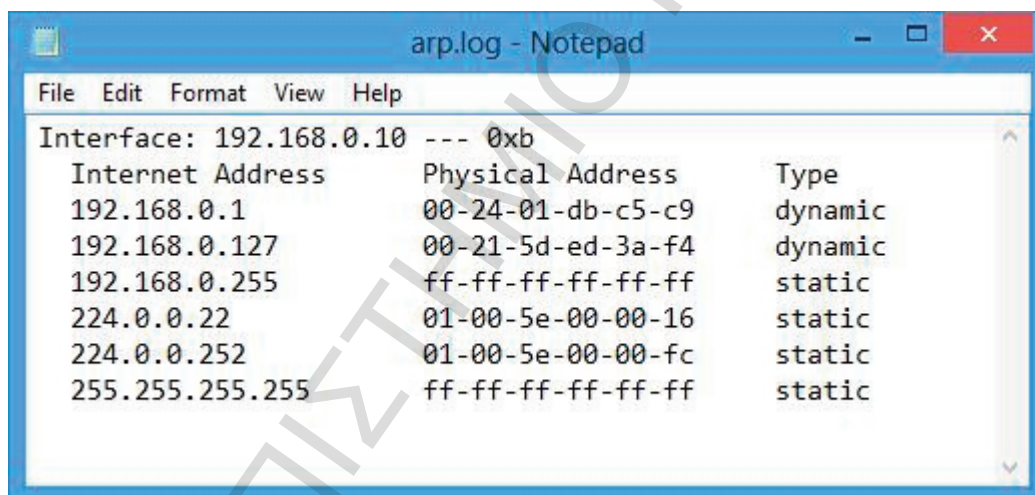
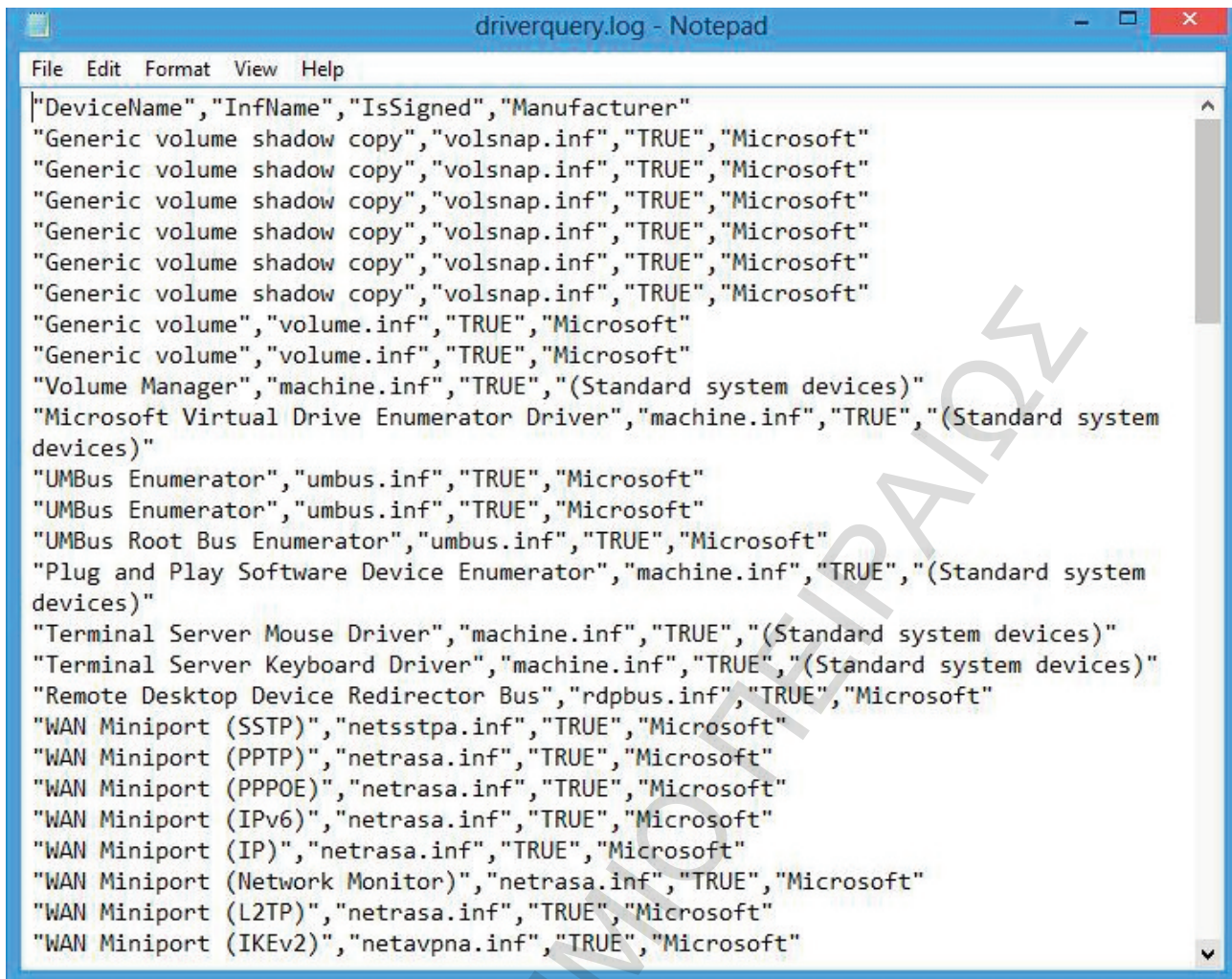


Image 2.2.13: Arp Table

Driverquery shows whether any malicious program is installed as a driver, the indication would be such driver is most likely unsigned or if signed, mostly it is from a conspicuous manufacturer. No such unsigned driver was found as shown below.



```

"DeviceName","InfName","IsSigned","Manufacturer"
"Generic volume shadow copy","volsnap.inf","TRUE","Microsoft"
"Generic volume shadow copy","volsnap.inf","TRUE","Microsoft"
"Generic volume shadow copy","volsnap.inf","TRUE","Microsoft"
"Generic volume shadow copy","volsnap.inf","TRUE","Microsoft"
"Generic volume shadow copy","volsnap.inf","TRUE","Microsoft"
"Generic volume shadow copy","volsnap.inf","TRUE","Microsoft"
"Generic volume","volume.inf","TRUE","Microsoft"
"Generic volume","volume.inf","TRUE","Microsoft"
"Volume Manager","machine.inf","TRUE","(Standard system devices)"
"Microsoft Virtual Drive Enumerator Driver","machine.inf","TRUE","(Standard system
devices)"
"UMBus Enumerator","umbus.inf","TRUE","Microsoft"
"UMBus Enumerator","umbus.inf","TRUE","Microsoft"
"UMBus Root Bus Enumerator","umbus.inf","TRUE","Microsoft"
"Plug and Play Software Device Enumerator","machine.inf","TRUE","(Standard system
devices)"
"Terminal Server Mouse Driver","machine.inf","TRUE","(Standard system devices)"
"Terminal Server Keyboard Driver","machine.inf","TRUE","(Standard system devices)"
"Remote Desktop Device Redirector Bus","rdpbus.inf","TRUE","Microsoft"
"WAN Miniport (SSTP)","netsstpa.inf","TRUE","Microsoft"
"WAN Miniport (PPTP)","netrasa.inf","TRUE","Microsoft"
"WAN Miniport (PPPOE)","netrasa.inf","TRUE","Microsoft"
"WAN Miniport (IPv6)","netrasa.inf","TRUE","Microsoft"
"WAN Miniport (IP)","netrasa.inf","TRUE","Microsoft"
"WAN Miniport (Network Monitor)","netrasa.inf","TRUE","Microsoft"
"WAN Miniport (L2TP)","netrasa.inf","TRUE","Microsoft"
"WAN Miniport (IKEv2)","netavpna.inf","TRUE","Microsoft"

```

Image 2.2.14: Driverquery

Ipconfig displays the installed NICs and their configuration as shown below. Nothing conspicuous was found.

Ethernet adapter Local Area Connection:

```

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-CE-01-0B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::21b7:c7ce:506d:22c6%11(Preferred)
IPv4 Address. . . . . : 192.168.0.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, October 24, 2013 4:07:03 PM
Lease Expires . . . . . : Thursday, October 24, 2013 10:07:05 PM
Default Gateway . . . . . : fe80::224:1ff:fedb:c5c9%11
                            192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpi. . . . . : Enabled

```

Image 2.2.15: Ipconfig

Handles.log file generated by mir-ror shows the processes and the associated threads and handles information. This log presented some interesting information like telnet service being started (which is disabled by default in Windows 7) and presence of an active telnet session.

```

6F8: Process      tlntsvr.exe(2256)
700: Process      tlntsess.exe(2360)
704: Process      taskmgr.exe(1788)
70C: File (---)   \Device\Tcp
714: ALPC Port

```

Image 2.2.16: Handles.log

Also apart from the user name 'T' indications of another session by user named 'backdoor' were found.

```

730: Key          HKLM\SYSTEM\WPA\8DEC0AF1-0341-4b93-85CD-72606C2DF94C-5P-8
734: File (R--)   C:\Users\t\NTUSER.DAT[6cced2f1-6e01-11de-8bed-
01e0bcd1824].TMContainer000000000000000001.regtrans-ms
738: Key          \REGISTRY\A\{36B21789-3C9C-11E3-837E-080027CE010B}\DefaultObjectStore
73C: Process      sppsvc.exe(552)
748: Token        NT AUTHORITY\LOCAL SERVICE:3e5
74C: File (R-D)   C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTMsMpPsSession7.etl
750: Process      svchost.exe(1732)
75C: Token        t-PC\t:3b179
76C: Token        NT AUTHORITY\LOCAL SERVICE:3e5
77C: Process      svchost.exe(848)
78C: File (RW-)   \cifs
790: Process      svchost.exe(1432)
794: File (---)   C:\System Volume Information\Syscache.hve.LOG2
798: File (---)   C:\System Volume Information\Syscache.hve.LOG1
7A4: File (---)   C:\System Volume Information\Syscache.hve
7A8: Key          \REGISTRY\A\{36B21789-3C9C-11E3-837E-080027CE010B}
7B0: Process      sppsvc.exe(552)
7B4: File (---)   \Device\Tcp
7C8: Process      handle.exe(3456)
7CC: Key          \REGISTRY\A\{36B21789-3C9C-11E3-837E-080027CE010B}\DefaultObjectStore
LruList
7D0: Key          \REGISTRY\A\{36B21789-3C9C-11E3-837E-080027CE010B}\DefaultObjectStore
ObjectTable
7D4: Key          \REGISTRY\A\{36B21789-3C9C-11E3-837E-080027CE010B}\DefaultObjectStore
IndexTable\FileIdIndex-{87b33115-61ff-11e2-a139-806e6f6e6963}
7D8: File (---)   C:\Users\t\NTUSER.DAT
7DC: Key          \REGISTRY\A\{36B21789-3C9C-11E3-837E-080027CE010B}\DefaultObjectStore
IndexTable
7E0: Token        t-PC\t:3b179
7E4: ALPC Port
7F0: Token        NT AUTHORITY\SYSTEM:3e7
7F4: File (R--)   C:\Users\backdoor\NTUSER.DAT[6cced2f1-6e01-11de-8bed-
01e0bcd1824].TMContainer000000000000000001.regtrans-ms
7F8: Token        t-PC\t:3b179
7FC: File (---)   C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-
.C7483456-A289-439d-8115-601632D005A0
804: File (---)   C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-
.C7483456-A289-439d-8115-601632D005A0
808: Process      svchost.exe(1732)
810: File (---)   C:\Users\t\ntuser.dat.LOG2

```

Image 2.2.17: Session by another user

Few suspicious processes were traced which are not normally found in a normal execution of Windows 7 as shown below.

```

2C0: Thread      svchost.exe(1732): 1748
2C4: Thread      nc.exe(2428): 3696
2C8: Thread      spoolsv.exe(1288): 2004
  
```

Image 2.2.18: Nc.exe (used as backdoor)

Nc.exe shares its name with Netcat, a famous tool used for multiple tasks including serving as a backdoor also.

```

5D0: Thread      explorer.exe(936): 2064
5E4: Thread      demo (1).exe(3968): 3056
5E8: Event
5EC: Process     demo (1).exe(3968)
5F0: Thread      conhost.exe(2992): 3260
5F4: ALPC Port
  
```

Image 2.2.19: Suspicious processes 1

```

270: Section
274: Process     hh.exe(2464)
278: Process     iexplore.exe(2912)
284: ALPC Port
288: Thread      explorer.exe(936): 2052
  
```

Image 2.2.20: Suspicious processes 2

These processes need further investigation.

Listdll.log displays process wise DLLs loaded by each process. For suspicious process identified earlier it shows that this process has loaded DLLs which open TCP sockets.

```

demo (1).exe pid: 3968
Command line: "C:\test\demo (1).exe"

Base      Size      Path
0x00400000 0x37000  C:\test\demo (1).exe
0x771f0000 0x13c000 C:\Windows\SYSTEM32\ntd11.dll
0x75a60000 0xd4000  C:\Windows\system32\kernel132.dll
0x75450000 0x4a000  C:\Windows\system32\KERNELBASE.dll
0x76c50000 0xac000  C:\Windows\system32\msvcrt.dll
0x76d90000 0x35000  C:\Windows\system32\WS2_32.DLL
0x76950000 0xa1000  C:\Windows\system32\RPCRT4.dll
0x771e0000 0x6000   C:\Windows\system32\NSI.dll
0x74d80000 0x3c000  C:\Windows\system32\mswsock.dll
0x757f0000 0xc9000  C:\Windows\system32\user32.dll
0x77330000 0x4e000  C:\Windows\system32\GDI32.dll
0x76ad0000 0xa000   C:\Windows\system32\LPK.dll
0x77380000 0x9d000  C:\Windows\system32\USP10.dll
0x76e50000 0x1f000  C:\Windows\system32\IMM32.DLL
0x76a00000 0xcc000  C:\Windows\system32\MSCTF.dll
0x748d0000 0x5000   C:\Windows\System32\wshtcpip.dll

```

Image 2.2.21: Listdll.log demo.exe

Similarly nc.exe and hh.exe were also found to have similar DLLs loaded.

```

nc.exe pid: 2428
Command line: nc.exe

Base      Size      Path
0x00400000 0x10000  C:\test\nc.exe
0x771f0000 0x13c000 C:\Windows\SYSTEM32\ntd11.dll
0x75a60000 0xd4000  C:\Windows\system32\kernel132.dll
0x75450000 0x4a000  C:\Windows\system32\KERNELBASE.dll
0x76d90000 0x35000  C:\Windows\system32\WS2_32.dll
0x76c50000 0xac000  C:\Windows\system32\msvcrt.dll
0x76950000 0xa1000  C:\Windows\system32\RPCRT4.dll
0x771e0000 0x6000   C:\Windows\system32\NSI.dll

```

Image 2.2.22: Listdll.log nc.exe

```

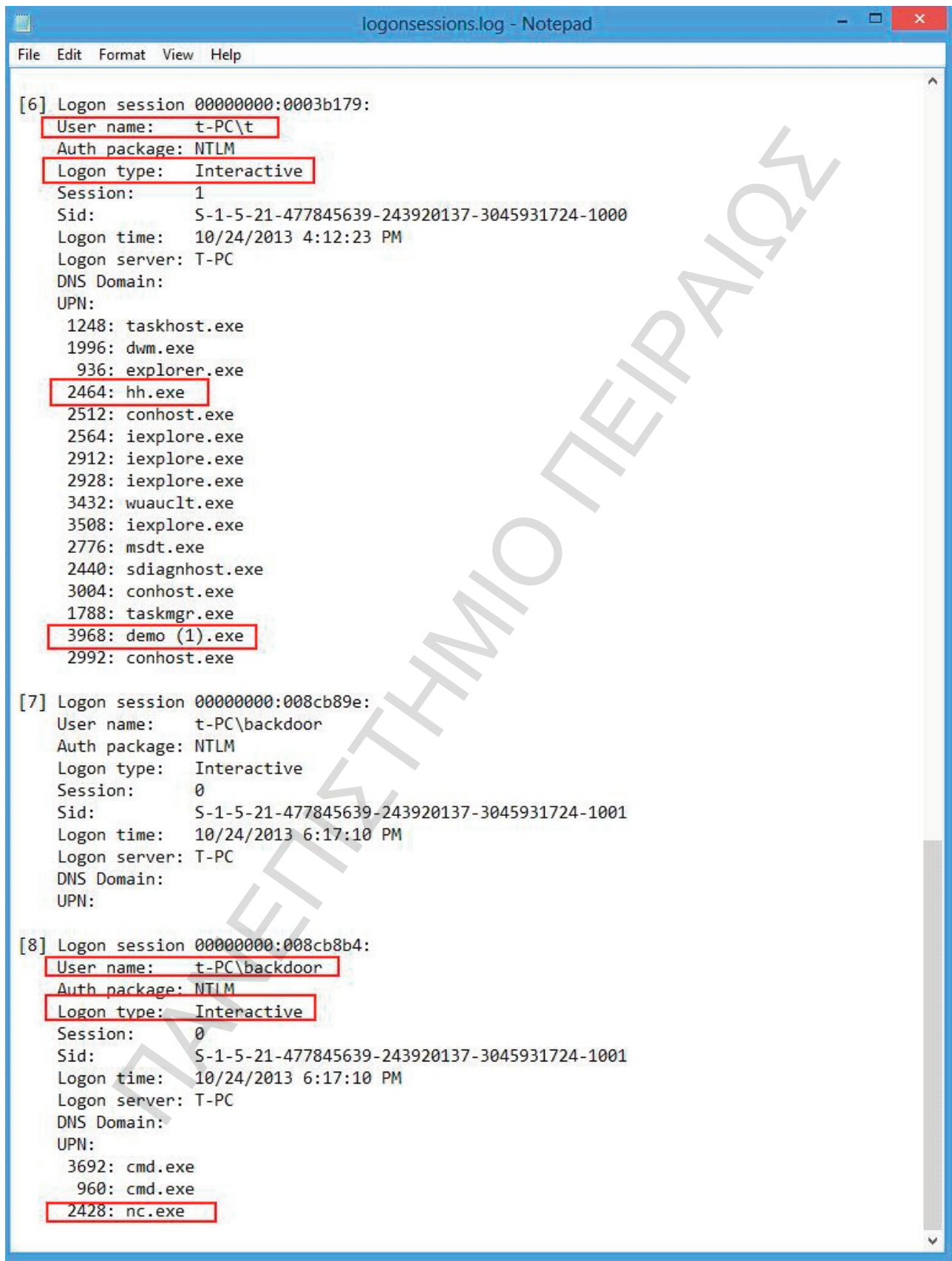
hh.exe pid: 2464
Command line: "C:\test\hh.exe"

Base      Size      Path
0x00400000 0xc4000  C:\test\hh.exe
0x771f0000 0x13c000 C:\Windows\SYSTEM32\ntd11.dll
0x75a60000 0xd4000  C:\Windows\system32\kernel132.dll
0x75450000 0x4a000  C:\Windows\system32\KERNELBASE.dll
0x76d90000 0x35000  C:\Windows\system32\WS2_32.DLL
0x76c50000 0xac000  C:\Windows\system32\msvcrt.dll
0x76950000 0xa1000  C:\Windows\system32\RPCRT4.dll
0x771e0000 0x6000   C:\Windows\system32\NSI.dll
0x757f0000 0xc9000  C:\Windows\system32\USER32.dll
0x77330000 0x4e000  C:\Windows\system32\GDI32.dll
0x76ad0000 0xa000   C:\Windows\system32\LPK.dll
0x77380000 0x9d000  C:\Windows\system32\USP10.dll
0x76e50000 0x1f000  C:\Windows\system32\IMM32.DLL
0x76a00000 0xcc000  C:\Windows\system32\MSCTF.dll
0x74d80000 0x3c000  C:\Windows\system32\mswsock.dll
0x748d0000 0x5000   C:\Windows\System32\wshtcpip.dll

```

Image 2.2.23: Listdll.log hh.exe

Logonsessions.log files shows the logged on sessions and it was found that there were two sessions open one by user named 'T' and it was an interactive session. The other user named 'backdoor'.



```
logonsessions.log - Notepad
File Edit Format View Help

[6] Logon session 00000000:0003b179:
  User name: t-PC\t
  Auth package: NTLM
  Logon type: Interactive
  Session: 1
  Sid: S-1-5-21-477845639-243920137-3045931724-1000
  Logon time: 10/24/2013 4:12:23 PM
  Logon server: T-PC
  DNS Domain:
  UPN:
  1248: taskhost.exe
  1996: dwm.exe
  936: explorer.exe
  2464: hh.exe
  2512: conhost.exe
  2564: iexplore.exe
  2912: iexplore.exe
  2928: iexplore.exe
  3432: wuauclt.exe
  3508: iexplore.exe
  2776: msdt.exe
  2440: sdiagnhost.exe
  3004: conhost.exe
  1788: taskmgr.exe
  3968: demo (1).exe
  2992: conhost.exe

[7] Logon session 00000000:008cb89e:
  User name: t-PC\backdoor
  Auth package: NTLM
  Logon type: Interactive
  Session: 0
  Sid: S-1-5-21-477845639-243920137-3045931724-1001
  Logon time: 10/24/2013 6:17:10 PM
  Logon server: T-PC
  DNS Domain:
  UPN:

[8] Logon session 00000000:008cb8b4:
  User name: t-PC\backdoor
  Auth package: NTLM
  Logon type: Interactive
  Session: 0
  Sid: S-1-5-21-477845639-243920137-3045931724-1001
  Logon time: 10/24/2013 6:17:10 PM
  Logon server: T-PC
  DNS Domain:
  UPN:
  3692: cmd.exe
  960: cmd.exe
  2428: nc.exe
```

Image 2.2.24: Logonsessions.log

Netsh.log shows the current state of Windows firewall rules and policies.

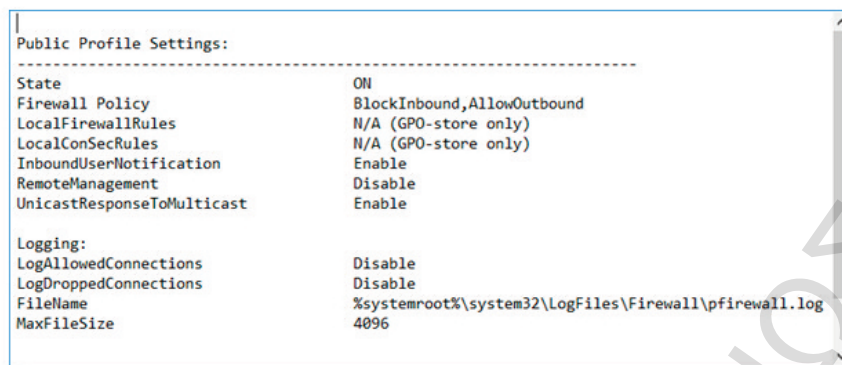


Image 2.2.25: Netsh.log

Netstat.log shows the result of netstat command which displays all the open TCP connections. The telnet session and hh.exe and demo(1).exe were found to be listening for connections.

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	2256
[tlntsvr.exe]				
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	688
RpcSs				
[svchost.exe]				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:1974	0.0.0.0:0	LISTENING	3968
[demo (1).exe]				
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	1188
CryptSvc				
[svchost.exe]				
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	376
[wininit.exe]				
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	808
eventlog				
[svchost.exe]				
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	876
Schedule				
[svchost.exe]				
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	488
[lsass.exe]				
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	476
[services.exe]				
TCP	192.168.0.10:23	192.168.0.127:34409	ESTABLISHED	2256
[tlntsvr.exe]				
TCP	192.168.0.10:139	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	192.168.0.10:49166	192.168.0.10:80	SYN_SENT	2464
[hh.exe]				
TCP	192.168.0.10:49579	82.178.158.19:80	CLOSE_WAIT	2928
[iexplore.exe]				
TCP	192.168.0.10:49860	173.194.35.125:443	ESTABLISHED	2912
[iexplore.exe]				
TCP	192.168.0.10:49863	173.194.35.125:443	ESTABLISHED	2912

Image 2.2.26: Netstat.log

Openports.log shows the ports open on the host and it was found that port 23 (telnet) was open and connected and port 80 was also found to be open.

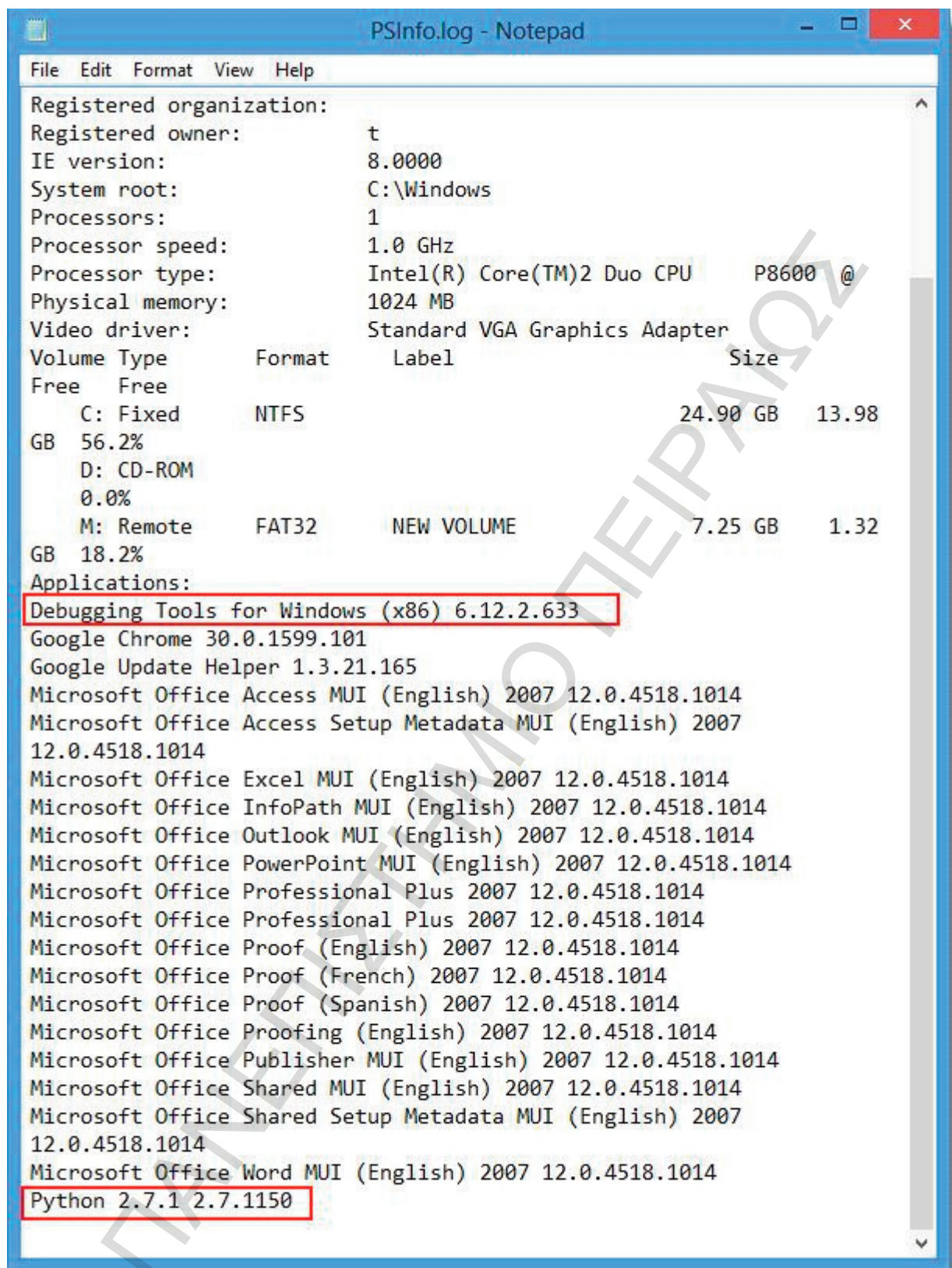
```

OpenPorts - DiamondCS Console Tools (www.diamondcs.com.au)
---
SYSTEM [0]
TCP 192.168.0.10:23      192.168.0.127:34409  ESTABLISHED
TCP 0.0.0.0:135         0.0.0.0:0           LISTENING
TCP 192.168.0.10:139   0.0.0.0:0           LISTENING
TCP 0.0.0.0:1974       0.0.0.0:0           LISTENING
TCP 0.0.0.0:3389       0.0.0.0:0           LISTENING
TCP 0.0.0.0:49152      0.0.0.0:0           LISTENING
TCP 0.0.0.0:49153      0.0.0.0:0           LISTENING
TCP 0.0.0.0:49154      0.0.0.0:0           LISTENING
TCP 0.0.0.0:49155      0.0.0.0:0           LISTENING
TCP 0.0.0.0:49156      0.0.0.0:0           LISTENING
TCP 192.168.0.10:49166 192.168.0.10:80     CONNECTING
TCP 192.168.0.10:49579 82.178.158.19:80    CLOSE_WAIT
TCP 192.168.0.10:49860 173.194.35.125:443  ESTABLISHED
TCP 192.168.0.10:49863 173.194.35.125:443  ESTABLISHED
TCP 0.0.0.0:23         0.0.0.0:0           LISTENING
TCP 0.0.0.0:445        0.0.0.0:0           LISTENING
TCP 0.0.0.0:5357       0.0.0.0:0           LISTENING
UDP 192.168.0.10:137   0.0.0.0:0           LISTENING
UDP 192.168.0.10:138   0.0.0.0:0           LISTENING
UDP 127.0.0.1:1900     0.0.0.0:0           LISTENING
UDP 192.168.0.10:1900  0.0.0.0:0           LISTENING
UDP 0.0.0.0:3702       0.0.0.0:0           LISTENING
UDP 0.0.0.0:3702       0.0.0.0:0           LISTENING
UDP 0.0.0.0:5355       0.0.0.0:0           LISTENING
UDP 0.0.0.0:51634     0.0.0.0:0           LISTENING
UDP 127.0.0.1:54717   0.0.0.0:0           LISTENING
UDP 127.0.0.1:54881   0.0.0.0:0           LISTENING
UDP 127.0.0.1:61186   0.0.0.0:0           LISTENING
UDP 127.0.0.1:62317   0.0.0.0:0           LISTENING
UDP 127.0.0.1:62318   0.0.0.0:0           LISTENING

```

Image 2.2.27: Openports.log

Pinfo.log shows the information about the host and the programs installed. It was found that debugging tools (debugger of some kind most probably windbg) and python was installed on the host.



```

PsInfo.log - Notepad
File Edit Format View Help
Registered organization:
Registered owner:      t
IE version:           8.0000
System root:          C:\Windows
Processors:           1
Processor speed:      1.0 GHz
Processor type:       Intel(R) Core(TM)2 Duo CPU   P8600  @
Physical memory:      1024 MB
Video driver:         Standard VGA Graphics Adapter
Volume Type           Format      Label              Size
Free   Free
C: Fixed             NTFS                24.90 GB    13.98
GB 56.2%
D: CD-ROM
0.0%
M: Remote            FAT32      NEW VOLUME         7.25 GB    1.32
GB 18.2%
Applications:
Debugging Tools for Windows (x86) 6.12.2.633
Google Chrome 30.0.1599.101
Google Update Helper 1.3.21.165
Microsoft Office Access MUI (English) 2007 12.0.4518.1014
Microsoft Office Access Setup Metadata MUI (English) 2007
12.0.4518.1014
Microsoft Office Excel MUI (English) 2007 12.0.4518.1014
Microsoft Office InfoPath MUI (English) 2007 12.0.4518.1014
Microsoft Office Outlook MUI (English) 2007 12.0.4518.1014
Microsoft Office PowerPoint MUI (English) 2007 12.0.4518.1014
Microsoft Office Professional Plus 2007 12.0.4518.1014
Microsoft Office Professional Plus 2007 12.0.4518.1014
Microsoft Office Proof (English) 2007 12.0.4518.1014
Microsoft Office Proof (French) 2007 12.0.4518.1014
Microsoft Office Proof (Spanish) 2007 12.0.4518.1014
Microsoft Office Proofing (English) 2007 12.0.4518.1014
Microsoft Office Publisher MUI (English) 2007 12.0.4518.1014
Microsoft Office Shared MUI (English) 2007 12.0.4518.1014
Microsoft Office Shared Setup Metadata MUI (English) 2007
12.0.4518.1014
Microsoft Office Word MUI (English) 2007 12.0.4518.1014
Python 2.7.1 2.7.1150

```

Image 2.2.28: Psinfo.log

Psloggedon.log shows the currently logged on users and it also confirmed that two users were logged on at the time of live response.

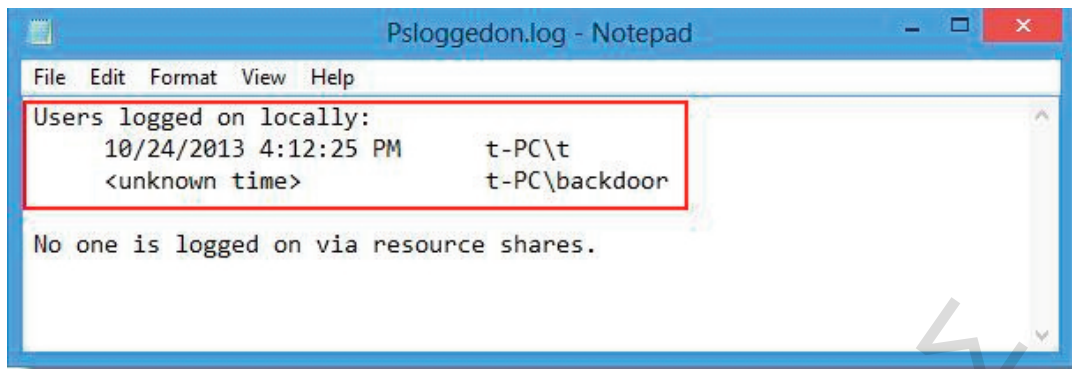


Image 2.2.29: Psloggedon.log

Pstasklist.log shows the running processes with threads and the execution state of the processes. The suspicious processes can be seen in this list too.

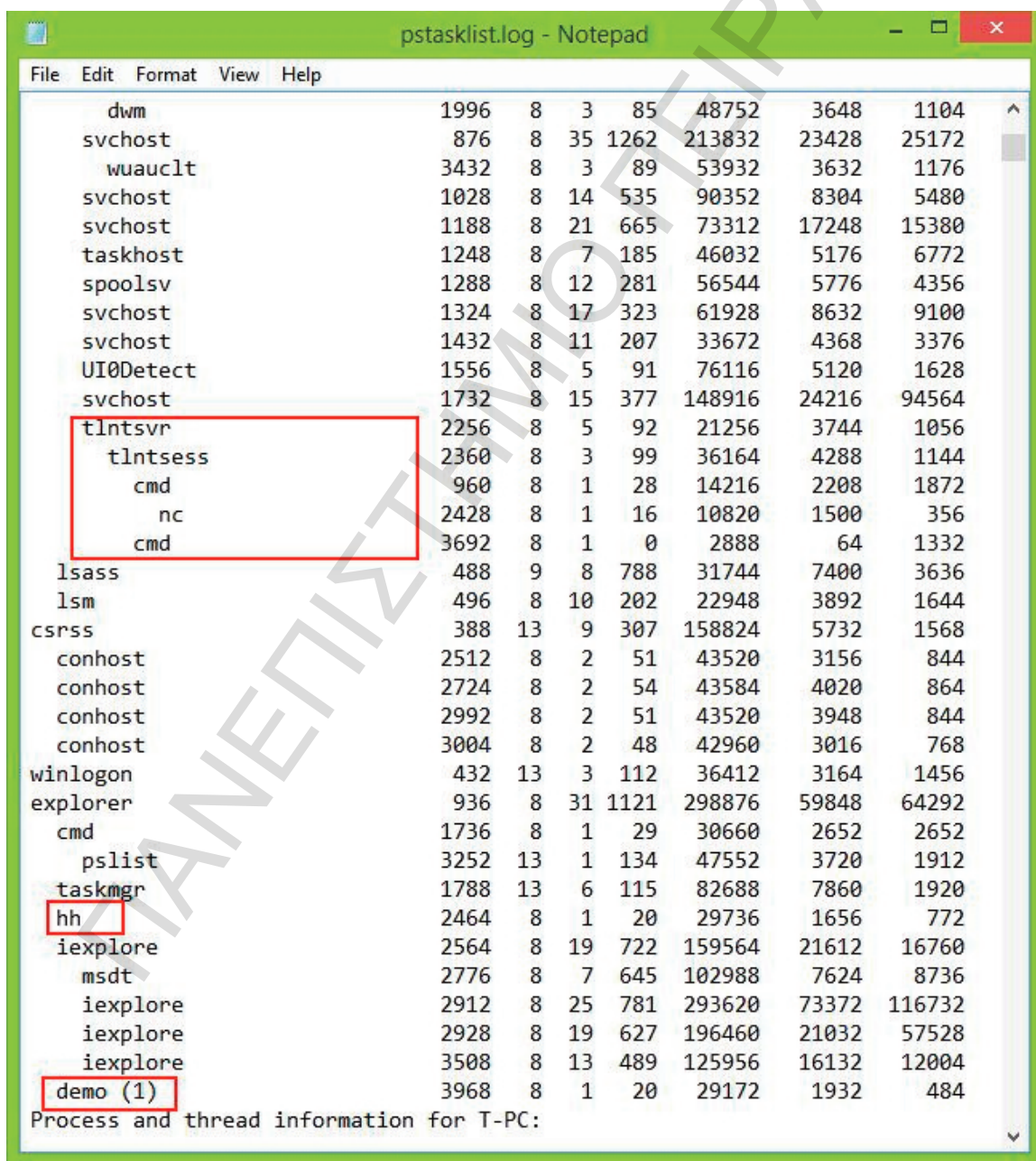
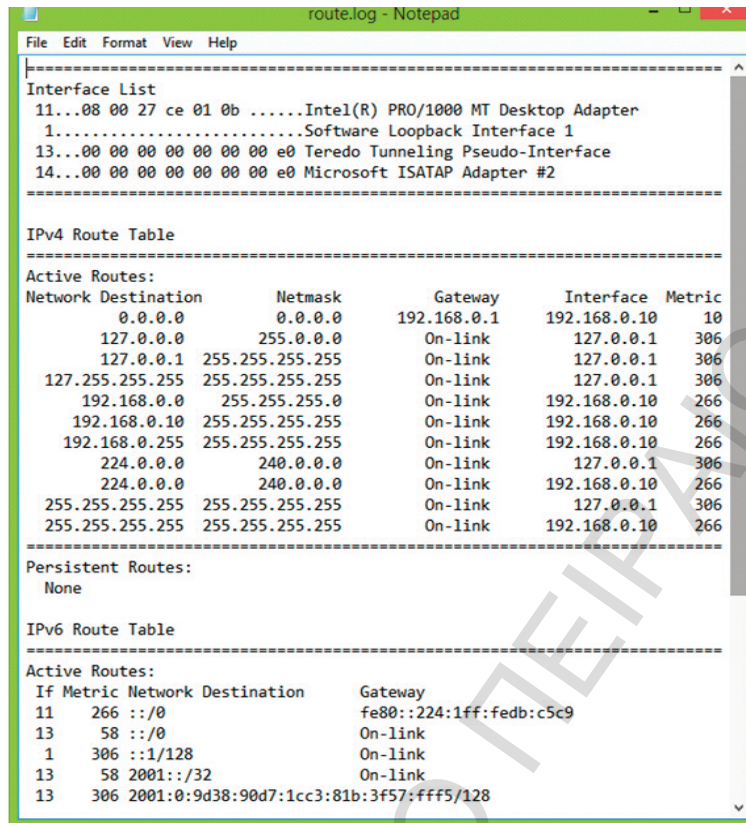


Image 2.2.30: Pstasklist.log

Route.log shows the routing table in the host. It is not showing any suspicious entry.



```

route.log - Notepad
File Edit Format View Help
-----
Interface List
11...08 00 27 ce 01 0b .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
14...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
-----

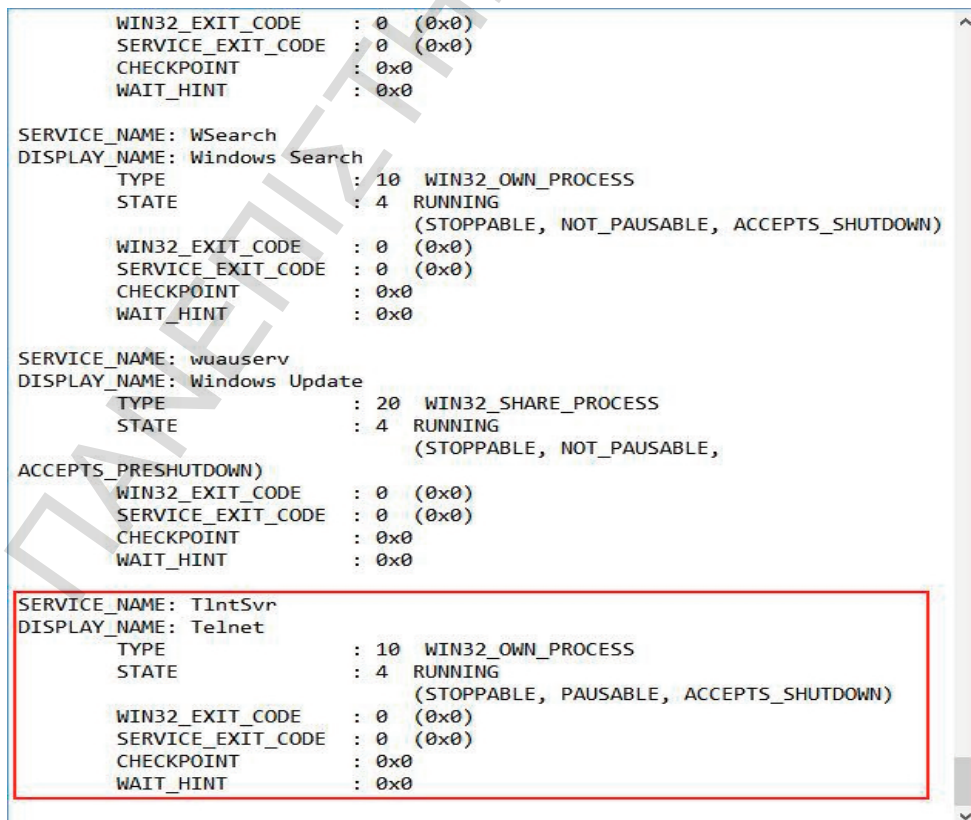
IPv4 Route Table
-----
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.0.1      192.168.0.10     10
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link          127.0.0.1        306
127.255.255.255           255.255.255.255 On-link          127.0.0.1        306
192.168.0.0                255.255.255.0    On-link          192.168.0.10     266
192.168.0.10              255.255.255.255 On-link          192.168.0.10     266
192.168.0.255             255.255.255.255 On-link          192.168.0.10     266
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          192.168.0.10     266
255.255.255.255           255.255.255.255 On-link          127.0.0.1        306
255.255.255.255           255.255.255.255 On-link          192.168.0.10     266
-----

Persistent Routes:
None

IPv6 Route Table
-----
Active Routes:
If Metric Network Destination      Gateway
11 266 ::/0                  fe80::224:1ff:fedb:c5c9
13 58 ::/0                    On-link
1 306 ::1/128                On-link
13 58 2001::/32              On-link
13 306 2001:0:9d38:90d7:1cc3:81b:3f57:fff5/128
  
```

Image 2.2.31: Route.log

Scquery.log displays the installed services and their status. Analysis shows the telnet service is enabled and running.



```

WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

SERVICE_NAME: WSearch
DISPLAY_NAME: Windows Search
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

SERVICE_NAME: wuauclt
DISPLAY_NAME: Windows Update
TYPE : 20 WIN32_SHARE_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE,
ACCEPTS_PRESHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

SERVICE_NAME: TlntSvr
DISPLAY_NAME: Telnet
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
  
```

Image 2.2.32: Scquery.log

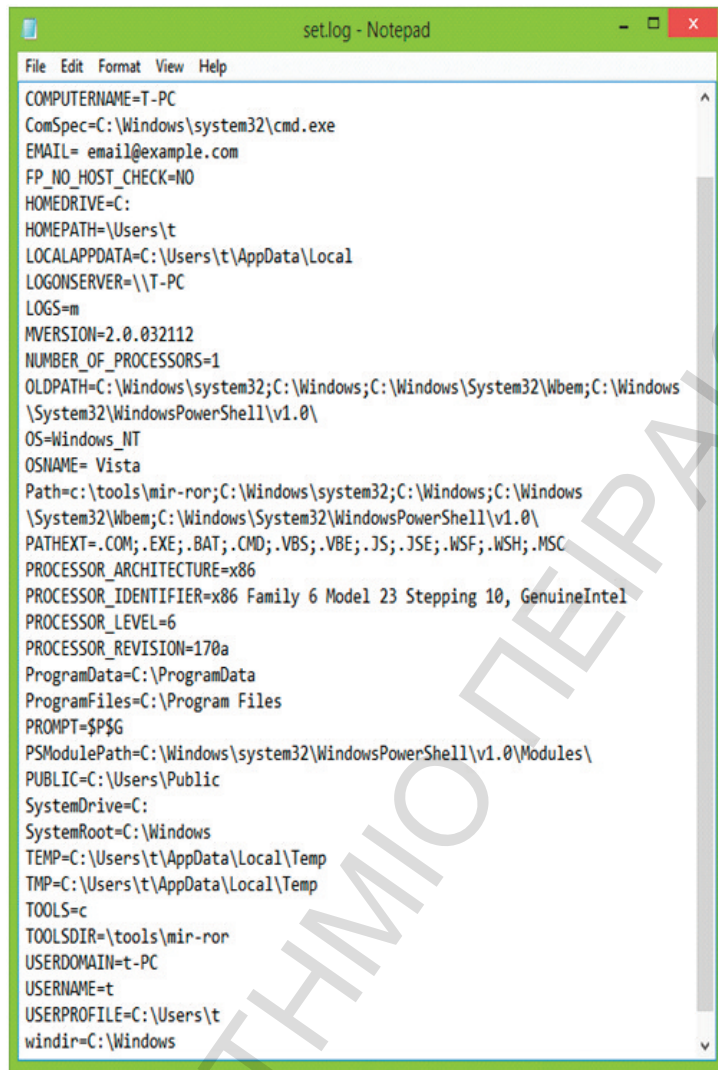
Schtasks.log displays the scheduled jobs which are set to run at predefined intervals / time an often are used in post exploitation stage to achieve persistence or hide activity by intruders. Analysis shows no signs of any such activity.



```
Folder: \  
HostName: T-PC  
TaskName: \GoogleUpdateTaskMachineCore  
Next Run Time: 10/25/2013 4:15:00 PM  
Status: Ready  
Logon Mode: Interactive/Background  
Last Run Time: 10/24/2013 4:15:00 PM  
Last Result: 0  
Author: t  
Task To Run: C:\Program Files\Google\Update  
\GoogleUpdate.exe /c  
Start In: N/A  
Comment: Keeps your Google software up to  
date. If this task is disabled or stopped, your Google software will not be  
kept up to date, meaning security vulnerabilities that may arise cannot be  
fixed and features may not work. This task uninstalls itself when the  
Scheduled Task State: Enabled  
Idle Time: Disabled  
Power Management:  
Run As User: SYSTEM  
Delete Task If Not Rescheduled: Enabled  
Stop Task If Runs X Hours and X Mins: Disabled  
Schedule: Scheduling data is not available in  
this format.  
Schedule Type: At logon time  
Start Time: N/A  
Start Date: N/A  
End Date: N/A  
Days: N/A  
Months: N/A  
Repeat: Every: N/A  
Repeat: Until: Time: N/A  
Repeat: Until: Duration: N/A  
Repeat: Stop If Still Running: N/A
```

Image 2.2.33: Schtasks.log

Set.log shows the state of environment variables.



```

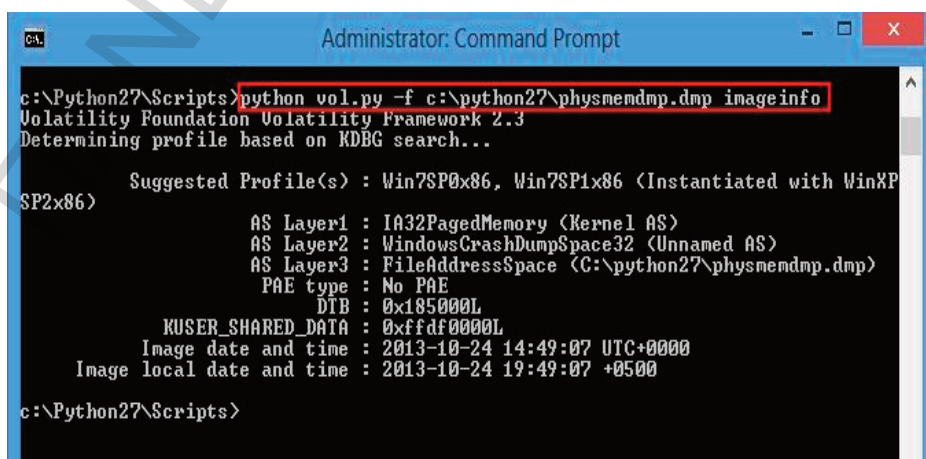
set.log - Notepad
File Edit Format View Help
COMPUTERNAME=T-PC
ComSpec=C:\Windows\system32\cmd.exe
EMAIL= email@example.com
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\t
LOCALAPPDATA=C:\Users\t\AppData\Local
LOGONSERVER=\\T-PC
LOGS=m
MVERSION=2.0.032112
NUMBER_OF_PROCESSORS=1
OLDPATH=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
OS=Windows_NT
OSNAME= Vista
Path=c:\tools\mir-ror;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=170a
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
PROMPT=$P$G
PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC=C:\Users\Public
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\t\AppData\Local\Temp
TMP=C:\Users\t\AppData\Local\Temp
TOOLS=c
TOOLS_DIR=\tools\mir-ror
USERDOMAIN=t-PC
USERNAME=t
USERPROFILE=C:\Users\t
windir=C:\Windows

```

Image 2.2.34: Set.log

2.3 Memory Analysis

Winpmem was used to create raw dump(.raw) and windows crash dump (.dmp) for the memory. These dumps were used with Volatility to find out any information from the memory. Imageinfo was used to acquire information about the memory dump.[5]



```

Administrator: Command Prompt
c:\Python27\Scripts>python vol.py -f c:\python27\physmemdmp.dmp image info
Volatility Foundation Volatility Framework 2.3
Determining profile based on KDBG search...

Suggested Profile(s) : Win7SP0x86, Win7SP1x86 <Instantiated with WinXP
SP2x86>
AS Layer1 : IA32PagedMemory (Kernel AS)
AS Layer2 : WindowsCrashDumpSpace32 (Unnamed AS)
AS Layer3 : FileAddressSpace (C:\python27\physmemdmp.dmp)
PAE type : No PAE
DTB : 0x185000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2013-10-24 14:49:07 UTC+0000
Image local date and time : 2013-10-24 19:49:07 +0500

c:\Python27\Scripts>

```

Image 2.3.1: Imageinfo

The hivelist command was used to list all the registry hives and their offsets.

```
c:\Python27\Scripts>python vol.py -f c:\python27\physmemdump.dmp --profile=Win7SP0x86 hivelist >>c:\forensic\hivelist.txt
Volatility Foundation Volatility Framework 2.3
```

Image 2.3.2: Hivelist

The result is shown below:

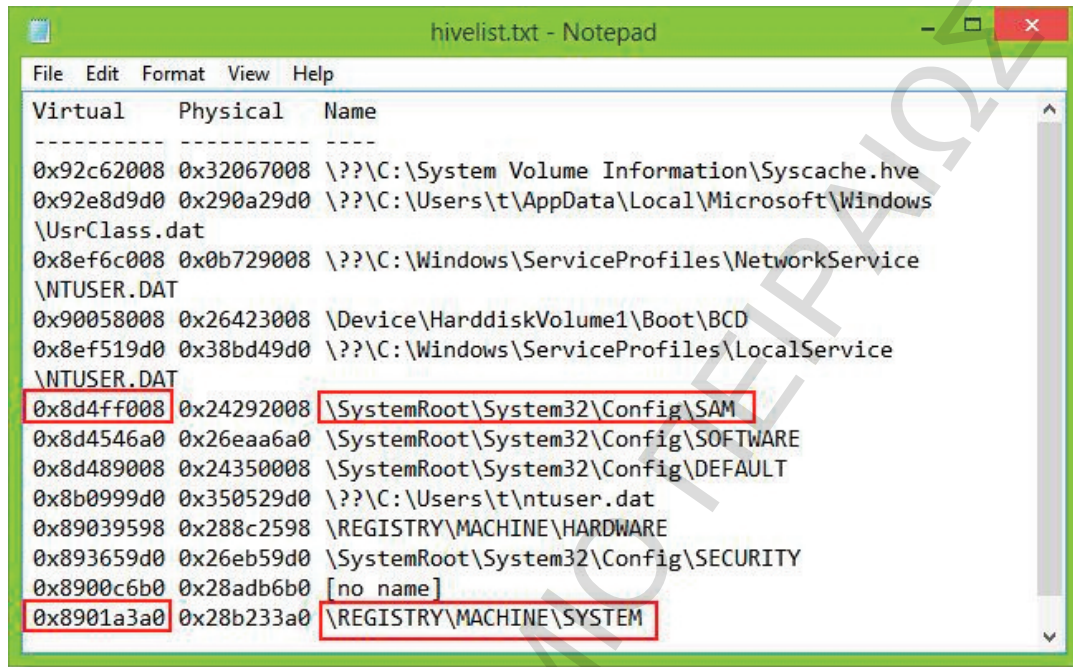


Image 2.3.3: Result if hivelist

The virtual address for SAM and SYSTEM hives will be used to get hash dump which are the credential hashes used by the Windows to authenticate users. These hashes can be used for implicit login through passing them through tools like Incognito etc.

```
c:\Python27\Scripts>python vol.py -f c:\python27\physmemdump.dmp --profile=Win7SP0x86 hashdump -y 0x8901a3a0 -s 0x8d4ff008 >>c:\forensic\hashdump.txt
Volatility Foundation Volatility Framework 2.3
```

Image 2.3.4: Get hash dump

The resultant hash dump is shown below which has hashes for 'T' and 'backdoor' user.

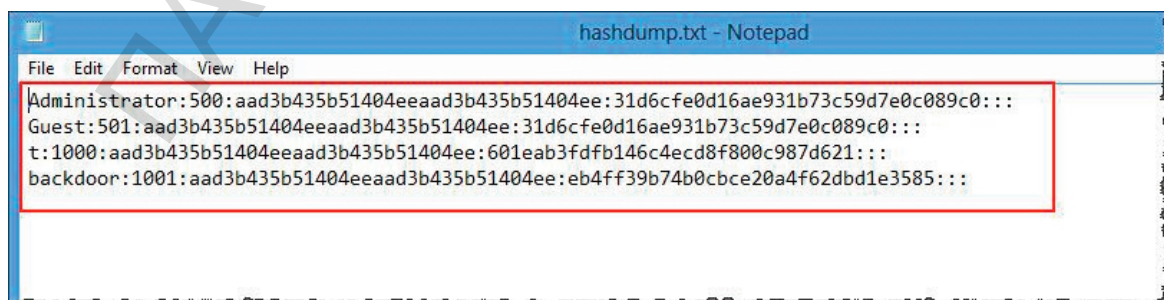


Image 2.3.5: Result of hash dump

Pstree command was used to get a list of processes as loaded in the memory.

```

Administrator: Command Prompt
c:\Python27\Scripts>python vol.py -f c:\python27\phymemdump.dmp --profile=Win7SP
0x86 pstree
Volatility Foundation Volatility Framework 2.3
Name                               Pid  PPid  Thds  Hnds  I
line
-----
.. 0x843df840:explorer.exe           936   964   31   1123  2
013-10-24 11:12:40 UTC+0000
.. 0x843d0400:deno C17.exe         3968  936    1    20  2
013-10-24 13:00:58 UTC+0000
.. 0x84383ac8:hh.exe                2464  936    1    20  2
013-10-24 11:13:33 UTC+0000
.. 0x84a3fac8:taskmgr.exe           1788  936    5   115  2
013-10-24 13:00:19 UTC+0000
.. 0x84cc3030:cmd.exe               1736  936    1    27  2
013-10-24 12:53:46 UTC+0000
.. 0x84b0e538:winpmen_1.4.exe       700   1736   1    21  2
013-10-24 14:49:03 UTC+0000
.. 0x84351528:ieexplorer.exe        2564  936   19   717  2
013-10-24 11:13:49 UTC+0000
.. 0x84509030:ieexplorer.exe        2928  2564   17   622  2
013-10-24 11:14:02 UTC+0000
.. 0x84a7d118:ieexplorer.exe        3508  2564   11   484  2
013-10-24 11:30:13 UTC+0000
.. 0x84440a58:ieexplorer.exe        2912  2564   24   772  2
013-10-24 11:14:01 UTC+0000
.. 0x8440aac0:msnbc.exe             2776  2564    7   645  2
013-10-24 11:23:37 UTC+0000
.. 0x8441ed40:chrome.exe            2548  936    0     0   2
013-10-24 11:13:48 UTC+0000
.. 0x85d08bf0:csrss.exe             388   368    9   337  2
013-10-24 11:06:37 UTC+0000
.. 0x84aa87b8:conhost.exe           2992  388    2    51  2
013-10-24 13:00:58 UTC+0000
.. 0x848cdd40:conhost.exe           2724  388    2    54  2
013-10-24 12:53:46 UTC+0000
.. 0x84538ab8:conhost.exe           2512  388    2    51  2
013-10-24 11:13:33 UTC+0000
.. 0x84d2b258:conhost.exe           3004  388    2    48  2
013-10-24 11:33:47 UTC+0000
.. 0x857a1030:winlogon.exe          432   368    3   112  2
013-10-24 11:06:40 UTC+0000
.. 0x84233bb0:System                 4     0    91   574  2
013-10-24 11:06:02 UTC+0000
.. 0x8521ed40:smss.exe              260    4     3    29  2
013-10-24 11:06:02 UTC+0000
.. 0x85747d40:csrss.exe             332   324   10   482  2
013-10-24 11:06:10 UTC+0000
.. 0x85b64168:wininit.exe           376   324    3    76  2
013-10-24 11:06:37 UTC+0000
.. 0x8505d150:services.exe          476   376    7   194  2
013-10-24 13:06:42 UTC+0000
.. 0x85b56190:spoolsv.exe           1288  476   12   281  2
013-10-24 11:07:02 UTC+0000
.. 0x8443d750:UIDetect.exe          1556  476    5    91  2
013-10-24 11:11:11 UTC+0000
.. 0x85c195c8:svchost.exe           1432  476   11   207  2
013-10-24 11:07:04 UTC+0000
.. 0x8599ead0:svchost.exe           1028  476   12   515  2
013-10-24 11:06:59 UTC+0000
.. 0x850fc350:svchost.exe           688   476    7   266  2
013-10-24 11:06:52 UTC+0000
.. 0x85ae98d8:svchost.exe           1188  476   21   670  2
013-10-24 11:07:01 UTC+0000
.. 0x84350648:spssvc.exe            552   476    4   149  2
013-10-24 11:09:13 UTC+0000
.. 0x85b80030:svchost.exe           1324  476   18   318  2
013-10-24 11:07:02 UTC+0000
.. 0x844569a0:SearchIndexer..       188   476   14   657  2
013-10-24 11:09:23 UTC+0000
.. 0x8443fd40:svchost.exe           1732  476   15   365  2
013-10-24 11:09:21 UTC+0000
.. 0x85940980:svchost.exe           848   476   17   446  2
013-10-24 11:06:57 UTC+0000
.. 0x843e1030:dwm.exe               1996  848    3    85  2
013-10-24 11:12:39 UTC+0000
.. 0x84d8e2c8:cmd.exe               2256  476    5    90  2
013-10-24 13:15:26 UTC+0000
.. 0x84410040:taskhost.exe          1248  476    7   185  2
013-10-24 11:12:25 UTC+0000

```

Image 2.3.6: Pstree

The PIDs for four processes of Internet Explorer (ieexplorer) were used to run iehistory command to get internet history and record of pages visited.

```

c:\Python27\Scripts>python vol.py -f c:\python27\phymemdump.dmp --profile=Win7SP0x86 iehistory >>c:\forensic\iehistory.txt
Volatility Foundation Volatility Framework 2.3

```

Image 2.3.7: Iehistory

The important results are shown below.

```

*****
Process: 1732 svchost.exe
Cache type "URL " at 0x7e60880
Record length: 0x300
Location: https://mail.google.com/_/scs/mail-
static/_/js/k=gmail.main.en.LTHDwu13yCs.O/m=sy333,sy320,sy380,sy389,sy392,sy391,sy588,sy589,sy324,sy332,sy334,sy381,sy382,
sy359,sy390,mo,sy321,sy570,cc,sy591,sy593,sy592,sy594,sy595,sy599,sy326,sy476,sy569,sy587,cw,sy596,sy597,sy598,sy601,yj/am
=fAEcTAoZa4dAGAZ2sJ9Q-u9_dln8BC2rSpQHECoAgZ3gafYkKH7gg7IDDA/rt=j/rs=AItrSTNR-z20Ygy04ZQ-WyEGioEG52h3xw
Last modified: 2013-10-17 10:11:35 UTC+0000
Last accessed: 2013-10-24 11:25:09 UTC+0000
File Offset: 0x300, Data Offset: 0x1e8, Data Length: 0x214
File: rs=AItrSTNR-z20Ygy04ZQ-WyEGioEG52h3xw[7]
Data: HTTP/1.1 200 OK
Content-Type: text/javascript; charset=UTF-8
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Alternate-Protocol: 443:quic
Content-Length: 465370
*****
Process: 1732 svchost.exe
Cache type "URL " at 0x7f8e200
Record length: 0x300
Location: https://www.amazon.com/gp/rate-it/ref=ysh_auto_redirect?ie=UTF8&hasNoRecs=1
Last modified: 1970-01-01 00:00:00 UTC+0000
Last accessed: 2013-10-24 11:18:13 UTC+0000
File Offset: 0x300, Data Offset: 0xb4, Data Length: 0xd4
File: ref=ysh_auto_redirect[1].htm
Data: HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
x-amz-id-1: 0EYW9256GQ55D3APM19T
p3p: policyref="http://www.amazon.com/w3c/p3p.xml",CP="CAO DSP LAW CUR ADM IVAo IVDo CONo OTPo OUR DELi PUBi OTRi BUS PHY
ONL UNI PUR FIN COM NAV INT DEM CNT STA HEA PRE LOC GOV OTC "
x-xss-protection: 1
x-amz-id-2: qsvgiV/P7VGRWmdgxX66PnWQaCRdlePprrd0/ssfJluBqGrFaLG9/kSydFc0mxnP
Vary:User-Agent
-----
Process: 936 explorer.exe
Cache type "URL " at 0x1996200
Record length: 0x200
Location: http://res2.windows.microsoft.com/Resources/3.6/WOL/shared/images/favicon.ico
Last modified: 2012-08-27 21:21:50 UTC+0000
Last accessed: 2013-01-18 17:37:51 UTC+0000
File Offset: 0x200, Data Offset: 0xb8, Data Length: 0xc8
File: favicon[1].ico
Data: HTTP/1.1 200 OK
Content-Type: image/x-icon
ETag: "06ba4f89984cd1:0"
X-Powered-By: ASP.NET
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
Content-Length: 7886
-----
~U:t
*****
Process: 936 explorer.exe
Cache type "URL " at 0x19b5180
Record length: 0x100
Location: Visited: t@http://debugger.immunityinc.com/favicon.ico
Last modified: 2013-10-24 11:14:30 UTC+0000
Last accessed: 2013-10-24 11:14:30 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa0
-----

```

```

*****
Process: 936 explorer.exe
Cache type "URL " at 0x19b5b80
Record length: 0x180
Location: Visited: t@https://login.yahoo.com/config/login_verify2?&.src=ym&.intl=us
Last modified: 2013-10-24 11:23:08 UTC+0000
Last accessed: 2013-10-24 11:23:08 UTC+0000
File Offset: 0x180, Data Offset: 0x0, Data Length: 0xb4
*****

Process: 2564 iexplore.exe
Cache type "URL " at 0x1145a00
Record length: 0x180
Location: Visited: t@https://www.amazon.com/gp/css/account/cards/view.html?ie=UTF8&ref_=_ya_add_cc&viewID=addCard
Last modified: 2013-10-24 11:18:52 UTC+0000
Last accessed: 2013-10-24 11:18:52 UTC+0000
File Offset: 0x180, Data Offset: 0x0, Data Length: 0xd0
*****

```

Image 2.3.8: Iehistory Results

The netscan command was used to trace network connections in the memory.

```

c:\Python27\Scripts>python vol.py -f c:\python27\physmem.dmp --profile=Win7SP0x86 yarascan -p 2912 -Y "/^4[0-9]{12}<?:[0-9]{3}>?$/
Volatility Foundation Volatility Framework 2.3

```

Image 2.3.9: Netscan

The results confirmed earlier findings related to open tcp sockets.

```

netscan.txt - Notepad
File Edit Format View Help
0x3f6e35d0 TCPv4 0.0.0.0:23 0.0.0.0:0
LISTENING 2256 tIntsvr.exe
0x3f6e35d0 TCPv6 :::23 :::0
LISTENING 2256 tIntsvr.exe
0x7bc008 TCPv4 192.168.0.10:49895 173.194.35.125:443
ESTABLISHED 2912 iexplore.exe
0x3e428858 TCPv4 192.168.0.10:49571 204.79.197.200:80
CLOSED 2928 iexplore.exe
0x3f20fb78 TCPv4 192.168.0.10:49928 173.194.35.125:443
ESTABLISHED 2912 iexplore.exe
0x3f2464c8 TCPv4 192.168.0.10:49166 192.168.0.10:80
CLOSED 2464 hh.exe
0x3f44cb48 TCPv4 192.168.0.10:49166 192.168.0.10:80
SYN_SENT 2464 hh.exe
0x3f553df8 TCPv4 192.168.0.10:49575 207.46.194.1:80
CLOSED 2928 iexplore.exe
0x3f60ddf8 TCPv4 192.168.0.10:49578 131.253.40.50:80
CLOSED 2928 iexplore.exe
0x3f6be9d0 TCPv6 fe80::21b7:c7ce:506d:22c6:49926
fe80::9538:6517:9fc5:1cb6:445 ESTABLISHED 4 System
0x3f70b650 TCPv4 -:49930 173.194.39.53:443
CLOSED 2912 iexplore.exe
0x3f7a2808 TCPv4 192.168.0.10:49923 173.194.35.125:443
CLOSED 2912 iexplore.exe
0x3f8ded38 TCPv4 192.168.0.10:49570 204.79.197.200:80
CLOSED 2928 iexplore.exe
0x3f99b668 TCPv4 192.168.0.10:49166 192.168.0.10:80
CLOSED 2464 hh.exe
0x3f9b8c48 TCPv4 192.168.0.10:49166 192.168.0.10:80
CLOSED 2464 hh.exe
0x3f9e6b10 TCPv4 192.168.0.10:49576 131.253.34.142:80
CLOSED 2928 iexplore.exe
0x3f9fd560 TCPv4 192.168.0.10:49579 82.178.158.19:80
CLOSE_WAIT 2928 iexplore.exe
0x3e029008 UDPv4 0.0.0.0:3702 *:*
1432 svchost.exe 2013-10-24 11:07:25 UTC+0000
0x3e029008 UDPv6 :::3702 *:*
1432 svchost.exe 2013-10-24 11:07:25 UTC+0000

```

Image 2.3.10: Opentcp sockets (netscan)

Yarascan is a useful tool to search for string and patterns inside the memory. It supports the use of regular expressions as search rules. It was used to look for email addresses and credit card numbers etc as various email service links and amazon.com link was found in internet explorer history. [6]

```
c:\Python27\Scripts>python vol.py -f c:\python27\physmem.dmp --profile=Win7SP0x86 yarascan -p 2912 -Y "/^4[0-9]{12}<?:[0-9]{3}>?5/"
Volatility Foundation Volatility Framework 2.3
```

Image 2.3.11: Yarascan

The regular expression used to identify credit card numbers is shown below.[7, 8]

```
^(?:4[0-9]{12}(?:[0-9]{3})? | 5[1-5][0-9]{14} | 3[47][0-9]{13} | 3(?:0[0-5]|68|[0-9])[0-9]{11}|6(?:011|5[0-9]{2})[0-9]{12} | (?:2131|1800|35\d{3})\d{11})$
```

Image 2.3.12: Regular expression(credit cards)

The results reveal presence of a credit card numbers in memory.

```
Rule: r1
Owner: Process iexplore.exe Pid 2912
0x0496b2a4 3d 34 37 39 37 36 36 30 30 30 30 31 34 32 32 35 =479766000014225
0x0496b2b4 37 26 63 61 72 64 2d 6e 61 6d 65 3d 66 6f 72 65 7&card-name=fore
0x0496b2c4 6e 73 69 63 5f 74 65 73 74 26 6e 65 77 43 72 65 nsic_test&newCre
0x0496b2d4 64 69 74 43 61 72 64 4d 6f 6e 74 68 3d 30 31 26 ditCardMonth=01&
Rule: r1
Owner: Process iexplore.exe Pid 2912
0x0496cbbc 3d 34 37 39 37 36 36 30 30 30 30 31 34 32 32 35 =479766000014225
0x0496cbcc 37 26 63 61 72 64 2d 6e 61 6d 65 3d 66 6f 72 65 7&card-name=fore
0x0496cbdc 6e 73 69 63 5f 74 65 73 74 26 6e 65 77 43 72 65 nsic_test&newCre
0x0496cbec 64 69 74 43 61 72 64 4d 6f 6e 74 68 3d 30 31 26 ditCardMonth=01&
Rule: r1
Owner: Process iexplore.exe Pid 2912
0x0780a616 3d 34 37 39 37 36 36 30 30 30 30 31 34 32 32 35 =479766000014225
0x0780a626 37 26 63 61 72 64 2d 6e 61 6d 65 3d 66 6f 72 65 7&card-name=fore
0x0780a636 6e 73 69 63 5f 74 65 73 74 26 6e 65 77 43 72 65 nsic_test&newCre
0x0780a646 64 69 74 43 61 72 64 4d 6f 6e 74 68 3d 30 31 26 ditCardMonth=01&
```

Image 2.3.13: Results (Credit cards)

Likewise email addresses were searched using following command.[7]

```
c:\Python27\Scripts>python vol.py -f c:\python27\physmem.dmp --profile=Win7SP0x86 yarascan -p 2912,2564,2928,3508 -Y "[a-zA-Z0-9\-\+@+{a-zA-Z0-9}
prensic\email.txt
```

Image 2.3.14: Email addresses command

The email addresses found are shown below.


```

0x05436697 70 72 65 6d 69 75 6d 2d 73 65 72 76 65 72 40 74 premium-server@
0x054366a7 68 61 77 74 65 2e 63 6f 6d 30 1e 17 0d 39 36 30 hawte.com0...960
0x054366b7 38 30 31 30 30 30 30 30 30 5a 17 0d 32 30 31 32 8010000007..2012
0x054366c7 33 31 32 33 35 39 35 39 5a 30 81 ce 31 0b 30 09 31235959Z0..1.0.
P...n1

Owner: Process iexplore.exe Pid 2564
0x054c8adc 43 50 53 2d 72 65 71 75 65 73 74 73 40 76 65 72 CPS-requests@ver
0x054c8aec 69 73 69 67 6e 2e 63 6f 6d 3b 20 6f 72 0a 62 79 isign.com;.or.by
0x054c8afc 20 6d 61 69 6c 20 61 74 20 56 65 72 69 53 69 67 .mail.at.Verisig
0x054c8b0c 6e 2c 20 49 6e 63 2e 2c 20 32 35 39 33 20 43 6f n,.Inc.,.2593.Co

Owner: Process iexplore.exe Pid 2912
0x0032c297 67 73 65 63 72 65 70 6f 72 74 31 32 33 40 67 6d gsecreport123@gm
0x0032c2a7 61 69 6c 2e 63 6f 6d 2f 39 32 36 39 36 32 3b 20 ail.com/926962;.
0x0032c2b7 6a 69 64 3d 67 73 65 63 72 65 70 6f 72 74 31 32 jid=gsecreport12
0x0032c2c7 33 40 67 6d 61 69 6c 2e 63 6f 6d 2f 39 32 36 39 3@gmail.com/9269

Owner: Process iexplore.exe Pid 2928
0x04638788 69 6c 40 79 61 68 6f 6f 2d 65 6d 61 69 6c 2e 63 il@yahoo-email.c
0x04638798 6f 6d 22 2c 22 78 61 70 70 61 72 65 6e 74 6c 79 om","xapparently
0x046387a8 74 6f 22 3a 22 79 5f 73 65 63 31 32 33 40 79 61 to":"y_sec123@ya
0x046387b8 68 6f 6f 2e 63 6f 6d 22 7d 2c 22 66 6c 61 67 73 hoo.com"},"flags

```

Image 2.3.14: Email addresses results

2.4 Disk Imaging and Registry copy

dd is an effective, powerful and simple tool for disk imaging. It can image a disk block by block including those which apparently are not being used for data storage by the file system. This fulfills the important forensics requirements and even the data belonging to deleted files and the slack space is also available for analysis and evidence retrieval. It also provides for automatic generation of MD5 hashes of the image along with the image. The machine used for forensic analysis in this research was actually a Virtual machine hosted in Oracle Virtual Box. The VM was using a .vdi based hard disk. This disk was imaged using dd tool from the SANS SIFT workstation.

We must mention though that we can use dcfldd tool(nowdays use more) which is the same tool as dd but with some extra features(Hashing on-the-fly, status output, Flexible disk wipes, etc). [9, 10]

```

root@SIFT-Workstation:/home/sansforensics/Desktop/VMware-Shared-Drive/win7# dd if="win7.vdi" bs=4K conv=sync,noerror | tee win7.img | md5sum > win7.md5
1792794+0 records in
1792794+0 records out
7343284224 bytes (7.3 GB) copied, 2847.76 s, 2.6 MB/s
root@SIFT-Workstation:/home/sansforensics/Desktop/VMware-Shared-Drive/win7#

```

Image 2.4.1: dd tool

The MD5 hash generated is shown below. This hash will be used to verify the integrity of this image at the time of analysis.

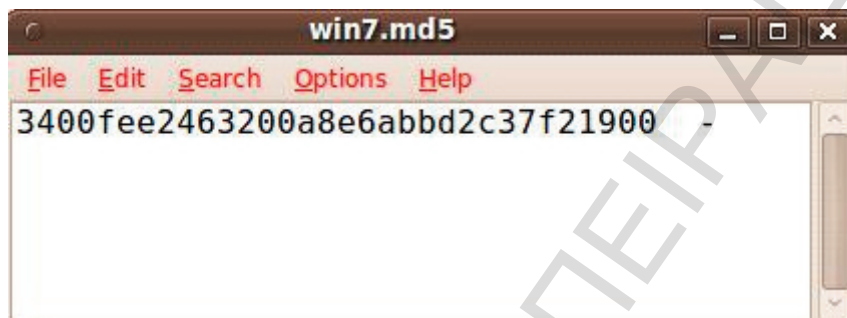


Image 2.4.2: MD5 hash

This image was later copied as Forensicbase.img for analysis purposes.

Extraction of Registry Hive Extraction of Registry Hives: Mirror incident response script does include ntfscopy, which is used to copy the complete registry hives from the target system.

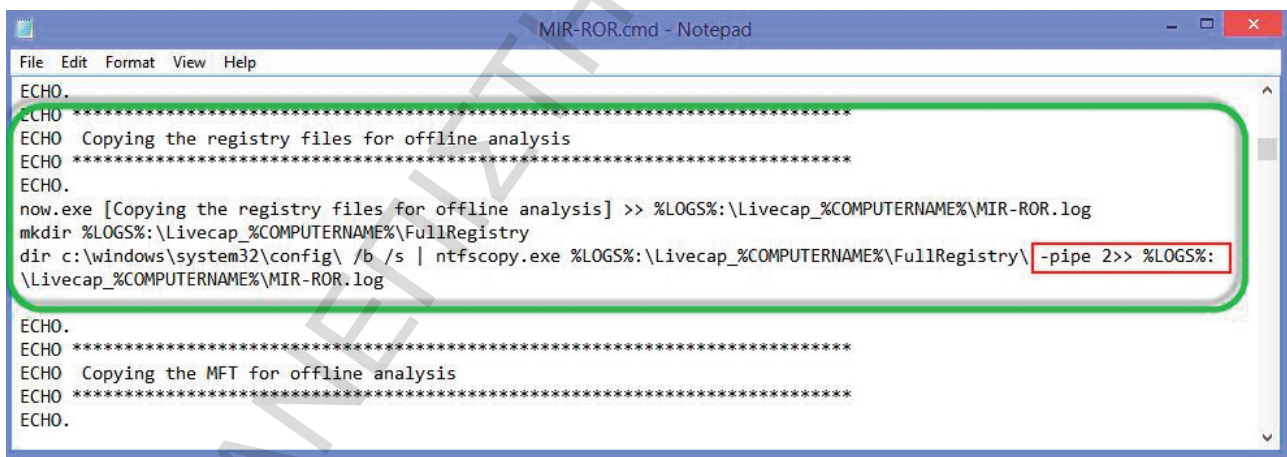


Image 2.4.3: Extraction of Registry Hive

But the ntfscopy tool requires a commercial license for the use of pipe option and hence the registry hives were not copied during the incident response. As an alternative the registry hives were extracted from the dd image using SANS SIFT autopsy browser. The registry hives are located in %SYSTEMROOT%\system32\config directory except NTUSER.DAT hive which is located in %USERPROFILE% folder.

Similarly SECURITY registry hive was also exported from the same directory.



Image 2.4.7: Security registry hive export

SOFTWARE and SYSTEM hives were also located from the same folder and extracted.

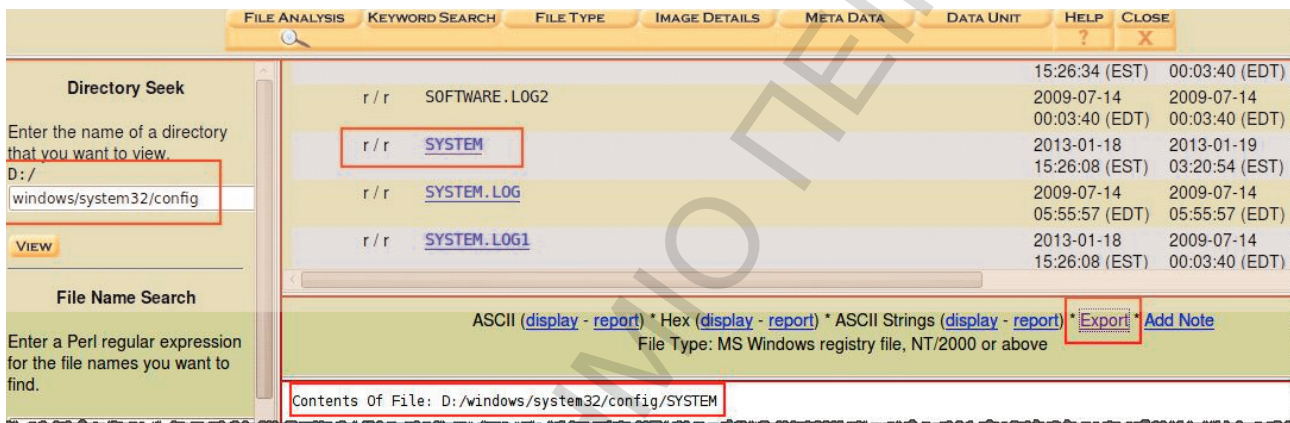


Image 2.4.8: Software and system hives export

For NTUSER.DAT registry hive Directory Seek path of Users was given and searched. The user profile of 'T' user was looked into and the required hive was located and exported.

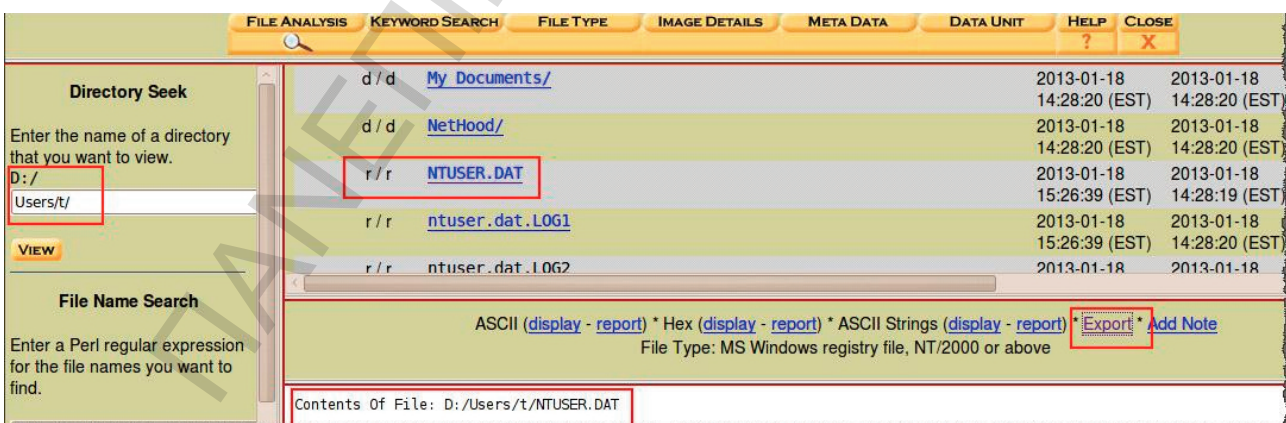


Image 2.4.9: NTUSER.DAT registry hive export

These hives were analyzed using regripper tool (described in a later section).

2.5 SANS SIFT ANALYSIS

SANS SIFT workstation provides comprehensive open source tools for carrying out forensics analysis which include autopsy browser etc.[11]

The disk image was analyzed using autopsy browser in SIFT workstation. A new case was created using the interface of autopsy.

Image 2.5.1: SIFT – Autopsy new case

Then a new host was created for analysis.

Image 2.5.2: Autopsy new host

The options were set especially the time settings so that necessary timelines can be effectively created and analysed.

ADD A NEW HOST

- Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
- Description:** An optional one-line description or note about this computer.
- Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
- Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
- Path of Alert Hash Database:** An optional hash database of known bad files.

Image 2.5.3: Autopsy options

The acquired image file was added to the case.

Adding host: host1 to case forensics_task

Host Directory (/forensics/forensics_task/host1/) created
 Configuration file (/forensics/forensics_task/host1/host.aut) created
 We must now import an image file for this host

ADD IMAGE

Case: forensics_task
Host: host1

No images have been added to this host yet
 Select the Add Image File button below to add one

Image 2.5.4: Add image to the case

The disk image was added to the case and its MD5 hash calculated so that integrity of the image can be confirmed by matching it with the hash taken at the time of image acquisition.



Image 2.5.5: Autopsy Calculate md5

Two NTFS partitions were found inside the image.

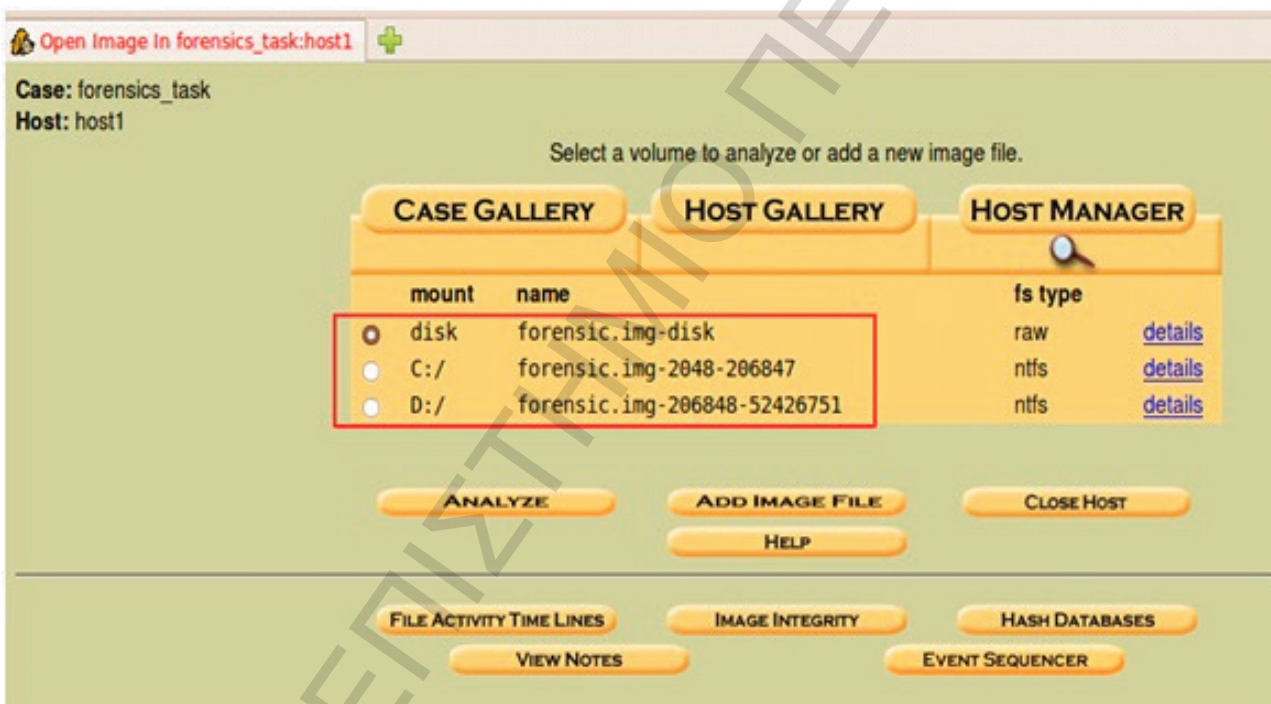


Image 2.5.6: NTFS partitions

File activity time lines were created and analysed.

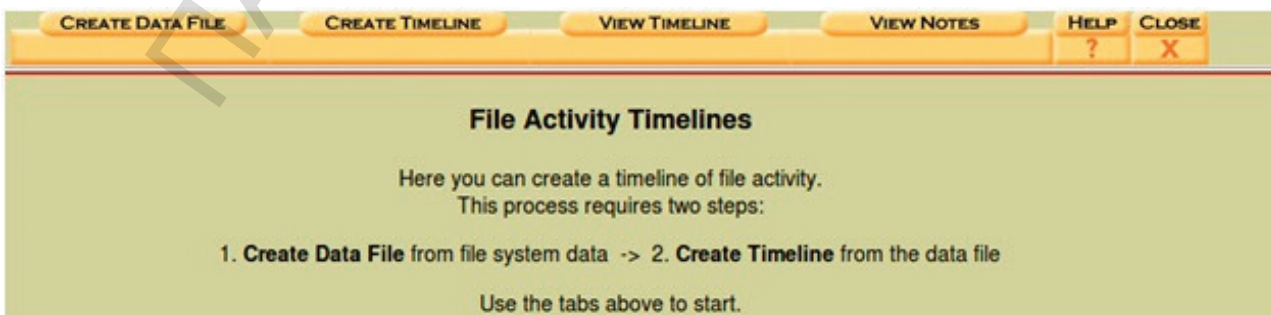


Image 2.5.7: Autopsy File activity timeline

First the data file was created as a pre requisite to the creation of time line.

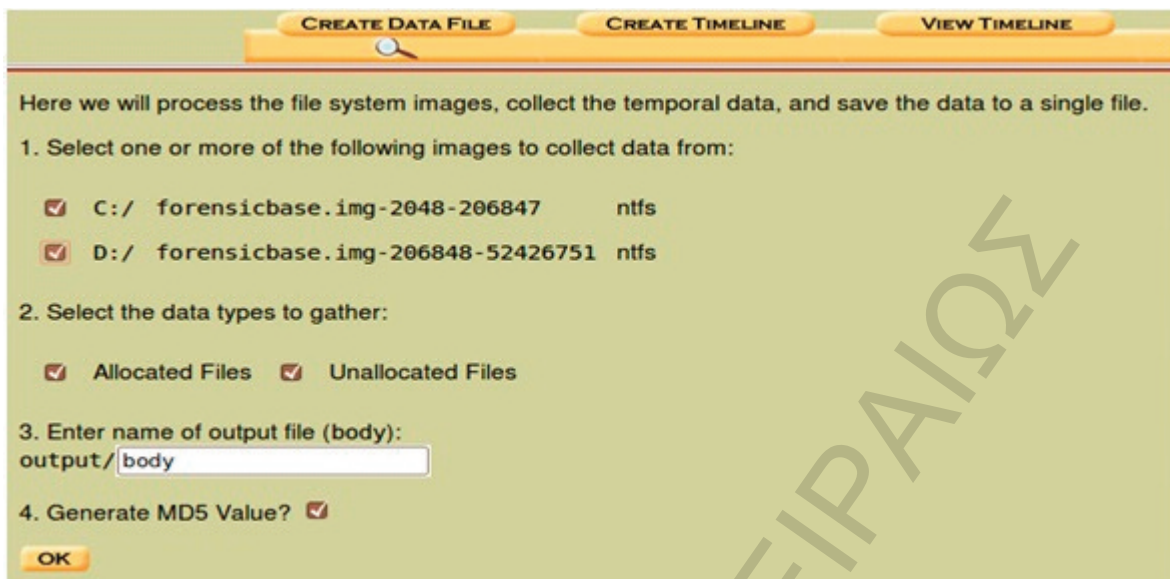


Image 2.5.8: Data file creation

The output/body data file can be assigned any name.

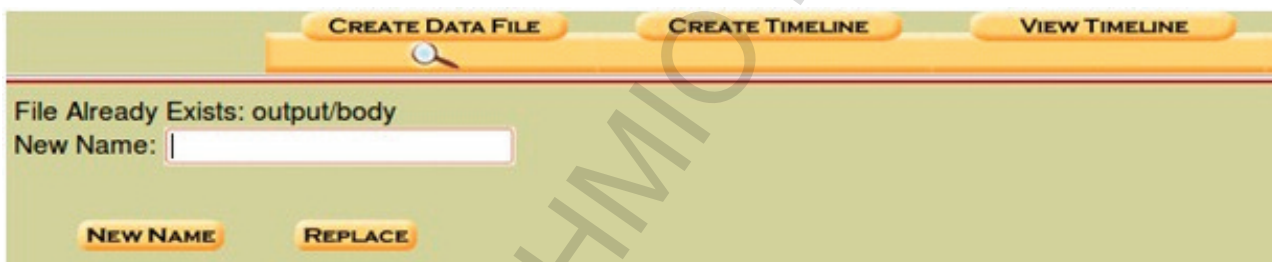


Image 2.5.9: Assign name output/body

After the data file is created then the time line creation tool is run so that the relative creation and modification times of various files can be analyzed to track any suspicious activities.

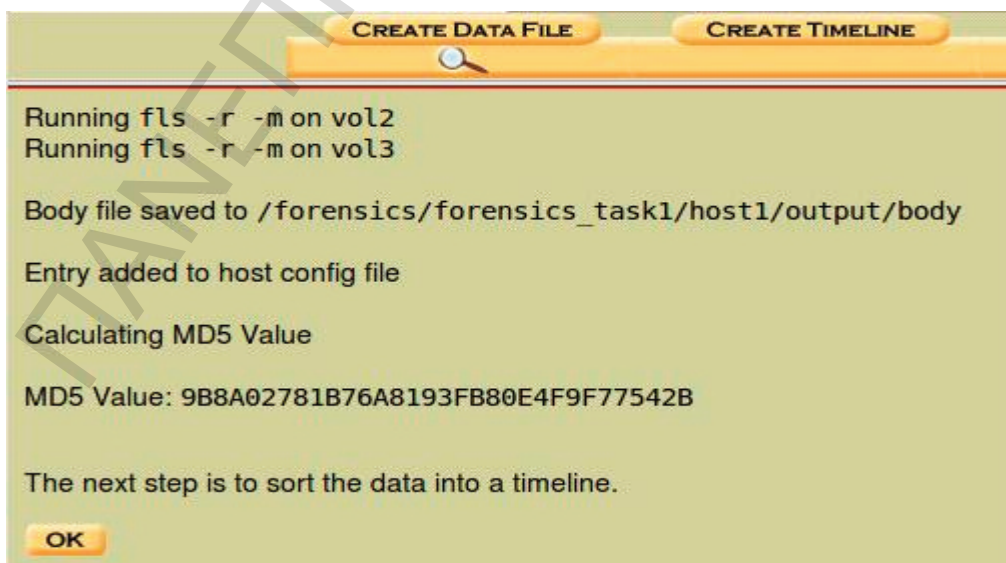


Image 2.5.10: Timeline creation tool

The timeline creation tool allows for setting the start and end dates (depending on the period of interest) and can also be generated in a csv format to be exported to some database also.

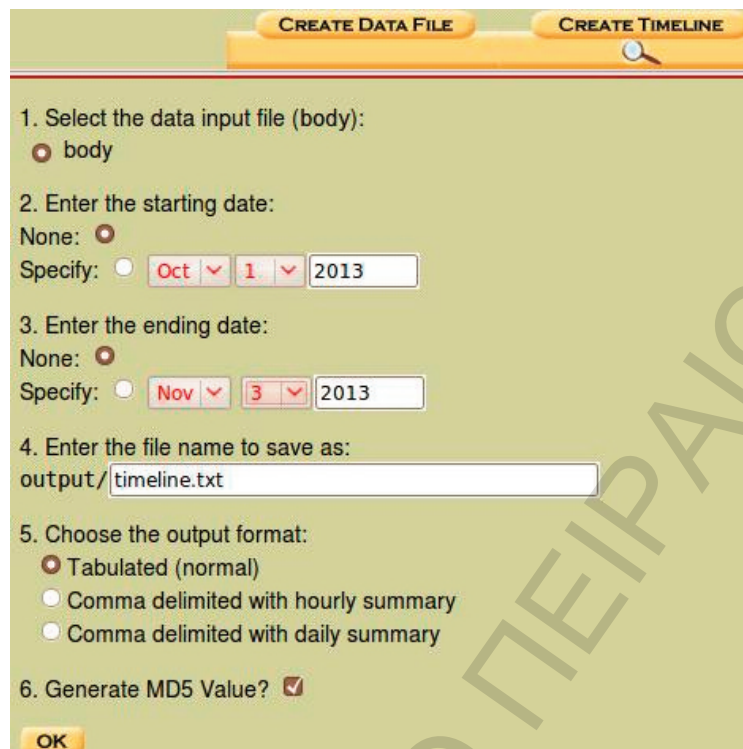


Image 2.5.11: Example of timeline tool

The time line thus created can be viewed in a text editor also.

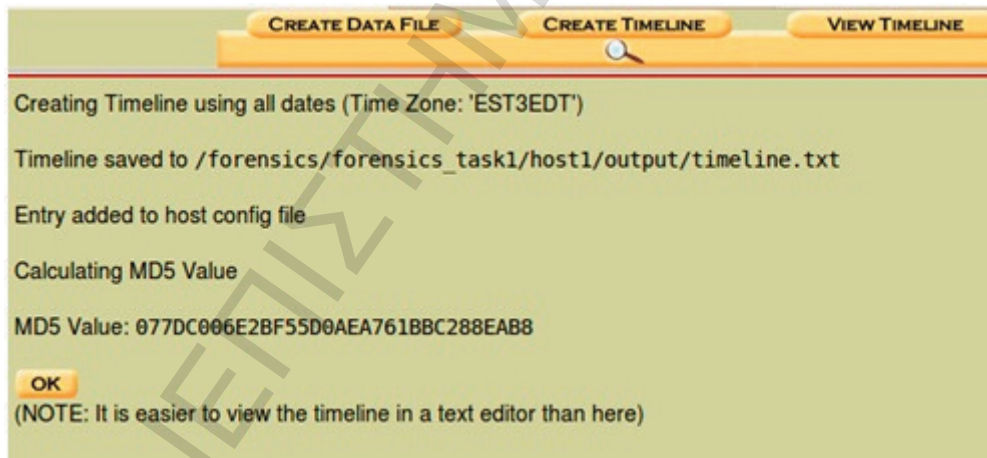


Image 2.5.12: Timeline text editor option

Timeline file was analyzed in text editor

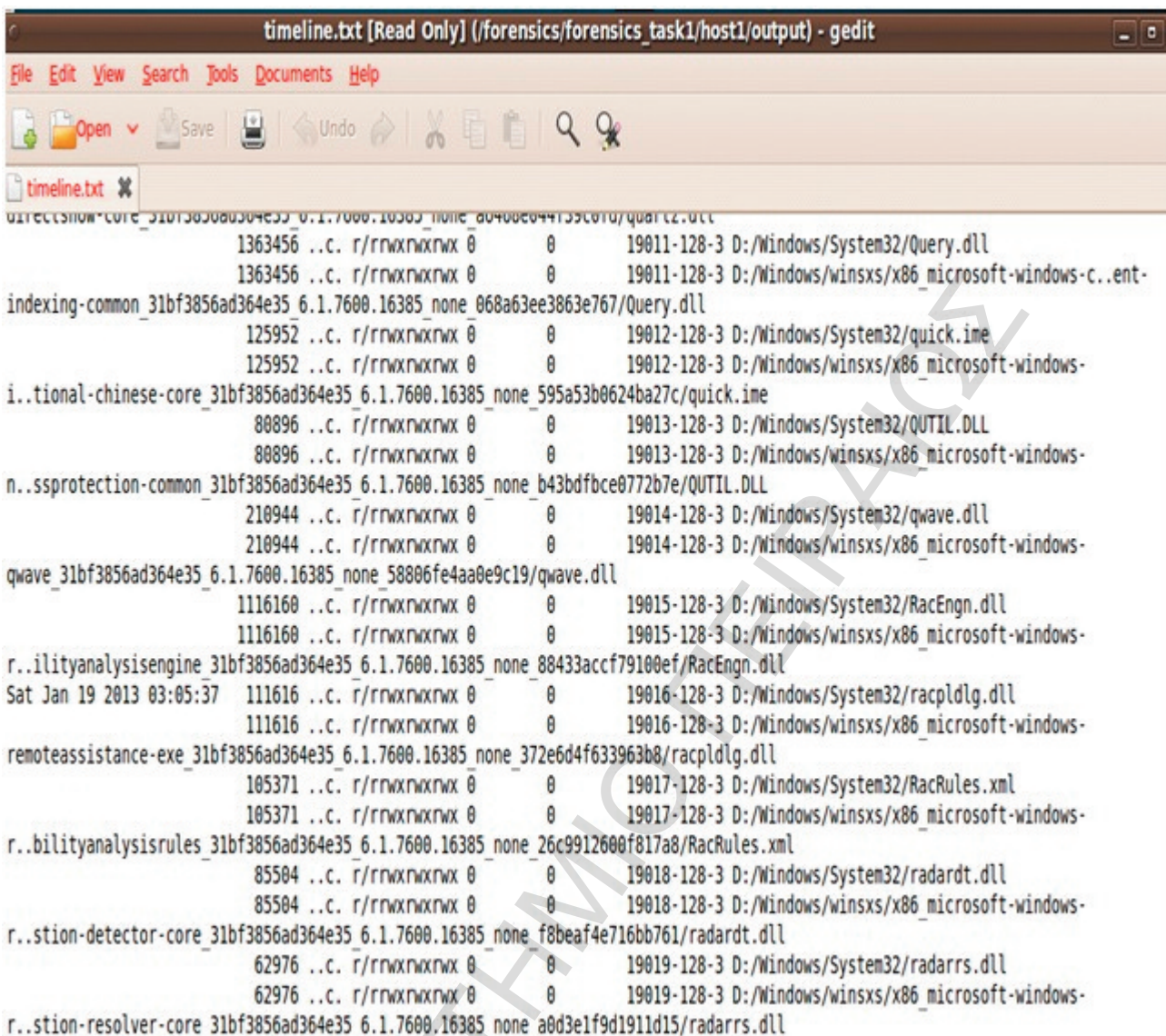


Image 2.5.13: Analyze timeline in text editor

The autopsy browser also allows for searching string in the disk image and also allows for file analysis using the types of file found and viewing them.

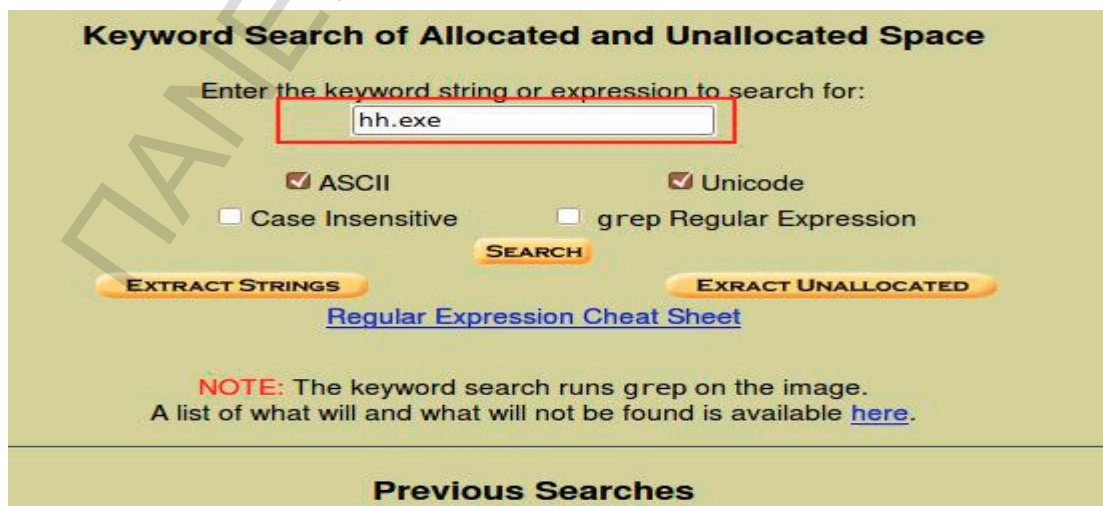


Image 2.5.14: Searching string in disk image

File analysis also allows for browsing and viewing the files.

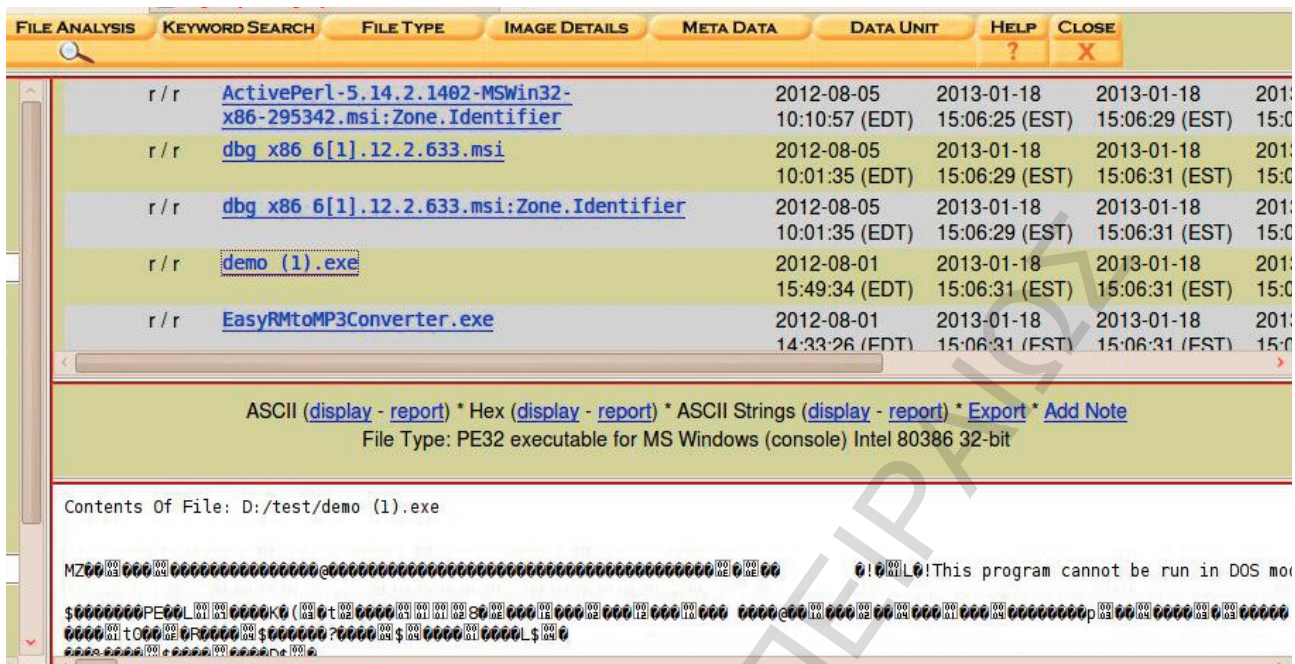


Image 2.5.15: Browsing and viewing the files

2.6 Registry Analysis

Regripper was used to analyze the registry hives acquired from the disk of the target host. Analysis of SAM hive from %WINDIR%\system32\config\SAM provided following results.[12, 13]

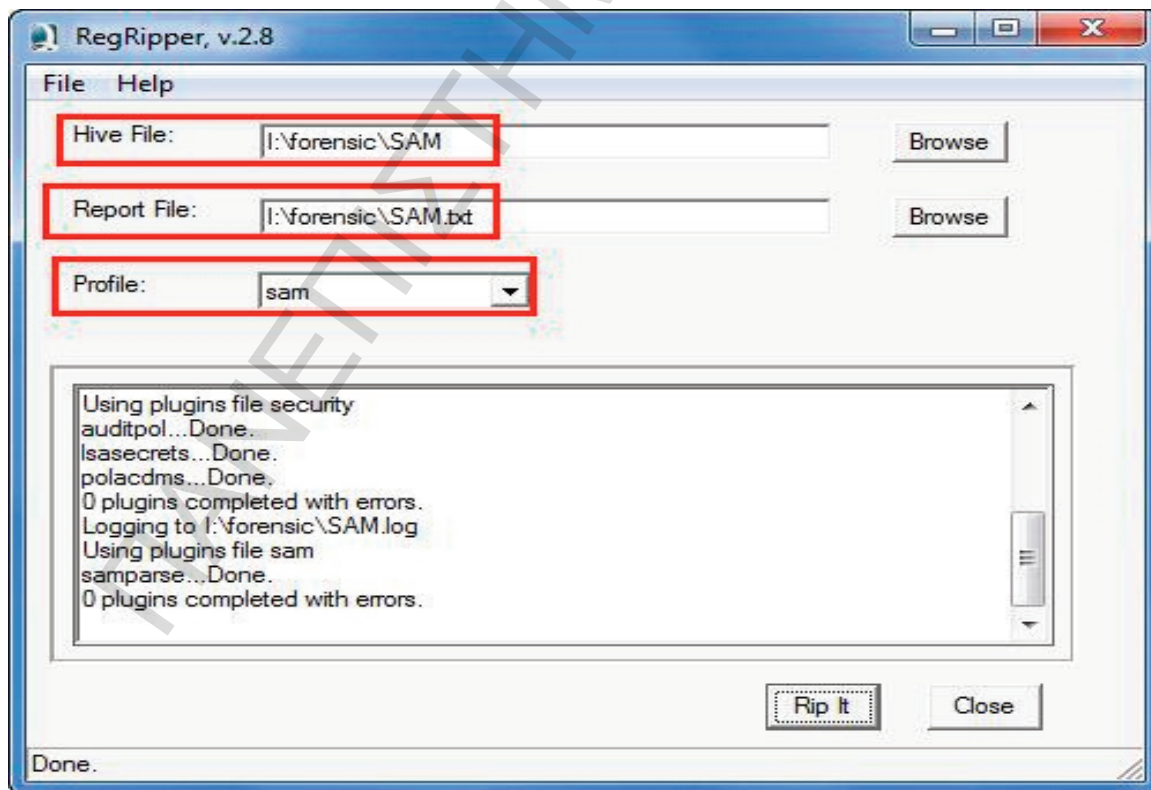


Image 2.6.1: Regripper registry analysis

Administrator account was found disabled.

```

samparse v.20120722
(SAM) Parse SAM file for user & group mbrshp info

User Information
-----
Username       : Administrator [500]
Full Name      :
User Comment   : Built-in account for administering the computer/domain
Account Type   : Default Admin User
Account Created : Sat Jan 19 06:26:24 2013 Z
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

```

Image 2.6.2: Admin accounts status

Username 'T' was created on 18 Jan 2013 with administrative privileges.

```

Username       : t [1000]
Full Name      :
User Comment   :
Account Type   : Default Admin User
Account Created : Fri Jan 18 17:27:47 2013 Z
Password Hint   : h
Last Login Date : Fri Jan 18 17:28:11 2013 Z
Pwd Reset Date  : Fri Jan 18 17:27:48 2013 Z
Pwd Fail Date   : Never
Login Count    : 1
--> Password does not expire
--> Password not required
--> Normal user account

```

Image 2.6.3: Username 'T' information

The SYSTEM hive was analyzed.

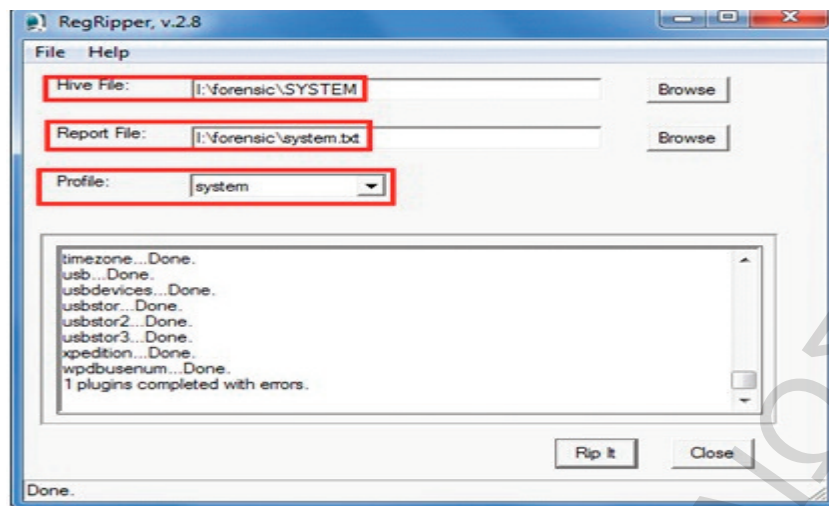


Image 2.6.4: System hive analyzed

The results are shown below

The USB devices connected to the system can be viewed using usbstor.pl. NO evidence of any USB device connecting to the system was found.

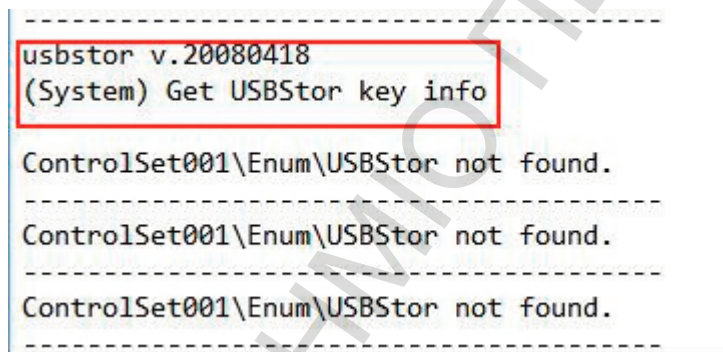


Image 2.6.5: Usbstor.pl

Mountdev.pl shows the drives ever mounted on the system whether removable or otherwise.



Image 2.6.6: Mountdev.pl

Fw_config.pl displays the firewall settings for the host. Analysis shows it was enabled.

```
fw_config v.20080328
(System) Gets the Windows Firewall config from the System hive

Windows Firewall Configuration
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile
LastWrite Time Tue Jul 14 04:37:09 2009 (UTC)
  EnableFirewall -> 1
  DisableNotifications -> 0

Windows Firewall Configuration
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
LastWrite Time Tue Jul 14 04:37:09 2009 (UTC)
  EnableFirewall -> 1
  DisableNotifications -> 0
```

Image 2.6.7: Fw_config.pl

Routes.pl shows the persistent routes some times used by malware to redirect traffic from legitimate sites and / or prevent anti-malware definition updates by antivirus programs etc. No persistent routes were found.

```
routes v.20100817
(System) Get persistent routes

ControlSet001\Services\Tcpip\Parameters\PersistentRoutes
LastWrite: Tue Jul 14 04:39:42 2009

ControlSet001\Services\Tcpip\Parameters\PersistentRoutes has no values.
```

Image 2.6.8: Routes.pl

Nic2.pl shows the information about the network interface card and DHCP configurations as shown below.

```

nic2 v.20100401
(System) Gets NIC info from System hive

Adapter: {43EB8366-E226-48E4-B857-28B12879D123}
LastWrite Time: Fri Jan 18 18:21:10 2013 Z
  UseZeroBroadcast           0
  EnableDeadGWDetect         1
  EnableDHCP                  1
  NameServer
  Domain
  RegistrationEnabled         1
  RegisterAdapterName        0
  DhcpIPAddress               192.168.0.13
  DhcpSubnetMask              255.255.255.0
  DhcpServer                  192.168.0.1
  Lease                       604800
  LeaseObtainedTime          Fri Jan 18 18:01:14 2013 Z
  T1                          Tue Jan 22 06:01:14 2013 Z
  T2                          Thu Jan 24 21:01:14 2013 Z
  LeaseTerminatesTime        Fri Jan 25 18:01:14 2013 Z
  AddressType                 0
  IsServerNapAware           0
  DhcpConnForceBroadcastFlag 0
  DhcpInterfaceOptions       ü
  DhcpGatewayHardware        À" - $ ÚÁÉ
  DhcpGatewayHardwareCount   1
  DhcpDomain                  localdomain
  DhcpNameServer              192.168.0.1
  DhcpDefaultGateway         192.168.0.1
  DhcpSubnetMaskOpt          255.255.255.0

Adapter: {e29ac6c2-7037-11de-816d-806e6f6e6963}
LastWrite Time: Sat Jan 19 06:26:15 2013 Z

```

Image 2.6.9: Nic2.pl

Security hive was analyzed to get the machine unique identifier for the host and get the information about the domains that the host was connected to. This host was connected not connected to any domain so the default primary domain SID can be seen below.

```

-----
polacdms v.20100531
(Security) Get local machine SID from Security hive

PolAcDmS
Policy\PolAcDmS
LastWrite Time Sat Jan 19 06:15:11 2013 (UTC)

Machine SID: S-1-5-21-477845639-243920137-3045931724

PolPrDmS
Policy\PolPrDmS
LastWrite Time Tue Jul 14 04:34:21 2009 (UTC)

Primary Domain SID: S-1-5-

```

Image 2.6.10: Polacdms.pl

Poladtev.pl plugin of reg_ripper shows the audit policy configurations and last write time. It was found that auditing was not enabled on this host.

```

Policy\PolAdtEv
LastWrite Time Tue Jul 14 04:34:05 2009 (UTC)

Length of data: 138 bytes.
0x00000000: 00 01 00 00 09 00 18 77 78 00 00 00 01 00 00 00 .....WX.....
0x00000010: 03 00 00 00 03 00 01 00 01 00 01 00 00 00 01 00 .....
0x00000020: 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 .....
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 .....
0x00000050: 01 00 00 00 00 00 00 00 00 00 01 00 00 00 01 00 .....
0x00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000070: 00 00 00 00 00 00 00 00 05 00 09 00 0c 00 03 00 .....
0x00000080: 04 00 06 00 06 00 04 00 04 00 .....
**Auditing is NOT enabled.

```

Image 2.6.11: Poladtev.pl

Software Hive - Windows recycle bin can be set such that no deleted file ever goes to recycle bin and delete is equal to shift + delete operation. Bit bucket key is set to one in such cases but this key was not found.

```

bitbucket v.20080418
(Software) Get HKLM\..\BitBucket keys\values

Microsoft\Windows\CurrentVersion\Explorer\BitBucket not found

```

Image 2.6.12: Bitbucket.pl

Browser helper objects are used by malware to modify pages and insert malicious links. No such BHOs were found.

```

bho v.20130408
(Software) Gets Browser Helper Objects from Software hive

Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects not found.
Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects not found

```

Image 2.6.13: Bho.pl

Every malware needs persistence to survive across re-boots. Soft_run.pl plugin checks for such ASEPs in registry.


```

soft_run v.20130425
(Software) [Autostart] Get autostart key contents from Software hive

Microsoft\Windows\CurrentVersion\Run
LastWrite Time Tue Jul 14 04:41:12 2009 (UTC)
Microsoft\Windows\CurrentVersion\Run has no values.
Microsoft\Windows\CurrentVersion\Run has no subkeys.

Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Fri Jan 18 17:28:32 2013 (UTC)
Microsoft\Windows\CurrentVersion\RunOnce has no values.
Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\RunServices not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce not found.

Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

```

Image 2.6.14: Soft_run.pl

Image file execution is used to launch another application (may be malware) whenever an application is launched. Imagefile.pl checks for presence of such keys.

```

imagefile v.20130425
(Software) Checks IFEO subkeys for Debugger & CWDIllegalInDllSearch values

Microsoft\Windows NT\CurrentVersion\Image File Execution Options
No Debugger/CWDIllegalInDllSearch values found.

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options not found.

```

Image 2.6.15: Imagefile.pl

NTUSER.DAT - This hive tracks the activities of individual users.
The list of files presented with open / save dialog.

```

OpenSavePid1MRU
LastWrite: Fri Jan 18 17:45:06 2013
OpenSavePid1MRU\*
LastWrite Time: Fri Jan 18 17:49:21 2013
Note: All value names are listed in MRUListEx order.

Users\ProcessMonitor.zip
Users\ProcessExplorer.zip
Users\Handle.zip
Users\Autoruns.zip
Users\TCPView.zip
Users\ImmunityDebugger_1_85_setup.exe
Users\id_public_key.asc
Users\ChromeSetup.exe

```

Image 2.6.16: OpenSavePid1MRU

Acmru.pl plugin tracks the searches done by user in Windows.

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

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

Image 2.6.17: Acmru.pl

Adoberdr.pl plugin finds the recently opened adobe reader (pdf) files and the version of adobe reader installed on the system.

```
-----
adoberdr v.20120716
(NTUSER.DAT) Gets user's Adobe Reader cRecentFiles values

Adoberdr v.20120716
Adobe Acrobat Reader version not found.
```

Image 2.6.18: Adoberdr.pl

Ccleaner.pl locates whether ccleaner was used on the system to clean up. This affects the analysis.

```
-----
ccleaner v.20120128
(NTUSER.DAT) Gets User's CCleaner Settings

Software\Piriform\CCleaner does not exist.
```

Image 2.6.19: Ccleaner.pl

Recentdocs.pl traces the recently opened documents by the user.

```
-----
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Fri Jan 18 18:20:59 2013 (UTC)
9 = office2007
8 = KEY.TXT
7 = Network and Internet
1 = Downloads
6 = ProcessMonitor.zip
5 = ProcessExplorer.zip
4 = Handle.zip
3 = Autoruns.zip
2 = TCPView.zip
0 = id_public_key.asc
```

Image 2.6.20: Recentdocs.pl

Proxysettings.pl plugin tracks the proxy settings for the host.

```
-----
proxysettings v.20081224
(NTUSER.DAT) Gets contents of user's Proxy Settings

ProxySettings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Fri Jan 18 17:37:09 2013 (UTC)
AutoConfigProxy          wininet.dll
CertificateRevocation    1
DisableCachingOfSSLPages 0
EmailName                User@
EnableHttp1_1            1
EnableNegotiate          1
IE5_UA_Backup_Flag      5.0
MigrateProxy             1
MimeExclusionListForCache multipart/mixed multipart/x-mixed-replace multipart/x-byteranges
PrivDiscUiShown          1
PrivacyAdvanced          0
ProxyEnable              0
SecureProtocols          160
UrlEncoding              0
UseSchannelDirectly     1
User Agent               Mozilla/4.0 (compatible; MSIE 8.0; Win32)
WarnOnIntranet           1
WarnOnPost               1
WarnonZoneCrossing      0
ZonesSecurityUpgrade     1049460144
-----
```

Image 2.6.21: Proxysettings.pl

Runmru.pl plugin lists all the most recently used (MRUs) commands in run option of Windows.

```
-----
runmru v.20080324
(NTUSER.DAT) Gets contents of user's RunMRU key

RunMru
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
LastWrite Time Fri Jan 18 18:05:37 2013 (UTC)
MRUList = a
a  \\192.168.0.12\te$\1
-----
```

Image 2.6.22: Runmru.pl

Typedurls.pl lists all the URLs typed by the user.

```
-----
typedurls v.20080324
(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Fri Jan 18 17:44:22 2013 (UTC)
ur11 -> tcpview
ur12 -> http://immunity/
ur13 -> http://go.microsoft.com/fwlink/?LinkId=69157
-----
```

Image 2.6.23: Typedurls.pl

Typedpaths.pl plugin lists all the paths typed by the user in explorer bar.

```
-----
typedpaths v.20100330
(NTUSER.DAT) Gets contents of user's typedpaths key

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
LastWrite Time Fri Jan 18 18:01:58 2013 (UTC)

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths has no values
-----
```

Image 2.6.24: Typedpaths.pl

User_run.pl plugin was used to list all the auto start points in the HKCU hive.

```
-----
user_run v.20130425
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive

Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Fri Jan 18 17:29:30 2013 (UTC)
|
Software\Microsoft\Windows\CurrentVersion\Run has no values.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Fri Jan 18 17:29:29 2013 (UTC)

Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.

Software\Microsoft\Windows\CurrentVersion\RunServices not found.

Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Software\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Fri Jan 18 17:28:27 2013 (UTC)
Run value not found.
run value not found.
load value =
-----
```

Image 2.6.25: User_run.pl

Userassist.pl plugin lists the files the user clicked in the Windows Explorer.

```
-----  
user_run v.20130425  
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive  
  
Software\Microsoft\Windows\CurrentVersion\Run  
LastWrite Time Fri Jan 18 17:29:30 2013 (UTC)  
|  
Software\Microsoft\Windows\CurrentVersion\Run has no values.  
  
Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.  
  
Software\Microsoft\Windows\CurrentVersion\RunOnce  
LastWrite Time Fri Jan 18 17:29:29 2013 (UTC)  
  
Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.  
  
Software\Microsoft\Windows\CurrentVersion\RunServices not found.  
  
Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.  
  
Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.  
  
Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.  
  
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.  
  
Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.  
  
Software\Microsoft\Windows NT\CurrentVersion\Windows  
LastWrite Time Fri Jan 18 17:28:27 2013 (UTC)  
Run value not found.  
run value not found.  
load value =  
-----
```

```

UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Fri Jan 18 17:29:21 2013 (UTC)

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Fri Jan 18 18:24:20 2013 Z
  C:\office2007\SETUP.EXE (4)
Fri Jan 18 18:23:36 2013 Z
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\msiexec.exe (3)
Fri Jan 18 18:20:59 2013 Z
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\NOTEPAD.EXE (1)
Fri Jan 18 18:12:23 2013 Z
  C:\Users\t\Downloads\ImmunityDebugger_1_85_setup.exe (1)
Fri Jan 18 17:37:07 2013 Z
  Microsoft.InternetExplorer.Default (1)
Fri Jan 18 17:27:34 2013 Z
  Microsoft.Windows.GettingStarted (14)
  Microsoft.Windows.MediaCenter (13)
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\calc.exe (12)
  Microsoft.Windows.StickyNotes (11)
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\SnippingTool.exe (10)
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\mspaint.exe (9)
  Microsoft.Windows.RemoteDesktop (8)
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\magnify.exe (7)
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Games\Solitaire\solitaire.exe (6)

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Fri Jan 18 17:37:07 2013 Z
  {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Internet Explorer.lnk (1)
Fri Jan 18 17:27:34 2013 Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories>Welcome Center.lnk (14)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Media Center.lnk (13)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Calculator.lnk (12)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Sticky Notes.lnk (11)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk (10)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk (9)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Remote Desktop Connection.lnk (8)
  {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Accessibility\Magnify.lnk (7)

```

Image 2.6.26: Userassist.pl

Chapter 3 - Forensics Analysis of a Windows 8 Host

3.1 Machine Details

The analysis was carried out on a Virtual Machine running in Oracle Virtualbox with 1 GB RAM and 20 GB Hard disk. Windows 8 Pro(32 bit) with version 6.2.9200 was analyzed for forensics evidence.

3.2 Live response using mir-ror

Mir-ror V2.0 was used to carry out live response evidence collection from the host to gather the state of the live system as present at the time of incident report. [2, 3]

Default script for Mir-ror was adapted to work under Windows 8 environment as it is originally designed for Windows XP and Windows 2003. The signatures were added to help the script in identifying The Windows version, otherwise script failed to run.

```

REM * OS Detection Function *
REM *****

findstr /i xp %LOGS%\Livecap_%COMPUTERNAME%\systeminfo.log >nul
IF %ERRORLEVEL% == 0 SET OSNAME= XP
findstr /i vista %LOGS%\Livecap_%COMPUTERNAME%\systeminfo.log >nul
IF %ERRORLEVEL% == 0 SET OSNAME= Vista
findstr /i windows.7 %LOGS%\Livecap_%COMPUTERNAME%\systeminfo.log >nul
IF %ERRORLEVEL% == 0 SET OSNAME= Vista
findstr /i windows.8 %LOGS%\Livecap_%COMPUTERNAME%\systeminfo.log >nul
IF %ERRORLEVEL% == 0 SET OSNAME= Vista

ECHO.
ECHO *****
ECHO OS Family Detected as: %OSNAME%
ECHO *****
ECHO.

ECHO.
ECHO *****
ECHO MIR-ROR is now copying the NTUSER.dat files for every user on the system
ECHO for offline analysis
ECHO *****
ECHO.

IF %OSNAME% == XP GOTO ntuser_XP
IF %OSNAME% == Vista GOTO ntuser_VISTA
GOTO SKIP_ntuser

:ntuser_XP
for /F %i in ('dir /b "c:\Documents and Settings%"') do ntfscopy.exe -raw "c:\Documents and Settings%\%i\NTUSER.dat" "%LOGS%\Livecap_%COMPUTERNAME%
\ntuser_%i.dat" 2>> %LOGS%\Livecap_%COMPUTERNAME%\MIR-ROR.log
GOTO FINISH_ntuser

:ntuser_VISTA
for /F %i in ('dir /b c:\Users') do ntfscopy.exe -raw "c:\Users%\%i\NTUSER.dat" "%LOGS%\Livecap_%COMPUTERNAME%\ntuser_%i.dat" 2>> %LOGS%\Livecap_
%COMPUTERNAME%\MIR-ROR.log
GOTO FINISH_ntuser

```

This signature helps in identifying correct OS version and subsequent use of correct directory to locate NTUSER.DAT hive

Image 3.2.1: Signature for Identify OS

Moreover another modification made was to comment out the calls to now .exe as they were valid for Windows 2003 only.

```

REM now.exe [Copying the registry files for offline analysis] >> %LOGS%\Livecap_%COMPUTERNAME%\MIR-ROR.log

```

Image 3.2.2: Comment out now.exe

Then there were few tools called in the script which were not available in the Sysinternal suite installation for Mir-ror and included in fetch.txt. They needed to be downloaded and included in the Mir-ror installation directory.

MIR-ROR v.2.0 as of 3/21/12

fetch.txt v.2.0.1 as of 4/11/12

- 1) Download the Sysinternals Suite: <http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>
- 2) Download **NTFScopy**: http://www.tzworks.net/prototype_page.php?proto_id=9
- 3) Download **The SleuthKit (TSK)**: <http://www.sleuthkit.org/sleuthkit/download.php>
- 4) Download **the Windows Server 2003 Resource Kit Tools**: <http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en>
- 5) Download **seccheck.exe** from Holisticinfosec.org: <http://holisticinfosec.org/toolsmith/files/seccheck/seccheck.exe>
- 6) Download **openports.exe** from Holisticinfosec.org: <http://holisticinfosec.org/toolsmith/files/openports/openports.exe>

Image 3.2.3: Extra tools

The files that were downloaded and included in the tools are shown below.

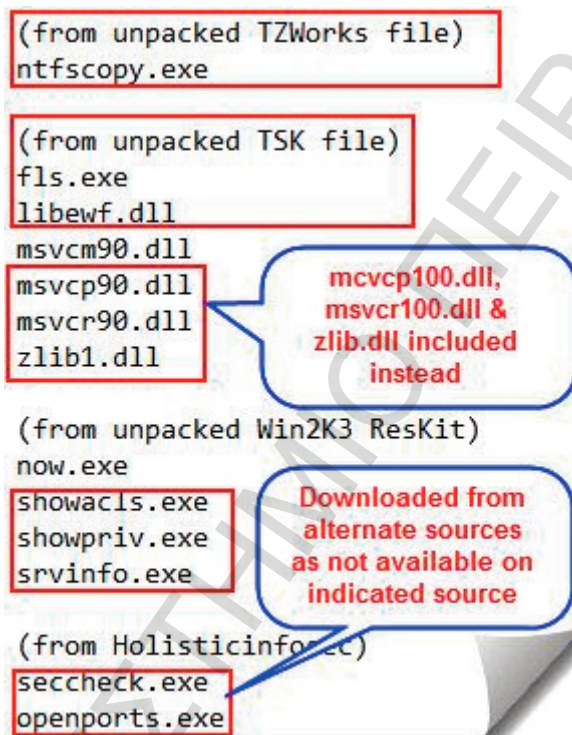


Image 3.2.4: Included tools

Additionally memory dump was created using winpmem v1.4.1 and for that purpose following command was added to the script.

```
ECHO    Running winpmem of %COMPUTERNAME%.
winpmem_1.4.exe %LOGS%\Livecap_%COMPUTERNAME%\physmem.raw
winpmem_1.4.exe -d %LOGS%\Livecap_%COMPUTERNAME%\physmemdmp.dmp
ECHO.
```

Image 3.2.5: Winpmem

To aid in browser forensics and collection of Skype history following tools were added to the script. (source: www.nirsoft.net)



Image 3.2.6: Browsers and Skype tools

All the tools were copied to a USB flash drive under \\tools\mir-ror directory and this drive was plugged in a host on the same network as the target system and this directory was mapped as a network drive 'M'. Therefore no tools were needed to be copied to the target host. After mir-ror was run it generated output in a directory with a suffix of the host name as the host-name was 'Forensic8, the directory was named 'Livecap_Forensic8'.

It must be noted here that cookies have been saved using a unique id and not domain names as done for earlier versions of Windows. A look at one of the cookies reveals following:

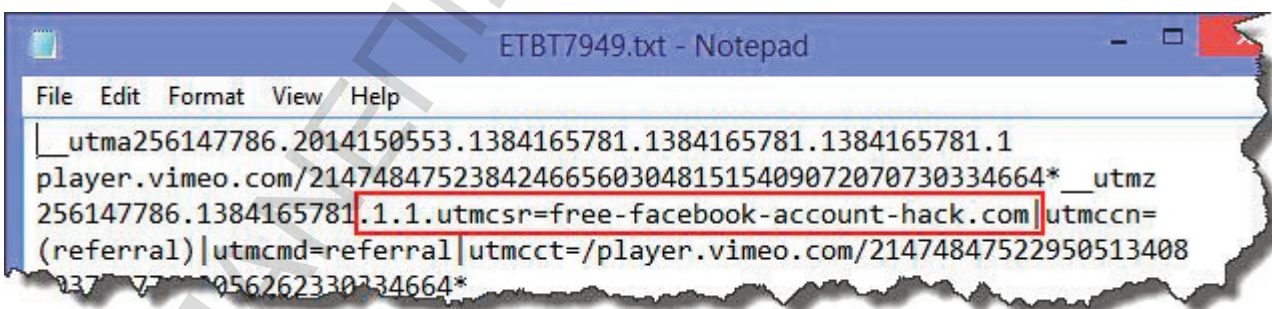


Image 3.2.7: Cookie example

Handles.log file generated by mir-ror shows the processes and the associated threads and handles information. This log presented some interesting information like telnet service being started (which is disabled by default in Windows 7) and presence of an active telnet session.

```

C0C: File (---) \Device\Tcp
C10: Process      tlntsvr.exe(1348)
C14: Key          HKLM\SOFTWARE\Policies\Microsoft\Windows
C1C: File (---)  \Device\Tcp

```

Image 3.2.8: Handles.log

One suspicious process was traced which is not normally found in a normal execution of Windows 8 as shown below.

```

4AC: Thread      dwm.exe(1092): 3960
4B0: Process     hh.exe(3208)

```

Image 3.2.9: Suspicious process example

This process needs further investigation.

Netstat.log shows the result of netstat command which displays all the open TCP connections. The telnet session and hh.exe were found to be listening for connections.

```

netstat.log - Notepad
File Edit Format View Help
[hh.exe]
TCP 192.168.1.5:23          192.168.1.3:50478    ESTABLISHED    1348
[tlntsvr.exe]
TCP 192.168.1.5:139        0.0.0.0:0            LISTENING      4
Can not obtain ownership information
TCP 192.168.1.5:50287      54.243.202.251:80    ESTABLISHED    3112
[iexplore.exe]
TCP 192.168.1.5:50336      64.4.61.207:443     ESTABLISHED    2544
[iexplore.exe]
TCP 192.168.1.5:50388      173.194.113.238:443 ESTABLISHED    2424
[iexplore.exe]
TCP 192.168.1.5:50430      192.168.1.3:445     ESTABLISHED    4
Can not obtain ownership information
TCP 192.168.1.5:50437      192.168.1.3:445     ESTABLISHED    4
Can not obtain ownership information
TCP 192.168.1.5:50441      207.46.129.137:80   ESTABLISHED    3936
[Explorer.EXE]
TCP 192.168.1.5:50445      125.56.199.99:80    CLOSE_WAIT     3936
[Explorer.EXE]
TCP 192.168.1.5:50448      125.56.199.99:80    CLOSE_WAIT     3936
[Explorer.EXE]
TCP 192.168.1.5:50449      125.56.199.129:80   CLOSE_WAIT     3936
[Explorer.EXE]
TCP 192.168.1.5:50450      125.56.199.129:80   CLOSE_WAIT     3936
[Explorer.EXE]
TCP 192.168.1.5:50453      125.56.199.99:80    CLOSE_WAIT     3936
[Explorer.EXE]
TCP 192.168.1.5:50454      125.56.199.99:80    CLOSE_WAIT     3936
[Explorer.EXE]
TCP 192.168.1.5:50476      173.194.113.238:443 ESTABLISHED    2424
[iexplore.exe]
TCP 192.168.1.5:50477      192.168.1.3:139     TIME_WAIT      0
TCP 192.168.1.5:50478      192.168.1.3:139     TIME_WAIT      0
TCP 192.168.1.5:50479      192.168.1.3:139     TIME_WAIT      0
TCP 192.168.1.5:50480      192.168.1.3:139     TIME_WAIT      0
TCP 192.168.1.5:50481      192.168.1.3:139     TIME_WAIT      0
TCP [::]:23                [::]:0              LISTENING      1348
[tlntsvr.exe]
TCP [::]:135                [::]:0              LISTENING      612

```

Image 3.2.10: Netstat.log

Openports.log shows the ports open on the host and it was found that port 23 (telnet) was open and connected and port 80 was also found to be open.

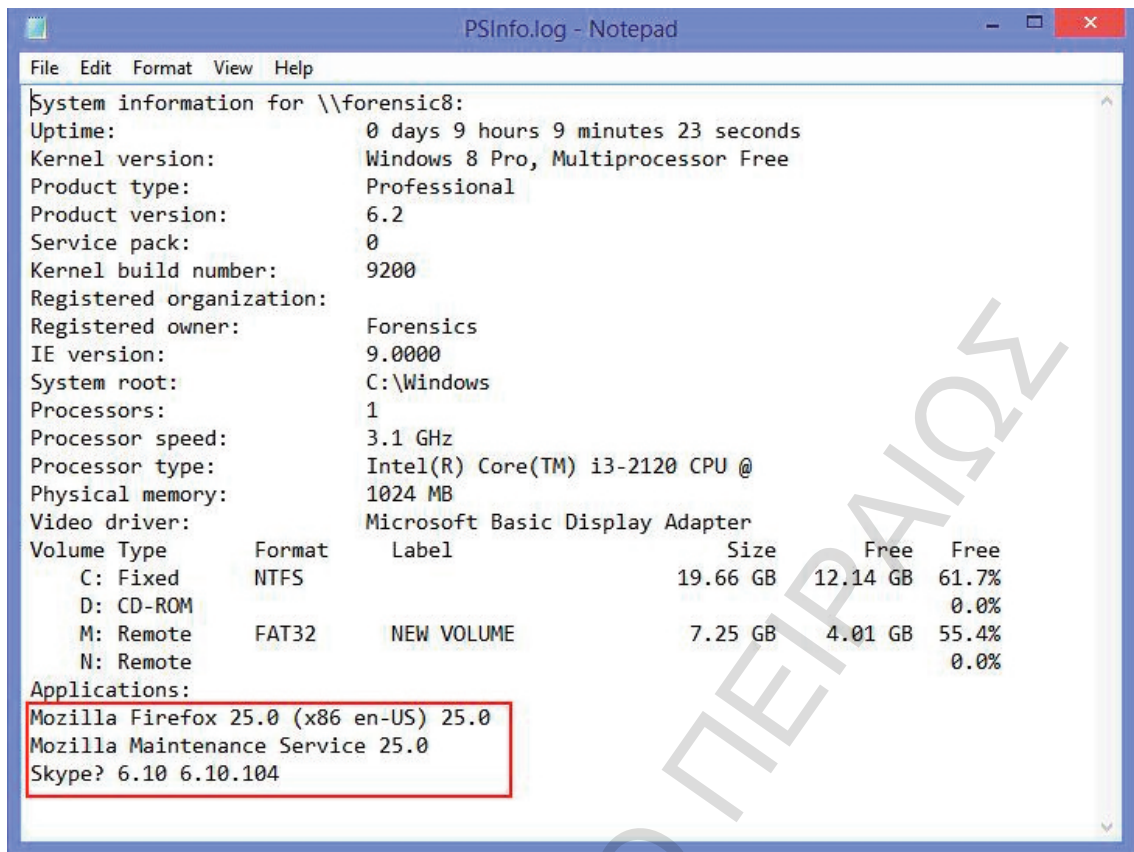
```

openports.log - Notepad
File Edit Format View Help
OpenPorts - DiamondCS Console Tools (www.diamondcs.com.au)
---
SYSTEM [0]
TCP 0.0.0.0:135          0.0.0.0:0           LISTENING
TCP 192.168.1.5:139     0.0.0.0:0           LISTENING
TCP 0.0.0.0:554         0.0.0.0:0           LISTENING
TCP 0.0.0.0:49152       0.0.0.0:0           LISTENING
TCP 0.0.0.0:49153       0.0.0.0:0           LISTENING
TCP 0.0.0.0:49154       0.0.0.0:0           LISTENING
TCP 0.0.0.0:49155       0.0.0.0:0           LISTENING
TCP 0.0.0.0:49156       0.0.0.0:0           LISTENING
TCP 0.0.0.0:50174       0.0.0.0:0           LISTENING
TCP 127.0.0.1:51126     127.0.0.1:51127     ESTABLISHED
TCP 127.0.0.1:51127     127.0.0.1:51126     ESTABLISHED
TCP 192.168.1.5:53121   64.4.46.96:443      ESTABLISHED
TCP 192.168.1.5:53139   64.4.46.99:443      ESTABLISHED
TCP 192.168.1.5:53145   173.194.113.228:443 ESTABLISHED
TCP 192.168.1.5:53185   157.55.236.69:443   ESTABLISHED
TCP 192.168.1.5:53372   192.168.1.2:445     ESTABLISHED
TCP 192.168.1.5:53411   168.63.124.173:80   ESTABLISHED
TCP 192.168.1.5:53414   125.56.199.129:80   CLOSE_WAIT
TCP 192.168.1.5:53415   125.56.199.99:80    CLOSE_WAIT
TCP 192.168.1.5:53416   125.56.199.99:80    CLOSE_WAIT
TCP 192.168.1.5:53430   173.194.113.226:443 ESTABLISHED
TCP 0.0.0.0:23         0.0.0.0:0           LISTENING
TCP 0.0.0.0:445        0.0.0.0:0           LISTENING
TCP 0.0.0.0:2869       0.0.0.0:0           LISTENING
TCP 0.0.0.0:5357       0.0.0.0:0           LISTENING
TCP 0.0.0.0:10243      0.0.0.0:0           LISTENING
UDP 192.168.1.5:137    0.0.0.0:0           LISTENING
UDP 192.168.1.5:138    0.0.0.0:0           LISTENING
UDP 0.0.0.0:500        0.0.0.0:0           LISTENING
UDP 127.0.0.1:1900     0.0.0.0:0           LISTENING
UDP 192.168.1.5:1900   0.0.0.0:0           LISTENING
UDP 0.0.0.0:3544       0.0.0.0:0           LISTENING

```

Image 3.2.11: Openports.log

Psinfo.log shows the information about the host and the programs installed. It was found that Mozilla Firefox and Skype were installed on the host.



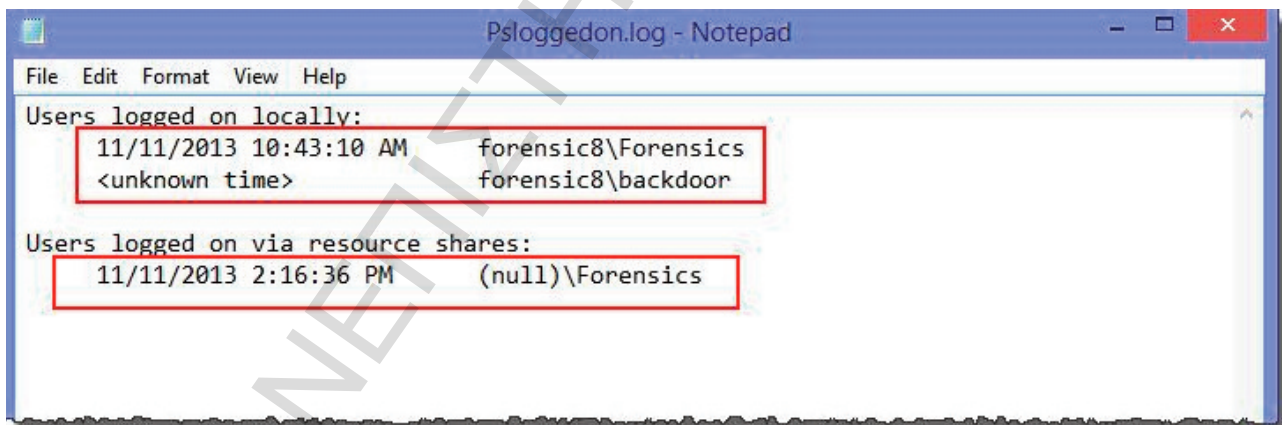
```

PSInfo.log - Notepad
File Edit Format View Help
System information for \\forensic8:
Uptime:                0 days 9 hours 9 minutes 23 seconds
Kernel version:        Windows 8 Pro, Multiprocessor Free
Product type:          Professional
Product version:       6.2
Service pack:          0
Kernel build number:   9200
Registered organization:
Registered owner:      Forensics
IE version:             9.0000
System root:           C:\Windows
Processors:            1
Processor speed:       3.1 GHz
Processor type:        Intel(R) Core(TM) i3-2120 CPU @
Physical memory:       1024 MB
Video driver:          Microsoft Basic Display Adapter
Volume Type            Format      Label              Size      Free      Free
C: Fixed              NTFS
D: CD-ROM
M: Remote             FAT32      NEW VOLUME         7.25 GB   4.01 GB   55.4%
N: Remote
Applications:
Mozilla Firefox 25.0 (x86 en-US) 25.0
Mozilla Maintenance Service 25.0
Skype? 6.10 6.10.104

```

Image 3.2.12: Psinfo.log

Psloggedon.log shows the currently logged on users and it also confirmed that two users were logged on at the time of live response and also there was a session through resource shares.



```

Psloggedon.log - Notepad
File Edit Format View Help
Users logged on locally:
11/11/2013 10:43:10 AM forensic8\Forensics
<unknown time> forensic8\backdoor
Users logged on via resource shares:
11/11/2013 2:16:36 PM (null)\Forensics

```

Image 3.2.13: Psloggedon.log

Pstasklist.log shows the running processes with threads and the execution state of the processes. The suspicious processes can be seen in this list too.

```

File Edit Format View Help
wmpnetwk          924  8  9  318  69052  2748  3432
SearchIndexer    928  8 13  570 130260 15408 17284
svchost          932  8 18  638  85252  9680  7352
svchost         1112  8 29  756  85516 10440  8072
tIntsvr         1348  8  4  100  22808  3580   856
tIntsess        800  8  2  115  40736  4388  1048
cmd             992  8  1  0    3156   80   1328
cmd            1384  8  1  22   9996  1808  1472
nc             3300  8  1  23  11232  1448   280
conhost        3828  8  2  33  18768  2224   500
svchost        1496  8 24  579  55488 10112  4972
spoolsv       1744  8 10  315  40128  5068  2212
svchost        1772  8 23  469  87764 12376 12360
MsMpEng       1920  8 15  479 215424 43528 156900
taskhostex    2304  8 13  322  91928  9908  3688
taskhost      2756  6  9  246  85568 11780  5860
svchost       3024  8  4  102  20964  3092   852
taskhost      3040  8  5  294  69868  5772  3492
svchost       3132  8  9  396  59940  8704  3600
TrustedInstaller 3212  8  9  105  24100  3656  1360
lsass         480  9  8 1065  31180  9632  4896
winlogon      416 13  3  153  50784  6300  1064
dwm           688 13  7  319 242716 84140 36136
explorer     3936  8 48 2208 689804 88472 54268
iexplore     220  8 10  631 170096 23216 10136
iexplore     2424  8 31 1141 535816 138048 216744
iexplore     2544  8 32 1034 416972 80140 121968
iexplore     3112  8 39 1094 437824 152020 133668
cmd          2812  8  1  31   35912  2780  1692
pslist       284 13  1  144  56464  4272  1888
conhost      2388  8  2  51  55224  5244   820
hh           3208  8  1  28   32964  2212   860
conhost      1516  8  2  47  41320  3520   748
Process and thread information for forensic8:

```

Image 3.2.14: Pstasklist.log

Scquery.log displays the installed services and their status. Analysis shows the telnet service is enabled and running.

```

File Edit Format View Help
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

SERVICE_NAME: wscsvc
DISPLAY_NAME: Security Center
TYPE : 20 WIN32_SHARE_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

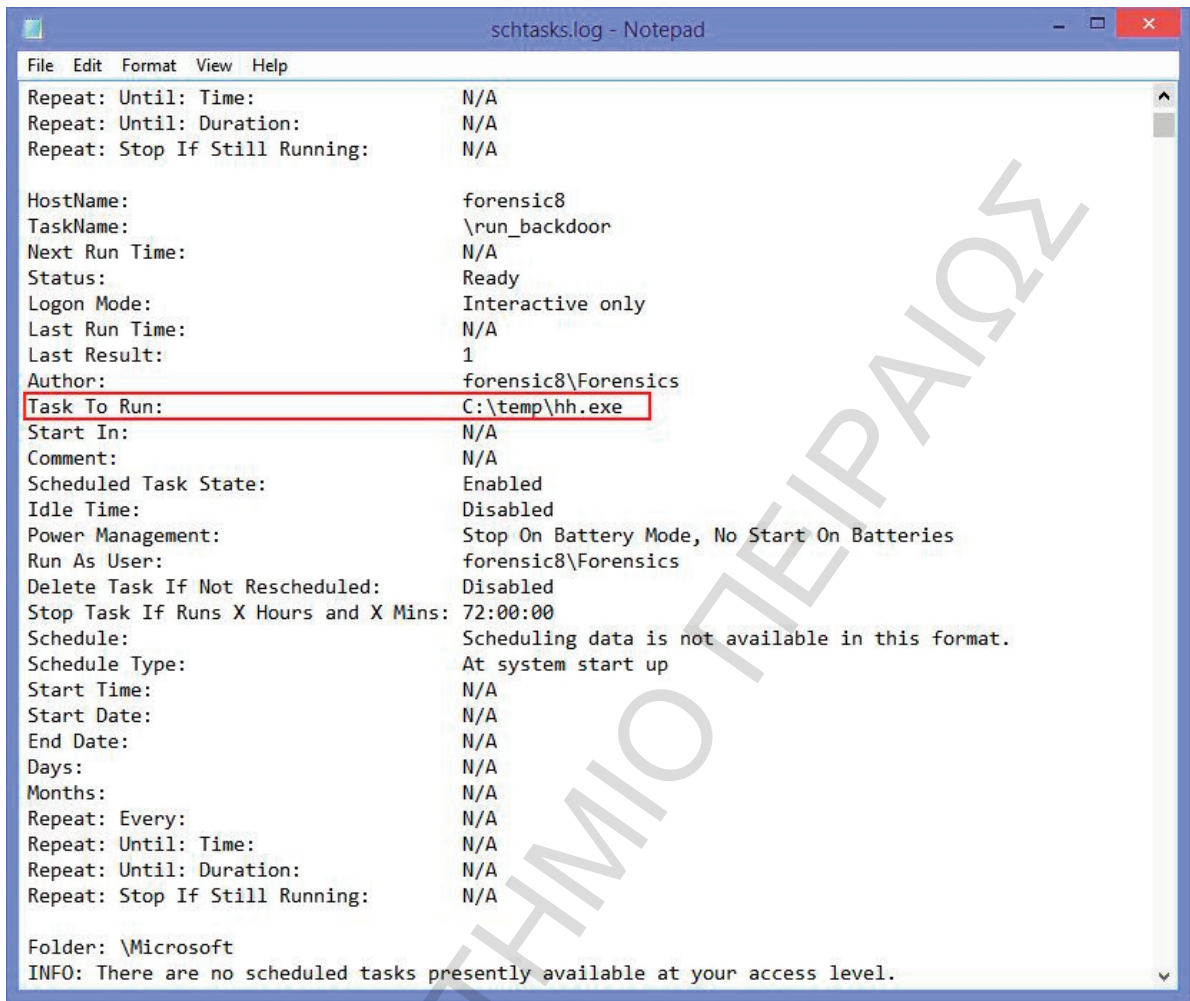
SERVICE_NAME: WSearch
DISPLAY_NAME: Windows Search
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

SERVICE_NAME: TlntSvr
DISPLAY_NAME: Telnet
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

```

Image 3.2.15: SC_Query.log

Schtasks.log displays the scheduled jobs which are set to run at predefined intervals / time and often are used in post exploitation stage to achieve persistence or hide activity by intruders. Analysis shows a scheduled task is created to start hh.exe on startup.



```

File Edit Format View Help
Repeat: Until: Time: N/A
Repeat: Until: Duration: N/A
Repeat: Stop If Still Running: N/A

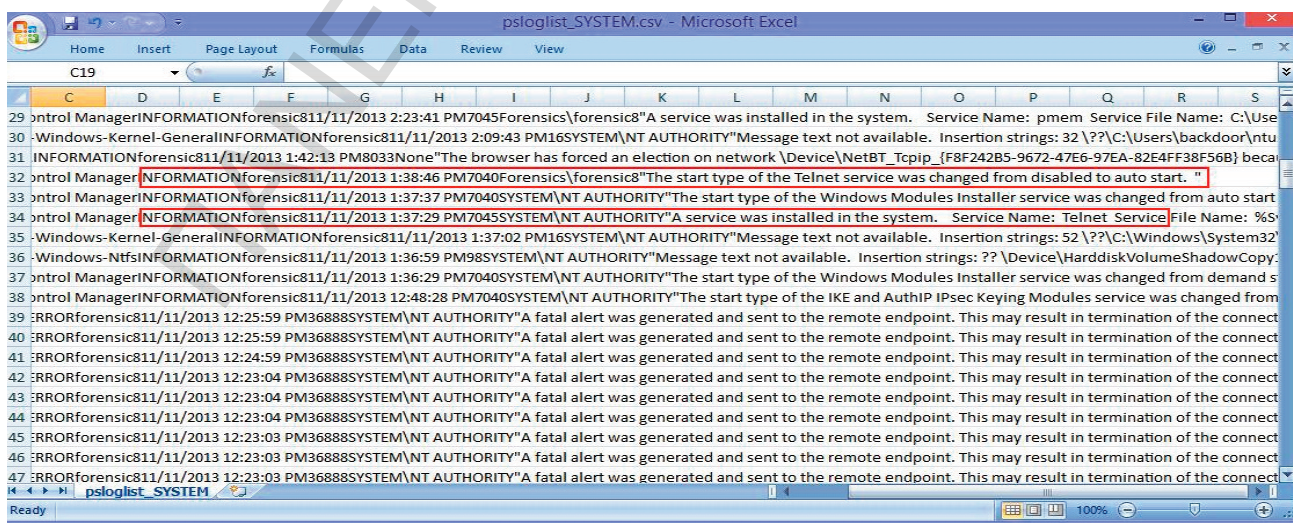
HostName: forensic8
TaskName: \run_backdoor
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive only
Last Run Time: N/A
Last Result: 1
Author: forensic8\Forensics
Task To Run: C:\temp\hh.exe
Start In: N/A
Comment: N/A
Scheduled Task State: Enabled
Idle Time: Disabled
Power Management: Stop On Battery Mode, No Start On Batteries
Run As User: forensic8\Forensics
Delete Task If Not Rescheduled: Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule: Scheduling data is not available in this format.
Schedule Type: At system start up
Start Time: N/A
Start Date: N/A
End Date: N/A
Days: N/A
Months: N/A
Repeat: Every: N/A
Repeat: Until: Time: N/A
Repeat: Until: Duration: N/A
Repeat: Stop If Still Running: N/A

Folder: \Microsoft
INFO: There are no scheduled tasks presently available at your access level.

```

Image 3.2.16: Schtasks.log

Psloglist_system.csv files lists the event log and reveals the time when telnet service was installed and set to auto start.



```

psloglist_SYSTEM.csv - Microsoft Excel
C19

29 \ntrol Manager\INFORMATIONforensic811/11/2013 2:23:41 PM7045Forensics\Forensic8"A service was installed in the system. Service Name: pmem Service File Name: C:\Use
30 \Windows-Kernel-General\INFORMATIONforensic811/11/2013 2:09:43 PM16SYSTEM\NT AUTHORITY"Message text not available. Insertion strings: 32 \??\C:\Users\backdoor\ntu
31 \INFORMATIONforensic811/11/2013 1:42:13 PM8033None"The browser has forced an election on network \Device\NetBT_Tcpip_{F8F242B5-9672-47E6-97EA-82E4FF38F56B} beca
32 \ntrol Manager\INFORMATIONforensic811/11/2013 1:38:46 PM7040Forensics\Forensic8"The start type of the Telnet service was changed from disabled to auto start. "
33 \ntrol Manager\INFORMATIONforensic811/11/2013 1:37:37 PM7040SYSTEM\NT AUTHORITY"The start type of the Windows Modules Installer service was changed from auto start
34 \ntrol Manager\INFORMATIONforensic811/11/2013 1:37:29 PM7045SYSTEM\NT AUTHORITY"A service was installed in the system. Service Name: Telnet Service File Name: %S
35 \Windows-Kernel-General\INFORMATIONforensic811/11/2013 1:37:02 PM16SYSTEM\NT AUTHORITY"Message text not available. Insertion strings: 52 \??\C:\Windows\System32
36 \Windows-Ntfs\INFORMATIONforensic811/11/2013 1:36:59 PM98SYSTEM\NT AUTHORITY"Message text not available. Insertion strings: ?? \Device\HarddiskVolumeShadowCopy:
37 \ntrol Manager\INFORMATIONforensic811/11/2013 1:36:29 PM7040SYSTEM\NT AUTHORITY"The start type of the Windows Modules Installer service was changed from demand s
38 \ntrol Manager\INFORMATIONforensic811/11/2013 12:48:28 PM7040SYSTEM\NT AUTHORITY"The start type of the IKE and AuthIP IPsec Keying Modules service was changed from
39 \ERRORforensic811/11/2013 12:25:59 PM3688SYSTEM\NT AUTHORITY"A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connect
40 \ERRORforensic811/11/2013 12:25:59 PM3688SYSTEM\NT AUTHORITY"A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connect
41 \ERRORforensic811/11/2013 12:24:59 PM3688SYSTEM\NT AUTHORITY"A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connect
42 \ERRORforensic811/11/2013 12:23:04 PM3688SYSTEM\NT AUTHORITY"A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connect
43 \ERRORforensic811/11/2013 12:23:04 PM3688SYSTEM\NT AUTHORITY"A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connect
44 \ERRORforensic811/11/2013 12:23:04 PM3688SYSTEM\NT AUTHORITY"A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connect
45 \ERRORforensic811/11/2013 12:23:03 PM3688SYSTEM\NT AUTHORITY"A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connect
46 \ERRORforensic811/11/2013 12:23:03 PM3688SYSTEM\NT AUTHORITY"A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connect
47 \ERRORforensic811/11/2013 12:23:03 PM3688SYSTEM\NT AUTHORITY"A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connect
48 \ERRORforensic811/11/2013 12:23:03 PM3688SYSTEM\NT AUTHORITY"A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connect

```

Image 3.2.317: Psloglist_system.csv

Psloglist_security.csv list all the security events and provides valuable information about when a particular account was created, logged in /out and modification of privileges and also indicates any failed logged in attempts.

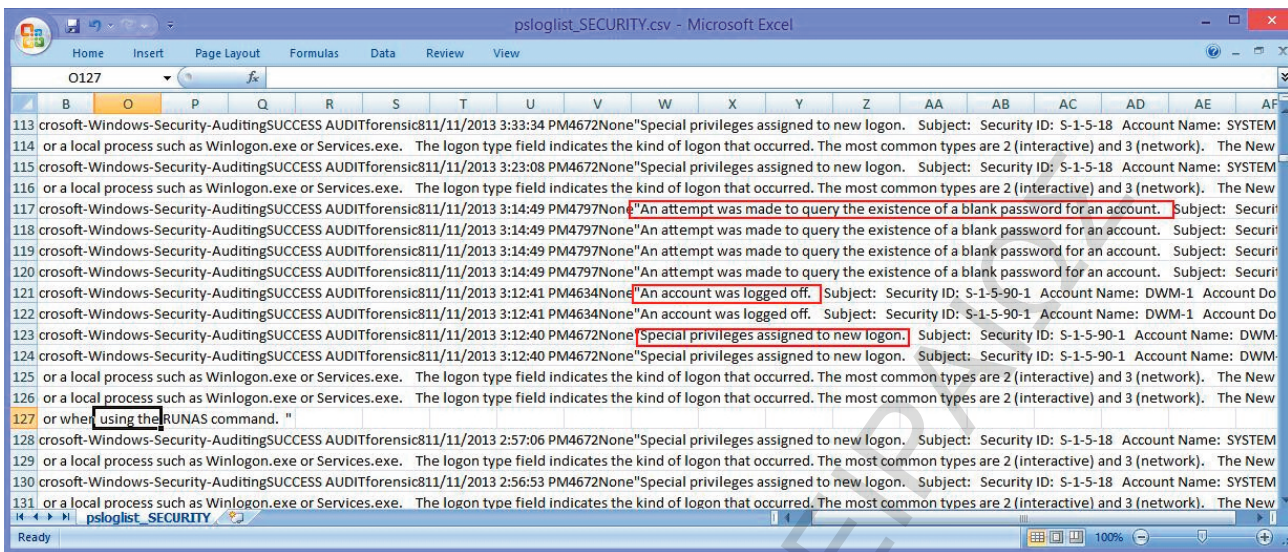


Image 3.2.18: Psloglist_security.csv

Firefox Download History - One file, probably a program to hack facebook accounts was downloaded using firefox as shown below.

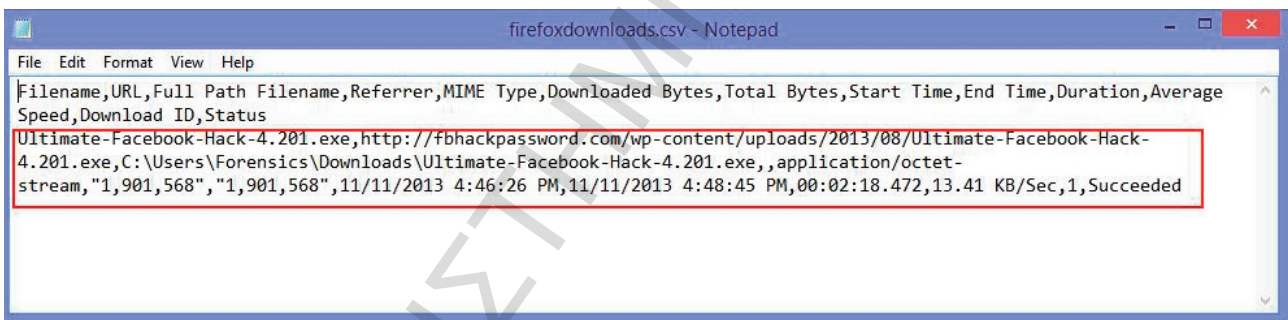


Image 3.2.19: Firefoxdownloads.csv

Browsing History - The browsing history for all the browsers is shown in BrowsingHistoryView.csv file and it contains a number of user ful information like email addresses and the sites visited.

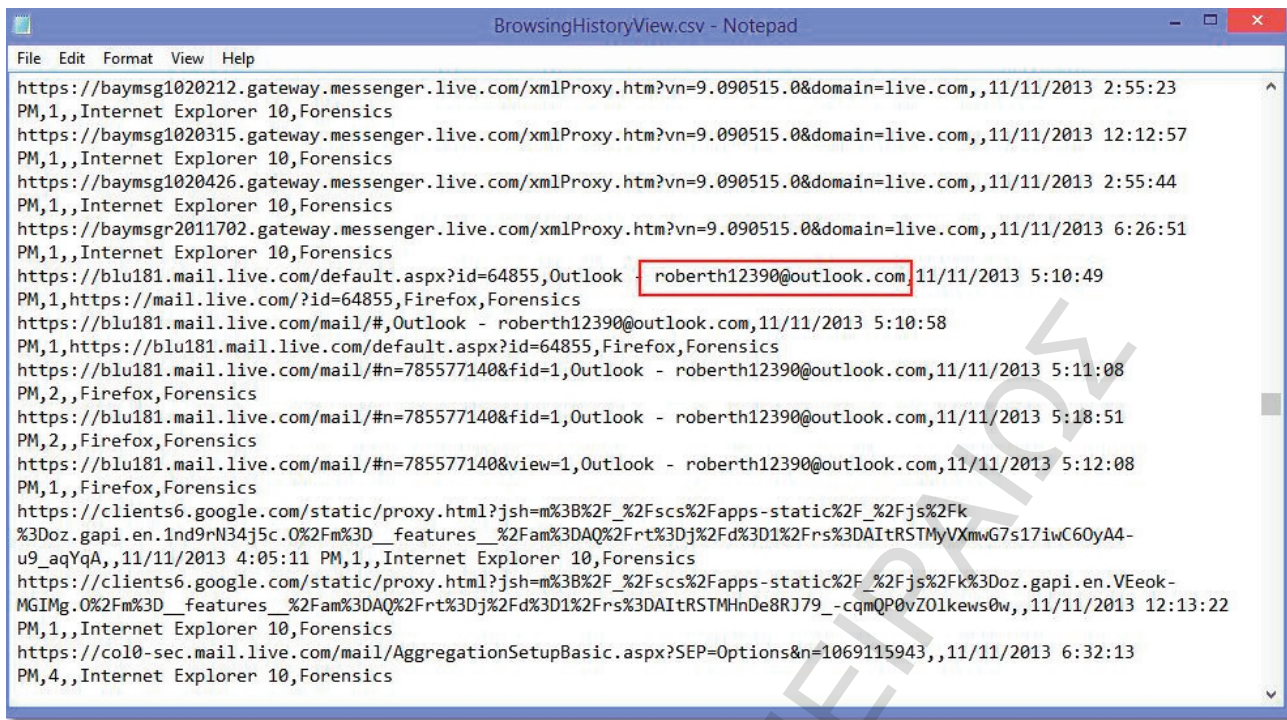


Image 3.2.20: BrowsingHistoryView.csv

Mozilla History View - Similarly MozillaHistoryView.csv shows the browsing history details for firefox only.

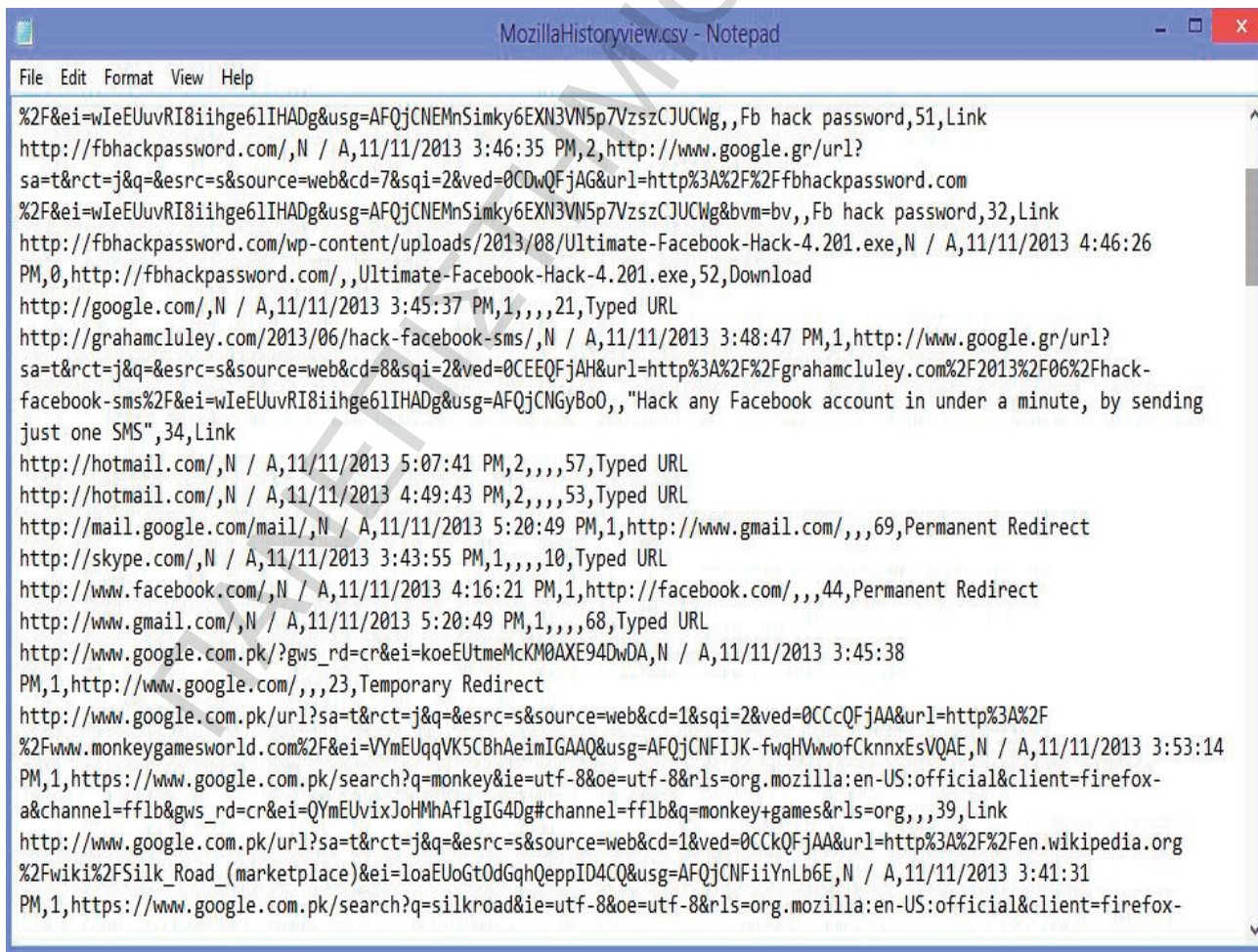
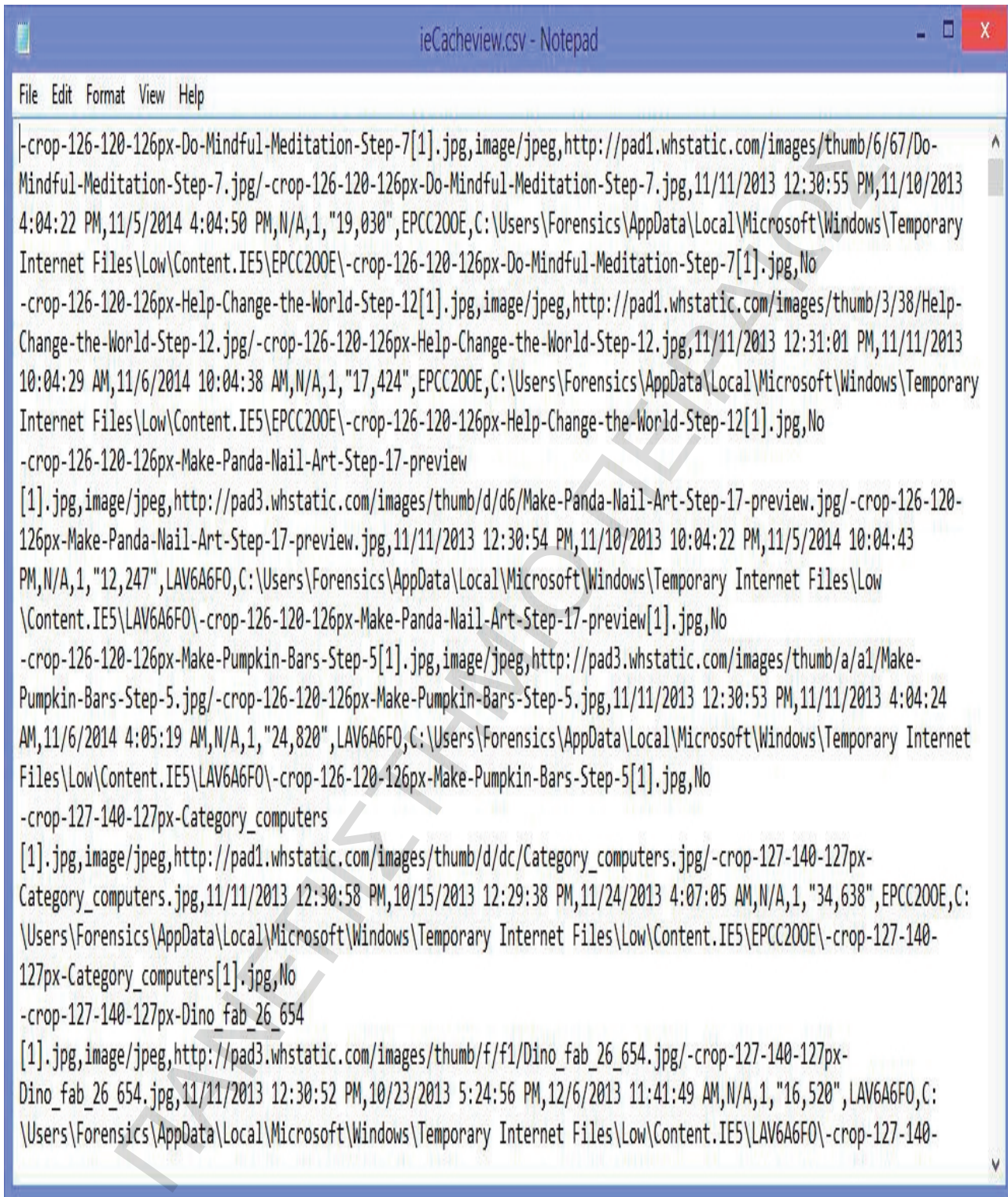


Image 3.2.21: MozillaHistoryView.csv

IECacheView.csv lists all the objects present in the browser cache of Internet Explorer, it can serve a valuable source of information for locating drive by download and other browser based attacks and forensic artifacts like images etc.



```

File Edit Format View Help
|-crop-126-120-126px-Do-Mindful-Meditation-Step-7[1].jpg,image/jpeg,http://pad1.whstatic.com/images/thumb/6/67/Do-
Mindful-Meditation-Step-7.jpg/-crop-126-120-126px-Do-Mindful-Meditation-Step-7.jpg,11/11/2013 12:30:55 PM,11/10/2013
4:04:22 PM,11/5/2014 4:04:50 PM,N/A,1,"19,030",EPCC200E,C:\Users\Forensics\AppData\Local\Microsoft\Windows\Temporary
Internet Files\Low\Content.IE5\EPCC200E\_-crop-126-120-126px-Do-Mindful-Meditation-Step-7[1].jpg,No
-crop-126-120-126px-Help-Change-the-World-Step-12[1].jpg,image/jpeg,http://pad1.whstatic.com/images/thumb/3/38/Help-
Change-the-World-Step-12.jpg/-crop-126-120-126px-Help-Change-the-World-Step-12.jpg,11/11/2013 12:31:01 PM,11/11/2013
10:04:29 AM,11/6/2014 10:04:38 AM,N/A,1,"17,424",EPCC200E,C:\Users\Forensics\AppData\Local\Microsoft\Windows\Temporary
Internet Files\Low\Content.IE5\EPCC200E\_-crop-126-120-126px-Help-Change-the-World-Step-12[1].jpg,No
-crop-126-120-126px-Make-Panda-Nail-Art-Step-17-preview
[1].jpg,image/jpeg,http://pad3.whstatic.com/images/thumb/d/d6/Make-Panda-Nail-Art-Step-17-preview.jpg/-crop-126-120-
126px-Make-Panda-Nail-Art-Step-17-preview.jpg,11/11/2013 12:30:54 PM,11/10/2013 10:04:22 PM,11/5/2014 10:04:43
PM,N/A,1,"12,247",LAV6A6F0,C:\Users\Forensics\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low
\Content.IE5\LAV6A6F0\_-crop-126-120-126px-Make-Panda-Nail-Art-Step-17-preview[1].jpg,No
-crop-126-120-126px-Make-Pumpkin-Bars-Step-5[1].jpg,image/jpeg,http://pad3.whstatic.com/images/thumb/a/a1/Make-
Pumpkin-Bars-Step-5.jpg/-crop-126-120-126px-Make-Pumpkin-Bars-Step-5.jpg,11/11/2013 12:30:53 PM,11/11/2013 4:04:24
AM,11/6/2014 4:05:19 AM,N/A,1,"24,820",LAV6A6F0,C:\Users\Forensics\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\LAV6A6F0\_-crop-126-120-126px-Make-Pumpkin-Bars-Step-5[1].jpg,No
-crop-127-140-127px-Category_computers
[1].jpg,image/jpeg,http://pad1.whstatic.com/images/thumb/d/dc/Category_computers.jpg/-crop-127-140-127px-
Category_computers.jpg,11/11/2013 12:30:58 PM,10/15/2013 12:29:38 PM,11/24/2013 4:07:05 AM,N/A,1,"34,638",EPCC200E,C:
\Users\Forensics\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\EPCC200E\_-crop-127-140-
127px-Category_computers[1].jpg,No
-crop-127-140-127px-Dino_fab_26_654
[1].jpg,image/jpeg,http://pad3.whstatic.com/images/thumb/f/f1/Dino_fab_26_654.jpg/-crop-127-140-127px-
Dino_fab_26_654.jpg,11/11/2013 12:30:52 PM,10/23/2013 5:24:56 PM,12/6/2013 11:41:49 AM,N/A,1,"16,520",LAV6A6F0,C:
\Users\Forensics\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\LAV6A6F0\_-crop-127-140-

```

Image 3.2.22: IECacheview.csv

Similar cache view can be seen for firefox using MozillaCacheView.csv.

```

File Edit Format View Help
|,application/font-woff,anon&uri=https://support.cdn.mozilla.net/static/fonts/MetaWebPro-Bold.woff?
v=1,"23,048",1,11/11/2013 3:40:37 PM,11/11/2013 3:40:36 PM,11/11/2014 3:39:45
PM,support4.webapp.phx1.mozilla.com,HTTP/1.1 200 OK,11/14/2013 10:14:29 AM,6/6/2013 8:29:03 PM,,EC8E4d01,No,max-
age=31535949,"""4de807d1bd9c0""
1.png,image/png,https://support.cdn.mozilla.net/static/img/firefox-32.png?v=1,"2,587",2,11/11/2013 3:40:33 PM,11/11/2013
3:40:31 PM,11/20/2013 4:00:06 PM,support2.webapp.phx1.mozilla.com,HTTP/1.1 200 OK,11/14/2013 10:14:26 AM,7/31/2013
12:05:27 AM,,No,max-age=778775,"""4e2c1ce7237c0""
1.png,image/png,https://support.cdn.mozilla.net/static/img/firefox-512.png?v=1,"143,753",2,11/11/2013 3:40:38
PM,11/11/2013 3:40:31 PM,11/20/2013 3:58:50 PM,support2.webapp.phx1.mozilla.com,HTTP/1.1 200 OK,11/14/2013 10:14:25
AM,7/31/2013 12:05:27 AM,,88134d01,No,max-age=778699,"""4e2c1ce7237c0""
1.png,image/png,https://support.cdn.mozilla.net/static/img/firefox-256.png?v=1,"55,421",2,11/11/2013 3:40:37
PM,11/11/2013 3:40:31 PM,11/20/2013 3:59:21 PM,support2.webapp.phx1.mozilla.com,HTTP/1.1 200 OK,11/14/2013 10:14:25
AM,7/31/2013 12:05:27 AM,,69c81d01,No,max-age=778730,"""4e2c1ce7237c0""
1.png,image/png,https://support.cdn.mozilla.net/static/img/firefox-64.png?v=1,"7,464",2,11/11/2013 3:40:33 PM,11/11/2013
3:40:31 PM,11/20/2013 3:59:34 PM,support5.webapp.phx1.mozilla.com,HTTP/1.1 200 OK,11/14/2013 10:14:25 AM,7/31/2013
12:05:27 AM,,No,max-age=778743,"""4e2c1ce7237c0""
1.png,image/png,https://support.cdn.mozilla.net/static/img/firefox-16.png?v=1,924,3,11/11/2013 3:40:33 PM,11/11/2013
3:40:38 PM,11/20/2013 3:59:01 PM,support5.webapp.phx1.mozilla.com,HTTP/1.1 200 OK,11/14/2013 10:14:25 AM,7/31/2013
12:05:27 AM,,No,max-age=778710,"""4e2c1ce7237c0""
1.png,image/png,https://support.cdn.mozilla.net/static/img/firefox-128.png?v=1,"20,806",2,11/11/2013 3:40:33
PM,11/11/2013 3:40:31 PM,11/20/2013 3:59:54 PM,support1.webapp.phx1.mozilla.com,HTTP/1.1 200 OK,11/14/2013 10:14:25
AM,7/31/2013 12:05:27 AM,,76A17d01,No,max-age=778763,"""4e2c1ce7237c0""
16px-
Folder_Hexagonal_Icon.svg.png,image/png,http://upload.wikimedia.org/wikipedia/en/thumb/4/48/Folder_Hexagonal_Icon.sv
g/16px-Folder_Hexagonal_Icon.svg.png,385,2,11/11/2013 3:41:35 PM,11/11/2013 3:43:18 PM,1/11/2014 11:25:48 PM,,HTTP/1.1
200 OK,11/14/2013 10:15:27 AM,3/7/2012 8:49:59 PM,,No,,6a7ed619571fcda29657f7b93b845016
16px-
Symbol_list_class.svg.png,image/png,http://upload.wikimedia.org/wikipedia/en/thumb/d/db/Symbol_list_class.svg/16px-
Symbol_list_class.svg.png,769,2,11/11/2013 3:41:35 PM,11/11/2013 3:43:18 PM,1/7/2014 8:47:58 PM,,HTTP/1.1 200
OK,11/14/2013 10:15:27 AM,4/18/2012 2:03:23 PM,,No,,e2d38ade56dc55a387dc57c440346784
2013,application/font-woff,anon&uri=https://mozorg.cdn.mozilla.net/media/fonts/OpenSans-Regular-webfont.woff?
2013,"84,928",2,11/11/2013 3:40:27 PM,11/11/2013 3:40:34 PM,8/26/2014 4:01:58

```

Image 3.2.23: MozillaCacheview.csv

LastSearches.csv lists all the web searches made on the host using various search engines. It was found that quite a few searches related to hacking and for website related to dealing in underground market were made.

```

LastSearches.csv - Notepad
File Edit Format View Help
firefox,Bing,General,11/11/2013 2:55:55 PM,Internet Explorer,1,http://www.bing.com/search?q=firefox&src=IE-TopResult&FORM=IE10TR
hackers websites,Google,General,11/11/2013 12:14:07 PM,Internet Explorer,1,"https://www.google.com /search?output=search&sclient=psy-ab&q=hackers+websites&oq=hackers+&gs_l=hp.1.0.014.1264.4514.0.9182.8.8.0.0.1.1496.4057.2-3j2j0j2j0j1.8.0....0...1c.1.31.psy-ab..1.7.3423.Cpx0zd_WeBo&pbx=1&bav=on.2,or.r_qf.&bvm=bv.56146854%2Cd.Yms%2Cpv.xjs.s.en_US.zw3S-PWncBk.0&fp=cea432073b442441&biw=1024&bih=673&dpr=1&tch=1&ech=1&psi=4a2AUtiJdcGetAaP5IDYAw.1384164836718.3"
how to hack facebook,Google,General,11/11/2013 12:29:33 PM,Internet Explorer,1,"https://www.google.gr/search?sclient=psy-ab&q=how%20to%20hack%20facebook&oq=&gs_l=&pbx=1&bav=on.2,or.r_qf.&bvm=bv.56146854,d.bGE&fp=31088428e6a9a074&biw=1024&bih=673&pf=p&pd1=300&tch=1&ech=19&psi=b7GAUoKELKXv4gSN2oGwDw.1384165744719.1"
how to hack web sites,Google,General,11/11/2013 12:30:43 PM,Internet Explorer,1,"https://www.google.gr/search?sclient=psy-ab&q=how+to+hack+web+sites&oq=how+to+hack+web+sites&gs_l=serp.3..0i1014.7599.9420.0.9598.9.9.0.0.0.0.381.2464.2-4j4.8.0....0...1c.1.31.psy-ab..1.8.2433.xZLQ0-tdBYo&pbx=1&bav=on.2,or.r_qf.&fp=31088428e6a9a074&biw=1024&bih=673&bvm=pv.xjs.s.en_US.zw3S-PWncBk.0&tch=1&ech=1&psi=b7GAUoKELKXv4gSN2oGwDw.1384165832718.3"
how to hack wifi,Google,General,11/11/2013 12:29:32 PM,Internet Explorer,1,"https://www.google.gr/search?sclient=psy-ab&q=how%20to%20hack%20wifi&oq=&gs_l=&pbx=1&bav=on.2,or.r_qf.&bvm=bv.56146854,d.bGE&fp=31088428e6a9a074&biw=1024&bih=673&pf=p&pd1=300&tch=1&ech=18&psi=b7GAUoKELKXv4gSN2oGwDw.1384165744719.1"
monkey,Google,General,11/11/2013 3:53:09 PM,Mozilla,1,https://www.google.com/search?q=monkey&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a&channel=fflb
silkroad,Google,General,11/11/2013 3:41:27 PM,Mozilla,1,https://www.google.com.pk/search?q=silkroad&ie=utf-8&oe=utf-8&rls=org.mozilla:en-US:official&client=firefox-a&channel=fflb&gws_rd=cr&ei=loaEUp3QBsGLhQFTz4C4Aw
silkroadf,Bing,General,11/11/2013 12:28:06 PM,Internet Explorer,1,http://www.bing.com/search?q=silkroadf&src=IE-TopResult&FORM=IE10TR
skype,Bing,General,11/11/2013 3:14:30 PM,Internet Explorer,1,http://www.bing.com/search?q=skype&src=IE-TopResult&FORM=IE10TR

```

Image 3.2.24: LastSearches.csv

SkypeHistory.csv lists all the chat, call and file transfer logs for skype users. The conversation related to hacking someone's facebook account and subsequent call and file transfers were all spotted in this log.

```

skypehistory.csv - Notepad
File Edit Format View Help
Record Number,Action Type,Action Time,User Name,Display Name,Duration,Chat Message,ChatID,Filename
50,Chat Message,11/11/2013 4:12:36 PM,maria.alice987,Maria Alice,,hi robert,#maria.alice987/$live:roberth12390;b129f39d6d3c29dc,
51,Chat Message,11/11/2013 4:12:40 PM,maria.alice987,Maria Alice,,how are you,#maria.alice987/$live:roberth12390;b129f39d6d3c29dc,
52,Chat Message,11/11/2013 4:12:50 PM,live:roberth12390,Robert Harold,,m gud,#maria.alice987/$live:roberth12390;b129f39d6d3c29dc,
53,Chat Message,11/11/2013 4:12:55 PM,live:roberth12390,Robert Harold,,wt abt u,#maria.alice987/$live:roberth12390;b129f39d6d3c29dc,
54,Chat Message,11/11/2013 4:13:19 PM,live:roberth12390,Robert Harold,,did you check how can we proceed about hacking,#maria.alice987/$live:roberth12390;b129f39d6d3c29dc,
55,Chat Message,11/11/2013 4:13:35 PM,live:roberth12390,Robert Harold,,julia&apos;s fb account,#maria.alice987/$live:roberth12390;b129f39d6d3c29dc,
56,Chat Message,11/11/2013 4:13:44 PM,maria.alice987,Maria Alice,,yes,#maria.alice987/$live:roberth12390;b129f39d6d3c29dc,
57,Chat Message,11/11/2013 4:13:56 PM,maria.alice987,Maria Alice,,I had been looking at quite a few of ways,#maria.alice987/$live:roberth12390;b129f39d6d3c29dc,
61,Outgoing Call,11/11/2013 4:36:22 PM,live:roberth12390,Robert Harold,,00:08:13,,,
64,Chat Message,11/11/2013 4:37:16 PM,live:roberth12390,Robert Harold,,i want to share this document with you,#maria.alice987/$live:roberth12390;b129f39d6d3c29dc,
66,Receive File,11/11/2013 4:39:01 PM,live:roberth12390,Robert Harold,,,,C:\Users\Forensics\Documents\Julia Home Pics.docx

```

Image 3.2.25: SkypeHistory.csv

3.3 Memory Analysis

Winpmem was used to create raw dump(.raw) and windows crash dump (.dmp) for the memory. These dumps were used with Memoryze and Redline memory Analysis tools from Mandiant to find out any information from the memory. Memoryze uses XML based batch scripts to configure various options. The provided ProcessAuditMemory.Batch.xml script was modified to make it analyze the captured memory image using pmem during Incident response.[14, 15]

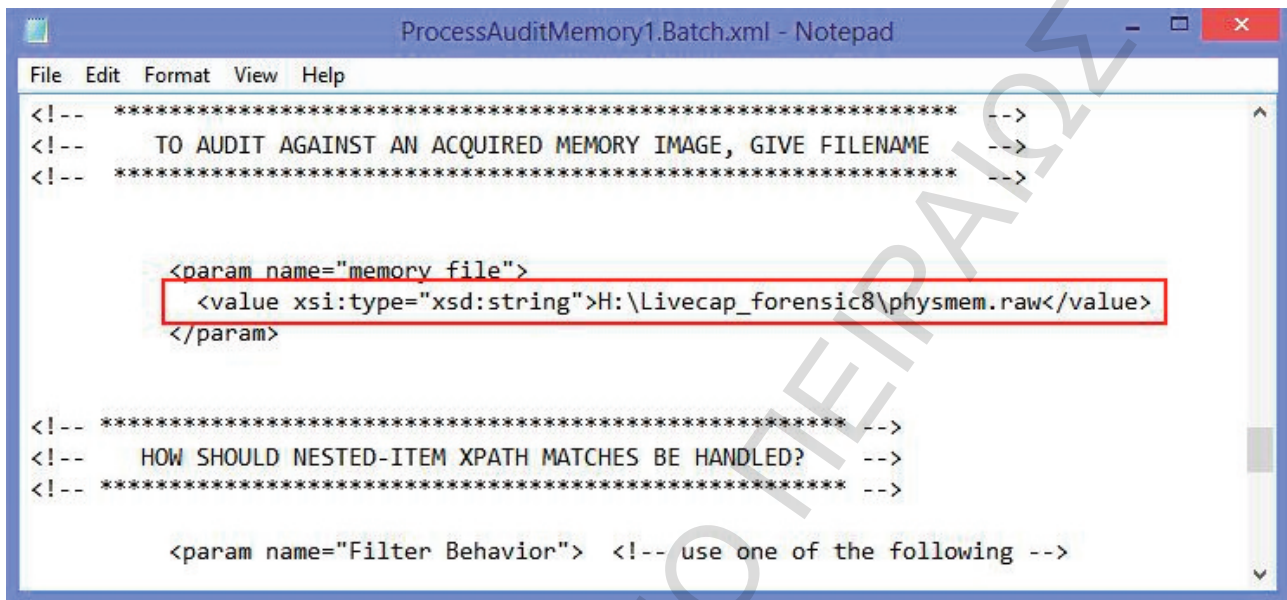


Image 3.3.1: ProcessAuditMemory1.Batch.xml

The Memoryze tool was run with modified batch script as shown below.

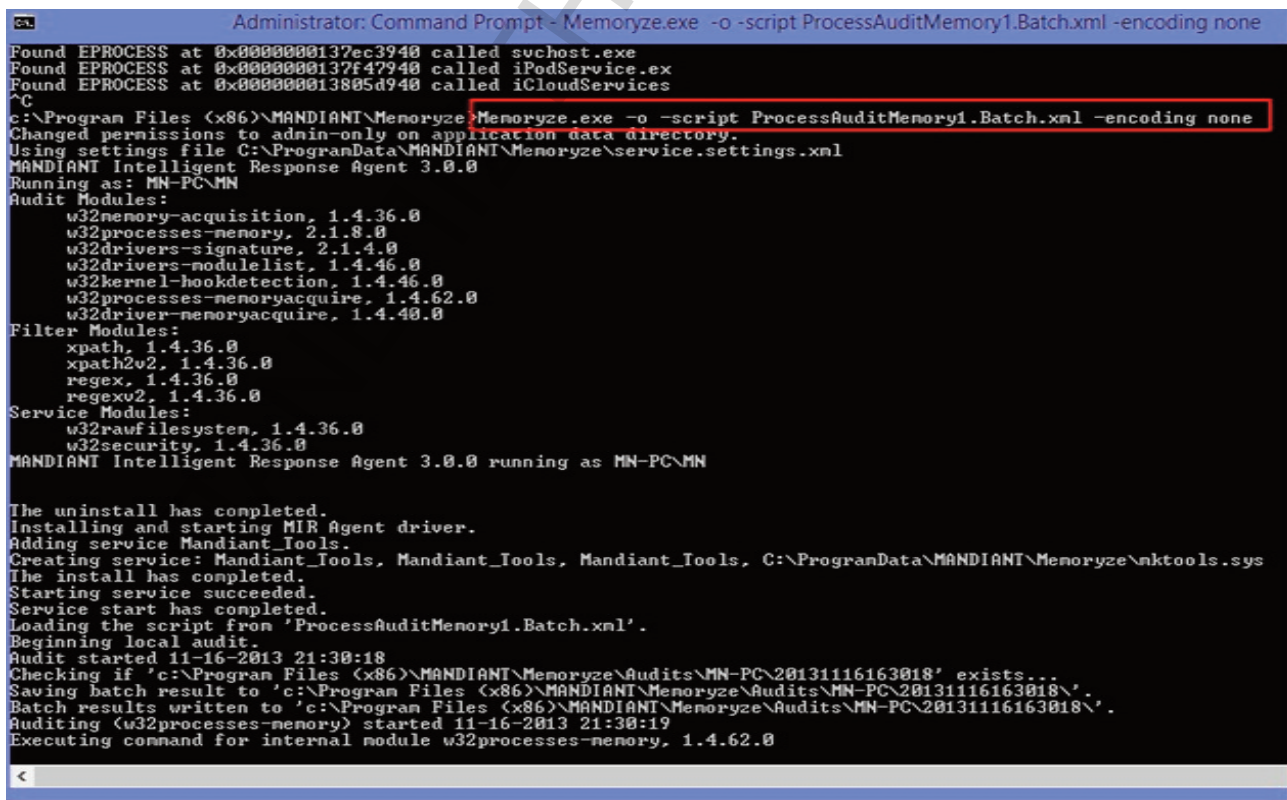


Image 3.3.2: Memoryze.exe

Memoryze has the capability to identify the OS for the memory image provided automatically and it correctly identified both the OS and the version.

```

Administrator: Command Prompt - Memoryze.exe -o -script ProcessAuditMemory1.Batch.xml -encoding none
MANDIANT Intelligent Response Agent 3.0.0 running as MN-PC\MN
The uninstall has completed.
Installing and starting MIR Agent driver.
Adding service Mandiant_Tools.
Creating service: Mandiant_Tools, Mandiant_Tools, Mandiant_Tools, C:\ProgramData\MANDIANT\Memoryze\mktools.sys
The install has completed.
Starting service succeeded.
Service start has completed.
Loading the script from 'ProcessAuditMemory1.Batch.xml'.
Beginning local audit.
Audit started 11-16-2013 21:30:18
Checking if 'c:\Program Files (x86)\MANDIANT\Memoryze\Audits\MN-PC\20131116163018' exists...
Saving batch result to 'c:\Program Files (x86)\MANDIANT\Memoryze\Audits\MN-PC\20131116163018\'.
Batch results written to 'c:\Program Files (x86)\MANDIANT\Memoryze\Audits\MN-PC\20131116163018\'.
Auditing (w32processes-memory) started 11-16-2013 21:30:19
Executing command for internal module w32processes-memory, 1.4.62.0
<Issue number="17000" level="Info" summary="Internal InformationPAE is enabled" context="FindOSVersion"/>
<Issue number="17003" level="Info" summary="Internal InformationAlgorithm found a major version of Windows 8." context="FindOSU
<Issue number="17002" level="Info" summary="Internal InformationAlgorithm found a minor version of Service Pack 0." context="Fi
>
Found EPROCESS at 0x0000000011282640 called iexplore.exe
<Issue number="17300" level="Warning" summary="Access ViolationUnable to translate or map Object Header Name Info at 0x8a7a51f0
8A85130-8683-4CFE-98A7-D6D9B5E906D6" context="ProcessHandleEntry"/>
<Issue number="17300" level="Warning" summary="Access ViolationUnable to translate or map Object Header Name Info at 0x8a7a51b0
FEABA81-3EDF-4E4A-933E-CB3984B031B1" context="ProcessHandleEntry"/>
Found EPROCESS at 0x00000000162c5b80 called svchost.exe
Found EPROCESS at 0x000000001e5515c0 called explorer.exe
<Issue number="17300" level="Warning" summary="Access ViolationUnable to translate or map Control Area at 0xdd38f676" ref="uui
D-444C-8C6D-66E433239CFB" context="EnumerateUAD"/>
<Issue number="17300" level="Warning" summary="Access ViolationUnable to translate or map Control Area at 0x05ffffed" ref="uui
C-40C0-A6EE-DE938C118E67" context="EnumerateUAD"/>
Found EPROCESS at 0x0000000038123900 called firefox.exe
<Issue number="17300" level="Warning" summary="Access ViolationUnable to translate or map Control Area at 0xffff2da6" ref="uui
1-4A7F-B311-D861A5BC3E7C" context="EnumerateUAD"/>

```

Image 3.3.3: Memoryze OS – Version identification

The results of analysis are stored by Memoryze in a folder in XML format and Redline tool is used to view them graphically. The option selected was to view already collected artifacts from a memory analysis performed by Memoryze and then We opted to investigate the entire memory image.

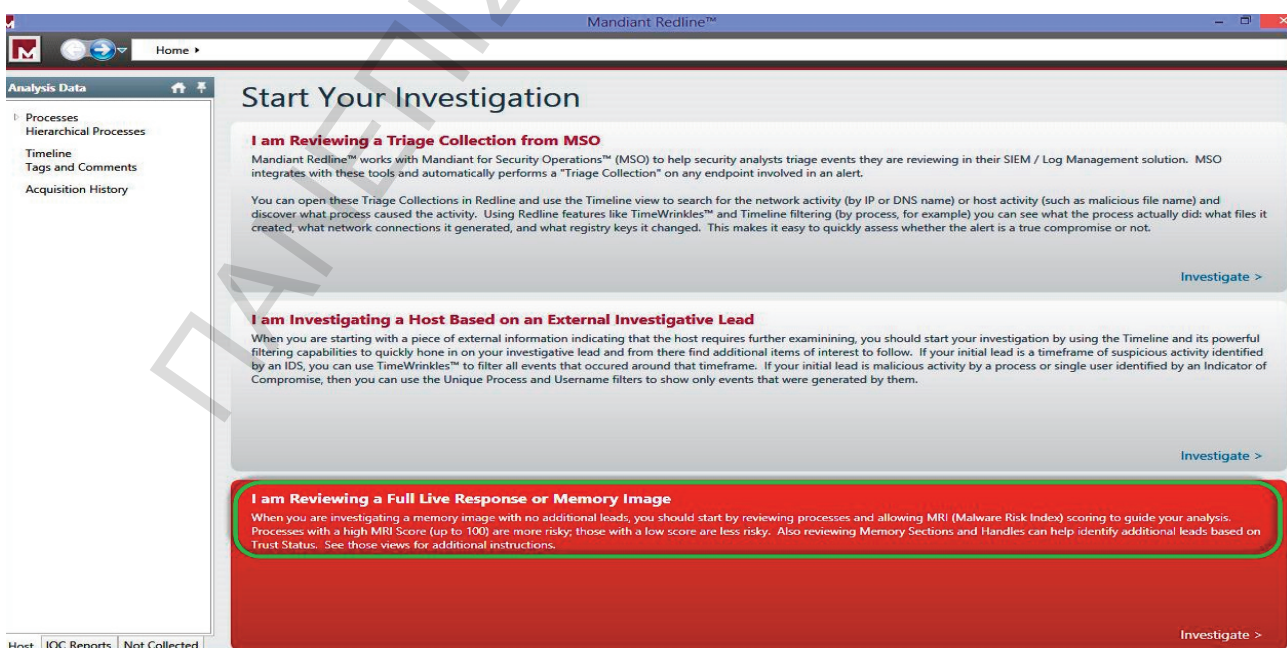


Image 3.3.4: Redline tool

Red line presents an interactive GUI for analyzing the results. The list of processes running in the memory can be seen by clicking Process link. A detailed description and path for each process is listed.

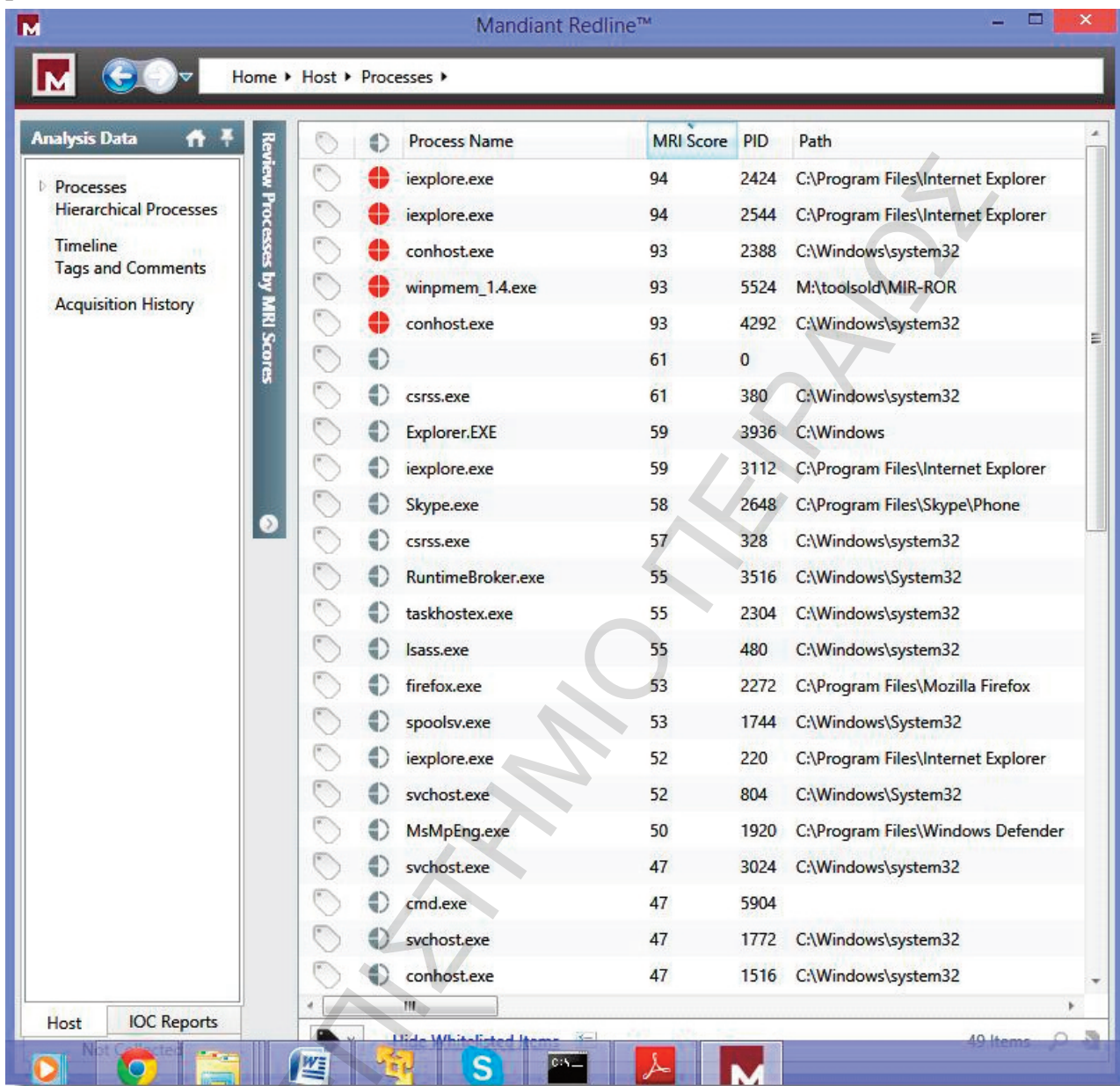


Image 3.3.5: Redline Process link

Clicking on Timelines link displays the process creation / stopping time line for every process.

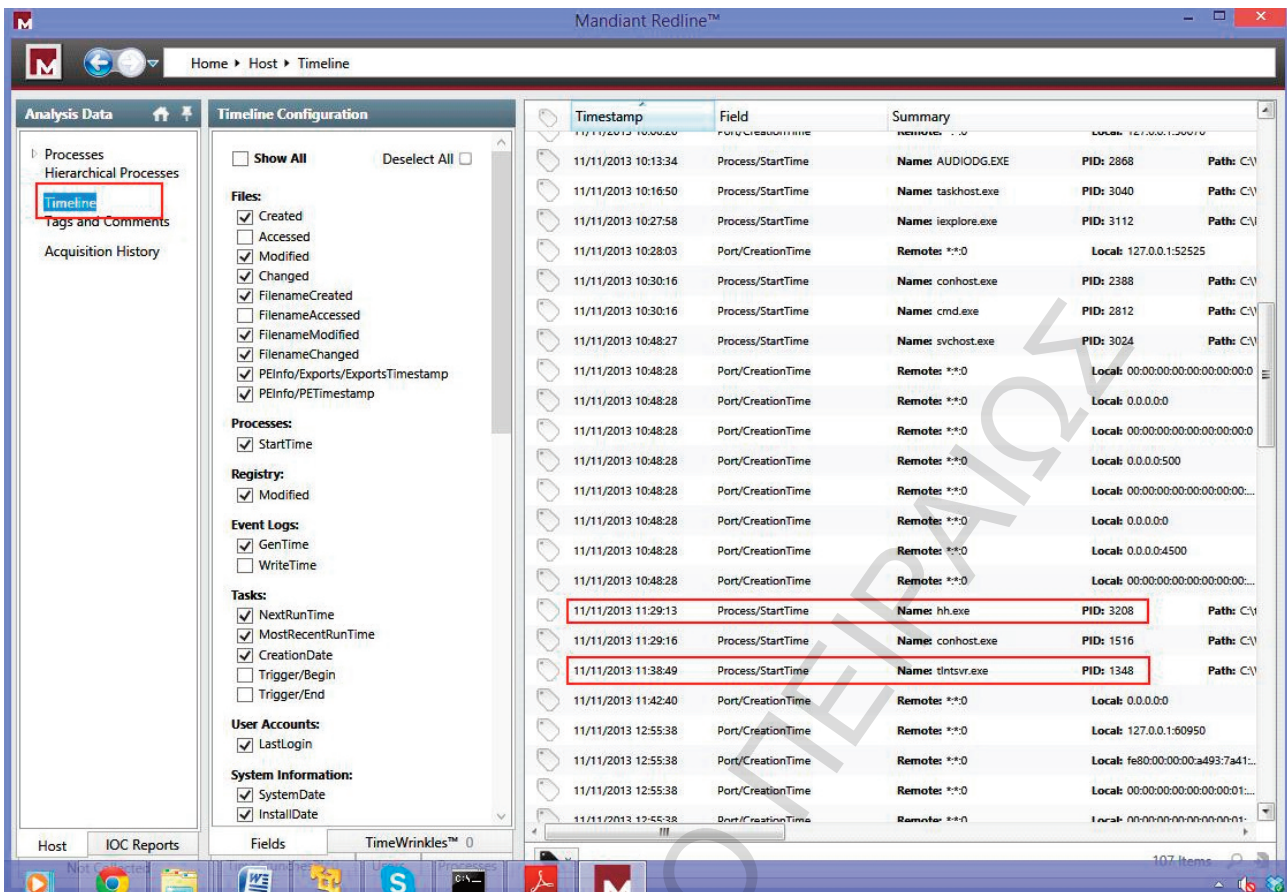


Image 3.3.6: Redline Timelines link

Handles opened by various processes can be seen by clicking Handles link.

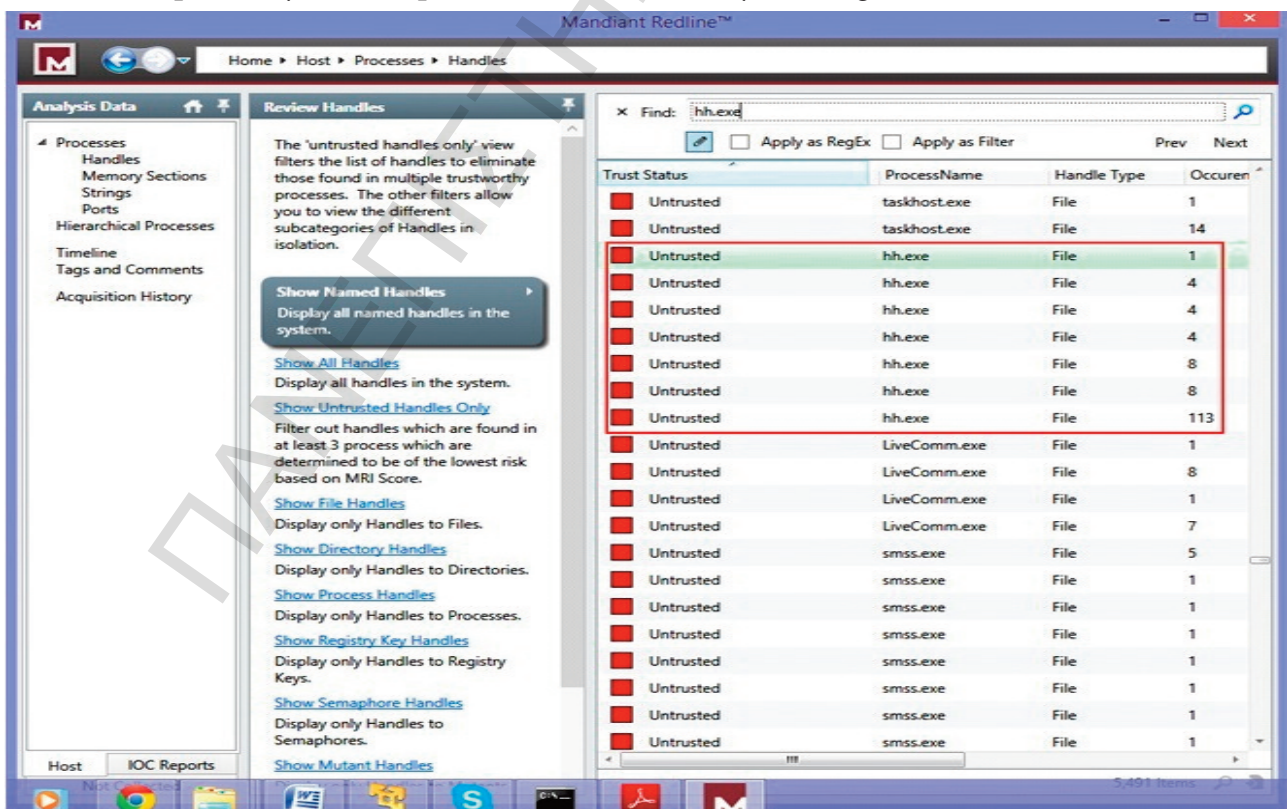


Image 3.3.7: Redline Handles

The ports opened by each process as present in the memory can be seen by clicking on Ports link. This list can be further filtered based on port state. 'Listening' and 'Established' ports. Telnet port 23 can be seen in the graphic below to be listening.

The screenshot shows the 'Review Network Ports' window in Mandiant Redline. The 'Listening Ports' section is highlighted with a red box. Below it, a table lists the following data:

Process Name	PID	State	Local IP Address	Loc...	Remote IP Add...	Re...	Protocol
winit.exe	388	LISTENING	0.0.0.0	491...	0	TCP	
iepl.exe	220	LISTENING	127.0.0.1	500...	*:*	0	UDP
iepl.exe	3112	LISTENING	127.0.0.1	525...	*:*	0	UDP
iepl.exe	2424	LISTENING	127.0.0.1	500...	*:*	0	UDP
iepl.exe	2544	LISTENING	127.0.0.1	619...	*:*	0	UDP
Skype.exe	2648	LISTENING	127.0.0.1	626...	*:*	0	UDP
Skype.exe	2648	LISTENING	0.0.0.0	0	*:*	0	UDP
wmpnetw.exe	924	LISTENING	0.0.0.0	554	0	TCP	
wmpnetw.exe	924	LISTENING	00:00:00:00:00:...	554	0	TCP	
wmpnetw.exe	924	LISTENING	00:00:00:00:00:...	5005	*:*	0	UDP
wmpnetw.exe	924	LISTENING	0.0.0.0	5005	*:*	0	UDP
wmpnetw.exe	924	LISTENING	0.0.0.0	5004	*:*	0	UDP
wmpnetw.exe	924	LISTENING	00:00:00:00:00:...	5004	*:*	0	UDP
svchost.exe	3024	LISTENING	00:00:00:00:00:...	0	*:*	0	UDP
svchost.exe	3024	LISTENING	0.0.0.0	501...	0	TCP	
svchost.exe	3024	LISTENING	00:00:00:00:00:...	501...	0	TCP	
svchost.exe	3024	LISTENING	0.0.0.0	0	*:*	0	UDP
tlntsvr.exe	1348	LISTENING	00:00:00:00:00:...	23	0	TCP	
svchost.exe	824	LISTENING	00:00:00:00:00:...	0	*:*	0	UDP
svchost.exe	824	LISTENING	0.0.0.0	3544	*:*	0	UDP
svchost.exe	824	LISTENING	0.0.0.0	500	*:*	0	UDP
svchost.exe	824	LISTENING	0.0.0.0	0	*:*	0	UDP

Image 3.3.8: Redline Ports

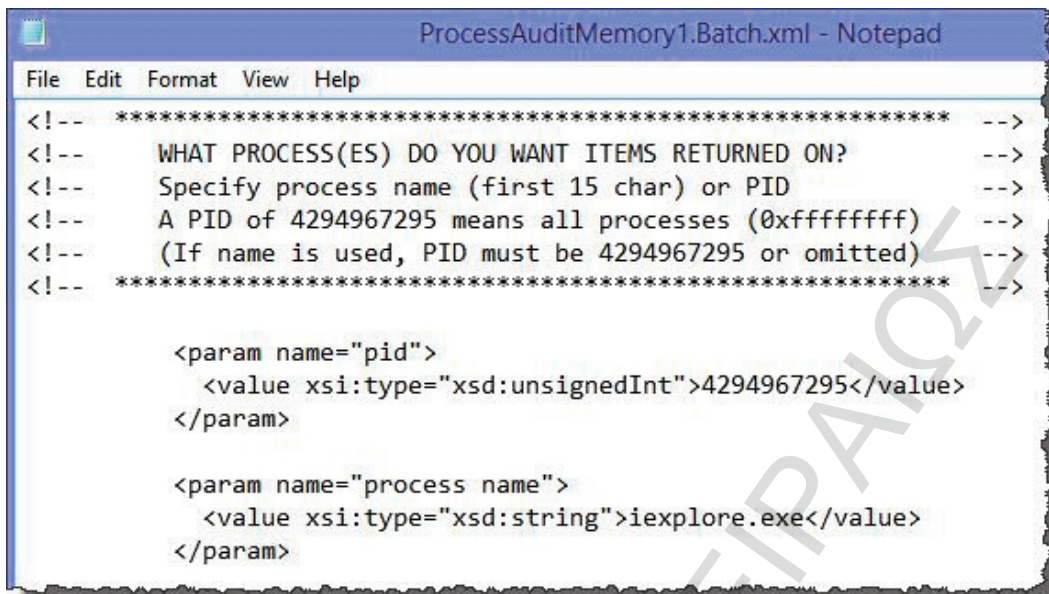
The ports in 'Established' state can be seen below.

The screenshot shows the 'Review Network Ports' window in Mandiant Redline. The 'Established Ports' section is highlighted with a red box. Below it, a table lists the following data:

Process Name	PID	State	Local IP Address	Loc...	Remote IP Add...	Re...	Protocol
System	4	ESTABLISHED	fe80:00:00:00:a...	521...	fe80:00:00:00:4...	445	TCP
System	4	ESTABLISHED	192.168.1.5	533...	192.168.1.2	445	TCP
System	4	ESTABLISHED	4.0.0.0	1024	4.0.0.0	1024	TCP
iepl.exe	2424	ESTABLISHED	192.168.1.5	531...	173.194.113.228	443	TCP
iepl.exe	2544	ESTABLISHED	192.168.1.5	531...	64.4.46.96	443	TCP
firefox.exe	2272	ESTABLISHED	192.168.1.5	531...	64.4.46.99	443	TCP
firefox.exe	2272	ESTABLISHED	127.0.0.1	511...	127.0.0.1	511...	TCP
firefox.exe	2272	ESTABLISHED	127.0.0.1	511...	127.0.0.1	511...	TCP
Explorer.EXE	3936	ESTABLISHED	192.168.1.5	535...	58.26.185.10	80	TCP
Explorer.EXE	3936	ESTABLISHED	192.168.1.5	531...	157.55.236.69	443	TCP
Explorer.EXE	3936	ESTABLISHED	192.168.1.5	535...	125.56.199.129	80	TCP
Explorer.EXE	3936	ESTABLISHED	192.168.1.5	535...	168.63.124.173	80	TCP
Explorer.EXE	3936	ESTABLISHED	192.168.1.5	535...	125.56.199.129	80	TCP
Explorer.EXE	3936	ESTABLISHED	192.168.1.5	535...	168.63.124.173	80	TCP

Image 3.3.9: Redline ports 'Established'

To see the strings in memory it is advisable to analyze one process at a time by providing Process ID (PID) or its process name in the batch file.



```

ProcessAuditMemory1.Batch.xml - Notepad
File Edit Format View Help
<!-- ***** -->
<!-- WHAT PROCESS(ES) DO YOU WANT ITEMS RETURNED ON? -->
<!-- Specify process name (first 15 char) or PID -->
<!-- A PID of 4294967295 means all processes (0xffffffff) -->
<!-- (If name is used, PID must be 4294967295 or omitted) -->
<!-- ***** -->

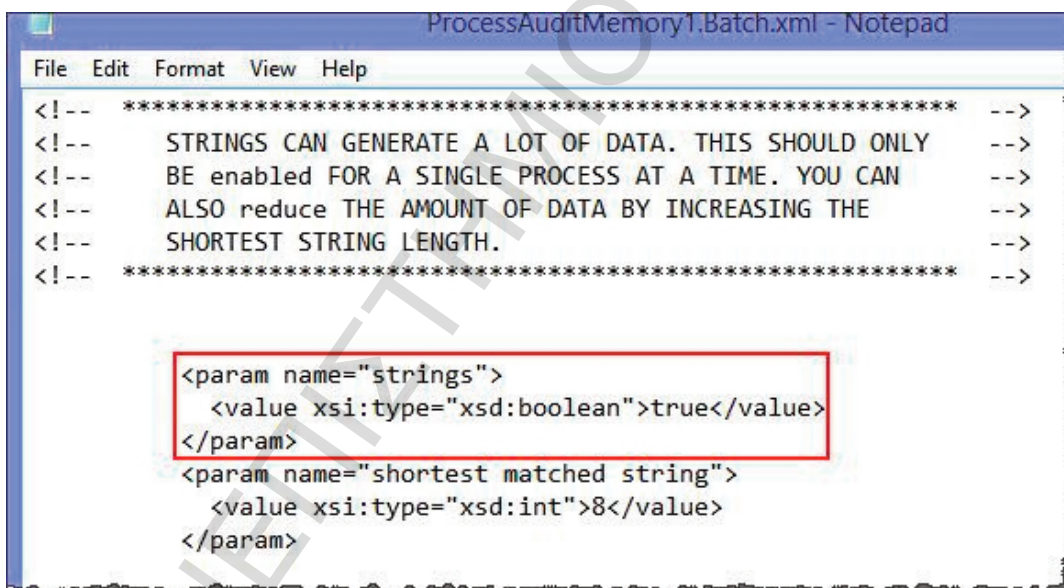
  <param name="pid">
    <value xsi:type="xsd:unsignedInt">4294967295</value>
  </param>

  <param name="process name">
    <value xsi:type="xsd:string">iexplore.exe</value>
  </param>

```

Image 3.3.10: Batch file process analyze

The strings analysis option is turned off by default and needs to be turned on, when needed.



```

ProcessAuditMemory1.Batch.xml - Notepad
File Edit Format View Help
<!-- ***** -->
<!-- STRINGS CAN GENERATE A LOT OF DATA. THIS SHOULD ONLY -->
<!-- BE enabled FOR A SINGLE PROCESS AT A TIME. YOU CAN -->
<!-- ALSO reduce THE AMOUNT OF DATA BY INCREASING THE -->
<!-- SHORTEST STRING LENGTH. -->
<!-- ***** -->

  <param name="strings">
    <value xsi:type="xsd:boolean">>true</value>
  </param>
  <param name="shortest matched string">
    <value xsi:type="xsd:int">8</value>
  </param>

```

Image 3.3.11: String Analysis option

The process memory for Internet Explorer was looked for and four instances were located in memory.

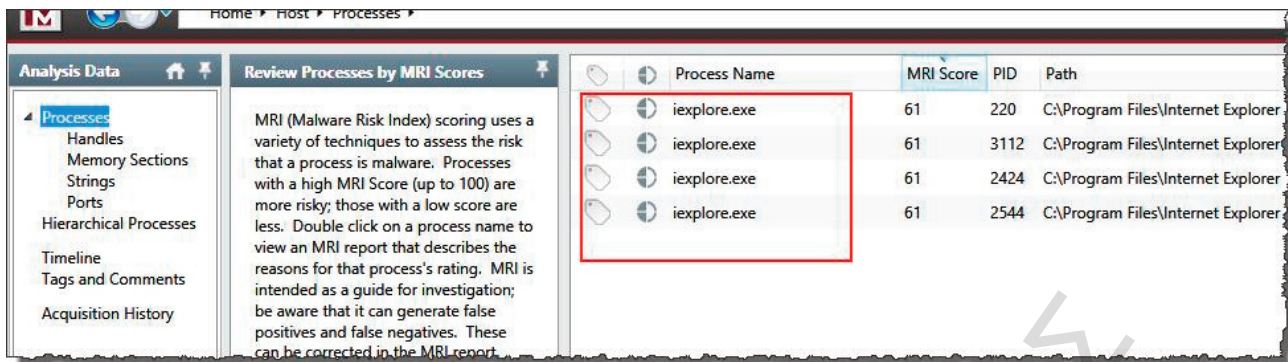


Image 3.3.12: Process memory for Internet Explorer

To look for email addresses in the memory major web mail providers were filtered and quite a few email addresses could be traced.

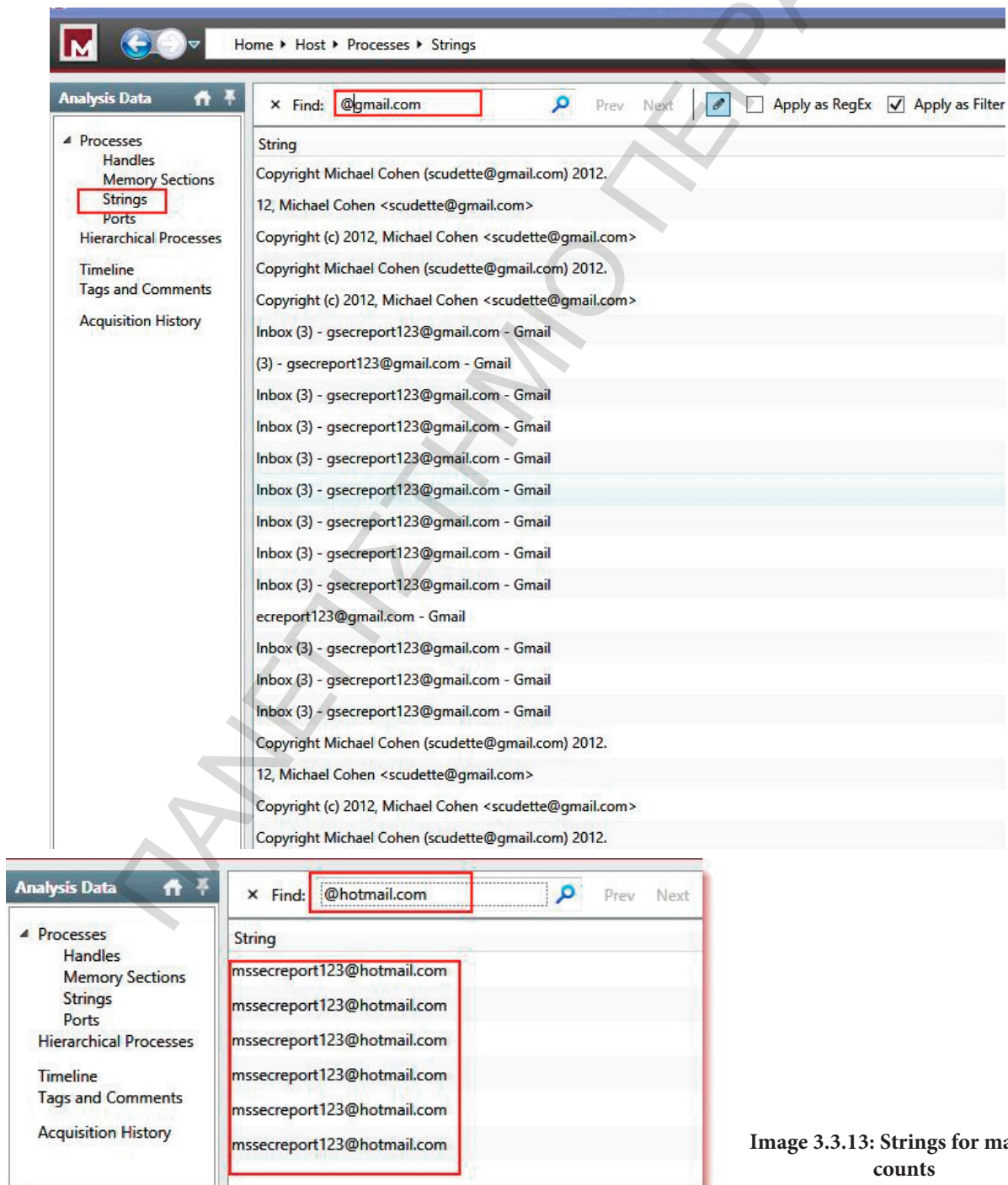


Image 3.3.13: Strings for mail accounts

Alternately regular expressions for email addresses were used to find out more email addresses.

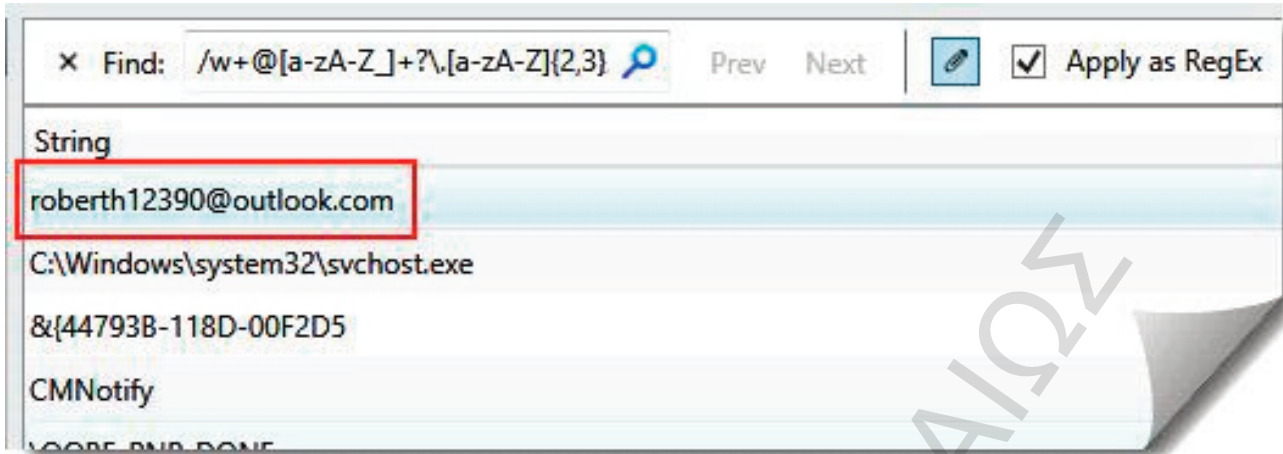


Image 3.3.14: Regular expression for email addresses

Passwords were looked for in the memory of Internet explorer.

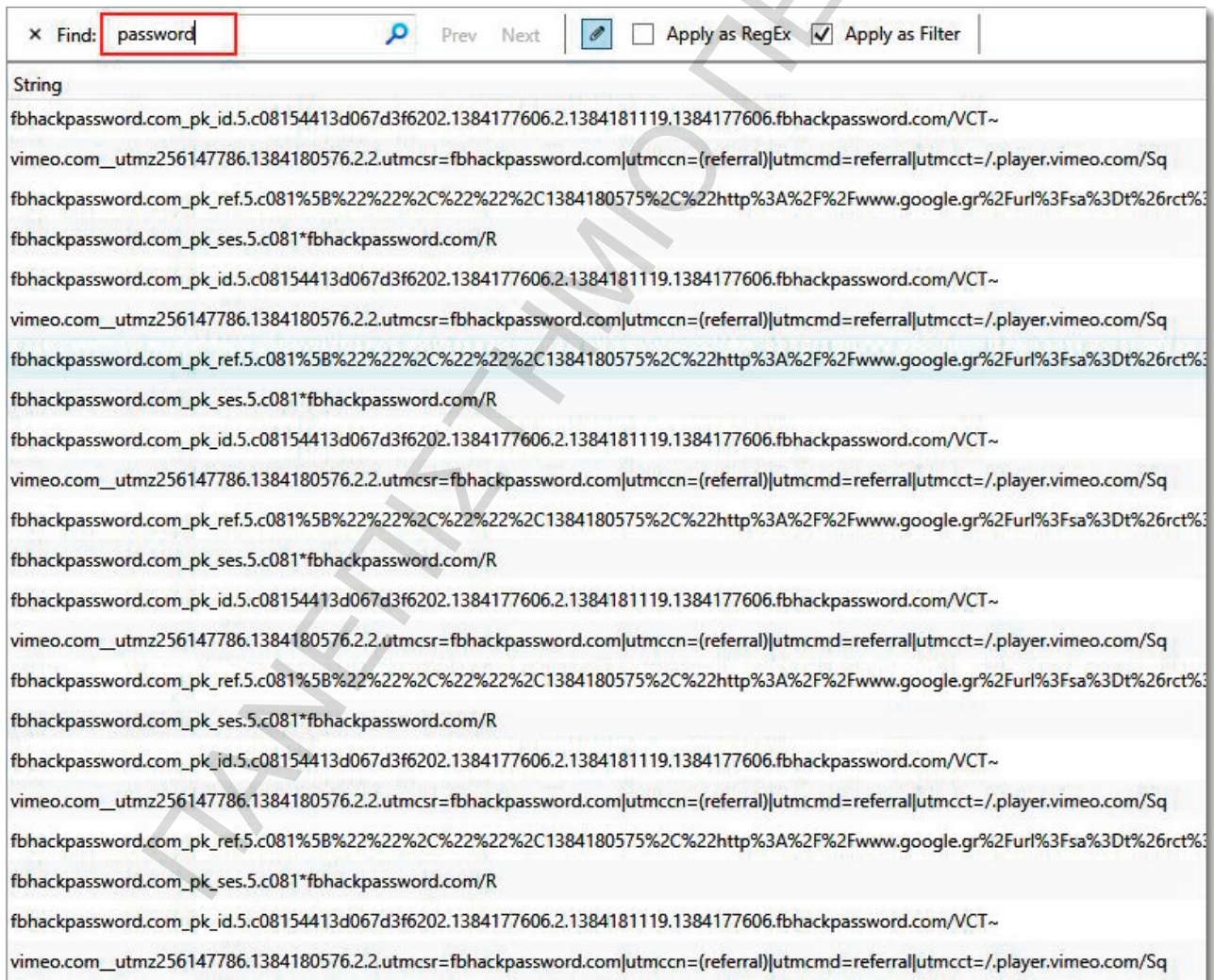


Image 3.3.15: Passwords in memory of explorer

Similarly memory analysis for Firefox.exe process was also carried out by providing the process name in the batch file.

```
<!-- ***** -->
<!-- WHAT PROCESS(ES) DO YOU WANT ITEMS RETURNED ON? -->
<!-- Specify process name (first 15 char) or PID -->
<!-- A PID of 4294967295 means all processes (0xffffffff) -->
<!-- (If name is used, PID must be 4294967295 or omitted) -->
<!-- ***** -->

<param name="pid">
  <value xsi:type="xsd:unsignedInt">4294967295</value>
</param>

<param name="process name">
  <value xsi:type="xsd:string">firefox.exe</value>
</param>
```

Image 3.3.16: Firefox.exe process in batch file

3.4 SANS SIFT ANALYSIS

The disk copy and registry copy is almost the same procedure as Windows 7 (Chapter 2.4) that's why we did not mention it.

SANS SIFT workstation provides comprehensive open source tools for carrying out forensics analysis which include autopsy browser etc. [11]

The disk image was analyzed using autopsy browser in SIFT workstation. A new case was created using the interface of autopsy.

The procedure and the results were similar with Windows 7 (2.4 SANS SIFT ANALYSIS) that's why we don't mention them again. The only result we want to check is mentioned below.

File analysis also allows for browsing and viewing files. We can see again processes hh.exe and nc.exe.

The screenshot shows the SANS SIFT workstation interface with the 'FILE ANALYSIS' tab selected. A table lists several files with their creation and modification dates and times. The files 'hh.exe' and 'nc.exe' are highlighted with a red box. Below the table, the file type is identified as 'PE32 executable for MS Windows (console) Intel 80386 32-bit'. At the bottom, the contents of the file 'D:/temp/hh.exe' are displayed, showing a message: 'This program cannot be run in DOS mode'.

Path	Creation Date/Time	Last Modified Date/Time	Accessed Date/Time	Size
d/d ../	2013-11-11 10:23:38 (EST)	2013-11-11 10:23:38 (EST)	2013-11-11 02:40:37 (EDT)	56
d/d ./	2013-11-11 08:28:46 (EST)	2013-11-11 08:28:46 (EST)	2013-11-11 06:19:21 (EST)	344
r/r hh.exe	2012-01-04 23:36:16 (EST)	2013-11-11 08:28:46 (EST)	1979-12-31 19:00:00 (EST)	778752
r/r mal-log.txt	2013-11-11 07:54:39 (EST)	2013-11-11 07:54:39 (EST)	2013-11-11 07:55:19 (EST)	0
r/r nc.exe	2012-08-17	2013-11-11	1979-12-31	61440

Image 3.4.1: Browsing and viewing files

3.5 Registry Analysis

Regripper was used to analyze the registry hives acquired from the disk of the target host. Analysis of SAM hive from %WINDIR%\system32\config\SAM provided following results. We prefer to mention only some critical points in this chapter because most of them was similar with windows 7(2.5 Registry Analysis).[12, 13]

Browser helper objects are used by malware to modify pages and insert malicious links. No such BHOs were found.

```
bho v.20130408
(Software) Gets Browser Helper Objects from Software hive

Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects not found.
Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects not found.
```

Image 3.5.1: Bho.pl

Every malware needs persistence to survive across re-boots. Soft_run.pl plugin checks for such ASEPs in registry.

```
-----
soft_run v.20130425
(Software) [Autostart] Get autostart key contents from Software hive

Microsoft\Windows\CurrentVersion\Run
LastWrite Time Thu Jul 26 06:54:12 2012 (UTC)
Microsoft\Windows\CurrentVersion\Run has no values.
Microsoft\Windows\CurrentVersion\Run has no subkeys.

Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time Mon Nov 11 08:44:37 2013 (UTC)
Microsoft\Windows\CurrentVersion\RunOnce has no values.
Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\RunServices not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce not found.

Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows
\CurrentVersion\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows
\CurrentVersion\RunOnce not found.
```

Image 3.5.2: Soft_run.pl

Image file execution is used to launch another application (may be malware) whenever an application is launched. Imagefile.pl checks for presence of such keys.

```
imagefile v.20130425
(Software) Checks IFEO subkeys for Debugger & CWDIllegalInDllSearch values

Microsoft\Windows NT\CurrentVersion\Image File Execution Options
No Debugger/CWDIllegalInDllSearch values found.

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options not found.
```

Image 3.5.3: Imagefile.pl

Ccleaner.pl locates whether ccleaner was used on the system to clean up. This affects the analysis.

```
ccleaner v.20120128
(NTUSER.DAT) Gets User's CCleaner Settings

Software\Piriform\CCleaner does not exist.
```

Image 3.5.4: Ccleaner.pl

Chapter 4 - Conclusions

4.1 Final Verification

Windows 7 and Windows 8 have an entirely different user interface and apparently seem to be different operating systems. From a forensics perspective, only few differences can be found between these two versions of Windows. Essentially, all Windows versions have inherited the basic structure in which the Windows operating system is built. In order to evaluate and compare these two operating systems from a forensics perspective, we applied suitable procedures and tools to them and compared the results to identify differences, if any. Forensics artifacts were specifically looked into.

4.2 File Downloads

File downloads may occur in various forms, like direct downloads using browsers and other software where Open/ Save dialog is used to specify the location for saving the downloaded file. The OpenSaveMRU key in NTUSER.DAT registry hive for individual user keeps a record of such downloads and it is common in both Windows 7 and 8.

Windows 7 has MS Outlook as email client bundled; it saves information about the files sent as attachments with email in the %USERPROFILE%\AppData\Local\Microsoft\Outlook folder. But in Windows 8 MS Outlook has been replaced with Mail app, which is a modified version of Windows Live Mail app. It saves the record email messages, attachments and contacts in the %USERPROFILE%\AppData\Local\Packages\microsoft.windowscommunicationsapps\Local- State\Indexed\LiveComm folder. The record of skype chats, sent / received files and calls is maintained in the same way in both version of Windows.

There is no difference in the way almost all the major browsers, such as IE, Firefox and Chrome, keep the browsing history and record of downloaded files in both these versions of the OS.

4.3 Program Execution

Due to the fact that both operating systems have the same basic structure, they follow similar program execution procedures. The user-assist mechanism helps in tracking user launched GUI-based programs with the help of icons placed on the desktop in both OS. Likewise, they keep the record of Last Visited MRU and Run MRU in the same location in registry NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Last VisitedPidlMRU and NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU respectively.

The application compatibility Cache keeps track of all the executed executables, in both Windows 7 and 8.

Jump lists are stored in Windows 8 and 7 in a similar way in the %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations folder.

4.4 File Opening/Creation

Both versions of Windows use the NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs registry key to store the record of recent documents accessed, on a per user basis.

Shell bags analysis also does not have any difference in Windows 8 and 7. It provides valuable information on how various resources, within and outside the system, were accessed using

Windows Explorer.

4.5 Deleted Information

Search -WordWheelQuery records the keyword searches in start menu in both Windows 8 and 7. The thumbnail cache system also works the same way in both OS. It stores the thumbnail copy of the pictures in the %USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer folder. There is no difference in the Recycle bin's structure as well.

4.6 Information About Physical Location

NetworkList in Software registry hive in Windows 8 and 7, maintains a list of networks / SSIDs to which the host was connected, including the MAC addresses and time. Sometimes it is also possible to pinpoint the physical location of a connection using triangulation for Wireless networks.

Cookies and Internet browsing history is also preserved in the same way in both OS.

4.7 USB Drive Usage

Both OS track the use of USB devices in a similar way and provide an identification of the devices attached to the system on a per user basis.

4.8 Account Usage

Like all the other versions of Windows, Windows 8 also tracks the account login attempts, creation times, password changes, logon type and remote access in a similar way with older versions.

4.9 Memory Forensics

Volatility is the tool of choice for memory analysis. Up till now the Windows 8 memory dump analysis is not supported by Volatility, hence it is proved to be a major stumbling block in analyzing memory. The only suitable alternate available was Memoryze but it was not proved to be as effective as Volatility. It lacked many features, such as the ability to find services, password hashes and excellent string search facility (using regex) provided by Yara plugin.

4.10 Disk Forensics

There was no difference found in the forensics details of the Hard disk image in Windows 8 and 7, as both these OS use the same file system and structure.

4.11 Live Response

The mirror script did not provide signatures of Windows 8, in order to handle the user profile location, which is the same for both OS. For this reason the script required minor modification in order to be compatible with Windows 8.

4.12 Summary

Through this research we conclude that, despite the differentiation between Windows 8 and Windows 7 in the User Interface, these two versions of Windows are very similar from a forensics point of view.

The differences found, such as mail client, user interface, memory forensics and live response, were very subtle and are largely due to the fact that the tools do not yet have signatures to identify Windows 8 and therefore fail in identifying the correct operating system.

On the other hand, the similarities between them lie in the application cache for executables programs, the way jump lists are stored, shell bags analysis and registry key, thumbnail cache and recycle bin, software registry hive, the way cookies and internet browsing history are stored, usb devices tracking, account details and disk analysis.

In summary, we conclude that almost all the tools functioned without a problem on both operating systems.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

References

1. <https://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf>.
2. “MIR-ROR: Motile Incident Response – Respond Objectively, Remediate”, <http://mirror.codeplex.com/>
3. “Mir-ror- User Instructions”, <http://holisticinfosec.org/toolsmith/pdf/june2009.pdf>
4. “Windows Sysinternals Suite”, <http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>
5. “The Volatility Framework”, online, <https://code.google.com/p/volatility/>
6. “Yara-Project, A malware identification and classification tool”, <https://code.google.com/p/yara-project/>
7. “Regular Expression Library”, <http://regexlib.com/Search.aspx?k=email&AspxAutoDetectCookieSupport=1>
8. “Finding or Verifying Credit Card Numbers”, <http://www.regular-expressions.info/creditcard.html>.
9. Dcfldd <http://dcfldd.sourceforge.net/>
10. Dcfldd <http://dcfldd.sourceforge.net/>
11. “SANS Investigate Forensic Toolkit (SIFT) Workstation Version 2.14”, <http://computer-forensics.sans.org/community/downloads#acquire>
12. “Regripper”, <https://code.google.com/p/regripper/wiki/RegRipper>
13. “Windows Registry Forensics: Advanced Digital Forensic Analysis”, <http://160.216.223.99/vyuka/forensics/Windows%20Registry%20Forensics.pdf>.
14. “Memoryze™, Find Evil in Live Memory”, <http://www.mandiant.com/resources/download/memoryze>
15. “Mandiant Redline™, Accelerated Live Response”, <https://www.mandiant.com/resources/download/redline>

