

# CIRCL - DFIR 1.0.3

Introduction: Windows-, Memory- and File Forensics



CIRCL *TLP:WHITE*

[info@circl.lu](mailto:info@circl.lu)

Edition May 2020

# Overview

---

1. Windows Registry
2. Event Logs
3. Other Sources of Information
4. Malware Analysis
5. Analysing files
6. Live Response
7. Memory Forensics
8. Bibliography and Outlook



# CIRCL **FORENSICS Training**

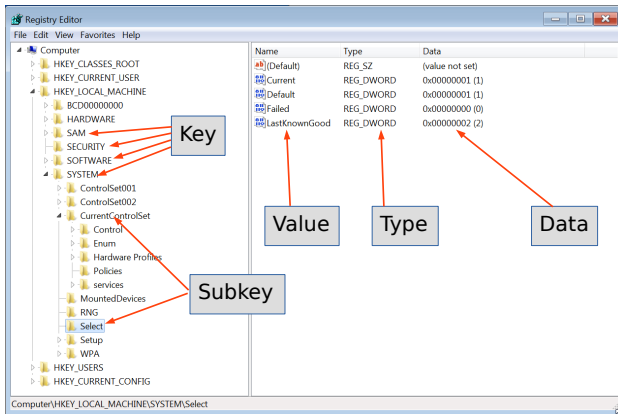
## 1. Windows Registry

## 1.1 About: Windows Registry

---

- MS DOS and old Windows
    - On system boot: What programs to load
    - How the system interact with the user
      - `autoexec.bat`
      - `config.sys`
      - `system.ini`
      - `win.ini`
  - <https://support.microsoft.com/en-us/help/256986/>
    - A central hierarchical database
    - Replace text based config files
    - Contains information for operating
      - Hardware in the system
      - All aspects of MS Windows
      - Installed applications
      - Each user
- A gold mine for forensics

# 1.1 About: Windows Registry



Key data structures contains a last write time stamp

## 1.1 About: Windows Registry

---

- Do you ever touch the Registry?
  - `regedit.exe`
  - Black Magic for many admins
    - Every user interacts with the Registry
- Location of the hive files
  - `%SystemRoot%\system32\config`
    - SAM, SECURITY, SYSTEM, SOFTWARE
  - `%UserProfile%\NTUSER.DAT`
  - `%UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat`
- Timestamps → Timeline

## 1.2 Under the hood: Key Cell

---

```
0000:  a0ff ffff  6e6b 2000  6f0f 0e3b b78d d101  ....nk .o..;....
0010:  0200 0000 085e 0500  0000 0000 0000 0000  ....^.....
0020:  ffff ffff ffff ffff  0200 0000 0021 0500  ....!...
0030:  102e 0000 ffff ffff  0000 0000 0000 0000  .....
0040:  1400 0000 1000 0000  0000 0000 0a00 0000  .....
0050:  496e 7465 7266 6163  6573 0080 0200 0000  Interfaces.....
```

Offsets:	0x00	0	4	Size
	0x04	4	2	Node ID
	0x06	6	2	Node type
	0x08	8	8	Last write time
	...	...		
	0x4c	76	2	Lenght of key name
	0x50	80	<76>	key name + padding

- Exercise: Calculate the size of the key cell  
a0 ff ff ff
- Exercise: Calculate the size of the key name  
0a 00

## 1.2 Under the hood: Value Cell

---

```
0000:                                d8ff ffff  766b 0d00          ....vk..
0010:  0400 0080 0200 0000  0400 0000 0100 0000  .....
0020:  4c61 7374 4b6e 6f77  6e47 6f6f 6400 0000  LastKnownGood...
```

Offset :	0x00	0	4	Size
	0x04	4	2	Node ID
	0x06	6	2	Value name length
	0x08	8	4	Data lenght
	0x0c	12	4	Data offset
	0x10	16	4	value typw

- Exercise: Calculate the size of the value cell

d8 ff ff ff

- Exercise: Calculate the size of the value name length

0d 00



## 1.3 Hive files

---

- SAM
  - Local users
- Security
  - Audit settings
  - Machine, domain SID
- System
  - General system configuration
  - Networking, Auto run
  - Program execution
  - USB devices
- Software
  - Windows version, Profiles list
  - Networking, Auto run
  - Shell extensions, Browser helper objects
  - Scheduled Tasks
  - Program execution

## 1.3 Hive files

---

- Windows XP:

`C:\Documents and Settings\<username>\NTUSER.DAT`

`C:\Documents and Settings\<username>\Local Settings\  
Application Data\Microsoft\Windows\UsrClass.dat`

- Windows Vista and above:

`C:\Users\<user>\NTUSER.DAT`

`C:\Users\<user>\AppData\Local\Microsoft\Windows\  
UsrClass.dat`

- `C:\Windows\inf\setupapi.log`

## 1.4 RegRipper

---

- Extract specific key values

```
$ rip.pl -p compname -r SYSTEM
    ComputerName = WIN7WS
    TCP/IP Hostname = Win7WS
```

- Alternative method

```
$ wine rip.exe -p compname -r SYSTEM
    ComputerName = WIN7WS
    TCP/IP Hostname = Win7WS
```

- RegRipper plugins

```
$ ls -l /usr/share/regripper/plugins | wc -l
397
```

- Ripping hive files with profiles

```
$ rip.exe -f sam -r SAM > out/sam.txt
$ rip.exe -f security -r SECURITY > out/security.txt
$ rip.exe -f system -r SYSTEM > out/system.txt
$ rip.exe -f software -r SOFTWARE > out/software.txt
$ rip.exe -f ntuser -r NTUser.dat > out/ntuser.txt
$ rip.exe -f usrclass -r UsrClass.dat > out/userClass.txt
```

## 1.5 RegRipper: Exercise

---

1. Extract Hive files from infected PC
2. Rip them with RegRipper profiles
3. Collect important general information
4. Try to find incident related artefacts
5. Add the information to report

## 1.6 Examples: System Hive

---

- Computer name
- Services
- Network configuration
- Devices / USB device
  - `SYSTEM/ControlSet001/Enum/USBStor`
    - Device class ID
    - Unique instance ID (SN)
    - First connect time stamp
  - `SYSTEM/ControlSet001/Enum/USB`
    - Last connect time stamp
  - `SYSTEM/MountedDevices`
    - Volume GUID
    - Mount Point

## 1.7 Examples: Software Hive

---

- OS version & configuration
- Applications installed & uninstalled
- Application configuration system wide
- Drivers
- Network lists & interfaces
- User profiles
- Schedules Tasks
- Auto start
- Example: Get Windows version:
  - `wine rip.exe -p winver -r SOFTWARE`

## 1.7 Examples: User Hive

---

- OS configuration user related
- Applications installed & uninstalled
- Application configuration user related
- Auto start
  - Run
    - Executed at user login
    - Provide *malware* persistence
    - No admin privileges required
  - RunOnce
  - Legacy and other AutoStart
    - `/Software/Microsoft/Windows/CurrentVersion/Policies/Explorer/Run/`
    - `/Software/Microsoft/Windows NT/CurrentVersion/Windows/'load','run'`
  - Much more auto start loctions...

## 1.7 Examples: User Hive

---

- WordWheelQuery
  - User search on localhost
  - MRU List
    - Consider VSS for historical data
- Shell Bags
  - User preferences for displaying Explorer windows
  - Position, size, view, icon
    - Folders accessed by the user
- UserAssist
  - User activities
    - Double-click icon
    - Launch application from 'START Menu'
  - Values stored:
    - Path, Run-Count, FileTime last access
    - ROT-13



## 1.7 Examples: User Hive

---

- MUICache
  - Program execution incl. called from CMD
- RecentDocs

Example: '.png' files

```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.png
LastWrite Time Fri Jan 12 15:00:52 2018 (UTC)
MRUListEx = 3,2,0,1
  3 = photo-123.png
  2 = paint.png
  0 = face.png
  1 = flower.png
```

- Common Dialogs

Example: 'Open' and 'Save As...'

```
OpenSavePidIMRU\exe
LastWrite Time: Tue Jul 5 14:40:46 2016
Note: All value names are listed in MRUListEx order.
```

```
Users\avast-free-antivirus-setup-online.exe
Users\Thunderbird Setup 45.1.1.exe
Users\Firefox Setup Stub 47.0.1.exe
```

## 1.8 Exercises

---

Identify computer name:

What services start during system boot:

Gather list of network connected:

What network cards are configured:

Get list of user profiles:

Get Windows version:

Detect Auto Start applications from the NTUser.dat hive:

.

## 1.8 Exercises

---

Identify computer name:

```
$ wine rip.exe -p compname -r SYSTEM
```

What services start during system boot:

```
$ wine rip.exe -p services -r SYSTEM
```

Gather list of network connected:

```
$ wine rip.exe -p networklist -r SOFTWARE
```

What network cards are configured:

```
$ wine rip.exe -p networkcards -r SOFTWARE
```

Get list of user profiles:

```
$ wine rip.exe -p profilelist -r SOFTWARE
```

Get Windows version:

```
$ wine rip.exe -p winver -r SOFTWARE
```

Detect Auto Start applications from the NTUser.dat hive:

```
$ wine rip.exe -p user_run -r JohnNTUser.DAT
```



## 2. Windows Event Logs

## 2.1 Introduction

---

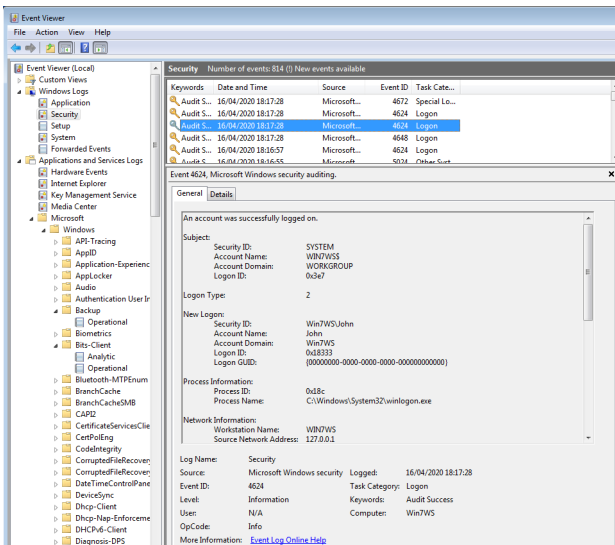
- Up to Windows XP
  - Binary Event Log file format
  - Mainly 3 categories:
    - Security: `secevent.evt`
    - System: `sysevent.evt`
    - Application: `appevent.evt`
    - ... maybe some server service specific
- Beginning with Vista
  - New binary XML format
  - New extension: `.evtx`
  - Location: `/Windows/System32/winevt/Logs/`
  - Many more files:
    - Security.evtx
    - System.evtx
    - Application.evtx
    - 120 files ++

## 2.1 Introduction

---

- Advantage
  - Full fledged logging
  - Logon Success: Important events are logged
  - Detailed important information
- Disadvantage
  - Cover only a limited period of time
  - Logon Fail: Important events are not logged per default
  - Much information, hard to read
- Always interesting
  - Logon / Logoff
  - System boot
  - Services started

## 2.2 Example: Logon event



The screenshot displays the Windows Event Viewer application. The left-hand pane shows the 'Event Viewer (Local)' tree with 'Security' logs expanded. The right-hand pane shows a list of security events. Event 4624, 'Logon', is selected. Below the list, the details for Event 4624 are shown, including the subject (SYSTEM), logon type (2), and process information.

Keywords	Date and Time	Source	Event ID	Task Category
Audit S...	16/04/2020 18:17:28	Microsoft...	4672	Special Lo...
Audit S...	16/04/2020 18:17:28	Microsoft...	4624	Logon
Audit S...	16/04/2020 18:17:28	Microsoft...	4624	Logon
Audit S...	16/04/2020 18:17:28	Microsoft...	4648	Logon
Audit S...	16/04/2020 18:16:57	Microsoft...	4624	Logon
Audit S...	16/04/2020 18:16:55	Microsoft...	5024	Other Secur...

Event 4624, Microsoft Windows security auditing.

**General** | Details

An account was successfully logged on.

**Subject:**

- Security ID: SYSTEM
- Account Name: WIN7WS
- Account Domain: WORKGROUP
- Logon ID: 0x3e7

**Logon Type:** 2

**New Logon:**

- Security ID: Win7WS\John
- Account Name: John
- Account Domain: Win7WS
- Logon ID: 0xd8333
- Logon GUID: {00000000-0000-0000-0000-000000000000}

**Process Information:**

- Process ID: 0x18c
- Process Name: C:\Windows\System32\winlogon.exe

**Network Information:**

- Workstation Name: WIN7WS
- Source Network Address: 127.0.0.1

**Log Name:** Security

**Source:** Microsoft Windows security    **Logged:** 16/04/2020 18:17:28

**Event ID:** 4624    **Task Category:** Logon

**Level:** Information    **Keywords:** Audit Success

**User:** N/A    **Computer:** Win7WS

**OpCode:** Info

**More Information:** [Event Log Online Help](#)

## 2.3 In Forensics

---

- Get support online:
  - Microsoft TechNet
  - <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>
  - <http://eventid.net/>
- Review logging policies

```
$ rip.pl -r SECURITY -p auditpol
.....
system:Other System Events                S/F
Logon/Logoff:Logon                        S
Logon/Logoff:Logoff                       S
Logon/Logoff:Account Lockout              S
Logon/Logoff:IPsec Main Mode              N
Logon/Logoff:IPsec Quick Mode             S
Logon/Logoff:IPsec Extended Mode          N
Logon/Logoff:Special Logon                N
Logon/Logoff:Other Logon/Logoff Events    N
Logon/Logoff:Network Policy Server        S/F
Object Access:File System                 N
.....
```



## 12.4 Explore and extract evtv

Untitled.elx - Event Log Explorer

File View Event Advanced Window Help

<Load filter>

Security on WIN8-SIFT

Showing 28541 event(s)

Type	Date	Time	Event	Source	Category	User	Comp
Audit Success	4/17/2020	6:18:17 AM	4624	Microsoft-Windows-SeLogon	N/A	N/A	Win8
Audit Success	4/17/2020	6:18:17 AM	4648	Microsoft-Windows-SeLogon	N/A	N/A	Win8
Audit Success	4/17/2020	6:18:04 AM	4672	Microsoft-Windows-SeSpecial Logon	N/A	N/A	Win8
Audit Success	4/17/2020	6:18:04 AM	4624	Microsoft-Windows-SeLogon	N/A	N/A	Win8
Audit Success	4/17/2020	6:06:49 AM	4672	Microsoft-Windows-SeSpecial Logon	N/A	N/A	Win8
Audit Success	4/17/2020	6:06:49 AM	4624	Microsoft-Windows-SeLogon	N/A	N/A	Win8
Audit Success	4/17/2020	6:06:20 AM	4672	Microsoft-Windows-SeSpecial Logon	N/A	N/A	Win8

Description

Account Domain: DFIR  
Logon ID: 000003E7

Logon Type: 5

Impersonation Level: Impersonation

New Logon:  
Security ID: S-1-5-18  
Account Name: SYSTEM  
Account Domain: NT AUTHORITY  
Logon ID: 000003E7  
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:  
Process ID: 00000234  
Process Name: C:\Windows\System32\services.exe

Network Information:  
Workstation Name: -  
Source Network Address: -  
Source Port: -

Detailed Authentication Information:  
Logon Process: Advapi  
Authentication Package: Negotiate  
Transited Services: -  
Package Name (NTLM only): -  
Key Length: 0

## 2.5 Example

---

- Logon Success

```
$ evtxexport Security.evtx | less
.....
Event number           : 668
Written time           : Apr 15, 2019 12:58:33.650031000 UTC
Event level             : Information (0)
Computer name          : Win7WS
Source name             : Microsoft—Windows—Security—Auditing
Event identifier        : 0x00001210 (4624)
Number of strings       : 20
String: 1               : S-1-5-18
String: 2               : WIN7WS$
String: 3               : WORKGROUP
String: 4               : 0x000000000000003e7
String: 5               : S-1-5-21-3408732720-2018246097-660081352-1000
String: 6               : John
String: 7               : Win7WS
String: 9               : 2
.....
String: 17              : 0x0000018c
String: 18              : C:\Windows\System32\winlogon.exe
String: 19              : 127.0.0.1
```

- Logon Fail

```
$ evtxexport Security.evtx | grep 4625
```

## 2.5 Example

Monterey Technology Group, ... (US) | https://www.ultimatewindowssecurity.com/se | ...

This is a valuable piece of information as it tells you HOW the user just logged on:

Logon Type	Description
2	Interactive (login at keyboard and screen of system)
3	Network (i.e. connection to shared folder on this computer from elsewhere on network)
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unattended workstation with password protected screen saver)
8	NetworkCleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authentication") <a href="#">See this article for more information.</a>
9	NewCredentials such as with RunAs or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. If you want to track users attempting to logon with alternate credentials see <a href="#">4648</a> . MS says "A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections."
10	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)

**Impersonation Level: (Win2012 and later)**

From MSDN

Anonymous	Anonymous COM impersonation level that hides the identity of the caller. Calls to WMI may fail with this impersonation level.
-----------	---

## 2.6 Other log files

---

- `/Windows/setuplog.txt`
  - Untill WinXP, when Windows is installed
- `/Windows//Debug/netsetup.log`
  - Untill WinXP, when Windows is installed
- `/Windows/setupact.log`
  - Graphical part of setup process

```
2019-04-05 11:39:56, Info CBS Starting the TrustedInstaller main loop.
2019-04-05 11:39:56, Info CBS TrustedInstaller service starts successfully.
2019-04-05 11:39:56, Info CBS Setup in progress, aborting startup processing check
2019-04-05 11:39:56, Info CBS Startup processing thread terminated normally
```
- `/Windows/setupapi.log`
  - `/Windows/inf/setupapi.dev.log`
  - `/Windows/inf/setupapi.app.log`
  - `/Windows/inf/setupapi.offline.log`
- `/Windows/Tasks/SCHEDLGU.TXT`
  - Task Scheduler Log

## 2.7 Exercise: Event Log

---

1. Which .evtx files could be interesting for forensics?
2. Extract promising .evtx files
3. Try tools like `evtx_dump.py` to read some logs
4. Find general information like:
  - What time the system boot up
  - What user was logged on
  - Was there much user activity before infection
  - What time the system shut down
5. Search for other incident related artefacts in .evtx files
6. Are artefacts within the other log files?

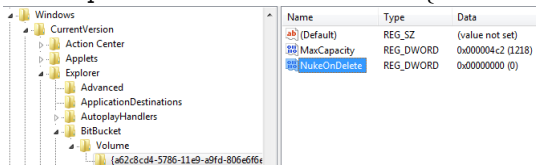


### 3. Other Sources of Information

## 3.1 Recycle Bin - User support to undelete

---

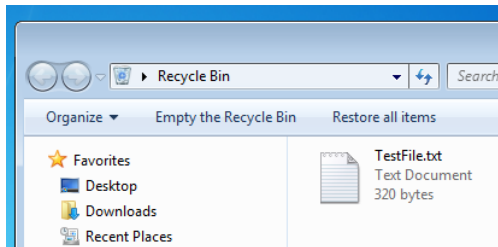
- Files move to Recycle Bin:
  - Moved by mouse
  - Right click: Delete
- Not move to Recycle Bin:
  - Right click: Delete + SHIFT
  - Command line: del
  - Files on network shares
- NukeOnDelete
  - HKEY\_USERS/\_UID\_/Software/Microsoft/Windows/CurrentVersion/Explorer/BitBucket/Volume/{\_Volume ID\_}/NukeOnDelete



## 3.1 Recycle Bin - Life-Investigate

---

- Play script: `TextFile.txt`
  - 2019-04-30 17:31:57 UTC+2: Born
  - 2019-04-30 17:34:44 UTC+2: Content Modified
  - 2019-04-30 17:35:32 UTC+2: Deleted
- Analyze Recycle.Bin:





## 3.1 Recycle Bin - Forensics

---

- Play script: `TextFile.txt`
  - 2019-04-30 17:31:57 UTC+2: Born
  - 2019-04-30 17:34:44 UTC+2: Content Modified
  - 2019-04-30 17:35:32 UTC+2: Deleted
- Analyze `Recycle.Bin` directory:

```
/$Recycle.Bin/S-1-5-21-3408732720-2018246097-660081352-1000/  
129 Apr  5 11:46  desktop.ini  
544 Apr 30 17:35  '$IOMHI9A.txt '  
320 Apr 30 17:34  '$ROMHI9A.txt '
```

```
strings \"$ROMHI9A.txt  
      Test File
```

```
=====
```

```
This is a test file. It is just created to test Forensic  
Artifacts for the 'Recycle Bin'.  
.....
```

```
strings -el \"$IOMHI9A.txt  
C:\Users\John\Documents\recycleTest\TestFile.txt
```

## 3.1 Recycle Bin - Forensics

---

- Play script: TextFile.txt
  - 2019-04-30 17:31:57 UTC+2: Born
  - 2019-04-30 17:34:44 UTC+2: Content Modified
  - 2019-04-30 17:35:32 UTC+2: Deleted
- Analyze Recycle.Bin directory:

```
Fri Apr 05 2019 11:46:49
  328 m.c.      57-144-1 /$Recycle.Bin
  376 ...b      9632-144-1 /$Recycle.Bin/S-1-5-21- ..... -1000
  129 m.cb      9634-128-1 /$Recycle.Bin/S-1-5-21- ..... -1000/desktop.ini

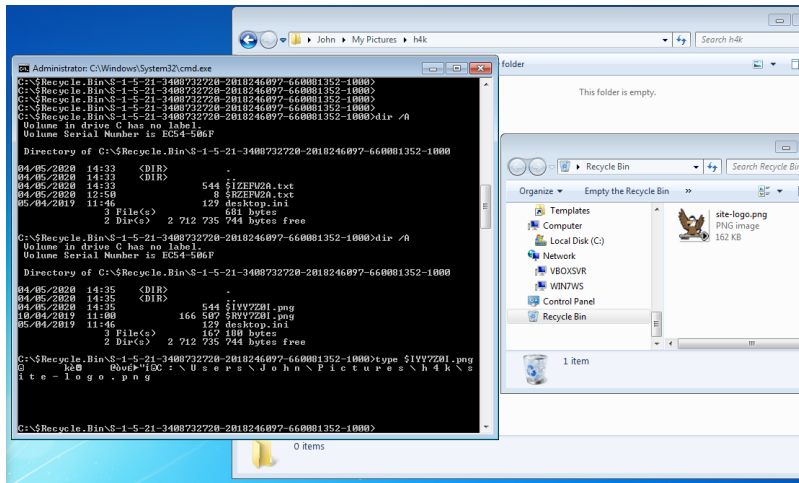
Tue Apr 30 2019 17:31:57
  320 ...b      47164-128-1 /$Recycle.Bin/S-1-5-21- ..... -1000/$ROMHI9A.txt

Tue Apr 30 2019 17:34:44
  320 ma..      47164-128-1 /$Recycle.Bin/S-1-5-21- ..... -1000/$ROMHI9A.txt

Tue Apr 30 2019 17:35:32
  544 macb      44155-128-1 /$Recycle.Bin/S-1-5-21- ..... -1000/$IOMHI9A.txt
  48 mac.       47022-144-1 /Users/John/Documents/recycleTest
  320 ..c.      47164-128-1 /$Recycle.Bin/S-1-5-21- ..... -1000/$ROMHI9A.txt
  376 mac.       9632-144-1 /$Recycle.Bin/S-1-5-21- ..... -1000
```

### 3.1 Recycle Bin - Exercise

Investigate extension of an index file \$I.....\$ for binary file:



## 3.2 LNK Files

---

- Provide information about files accessed
  - Local
  - Network shares
  - Appached devices

Thu May 02 2019 14:54:02  
280 ...b 43701-144-1 /Users/John/Documents/prefetchTest

Thu May 02 2019 14:54:28  
66 macb 43702-128-1 /Users/John/Documents/prefetchTest/  
PreFetchTest.txt  
2779 macb 43716-128-4 /Users/John/AppData/Roaming/Microsoft/  
Windows/Recent/PreFetchTest.txt.lnk  
1573 macb 43922-128-4 /Users/John/AppData/Roaming/Microsoft/  
Windows/Recent/prefetchTest.lnk

## 3.2 LNK Files

---

- Provide information about files accessed
  - Local
  - Network shares
  - Appached devices

exiftool PreFetchTest.txt.lnk

```
...
Create Date       : 2019:05:02 14:54:28+02:00
Access Date       : 2019:05:02 14:54:28+02:00
Modify Date       : 2019:05:02 14:54:28+02:00
Target File Size  : 66
Icon Index        : (none)
Run Window        : Normal
Hot Key           : (none)
Drive Type        : Fixed Disk
Volume Label      :
Local Base Path   : C:\Users\John\Documents\prefetchTest\
                  PrefetchTest.txt
...
```

## 3.3 XP Restore Points

---

- Backup of:
  - Critical system files
  - Registry partially
  - Local user profiles
  - But NO user data!
- Created automatically:
  - Every 24 hours
  - Windows Update
  - Installation of applications incl. driver
  - Manually
- For user: Useful to recover a broken system
- For analyst:
  - `rp.log`
  - Description of the cause
  - Time stamp
  - State of the system at different times

## 3.4 VSS - Volume Shadow Copy Service

---

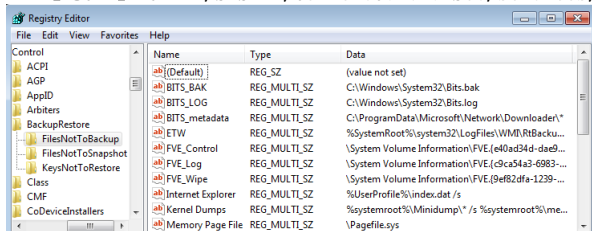
- Backup Service
  - System files
  - User data files
  - Operates on block level
- On live system
  - Run CMD as administrator

```
>vssadmin list shadows /for=c:/  
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool  
(C) Copyright 2001-2005 Microsoft Corp.
```

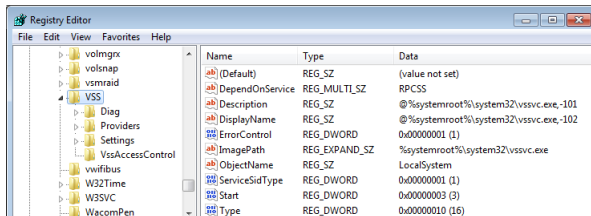
```
Contents of shadow copy set ID: {33eb3a7b-6d03-4045-aa70-37b714d49c72}  
  Contained 1 shadow copies at creation time: 10/04/2019 16:06:30  
    Shadow Copy ID: {34d9910b-ac1d-4b10-b282-89dde217d0fb}  
      Original Volume: (C:)\?\?\Volume{a62c8cd4-5786-11e9-a9fd-806e6f6e6963}\  
      Shadow Copy Volume: \?\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1  
      Originating Machine: Win7WS  
      Service Machine: Win7WS  
      Provider: 'Microsoft Software Shadow Copy provider 1.0'  
      Type: ClientAccessibleWriters  
      Attributes: Persistent, Client-accessible, No auto release, Differential,  
      Auto recovered
```

## 3.4 VSS - Configuration

HKEY\_LOCAL\_MACHINE/SYSTEM/CurrentControlSet/services/VSS



HKEY\_LOCAL\_MACHINE/SYSTEM/CurrentControlSet/Control/BackupRestore





## 3.4 VSS - Analysis

---

### Analyze disk image

```
vshadowinfo -o $((512*206848)) 8d34ce.raw
```

Volume Shadow Snapshot information:

Number of stores: 1

Store: 1

Identifier	: 237c8de3-5b99-11e9-9925-080027062798
Shadow copy set ID	: 33eb3a7b-6d03-4045-aa70-37b714d49c72
Creation time	: Apr 10, 2019 14:06:30.365699200 UTC
Shadow copy ID	: 34d9910b-ac1d-4b10-b282-89dde217d0fb
Volume size	: 11 GiB (12777947136 bytes)
Attribute flags	: 0x0042000d

### Mounting VSC: A 2 step approach

```
sudo vshadowmount -o $((512*206848)) 8d34ce.raw /mount/vss/
```

```
sudo ls -l /mount/vss/  
-r--r--r-- 1 root root 12777947136 Jan  1  1970 vss1
```

```
sudo file /mount/vss/vss1  
/mount/vss/vss1: DOS/MBR boot sector, code offset 0x52+2, OEM-ID "NTFS"
```

```
sudo mount -o ro /mount/vss/vss1 /mnt/
```

## 3.5 Prefetch Files & SuperFetch

---

- Boot prefetching for all Windows
- Application prefetching since XP
  - Monitor an application when it starts
  - Collect information about all resources needed
  - Wait 10sec after application started
    - Know where to find the resources
    - Better performance: App launch faster
    - Better user experience
- Forensics value:
  - Proof an application was started
    - Secondary artifact
    - Created by the OS
    - Not deleted by the attacker
  - Even if the application don't exists anymore
  - And more .....

## 3.5 Prefetch Files & SuperFetch

---

- Elements of the file name at /Windows/Prefetch
  - Application name
  - One way hash of path to the application
  - File extension: .pf
- Example: File system time line

```
Thu May 02 2019 14:52:40
179712 .a.. 10940-128-3 /Windows/notepad.exe
```

```
Thu May 02 2019 14:52:50
56 mac. 42729-144-6 /Windows/Prefetch
16280 macb 43700-128-4 /Windows/Prefetch/NOTEPAD.EXE-D8414F97.pf
```

- Information found inside a Prefetch file:
  - Run count: How often launched
  - Last time executed
  - Application name incl. parameter
  - Path to application and resources

## 3.5 Prefetch Files & SuperFetch

---

- Parsing a Prefetch file

```
prefetch.py -f NOTEPAD.EXE-D8414F97.pf
```

```
Executable Name: NOTEPAD.EXE
```

```
Run count: 1
```

```
Last Executed: 2019-05-02 12:52:40.339584
```

```
Resources loaded:
```

```
1:      \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\NTDLL.DLL
```

```
2:      \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNEL32.DLL
```

```
3:      \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
```

```
4:      \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNELBASE.DLL
```

```
.....
```

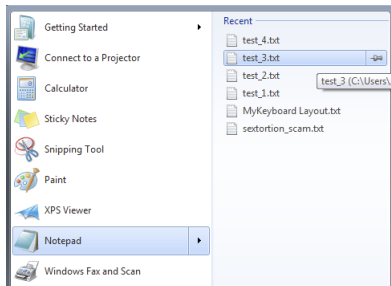
```
.....
```

- Additional benefits like:
  - User folder where the malware got executed
  - Compare Run count of different VSS could  
→ Behavior of user

## 3.6 Jump Lists

---

- Since Windows 7
- Recently opened documents of an application
- Similar RecentDocs Registry Key



- Rotate or Pin
- AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations

## 3.6 Jump Lists

---

- Jump List file names start with 16 hex characters
- File names end with `.automaticDestinations-ms`

```
C:> dir \Users\John\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
```

```
04/05/2020  12:50          33 792 1b4dd67f29cb1962.automaticDestinations-ms
14/06/2019  16:43           4 608 28c8b86deab549a1.automaticDestinations-ms
10/04/2019  14:32          29 696 6824f4a902c78fbd.automaticDestinations-ms
10/04/2020  14:12           9 216 7e4dca80246863e3.automaticDestinations-ms
04/05/2020  12:50           8 704 918e0ecb43d17e23.automaticDestinations-ms
10/04/2019  14:30           3 072 b74736c2bd8cc8a5.automaticDestinations-ms
09/04/2019  14:43           6 144 de48a32edcbe79e4.automaticDestinations-ms
```

- Each Hex value correspond to an application
- 918e0ecb43d17e23 = Notepad.exe
- Hex values are fixed world wide
- Search for Jump List IDs

## 3.6 Jump Lists

---

- Exercise: Identify applications

```
$ cd JumpLists/AutomaticDestinations/  
$ ll  
  
1b4dd67f29cb1962 . automaticDestinations-ms —>  
28c8b86deab549a1 . automaticDestinations-ms —>  
6824f4a902c78fbd . automaticDestinations-ms —>  
7e4dca80246863e3 . automaticDestinations-ms —>  
918e0ecb43d17e23 . automaticDestinations-ms —>  
b74736c2bd8cc8a5 . automaticDestinations-ms —>  
de48a32edcbe79e4 . automaticDestinations-ms —>
```

- Exercise: Analyze the Notepad Jump List file

## 3.6 Jump Lists

---

- Exercise: Identify applications

```
$ cd JumpLists/AutomaticDestinations/  
$ ll
```

```
1b4dd67f29cb1962.automaticDestinations-ms -> Windows Explorer  
28c8b86deab549a1.automaticDestinations-ms -> Internet Explorer 8  
6824f4a902c78fbd.automaticDestinations-ms -> Firefox 64.x  
7e4dca80246863e3.automaticDestinations-ms -> Control Panel  
918e0ecb43d17e23.automaticDestinations-ms -> Notepad (32-bit)  
b74736c2bd8cc8a5.automaticDestinations-ms -> WinZip  
de48a32edcbe79e4.automaticDestinations-ms -> Acrobat Reader 15.x
```

- Exercise: Analyze the Notepad Jump List file



## 3.6 Jump Lists

---

- Exercise: Identify applications

```
$ cd JumpLists/AutomaticDestinations/  
$ ll
```

```
1b4dd67f29cb1962.automaticDestinations-ms -> Windows Explorer  
28c8b86deab549a1.automaticDestinations-ms -> Internet Explorer 8  
6824f4a902c78fbd.automaticDestinations-ms -> Firefox 64.x  
7e4dca80246863e3.automaticDestinations-ms -> Control Panel  
918e0ecb43d17e23.automaticDestinations-ms -> Notepad (32-bit)  
b74736c2bd8cc8a5.automaticDestinations-ms -> WinZip  
de48a32edcbe79e4.automaticDestinations-ms -> Acrobat Reader 15.x
```

- Exercise: Analyze the Notepad Jump List file

```
$ 7z l 918e0ecb43d17e23.automaticDestinations-ms
```

Date	Time	Attr	Size	Compressed	Name
		.....	1398	1408	2
		.....	1368	1408	1
		.....	436	448	4
		.....	392	448	3

```
-> file  
-> exiftool  
-> strings  
-> $ strings -el DestList
```



## 4. Basic Malware Analysis

## 4.1 PE - Portable Execution format

---

- Describe program files
- Contain:
  - Meta data
  - Instructions
  - Text data
  - Pictures and alike
- Tell Windows how to load a program
- Provide resources to running program
- Provide resources like code signature

- |   |
|---|
| 1. DOS Header                           |
| 2. PE Header                            |
| 3. OPtional Header                      |
| 4. Section Headers                      |
| 5. .text Section (Program Code)         |
| 6. .idata Section (Importd Libs)        |
| 7. .rsrc Section (Strings, Images, ...) |
| 8. .reloc Section (Memory Translation)  |

## 4.2 PE - Basic Analysis

---

```
$ file 1.exe
malware/1.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

```
$ exiftool 1.exe
```

```
File Name           : 1.exe
File Size           : 300 kB
.....
Machine Type        : Intel 386 or later, and compatibles
Time Stamp          : 2007:08:29 02:37:01+02:00
PE Type             : PE32
Linker Version       : 8.0
Code Size           : 57344
Initialized Data Size : 3940352
Uninitialized Data Size : 0
Entry Point         : 0x80c0
OS Version          : 4.0
Subsystem           : Windows GUI
File OS             : Windows NT 32-bit
Object File Type    : Executable application
.....
Company Name        : iWin Inc.
File Description     : Furnishings
Internal Name       : Gem
Legal Copyright      : Dissipates (C) 2014
Original File Name   : Glittering.exe
```

## 4.2 PE - Basic Analysis

---

```
$ file Quotation.exe
```

```
Quotation.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

```
$ exiftool Quotation.exe
```

```
...
Machine Type           : Intel 386 or later, and compatibles
Time Stamp             : 2005:08:14 14:47:46+02:00
PE Type               : PE32
Linker Version         : 6.0
Code Size              : 647168
Initialized Data Size  : 32768
Uninitialized Data Size : 0
Entry Point            : 0x15f4
OS Version             : 4.0
...
Character Set          : Unicode
Comments              : Natcher
Company Name           : Glucosazone
Legal Copyright        : CRUSTER3
Legal Trademarks       : Forearming
Product Name           : UNKLE
File Version           : 1.02.0009
Product Version        : 1.02.0009
Internal Name          : Aurous
Original File Name     : Aurous.exe
```

## 4.2 PE - Basic Analysis

---

\$ python

```
>>> import pefile
>>> pe = pefile.PE("1.exe")
>>> for section in pe.sections:
...     print(section.Name, section.VirtualAddress,
              section.Misc_VirtualSize, section.SizeOfRawData)
('.text\x00\x00\x00', 4096, 54028, 57344)
('.rdata\x00\x00', 61440, 4360, 8192)
('.data\x00\x00\x00', 69632, 3695044, 4096)
('.rsrc\x00\x00\x00', 3768320, 230456, 233472)
```

```
>>> for entry in pe.DIRECTORY_ENTRY_IMPORT:
...     print(entry.dll)
...     for function in entry.imports:
...         print "\t",function.name
```

ADVAPI32.dll

```
RegOpenKeyExA
MapGenericMask
AdjustTokenGroups
SetSecurityDescriptorDacl
GetSecurityDescriptorLength
StartServiceA
OpenServiceA
```

.....

## 4.2 PE - Basic Analysis

---

```
$ strings 1.exe | less
```

```
Microsoft Visual C++ Runtime Library
]]      ))
ImageList_DragEnter
ImageList_GetDragImage
UninitializeFlatSB
ImageList_SetOverlayImage
ImageList_Merge
COMCTL32.dll
OLEAUT32.dll
RegOpenKeyExA
OpenServiceA
StartServiceA
GetSecurityDescriptorLength
SetSecurityDescriptorDacl
AdjustTokenGroups
MapGenericMask
ADVAPI32.dll
.....
```

```
mkdir images
$ wrestool -x 1.exe -o images/
```

## 4.2 PE - Basic Analysis

---

```
$ strings Quotation.exe | less
```

```
.....  
Damenization  
royle6  
nonexpedience  
incorporating1  
PEAS  
SIMOONS  
extramarginal  
ursula  
floricultural  
brainstorms  
NODDIES  
SCALOPUS9  
DEADHEADED  
lushai5  
elenchi7  
k40[  
VB5!6&*
```

```
mkdir images  
$ wrestool -x Quotation.exe -o images/
```



## 4.3 Enrich Online

---

- Calculate hash values












```
$ md5sum 1.exe  
a3bd288dec191caaed2057590e0dc34f
```

```
$ md5sum Quotation.*  
e3f0a2033a78e307a71320217ef738bc Quotation.exe  
84617d594af613f77deb32927123f779 Quotation.zip
```




- [www.virustotal.com](http://www.virustotal.com)
  - Live Demo
  - Pro. Account
  - Why not uploading office documents?
- MISP - Open Source Threat Intelligence Platform
  - <https://www.misp-project.org/>
  - <https://circl.lu/services/misp-malware-information-sharing-platform/>
  - Live Demo

## 4.3 Enrich Online

### Test-Event: For internal use only

Event ID	14740
UUID	5cd2fb05-5ef4-4208-b590-98d1950d210f 
Creator org	<a href="#">CIRCL</a>
Owner org	<a href="#">CIRCL</a>
Email	michael.hamm@circl.lu
Tags	 <a href="#">tip:green</a> x  <a href="#">circl:incident-classification="malware"</a> x  <a href="#">circl:topic="industry"</a> x  <a href="#">ecsirt:malicious-code="malware"</a> x   
Date	2019-05-08
Threat Level	Low
Analysis	Completed
Distribution	<b>Your organisation only</b>   
Info	Test-Event: For internal use only
<b>Published</b>	<b>No</b>
#Attributes	2 (0 Object)
First recorded change	2019-05-08 15:52:06
Last change	2020-05-26 07:08:15

### Related Events

 <a href="#">RagnarLocker Ransomware</a> 2020-02-24 1
CE... <a href="#">"Subject: RE: RE: Our Purchase C</a> 2019-09-29
total... <a href="#">Actividad de phishing: Fw: SHCP</a> 2019-07-24
CE... <a href="#">Trojan.Gamaredon</a> 2019-05-07 1
CE... <a href="#">LokiBot Malspam Run</a> (2019-04-2 2019-04-28
 <a href="#">Malware RE test</a> 2019-04-15 1  <a href="#">Test - illu</a> 2018-11-
CE... <a href="#">Trojan.Gamaredon</a>

### 4.3 Enrich Online

[illegible]

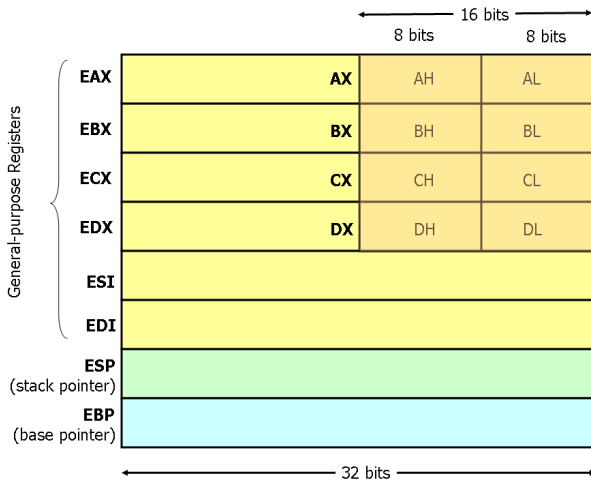
Correlation Graph: <https://misppriv.circl.lu/>

## 4.4 Static Analysis

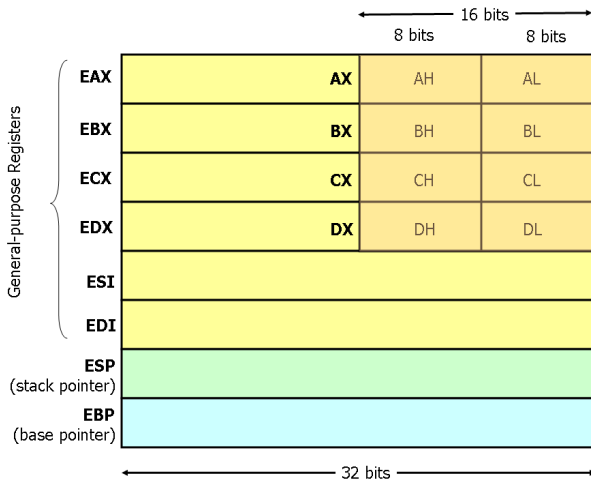
---

- Perfect disassembly → Unsolved problem
- Linear disassembly
  - Identify the program code
  - Decode the bytes
- Linear disassembly limitations
  - Don't know how instructions get decoded by CPU
  - Could not counter fight obfuscation
- Obfuscation techniques
  - Packing
  - Resource Obfuscation
  - Anti-Disassembly
  - Dynamic Data Download
- Counter fight obfuscation
  - Dynamic Analysis
  - Run malware in isolated environment

## 4.5 x86 Assembly: General-Purpose Registers



## 4.5 x86 Assembly: Stack and Control Flow Registers



## 4.5 x86 Assembly: Instructions

---

Arithmetic:	add ebx, 100	Adds 100 to the value in EBX
	sub ecx, 123	Subtract 123 from the value in ECX
	inc ah	Increments value in AH by 1
	dec al	Decrements value in AL by 1
Data Movement:	mov eax, ebx	Move value in EBX into register EAX
	mov eax, [0x4711]	Move value at memory 0x4711 into EAX
	mov eax, 1	Move the value 1 into register EAX
	mov [0x4711], eax	Move value of EAX into memory 0x4711
Stack:	push 1	Increment ESP; Store 1 on top of stack
	pop eax	Store highest value in EAX; Decrement ESP
Control Flow:	call [address]	1. Put EIP on top of the stack 2. Put [address] into EIP
	ret	1. Popped top of the stack into EIP 2. Resume execution
	jmp 0x1234	Start executing program code at 0x1234
	cmp eax, 100	1. Compares value in EAX with 100 2. Based on result set EFLAGS register
	jge 0x1234	1. Interpret EFLAGS register 2. If 'greater' or 'equal' flag then jump

## 4.5 x86 Assembly: Control Flow Graphs

---

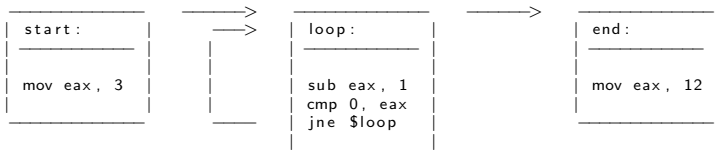
<code>start:</code>	Symbol for address of next instruction
<code>mov eax, 3</code>	Initialize a counter of 3 into EAX
<code>loop:</code>	Symbol for address of next instruction
<code>sub eax, 1</code>	Subtract 1 from value in EAX
<code>cmp 0, eax</code>	Compare value in EAX with 0; Set EFLAGS
<code>jne \$loop</code>	IF EFLAGS 'not equal' jump to 'loop'
<code>end:</code>	Symbol for address of next instruction
<code>mov eax, 12</code>	



## 4.5 x86 Assembly: Control Flow Graphs


---

start:	Symbol for address of next instruction
mov eax, 3	Initialize a counter of 3 into EAX
loop:	Symbol for address of next instruction
sub eax, 1	Subtract 1 from value in EAX
cmp 0, eax	Compare value in EAX with 0; Set EFLAGS
jne \$loop	IF EFLAGS 'not equal' jump to 'loop'
end:	Symbol for address of next instruction
mov eax, 12	



## 4.6 Dynamic Analysis

[Fork me on GitHub](#)



**CIRCL  
DMA**  
Dynamic Malware Analysis

(BETA v2)

Logg

You can upload suspicious executables or documents to obtain a dynamic analysis report. The documents or executables files are not shared with external parties. An analysis can take up to 15 minutes.

Malicious sample upload interface  
Sample (EXE, DLL or PDF) to submit

Browse...

1.exe

System to use

☒ Windows\_xp\_pro\_sp3\_en\_03

Analysis package

exe

Submit for analysis

## 4.6 Dynamic Analysis

---

### Signatures

Creates RWX memory

Reads data out of its own binary image

A process created a hidden window

Drops a binary and executes it

Executed a process and injected code into it, probably while unpacking

Attempts to remove evidence of file being downloaded from the Internet

Likely date expiration check, exits too soon after checking local time

Deletes its original binary from disk

Exhibits behavior characteristic of Alphacrypt/Teslacrypt ransomware

Signatures and Screenshots: <https://circl.lu/services/dynamic-malware-analysis/>

## 4.6 Dynamic Analysis

---

Modifies boot configuration settings

Attempts to identify installed AV products by registry key

Clamav Hits in Target/Dropped/SuriExtracted

Creates a copy of itself

Anomalous binary characteristics

### Screenshots




### Network Analysis

Signatures and Screenshots: <https://circl.lu/services/dynamic-malware-analysis/>

## 4.6 Dynamic Analysis

[Fork me on GitHub](#)



**CIRCL  
DMA**  
Dynamic Malware Analysis

(BETA v2)

Logg

You can upload suspicious executables or documents to obtain a dynamic analysis report. The documents or executables files are not shared with external parties. An analysis can take up to 15 minutes.

Malicious sample upload interface

Sample (EXE, DLL or PDF) to submit

System to use

☒ Windows\_xp\_pro\_sp3\_en\_03

Analysis package

## 4.6 Dynamic Analysis

### Processes

registry filesystem process **threading** services device network synchronization crypto browser

**Quotation.exe** PID: 1328, Parent PID: 500

#### Accessed Files

- C:\Documents and Settings\j\Local Settings\Temp\Quotation.exe.cfg
- C:\Documents and Settings\j\Local Settings\Temp
- C:\Documents and Settings\j\Local Settings\Temp\~DF3495.tmp

#### Read Files

- C:\Documents and Settings\j\Local Settings\Temp\~DF3495.tmp

#### Modified Files

- C:\Documents and Settings\j\Local Settings\Temp\~DF3495.tmp

**Deleted Files** Nothing to display.

#### Registry Keys

- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\SafeProcessSearchMode
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Nls\Codepage
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\VBA\Monitors



## 5. Analysing files

## 5.1 Analysing files

---

- Standard Linux commands

- `file`
  - `strings`
  - `exiftool`
  - `md5sum`, `sha1sum`
  - `7z`
  - .....

- Dedicated tools

- `oledump.py`
  - `pdfid.py`, `pdf-parser.py`
  - VirusTotal tools
  - .....

- Exercise: Run `exiftool` on carving recovered documents



## 5.2 Analysing files

---

- Online resources
  - NSRL - National Software Reference Library
  - VirusTotal
  - CIRCL: DMA
  - CIRCL: MISP Threat Sharing Platform
- Demo: Search MD5
  - A479C4E7ED87AEDAFAD7D9936DC80115
  - 81e9036aed5502446654c8e5a1770935
- Analysing files could become a training on it's own



## 6. Live Response

## 6.1 Volatile Data

---

- Memory dump
- Live analysis:
  - System time
  - Logged-on users
  - Open files
  - Network -connections -status
  - Process information -memory
  - Process / port mapping
  - Clipboard content
  - Services
  - Command history
  - Mapped drives / shares
  - !!! Do not store information on the subject system !!!
- Image of live system (Possible issues)
- Shutdown and image if possible

## 6.1 Collecting Volatile Data

---

<https://docs.microsoft.com/en-us/sysinternals/>

---

- System Time

```
> date /t & time /t           # Don't forget to note wall-clock-time
    Tue 03/26/2019           # Note timezone of PC
    01:31 PM
```

- Loggedon Users

```
> net session

> .\PsLoggedon.exe
    Users logged on locally:
        3/26/2019 1:30:23 PM      John-PC\John
    No one is logged on via resource shares.

> .\logonsessions.exe
    [5] Logon session 00000000:0001ad9d:
        User name:      John-PC\John
        Auth package:   NTLM
        Logon type:     Interactive
        Session:        1
        Sid:             S-1-5-21-3031575581-801213887-4188682232-1001
        Logon time:      3/26/2019 1:30:23 PM
        Logon server:    JOHN-PC
```

## 6.1 Collecting Volatile Data

---

- Open Files

```
> net file  
  
> .\psfile.exe
```

- Network Connections and Status

```
> netstat -anob
```

Proto	Local Address	Foreign Address	State	PID	RpcSs
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	696	[svchost.exe]
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:554	0.0.0.0:0	LISTENING	2504	[wmpnetwk.exe]
TCP	0.0.0.0:10243	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	364	[wininit.exe]

```
> netstat -rn
```

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	10.0.2.2	10.0.2.15	10
	10.0.2.0	255.255.255.0	On-link	10.0.2.15	266
	10.0.2.15	255.255.255.255	On-link	10.0.2.15	266

```
> ipconfig /all
```

## 6.1 Collecting Volatile Data

- Running Processes

> tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System	4	Services	0	600 K
smss.exe	252	Services	0	792 K
csrss.exe	328	Services	0	3,224 K
wininit.exe	364	Services	0	3,316 K
csrss.exe	372	Console	1	4,196 K
winlogon.exe	400	Console	1	6,272 K
services.exe	460	Services	0	6,628 K
lsass.exe	468	Services	0	8,428 K
lsmd.exe	476	Services	0	3,040 K
svchost.exe	584	Services	0	6,596 K
cmd.exe	3100	Console	1	2,480 K

> tasklist /svc

Image Name	PID	Services
svchost.exe	584	DcomLaunch, PlugPlay, Power
svchost.exe	696	RpcEptMapper, RpcSs
svchost.exe	792	Audiosrv, Dhcp, eventlog, HomeGroupProvider, lmhosts, wscsv
svchost.exe	844	AudioEndpointBuilder, CscService, HomeGroupListener, Netman, TrkWks, UxSms,
svchost.exe	876	EventSystem, fdPHost, FontCache, netprofm, nsi, WdiServiceHost

## 6.1 Collecting Volatile Data

---

- Running Processes

```
> .\pslist.exe -x
```

```
> .\pslist.exe -t
```

Name	Pid	Pri	Thd	Hnd	VM	WS	Priv
explorer	1252	8	26	912	212044	47672	36304
VBoxTray	360	8	12	153	61384	5624	1476
cmd	548	8	1	24	29256	2564	2628
pslist	3452	13	1	123	45908	3640	1652
WzPreloader	1244	8	6	119	109748	9064	11224
cmd	3100	8	1	20	27464	2480	1804

```
> .\Listdlls.exe
```

```
> .\handle.exe
```

- Processes/Port Mapping

```
> .\tcpvcon -n -c -a
```

```
TCP,svchost.exe,692,LISTENING,0.0.0.0,0.0.0.0
TCP,System,4,LISTENING,10.0.2.15,0.0.0.0
TCP,wmpnetwk.exe,2428,LISTENING,0.0.0.0,0.0.0.0
TCP,wininit.exe,364,LISTENING,0.0.0.0,0.0.0.0
TCP,svchost.exe,776,LISTENING,0.0.0.0,0.0.0.0
TCP,svchost.exe,896,LISTENING,0.0.0.0,0.0.0.0
TCP,services.exe,460,LISTENING,0.0.0.0,0.0.0.0
```

## 6.1 Collecting Volatile Data

---

- Command History

```
> doskey /history
netstat -anob
.\Listdlls.exe
.\handle.exe
.\tcpvcon -n -c -a
cls
doskey /history
```

- Processes/Port Mapping



## 6.2 Non Volatile Data

- Clear Pagefile at shutdown

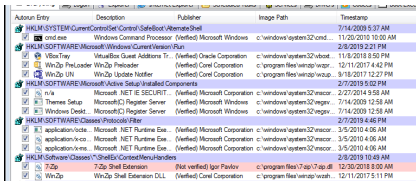
```
> reg QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management"  
.....  
ClearPageFileAtShutdown    REG.DWORD    0x0  
.....
```

- Update Last Access disabled

```
> reg QUERY "HKLM\SYSTEM\CurrentControlSet\Control\FileSystem"  
.....  
NtfsDisableLastAccessUpdate    REG.DWORD    0x0  
.....
```

- Autostart locations

```
> .\Autoruns.exe
```



Autounit Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/14/2009 5:37 AM
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd...	11/20/2010 10:00 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2/8/2019 2:21 PM
VBoxTray	VirtualBox Guest Additions Tr...	(Verified) Oracle Corporation	c:\windows\system32\vboxd...	11/8/2018 8:50 PM
WinZip Pro Launcher	WinZip Pro Launcher	(Verified) Corel Corporation	c:\program files\winzip\wzup...	12/11/2017 4:42 PM
WinZip UN	WinZip Update Notifier	(Verified) Corel Corporation	c:\program files\winzip\wzup...	9/18/2017 12:27 PM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2/7/2019 5:02 PM
n/a	Microsoft .NET IE SECURIT...	(Verified) Microsoft Corporation	c:\windows\system32\mscor...	2/27/2014 9:58 AM
Themes Setup	Microsoft(R) Register Server	(Verified) Microsoft Windows	c:\windows\system32\regsvr...	7/14/2009 12:58 AM
Windows Desk...	Microsoft(R) Register Server	(Verified) Microsoft Windows	c:\windows\system32\regsvr...	7/14/2009 12:58 AM
HKLM\SOFTWARE\Classes\Protocols\Fiber				2/7/2019 4:46 PM
application\code...	Microsoft .NET Runtime Ee...	(Verified) Microsoft Corporation	c:\windows\system32\mscor...	3/5/2010 4:06 AM
application\ic...	Microsoft .NET Runtime Ee...	(Verified) Microsoft Corporation	c:\windows\system32\mscor...	3/5/2010 4:06 AM
application\ic...	Microsoft .NET Runtime Ee...	(Verified) Microsoft Corporation	c:\windows\system32\mscor...	3/5/2010 4:06 AM
HKLM\Software\Classes\ShellEx\ContextMenuHandlers				2/8/2019 10:49 AM
WinZip	WinZip Shell Extension	(Not verified) Igor Pavlov	c:\program files\7zip\7zip.dl...	12/20/2018 8:00 AM
WinZip	WinZip Shell Extension DLL	(Verified) Corel Corporation	c:\program files\winzip\wzsh...	12/11/2017 5:11 PM

## 6.3 Across the network

---

- Get Nmap command-line zipfile  
`https://nmap.org/download.html`

- On Linux set up a netcat listener

```
nc -k -l 9999 >> logfile.txt
```

- Sending from subject system

```
ncat aaa.bbb.ccc.ddd 9999
```

```
echo "Date and Time" | ncat.exe aaa.bbb.ccc.ddd 9999
```

```
date /t | ncat.exe aaa.bbb.ccc.ddd 9999
```

```
time /t | ncat.exe aaa.bbb.ccc.ddd 9999
```

```
echo "_____" | ncat.exe aaa.bbb.ccc.ddd 9999
```



## 7. Memory Forensics

## 7.1 About Memory Forensics

---

- Information expected
  - Network connections
  - Processes (hidden)
  - Services (listening)
  - Malware
  - Registry content
  - DLL analysis
  - Passwords in clear text
- History
  - 2005: String search
  - → EProcess structures
- Finding EProcess structures
  - Find the doubly linked list (ntoskrnl.exe)
  - Brute Force searching

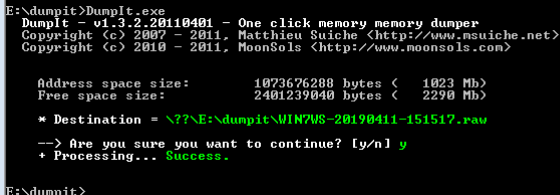
## 7.2 Get your memory dump

---

- Page file, swap area: `pagefile.sys`
- Memory dump

`http://www.msuiche.net`

`DumpIt.exe`



```
E:\dumpit>DumpIt.exe
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

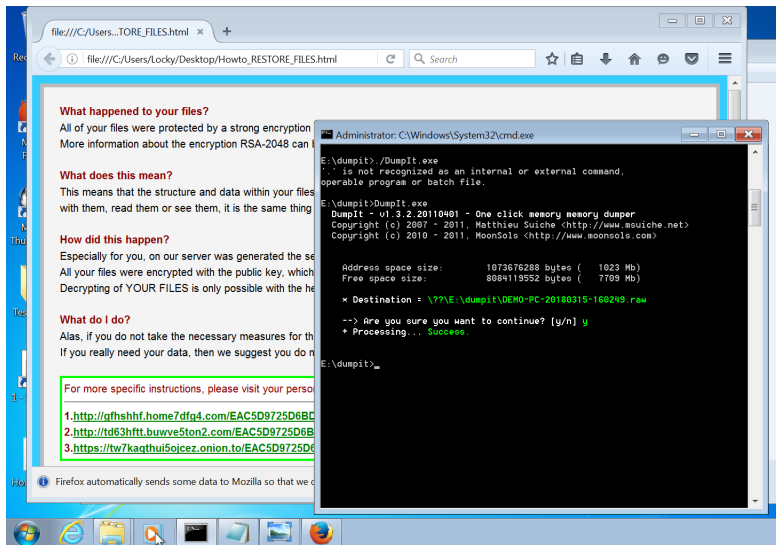
Address space size:      1073676288 bytes <   1023 Mb>
Free space size:        2401239040 bytes <   2290 Mb>

* Destination = \\??\E:\dumpit\WIN7WS-20110411-151517.raw
-> Are you sure you want to continue? [y/n] y
+ Processing... Success.

E:\dumpit>
```

- Hibernation file: `hiberfil.sys`  
`powercfg /h[ibernate] [on|off]`  
`psshutdown -h`

## 7.2 DumpIt



## 7.3 Mandiant Redline - Malware Risk Index

		Process Name	MRI Score	PID	Path	Arguments	Start Time
		owxxb-a.exe	93	3432	C:\Users\Uohn\AppData\Roaming	C:\Users\Uohn\AppData\Roaming\owxxb-a.exe	04/15/2019 15:07:13
		svchost.exe	93	3728	C:\Windows\System32	C:\Windows\System32\svchost.exe -k swprv	04/15/2019 15:07:23
		csrss.exe	59	360	C:\Windows\system32	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024...	04/15/2019 15:02:54
		csrss.exe	57	324	C:\Windows\system32	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024...	04/15/2019 15:02:54
		Explorer.EXE	56	920	C:\Windows	C:\Windows\Explorer.EXE	04/15/2019 15:03:42
		svchost.exe	55	2884	C:\Windows\System32	C:\Windows\System32\svchost.exe -k secsvcs	04/15/2019 15:05:41
		powershell.exe	52	2748	C:\Windows\System32\WindowsPowerSh...	powershell	04/15/2019 15:05:26
		spoolsv.exe	52	1296	C:\Windows\System32	C:\Windows\System32\spoolsv.exe	04/15/2019 15:03:02
		lsass.exe	52	464	C:\Windows\system32	C:\Windows\system32\lsass.exe	04/15/2019 15:02:55
		svchost.exe	52	852	C:\Windows\system32	C:\Windows\system32\svchost.exe -k netsvcs	04/15/2019 15:02:58
		WzPreloader.exe	52	1852	C:\Program Files\WinZip	"C:\Program Files\WinZip\WzPreloader.exe"	04/15/2019 15:03:44
		svchost.exe	47	1444	C:\Windows\system32	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation	04/15/2019 15:03:03
		services.exe	47	456	C:\Windows\system32	C:\Windows\system32\services.exe	04/15/2019 15:02:55

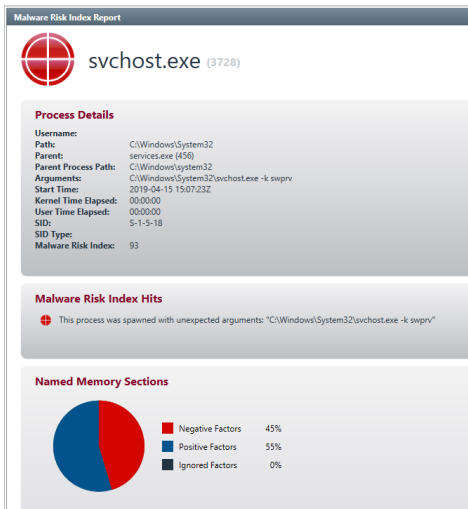
## 7.3 Mandiant Redline - Malware Risk Index



Process Name	PID	Path	State	Created	Local IP Address	Local...	Remote IP Add...	Re...	Protocol
owxxb-a.exe	3432	C:\Users\John\AppData\Roaming	ESTABLISHED		10.0.2.15	49161	216.239.32.21	443	TCP
owxxb-a.exe	3432	C:\Users\John\AppData\Roaming	CLOSED		10.0.2.15	49164	139.99.68.76	80	TCP
owxxb-a.exe	3432	C:\Users\John\AppData\Roaming	ESTABLISHED		10.0.2.15	49160	216.239.32.21	80	TCP
owxxb-a.exe	3432	C:\Users\John\AppData\Roaming	ESTABLISHED		10.0.2.15	49162	2.17.201.8	80	TCP



## 7.3 Mandiant Redline - Malware Risk Index



## 7.3 Mandiant Redline - Hierarchical

System	0	4		04/15/2019 15:02:52	0
smss.exe	47	248	\SystemRoot\System32\smss.exe	04/15/2019 15:02:52 System	4
csrss.exe	57	324	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection...	04/15/2019 15:02:54	308
wininit.exe	47	368	wininit.exe	04/15/2019 15:02:54	308
services.exe	47	456	C:\Windows\system32\services.exe	04/15/2019 15:02:55 wininit.exe	368
taskhost.exe	47	352	"taskhost.exe"	04/15/2019 15:03:42 services.exe	456
csrss.exe	59	360	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection...	04/15/2019 15:02:54 taskhost.exe	352
conhost.exe	47	2552	??C:\Windows\system32\conhost.exe	04/15/2019 15:04:43 csrss.exe	360
winlogon.exe	47	396	winlogon.exe	04/15/2019 15:02:54 taskhost.exe	352
svchost.exe	47	564	C:\Windows\system32\svchost.exe -k DcomLaunch	04/15/2019 15:02:57 services.exe	456
wmiprvse.exe	47	3268		04/15/2019 15:06:52 svchost.exe	564
VBoxService.exe	47	624	C:\Windows\System32\VBoxService.exe	04/15/2019 15:02:57 services.exe	456
powershell.exe	52	2748	powershell	04/15/2019 15:05:26	2544
owxb-a.exe	93	3432	C:\Users\John\AppData\Roaming\owxb-a.exe	04/15/2019 15:07:13	3368
NOTEPAD.EXE	52	3820	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\John\Desktop\Howto_RESTORE_FILES.txt	04/15/2019 15:08:05 owxb-a.exe	3432
iexplore.exe	52	3832	"C:\Program Files\Internet Explorer\iexplore.exe" -nohome	04/15/2019 15:08:06 owxb-a.exe	3432
iexplore.exe	47	3908	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3832 CREDAT:14337	04/15/2019 15:08:07 iexplore.exe	3832

## 7.3 Mandiant Redline - Timeline

04/15/2019 15:05:26	Process/StartTime	Name: powershell.exe	PID: 2748	Path: C:\Windows\System32\WindowsPowerShell\v1.0	Args: powershell		
04/15/2019 15:05:41	Process/StartTime	Name: svchost.exe	PID: 2884	Path: C:\Windows\System32	Args: C:\Windows\System32\svchost.exe -k secsvcs		
04/15/2019 15:05:41	Process/StartTime	Name: sppvc.exe	PID: 2844	Path: C:\Windows\system32	Args: C:\Windows\system32\sppvc.exe		
04/15/2019 15:06:50	Port/CreationTime	Remote: **0	Local: 0.0.0.0	Protocol: UDP	State: LISTENING	PID: 2748	Process: powershell.exe
04/15/2019 15:06:50	Port/CreationTime	Remote: **0	Local: 00:00:00:00:00:00:00:00:00	Protocol: UDP	State: LISTENING	PID: 2748	Process: powershell.exe
04/15/2019 15:06:50	Port/CreationTime	Remote: **0	Local: 0.0.0.0	Protocol: UDP	State: LISTENING	PID: 2748	Process: powershell.exe
04/15/2019 15:06:50	Port/CreationTime	Remote: **0	Local: 00:00:00:00:00:00:00:00	Protocol: UDP	State: LISTENING	PID: 2748	Process: powershell.exe
04/15/2019 15:06:52	Process/StartTime	Name: wmiiprse.exe	PID: 3268	Path: C:\Windows\system32\wbem	Args:		
04/15/2019 15:07:13	Process/StartTime	Name: owvob-a.exe	PID: 3432	Path: C:\Users\John\AppData\Roaming	Args: C:\Users\John\AppData\Roaming\owvob-a.exe		
04/15/2019 15:07:22	Process/StartTime	Name: vssvc.exe	PID: 3676	Path: C:\Windows\system32	Args: C:\Windows\system32\vssvc.exe		
04/15/2019 15:07:23	Process/StartTime	Name: svchost.exe	PID: 3728	Path: C:\Windows\System32	Args: C:\Windows\System32\svchost.exe -k swprv		
04/15/2019 15:07:13	Name: owvob-a.exe	PID: 3432	Path: C:\Users\John\AppData\Roaming	Args: C:\Users\John\AppData\Roaming\owvob-a.exe			
04/15/2019 15:07:22	Name: vssvc.exe	PID: 3676	Path: C:\Windows\system32	Args: C:\Windows\system32\vssvc.exe			
04/15/2019 15:07:23	Name: svchost.exe	PID: 3728	Path: C:\Windows\System32	Args: C:\Windows\System32\svchost.exe -k swprv			
04/15/2019 15:08:05	Name: NOTEPAD.EXE	PID: 3820	Path: C:\Windows\system32	Args: "C:\Windows\system32\notepad.exe" C:\Users\John\Desktop\H...			
04/15/2019 15:08:06	Name: iexplore.exe	PID: 3832	Path: C:\Program Files\Internet Explorer	Args: "C:\Program Files\Internet Explorer\iexplore.exe" -nohome			
04/15/2019 15:08:07	Name: iexplore.exe	PID: 3908	Path: C:\Program Files\Internet Explorer	Args: "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF3832 C...			
04/15/2019 15:08:07	Name: DllHost.exe	PID: 3928	Path: C:\Windows\system32	Args: C:\Windows\system32\DllHost.exe /Processid{A8B902B4-09CA-4...			

## 7.4 Volatility: Overview

---

`volatility --info`

`volatility -h`

```
...
imagecopy      Copies a physical address space out as a raw DD image
imageinfo      Identify information for the image
...
pslist         Print all running processes by following the EPROCESS lists
psscan         Scan Physical memory for _EPROCESS pool allocations
pstree         Print process list as a tree
psxview        Find hidden processes with various process listings
...
sockets        Print list of open sockets
sockscan       Scan Physical memory for _ADDRESS_OBJECT objects (tcp sockets)
...
```

`volatility -f [filename] [plugin] [options]`

`volatility -f memdump.raw imageinfo`

## 7.4 Volatility: Overview

---

```
volatility -f memdump.raw imageinfo
```

```
Volatility Foundation Volatility Framework 2.6
```

```
INFO      : volatility.debug      : Determining profile based on KDBG search...
```

```
    Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
```

```
        AS Layer1 : IA32PagedMemory (Kernel AS)
```

```
        AS Layer2 : FileAddressSpace
```

```
        PAE type : No PAE
```

```
        DTB : 0x185000L
```

```
        KDBG : 0x82968c28L
```

```
    Number of Processors : 1
```

```
    Image Type (Service Pack) : 1
```

```
        KPCR for CPU 0 : 0x82969c00L
```

```
        KUSER.SHARED.DATA : 0xffdf0000L
```

```
    Image date and time : 2019-04-15 15:08:11 UTC+0000
```

```
    Image local date and time : 2019-04-15 17:08:11 +0200
```

```
volatility -f memdump.raw kdbgscan
```

```
volatility --profile=Win7SP1x86 -f [filename] [plugin]
```

```
export VOLATILITY_PROFILE=Win7SP1x86
```

## 7.5 Volatility: Process Analysis

---

### `pslist`

- Running processes
- Process IP - PID
- Parent PIP - PPID
- Start time

### `pstree`

- Like `pslist`
- Visual child-parent relation

### `psscan`

- Brute Force
- Find inactive and/or hidden processes

### `psxview`

- Run and compare some tests
- Correlate `psscan` and `pslist`

## 7.5 Volatility: Process Analysis

```
volatility --profile=Win7SP1x86 -f Win-Enc-20190415.raw pslist
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Ses	Wow64	Start	
0x84233af0	System	4	0	70	505	—	0	2019-04-15 15:02:52	UTC+0000
0x848d8288	smss.exe	248	4	2	29	—	0	2019-04-15 15:02:52	UTC+0000
0x8487a700	csrss.exe	324	308	9	384	0	0	2019-04-15 15:02:54	UTC+0000
0x84fbb530	csrss.exe	360	352	7	274	1	0	2019-04-15 15:02:54	UTC+0000
0x84fc3530	wininit.exe	368	308	3	77	0	0	2019-04-15 15:02:54	UTC+0000
0x84fd0530	winlogon.exe	396	352	4	112	1	0	2019-04-15 15:02:54	UTC+0000
0x85048a18	services.exe	456	368	8	203	0	0	2019-04-15 15:02:55	UTC+0000
0x8505ac00	lsass.exe	464	368	7	580	0	0	2019-04-15 15:02:55	UTC+0000
0x8505caa0	lsmd.exe	472	368	10	145	0	0	2019-04-15 15:02:55	UTC+0000
...									
...									
...									
0x85050b60	WmiPrvSE.exe	3268	564	9	175	0	0	2019-04-15 15:06:52	UTC+0000
0x8438bd40	owxxb-a.exe	3432	3368	15	471	1	0	2019-04-15 15:07:13	UTC+0000
0x84394030	VSSVC.exe	3676	456	6	123	0	0	2019-04-15 15:07:22	UTC+0000
0x84394488	svchost.exe	3728	456	6	70	0	0	2019-04-15 15:07:23	UTC+0000
0x84a243c8	notepad.exe	3820	3432	1	64	1	0	2019-04-15 15:08:05	UTC+0000
0x846d8030	ieexplore.exe	3832	3432	19	427	1	0	2019-04-15 15:08:06	UTC+0000
0x846d2d40	ieexplore.exe	3908	3832	11	293	1	0	2019-04-15 15:08:07	UTC+0000
0x846e5a58	dllhost.exe	3928	564	6	94	1	0	2019-04-15 15:08:07	UTC+0000
0x84684d40	dllhost.exe	4012	564	10	212	1	0	2019-04-15 15:08:08	UTC+0000

## 7.5 Volatility: Process Analysis

---

volatility --profile=Win7SP1x86 -f Win-Enc-20190415.raw pslist

Offset(P)	Name	PID	pslist	psscan	thrdproc	pspcid	csrss	session	deskthrd
.....									
.....									
0x3f60f030	taskhost.exe	352	True	True	True	True	True	True	True
0x3fa84d40	dllhost.exe	4012	True	True	True	True	True	True	True
0x3ec23148	spoolsv.exe	1296	True	True	True	True	True	True	True
0x3f63f470	explorer.exe	920	True	True	True	True	True	True	True
0x3ff0bd40	owxb-a.exe	3432	True	True	True	True	True	True	True
0x3f3d0530	winlogon.exe	396	True	True	True	True	True	True	True
0x3f3c3530	wininit.exe	368	True	True	True	True	True	True	True
0x3ec9f030	svchost.exe	688	True	True	True	True	True	True	True
0x3ef3d758	VBoxTray.exe	1832	True	True	True	True	True	True	True
0x3fae5a58	dllhost.exe	3928	True	True	True	True	True	True	True
0x3ec50b60	WmiPrvSE.exe	3268	True	True	True	True	True	True	True
0x3ec88b90	svchost.exe	564	True	True	True	True	True	True	True
0x3ecd3768	svchost.exe	820	True	True	True	True	True	True	True
0x3ef4f030	SearchIndexer.exe	2008	True	True	True	True	True	True	True
0x3ec08d40	svchost.exe	1444	True	True	True	True	True	True	True
0x3ed10d40	svchost.exe	1008	True	True	True	True	True	True	True
0x3f6243c8	notepad.exe	3820	True	True	True	True	True	True	True
0x3ecd95f8	svchost.exe	852	True	True	True	True	True	True	True
0x3fad2d40	ieexplore.exe	3908	True	True	True	True	True	True	True

.....  
.....



## 7.6 Volatility: Network Analysis

---

- Windows XP and 2003 Server
  - connections
  - connscan
  - sockets
- Windows 7
  - netscan

```
volatility --profile=Win7SP1x86 -f Win-Enc-20190415.raw netscan
```

Proto	Local Address	Foreign Address	State	Pid	Owner
.....					
UDPv4	0.0.0.0:0	::*		2748	powershell.exe
UDPv6	:::0	::*		2748	powershell.exe
TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	456	services.exe
TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	464	lsass.exe
TCPv6	:::49156	:::0	LISTENING	464	lsass.exe
TCPv4	10.0.2.15:49167	2.17.201.11:80	ESTABLISHED	1128	svchost.exe
TCPv4	10.0.2.15:49166	93.184.220.29:80	ESTABLISHED	1128	svchost.exe
TCPv4	10.0.2.15:49165	50.62.124.1:80	ESTABLISHED	3432	owxxb-a.exe
TCPv4	10.0.2.15:49160	216.239.32.21:80	ESTABLISHED	3432	owxxb-a.exe
TCPv4	10.0.2.15:49162	2.17.201.8:80	ESTABLISHED	3432	owxxb-a.exe
TCPv4	10.0.2.15:49168	13.107.21.200:80	ESTABLISHED	3832	iexplore.exe
TCPv4	10.0.2.15:49159	94.23.7.52:80	CLOSE_WAIT	2748	powershell.exe
.....					

## 7.7 Volatility: Other plugins

---

- Exercise: Explore other useful plugins

```
volatility -f memdump.raw sessions
volatility -f memdump.raw privs | less
volatility -f memdump.raw hivelist
volatility -f memdump.raw filescan | less
volatility -f memdump.raw timeliner | less
volatility -f memdump.raw hashdump
```

- Exercise: Get SIDs

```
volatility --profile=Win7SP1x86 -f Win-Enc-20190415.raw getsids

powershell.exe (2748): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
owxxb-a.exe (3432): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
notepad.exe (3820): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
iexplore.exe (3832): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
iexplore.exe (3908): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
dllhost.exe (3928): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
```

## 7.8 Volatility: Exercise

---

- Exercise: Command line history

```
vol.py —profile=Win7SP1x86 -f memdump.raw cmdline
vol.py —profile=Win7SP1x86 -f memdump.raw cmdscan
vol.py —profile=Win7SP1x86 -f memdump.raw consoles
```

- Exercise: Find suspicious processes

```
volatility —profile=Win7SP1x86 -f Win-Enc-20190415.raw malfind
```

```
Process: owxxb—a.exe Pid: 3432 Address: 0x400000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 134, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
0x00400000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x00400010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x00400020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00400030 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 .....

```

```
0x00400000 4d          DEC EBP
0x00400001 5a          POP EDX
0x00400002 90          NOP
```

- Exercise: Dump suspicious process and analyze!



## 8. Bibliography and Outlook

## 8.1 Bibliography

---

- Windows Forensic Analysis 2E  
Harlan Carvey  
Syngress 2nd edition  
ISBN-13: 978-1-59-749422-9
- Windows Forensics  
Dr. Philip Polstra  
CreateSpace Independent Publishing  
ASIN: B01K3RPWIY
- Windows Forensic Analysis for Windows 7 3E  
Harlan Carvey  
Syngress  
ISBN-13: 978-1-59-749727-5

## 8.2 Outlook

---

- Scheduled Tasks
- Windows 8 analyzis
- Windows 10 analyzis
- Internet artifacts
- Mobile Forensics

# Overview

---

1. Windows Registry
2. Event Logs
3. Other Sources of Information
4. Malware Analysis
5. Analysing files
6. Live Response
7. Memory Forensics
8. Bibliography and Outlook