

# Digital Forensics 1.0.2

An introduction into MS Windows Digital Forensics



CIRCL *TLP:WHITE*

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

Edition May 2019

# Overview

---

- 11. Live Response
- 12. Memory Forensics
- 13. Windows Registry
- 14. Event Logs
- 15. Other Sources of Information
- 16. Analysing files
- 17. Bibliography and Outlook



## 11. Live Response

## 11.1 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

## 11.1 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
```

## 11.1 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
```

## 11.1 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

## 11.1 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
```



## 11.1 Collecting Volatile Data

---

- Command History

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

- Processes/Port Mapping

## 11.2 Non Volatile Data

- Clear Pagefile at shutdown

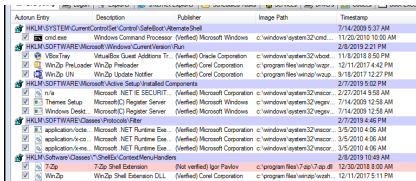
```
> reg QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management"  
.....  
ClearPageFileAtShutdown    REG.DWORD    0x0  
.....
```

- 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\vboxad...	11/8/2018 8:50 PM
WinZip Pro Launcher	WinZip Pro Launcher	(Verified) Corel Corporation	c:\program files\winzip\wzup...	12/17/2017 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 SECURITY...	(Verified) Microsoft Corporation	c:\windows\system32\mscor...	2/27/2014 9:58 AM
Themes Setup	Microsoft(.C) Register Server	(Verified) Microsoft Windows	c:\windows\system32\regsvr...	7/14/2009 12:58 AM
Windows Desk...	Microsoft(.C) 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
7Zip	7-Zip 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

## 11.3 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
```



## 12. Memory Forensics

## 12.1 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

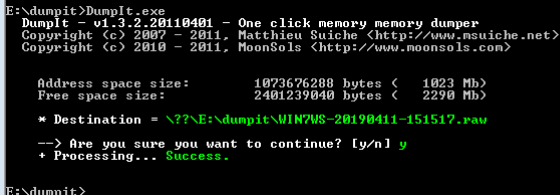
## 12.2 Get your memory dump

---

- 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>

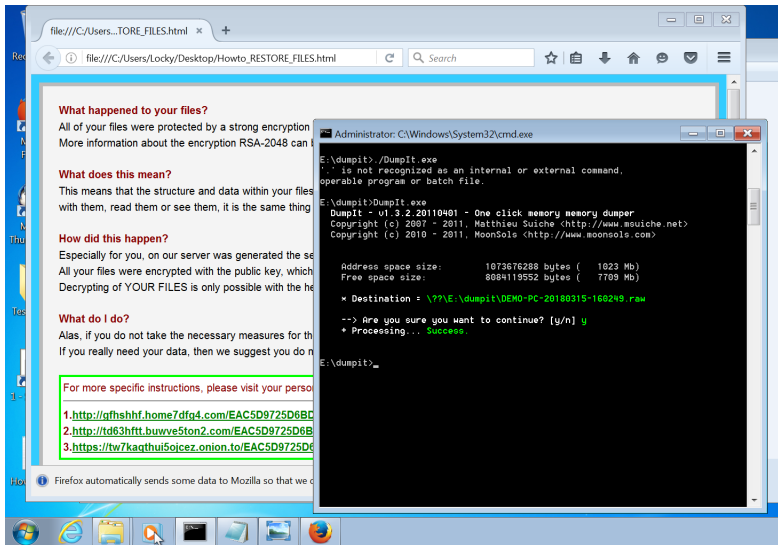
Address space size:      1073676288 bytes <   1023 Mb>
Free space size:        2401239040 bytes <   2290 Mb>

* Destination = \\??\E:\dumpit\WIN7WS-20190411-151517.raw
-> Are you sure you want to continue? [y/n] y
+ Processing... Success.

E:\dumpit>
```

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

## 12.2 DumpIt



## 12.3 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

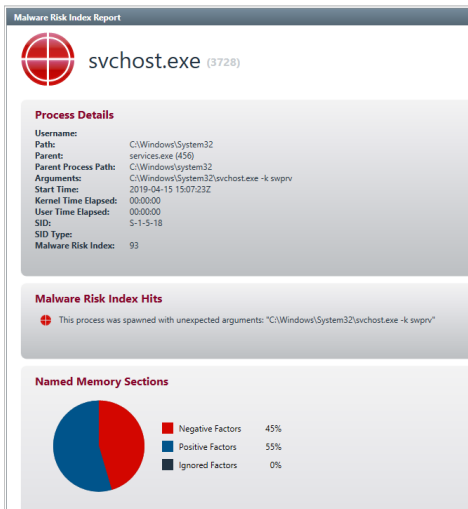


## 12.3 Mandiant Redline - Malware Risk Index



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

## 12.3 Mandiant Redline - Malware Risk Index



## 12.3 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
owxob-a.exe	93	3432	C:\Users\John\AppData\Roaming\owxob-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 owxob-a.exe	3432
iexplore.exe	52	3832	"C:\Program Files\Internet Explorer\iexplore.exe" -nohome	04/15/2019 15:08:06 owxob-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

## 12.3 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: sppsvc.exe	PID: 2844	Path: C:\Windows\system32	Args: C:\Windows\system32\sppsvc.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: owioob-a.exe	PID: 3432	Path: C:\Users\John\AppData\Roaming	Args: C:\Users\John\AppData\Roaming\owioob-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: owioob-a.exe	PID: 3432	Path: C:\Users\John\AppData\Roaming	Args: C:\Users\John\AppData\Roaming\owioob-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...			

## 12.4 Volatility: Overview

---

`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 DEMO-PC-20180315.raw imageinfo`

## 12.4 Volatility: Overview

---

```
volatility -f Win-Enc-20190415.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 --profile=Win7SP1x86 -f [filename] [plugin]  
[options]
```

## 12.5 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

## 12.5 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



## 12.5 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

.....

.....

## 12.6 Volatility: Network Analysis

---

- Windows XP and 2003 Server
  - connections
  - conncan
  - 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
.....					

## 12.7 Volatility: Exercise

---

```
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

```

```
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)

```

Create memdump of malicious process and search for suspicious URLs!



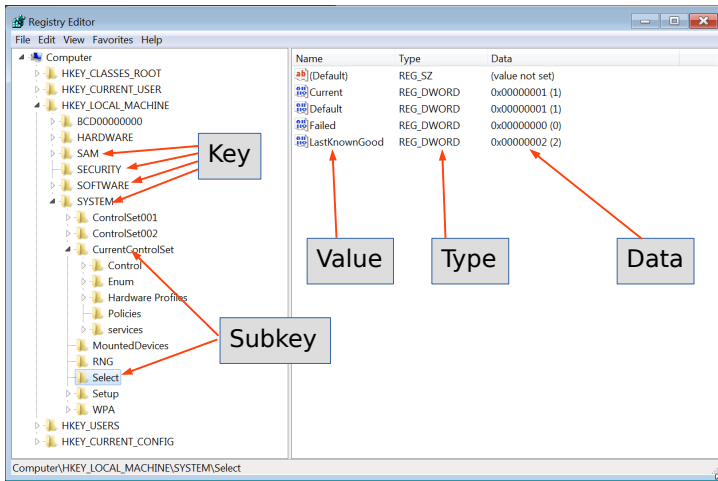
## 13. Windows Registry

## 13.1 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/>
    - Replace text based config files
    - A central hierarchical database
    - Contains information for operating
      - Hardware in the system
      - All aspects of MS Windows
      - Installed applications
      - Each user
- A gold mine for forensics

# 13.1 About: Windows Registry



## 13.1 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

## 13.2 Under the hood: Key Cell

---

```
a0 ff ff ff 6e 6b 20 00 6f 0f 0e 3b b7 8d d1 01 .....nk .o...;....
02 00 00 00 08 5e 05 00 00 00 00 00 00 00 00 .....^.....
ff ff ff ff ff ff ff ff 02 00 00 00 00 21 05 00 .....!...
10 2e 00 00 ff ff ff ff 00 00 00 00 00 00 00 .....
14 00 00 00 10 00 00 00 00 00 00 00 0a 00 00 .....
49 6e 74 65 72 66 61 63 65 73 00 80 02 00 00 Interfaces.....
```

Offsets in Bytes:		Size
	0	4
	4	2
	6	2
	8	8
	...	
	76	2
	80	<76>
		Length of key name
		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



## 13.2 Under the hood: Value Cell

---

```
          d8 ff ff ff 76 6b 0d 00          ....vk..
04 00 00 80 02 00 00 00 04 00 00 00 01 00 00 00 .....
4c 61 73 74 4b 6e 6f 77 6e 47 6f 6f 64 00 00 00 LastKnownGood...
```

Offsets in Bytes:		Size
	0	4
	4	2
	6	2
	8	4
	12	4
	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

## 13.3 Hive files

---

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

## 13.3 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`

## 13.4 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
362
```

- 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
```

## 13.5 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

## 13.6 Important user keys

---

- AutoStart
  - RunOnce
  - Run
    - /Software/Microsoft/Windows/CurrentVersion/Run/
    - Executed at user login
    - Provide *malware* persistence
    - No admin privileges required
  - Much more...
  - Legacy and other AutoStart
    - /Software/Microsoft/Windows/CurrentVersion/Policies/Explorer/Run/
    - /Software/Microsoft/Windows NT/CurrentVersion/Windows/'load','run'
- Program execution: By 'cmd.exe'
  - MUI Cache
    - XP: Software/Microsoft/Windows/ShellNoRoam/MUICache/
    - Vista: Local Settings/Software/Microsoft/Windows/Shell/MUICache/

## 13.6 Important user keys

---

- Program execution
  - UserAssist - Track user activities
    - `/Software/Microsoft/Windows/CurrentVersion/Explorer/UserAssist/`
    - `rip.pl -r john.dat -p userassist | less`
    - 'Windows Explorer Shell' & 'START menu' users interaction
    - Subkey values: Path, Run-Count, FileTime last access
    - Subkey values: ROT-13
  - Application Compatibility Assistant
- File-, Folder-, Share access
  - Shell Bags
    - Track views, sizes and positions of a folders
    - Incl. time stamps
    - Incl. ZIP subfolders & IE FTP
  - MRU Lists
    - RecentDocs
    - RunMRU

## 13.6 Important user keys

---

- File access

- RecentDocs

Example: '.png' files

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

- Common Dialogs

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

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

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





## 14. Event Logs

## 14.1 Overview: Windows Event Logs

---

- Up to Windows XP
  - Binary Event Log file format
  - Mainly 3 categories:
    - Security
    - System
    - Application
    - ... some server service specific
- Beginning with Vista
  - New extension: .evtx
  - New format based on XML
  - Location: /Windows/System32/winevt/Logs/
  - Many more files:
    - Security
    - System
    - Application

```
$ ls | wc -l
```

59

## 14.1 Overview: Windows Event Logs

---

- 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
.....
```

- Get details online:
  - Microsoft TechNet
  - <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>
  - <http://eventid.net/>

## 14.2 Example: Login

---

- Successful

```
$ 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              : 0x0000000000000003e7
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
```

- Failed

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

## 14.2 Example: Login

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.
-----------	---

## 14.3 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

## 14.4 Event Logs: Exercise

---

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?

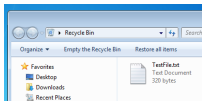


## 15. Other Sources of Information



## 15.1 Recycle Bin

---



- - 2019-04-30 17:31:57 UTC+2: Text file created
  - 2019-04-30 17:34:44 UTC+2: Text file modified
  - 2019-04-30 17:35:32 UTC+2: Text file deleted

- Analyze Recycle.Bin:

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

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

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

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

.....

## 15.1 Recycle Bin

---

- Play Script:
  - 2019-04-30 17:31:57 UTC+2: Text file created
  - 2019-04-30 17:34:44 UTC+2: Text file modified
  - 2019-04-30 17:35:32 UTC+2: Text file deleted
- File system time line

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
```

## 15.2 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

## 15.2 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
...
```

## 15.3 XP Restore Points

---

- Backups include:
  - Registry hives
  - Local profiles
  - ...
- Created:
  - Windows XP: 24 hours
  - Windows AutoUpdate
  - Installation of applications & unsigned driver
  - Restore operation
  - Manually
- Provides:
  - `rp.log`
  - Description of the cause
  - Time stamp
  - State of the system at different times

## 15.4 Volume Shadow Copy

---

- On Windows: C:/>vssadmin list shadows /for=c:/
- Infected PC:

```
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
```

```
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/
```

## 15.5 Prefetch Files & SuperFetch

---

- Improve performance
- Boot prefetching
- Application prefetching
- Collect information about all files accessed
- Take all resources as one file
- Resources are not spread around the disk
- Wait 10sec after application started
  - Better performance
  - Example:

Thu May 02 2019 14:52:40

179712	.a..	10940-128-3	/Windows/System32/notepad.exe
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

## 15.5 Prefetch Files & SuperFetch

---

- Information found:
  - Application launched number of times
  - Application launched last time
  - Path to application
  - Path to other resources
- Indirect benefits:
  - Which user was logged in run the application
  - Deleted applications run once in time

```
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
.....
```





## 16. Analysing files

## 16.1 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

## 16.2 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



## 17. Bibliography and Outlook

## 17.1 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  
Harlan Carvey  
Syngress  
ISBN-13: 978-1-59-749727-5

## 17.2 Outlook

---

- Windows 8 analysis
- Windows 10 analysis
- Document file analysis
- Executable file analysis
- Internet artifacts

# Overview

---

- 11. Live Response
- 12. Memory Forensics
- 13. Windows Registry
- 14. Event Logs
- 15. Other Sources of Information
- 16. Analysing files
- 17. Bibliography and Outlook