Intro to Digital Forensics

By Thanasis Konstantopoulos & Maria Tzevelekou

TABLE OF CONTENTS

What is Digital Forensics?

Digital forensics is a forensic science branch that deals with recovering, investigating, and preserving digital evidence while upholding legal standards.

What is “digital evidence”?

‘Digital evidence’ depends on the device type being scraped through. This can be anything from user account data to electronic door logs.

Digital evidence can be any sort of digital file from an electronic source. These include:

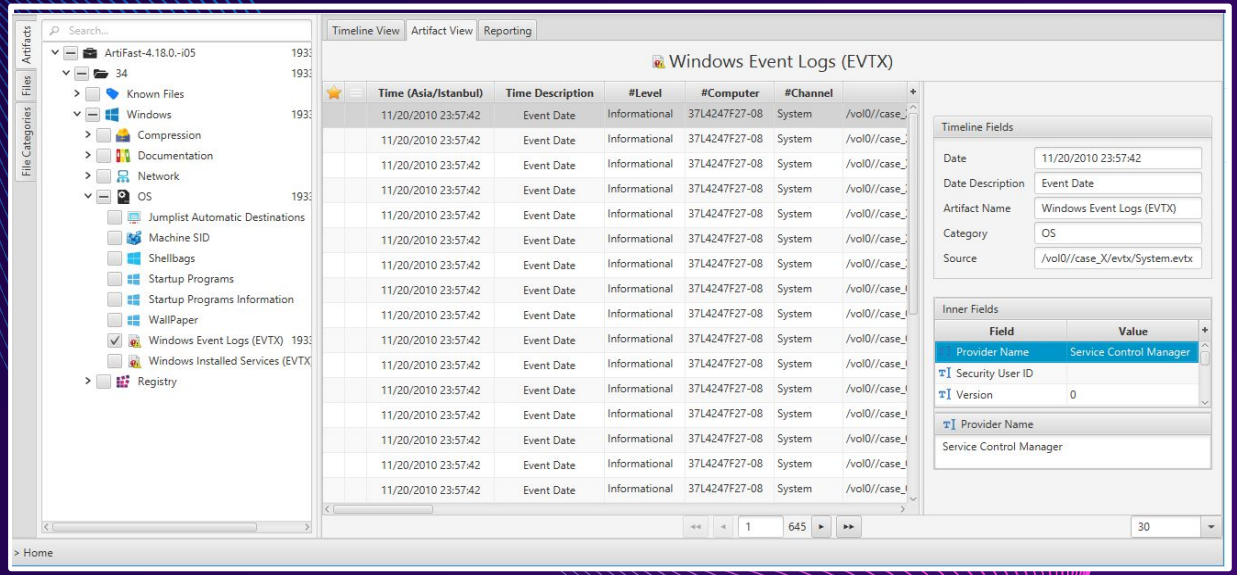
- Emails
- Text & instant messages
- Files and documents extracted from hard drives
- Electronic financial transactions
- Audio files, video files
- And many more.

Event Logs

- Event logs are a specific type of file that store information about significant actions or occurrences in a computer system.

- They contain:
  - System-related events from the OS – These are typically system events, such as issues encountered during startup and other OS-related events.
  - Application-specific events from programs running on the machine – These are events logged by individual applications.
  - Security-related events such as login and logout

Common Event Log Fields

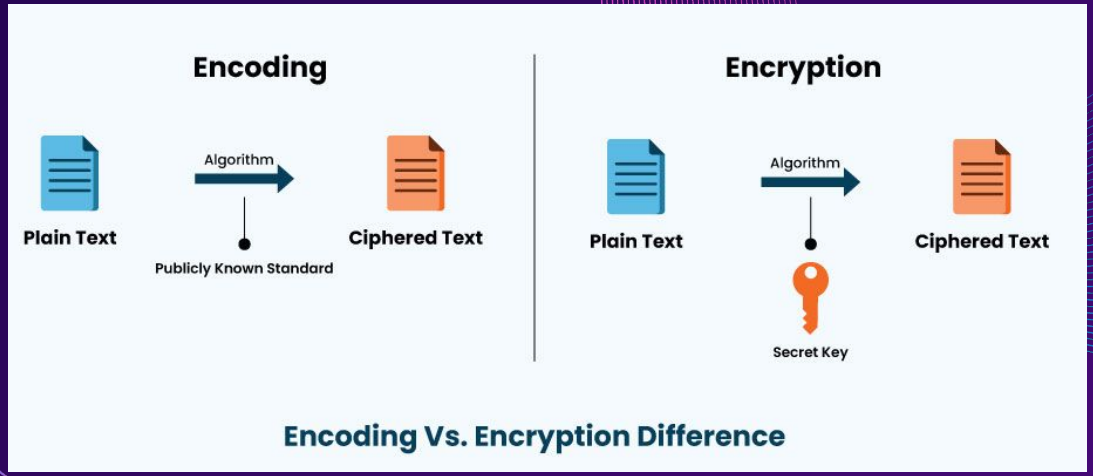


- The timestamp of the event
- A severity or logging level field. This could be labeled “general information,” “warning,” or “critical error.”
- The user name if it’s a user-generated action
- A description of the actual event

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/?fbclid=IwAR1uApS3aCrje9iIRO7hETV3fdu-CK0sFXGiSJCtZG2Y7PChFQ2esem9mA

Encodings & Obfuscation

- The transformation of data from one format to another
  - NOT encryption
- Different/popular types of encodings:
  - Binary, hex, base64
  - URL encoded data



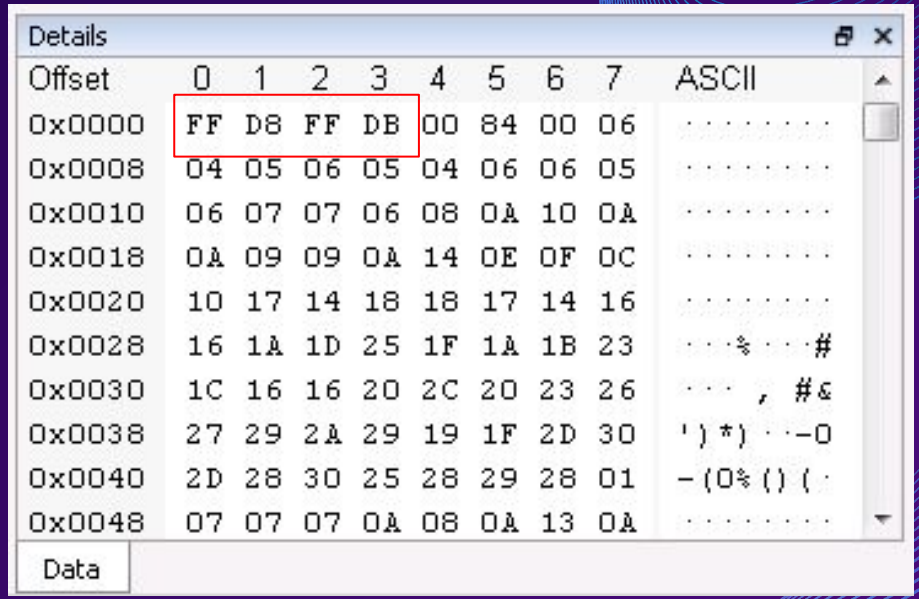
Binary, Hex & Base64 Examples

- Binary
  - Base-2 numbering system
  - Used for low level machine operations

Dec	Symbol	Binary	Dec	Symbol	Binary
65	A	0100 0001	83	S	0101 0011
66	B	0100 0010	84	T	0101 0100
67	C	0100 0011	85	U	0101 0101
68	D	0100 0100	86	V	0101 0110
69	E	0100 0101	87	W	0101 0111
70	F	0100 0110	88	X	0101 1000
71	G	0100 0111	89	Y	0101 1001
72	H	0100 1000	90	Z	0101 1010
73	I	0100 1001	91	[	0101 1011
74	J	0100 1010	92	\	0101 1100
75	K	0100 1011	93	]	0101 1101
76	L	0100 1100	94	^	0101 1110
77	M	0100 1101	95	_	0101 1111
78	N	0100 1110	96	`	0110 0000
79	O	0100 1111	97	a	0110 0001
80	P	0101 0000	98	b	0110 0010
81	Q	0101 0001	99	c	0110 0011
82	R	0101 0010	100	d	0110 0100

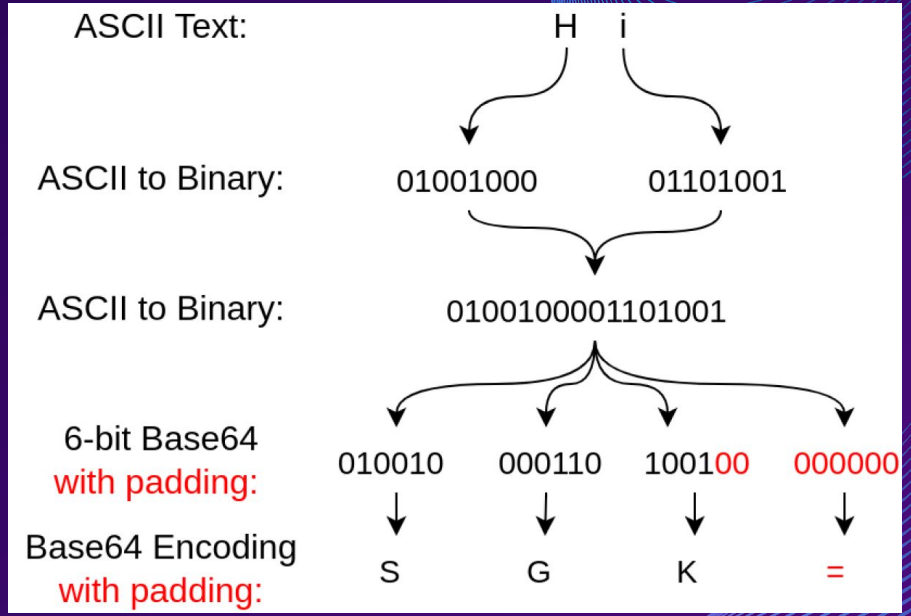
Binary, Hex & Base64 Examples

- Hex
  - Base-16 numbering system
  - 00 to FF
  - Hexeditors are important for file headers
    - Allow in forensic analysis to see if a file has been deleted
    - Or if the file has been corrupt



Binary, Hex & Base64 Examples

- Base64
  - Uses 64 ASCII characters
  - Each 6 bits are encoded into a letter from the alphabet
  - Usually identifiable by the ‘==’ at the end
  - Used in email attachments, encryption, web dev, and URLS



Try them out at https://gchq.github.io/CyberChef/

What does the following message say?

00110101 00110100 00100000 00110110 01100011 00100000 00110101
00110010 00100000 00110101 00110110 00100000 00110101 00110001
00100000 00110101 00110110 00100000 00110011 00111001 00100000
00110100 00111001 00100000 00110100 01100101 00100000 00110100
00110101 00100000 00110100 01100101 00100000 00110100 01100011
00100000 00110000 01100001 00100000 00110110 00111001 00100000
00110111 00110011 00100000 00110010 00110000 00100000 00110111
00110100 00100000 00110110 00111000 00100000 00110110 00110101
00100000 00110010 00110000 00100000 00110110 00110010 00100000
00110110 00110101 00100000 00110111 00110011 00100000 00110111
00110100 00100000 00110010 00110000 00001010 01100101 01110110
01100101 01101110 01110100 00100000 01101001 01101110 00100000
01110100 01101000 01100101 00100000 01110000 01101100 01100001
01101110 01100101 01110100

URL Encodings

- URL encoding converts characters into a format that can be transmitted over the Internet.

- URLs can only be sent over the Internet using the ASCII character-set.

- Since URLs often contain characters outside the ASCII set, the URL has to be converted into a valid ASCII format.

- URL encoding replaces unsafe ASCII characters with a "%" followed by two hexadecimal digits.
- URLs cannot contain spaces. URL encoding normally replaces a space with a plus (+) sign or with %20.

URL Encodings Example

(index)	character	encodeURI	encodeURIComponent
0	"#"	"#"	"%23"
1	"$"	"$"	"%24"
2	"&"	"&"	"%26"
3	"+"	"+"	"%2B"
4	","	","	"%2C"
5	"/"	"/"	"%2F"
6	":"	":"	"%3A"
7	";"	";"	"%3B"
8	"="	"="	"%3D"
9	"?"	"?"	"%3F"
10	"@"	"@"	"%40"

For example- Hello, World! as a Google search
https://google.com/search?q=Hello%2C+World%21

For more information:
https://www.w3schools.com/tags/ref_urlencode.ASP?fbclid=IwAR102ly4sAZCBxOFX-NIgXYZy8uHrds_L8js0r6Vs9u78SjIW0Kz1XZFkgo

;	%3B
<	%3C
=	%3D
>	%3E
?	%3F
@	%40
A	%41
B	%42
C	%43
D	%44
E	%45
F	%46
G	%47
H	%48

Obfuscation

- A way to make a program difficult to understand and read, no matter how simple it is
  - Used to conceal important pieces of code
  - Via encoding, replacing class/variable names to gibberish or adding unused code
- For example:
  - Javascript obfuscator: https://www.javascriptobfuscator.com/Javascript-Obfuscator.aspx
- This is usually done by malicious code writers (ie. for malware, viruses etc.)
  - difficult for a file to be detected by antimalware tools and for it to be reverse engineered

Obfuscation

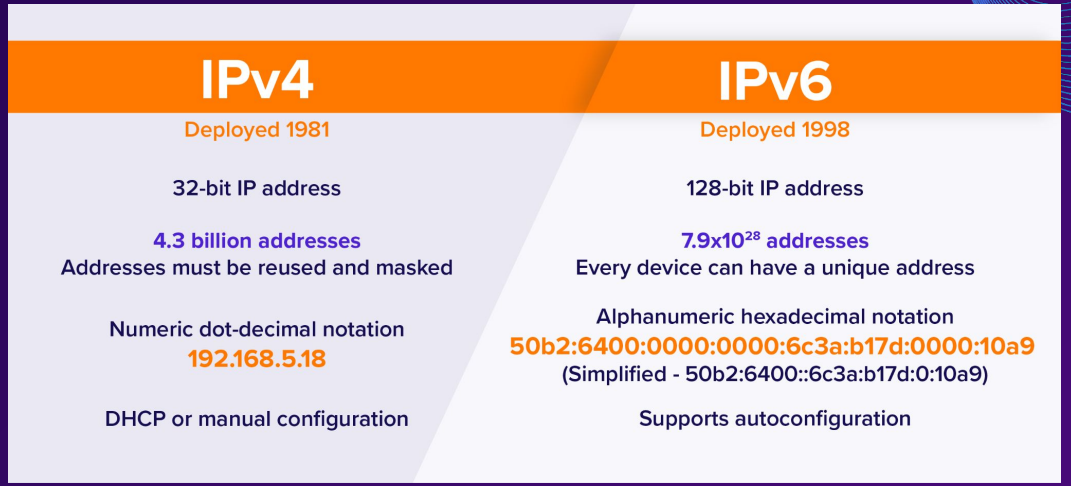
- For example: obfuscation of console.log(“Hello world!”);

```
var _0x31fb1d=_0x1fa7;function _0x1fa7(_0x20dafa,_0x2fcfe0){var _0x2f53b0=_0x2f53();return _0x1fa7=function(_0x1fa7cb,_0x373207)
{_0x1fa7cb=_0x1fa7cb-0x79;var _0x16f03f=_0x2f53b0[_0x1fa7cb];return _0x16f03f;},_0x1fa7(_0x20dafa,_0x2fcfe0);}
(function(_0x575631,_0x46dab7){var _0x1800da=_0x1fa7,_0x3fd047=_0x575631();while(!![]){try{var
_0x3610cb=parseInt(_0x1800da(0x81))/0x1+parseInt(_0x1800da(0x83))/0x2*(parseInt(_0x1800da(0x7b))/0x3)+parseInt(_0x1800da(0x79))/0x4+-
parseInt(_0x1800da(0x7c))/0x5*(parseInt(_0x1800da(0x7a))/0x6)+parseInt(_0x1800da(0x80))/0x7*(parseInt(_0x1800da(0x7d))/0x8)+-
parseInt(_0x1800da(0x82))/0x9+-parseInt(_0x1800da(0x7e))/0xa;if(_0x3610cb===_0x46dab7)break;else _0x3fd047['push'](_0x3fd047['shift']
());}catch(_0x1de9c2){_0x3fd047['push'](_0x3fd047['shift']());}}}(_0x2f53,0x852c0),console['log'](_0x31fb1d(0x7f)));function _0x2f53(){var _0x477924=
['886510tlAliH','5416wUArVd','11418890rpxbeS','Hello\x20World!','1778NVYTWR','1040225uDWEbD','2391480IXDywU','922258PpPunl','692976kXlPp
K','12JCciCj','6blMPeq'];_0x2f53=function(){return _0x477924;};return _0x2f53();}
```

- Solution: online deobfuscator,
  - Program slicing: trying to understand what the code is doing (via substitutions) and narrowing it down to its important parts

Network Traffic

- The amount of data moving across a computer network at some point in time
- Usually stored in network traffic logs with .pcap or .pcapng file- programs like Wireshark can help analyze them
- IP Addresses- show the source and destination of the packet



Wireshark Basics

Network Forensics, Wireshark Basics:

https://www.hackers-arise.com/post/2018/09/24/network-forensics-wireshark-basics-part-1

Memory Dumps

A memory dump is the process of taking all information content in RAM and writing it to a storage drive as a memory dump file.

Common types of memory dumps

- Complete memory dump: contains a copy of all the data used in physical memory.
- Kernel memory dump: contains about one-third of the physical memory on the system.
- Small memory dump (64 KB): contains very little information (e.g., a list of loaded drivers, blue-screen information).
- Automatic memory dump: contains the same information as a kernel memory dump.

Memory Dumps

What is RAM on a computer?

RAM (random access memory) is a computer's short-term memory, where the data that the processor is currently using is stored. Your computer can access RAM memory much faster than data on a hard disk, SSD, or other long-term storage device, which is why RAM capacity is critical for system performance. **RAM is a form of temporary storage that gets wiped when you turn your computer off.**

Memory Dumps

A complete memory dump will contain all data from memory (RAM) when the device stopped, including information like:

- Activities the user has undertaken in a session.
- Detailed system information.
- Disk passwords and encryption keys.
- Details of documents that were open.
- Account usernames and passwords.

Memory Dumps

Process Dump

A process memory dump is the writing of a piece of operating memory to the computer's disk for further analysis. The resulting data file will contain the machine code of the process, variables in memory, such as subtitles or numeric values, and other data contained in the process. It is worth mentioning that the snapshot will preserve the memory state of the process from a "specific moment". For example, if we take a memory dump before the user logs in, the credentials will not be there. On the other hand, if the dump is taken after the user has logged in, then with a bit of luck it will be possible to find, for example, password hashes in it.

Memory Dumps

Why do adversaries use LSASS Memory?

Adversaries commonly abuse the Local Security Authority Subsystem Service (LSASS) to dump credentials for privilege escalation, data theft, and lateral movement. The process is a fruitful target for adversaries because of the sheer amount of sensitive information it stores in memory. Upon starting up, LSASS contains valuable authentication data such as:

- encrypted passwords
- NT hashes
- LM hashes
- Kerberos tickets

The LSASS process is typically the first that adversaries target to obtain credentials. Post-exploitation frameworks like Cobalt Strike import and customize existing code from credential theft tools like Mimikatz, allowing operators to easily access LSASS via beacons.

Memory Dumps

Volatility Framework

Volatile data is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory (RAM).

Volatility is the world's most widely used framework for extracting digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer visibility into the runtime state of the system. The framework is intended to introduce people to the techniques and complexities associated with extracting digital artifacts from volatile memory samples and provide a platform for further work into this exciting area of research.

Memory Dumps

Everything about volatility2 can be found here:

https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

Installation:

$ git clone https://github.com/volatilityfoundation/volatility3.git

$ cd volatility3

$ python3 vol.py -h

$ python3 vol.py -f <imagepath> windows.info

Memory Dumps

Plugin: windows.pslist

```
└─$ python3 ~/volatility3/vol.py -f Win10.raw windows.pslist
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x8a05cba83040  157     -       N/A     False   2023-12-07 20:33:44.000000      N/A     Disabled
140     4       Registry        0x8a05cbbd9040  4       -       N/A     False   2023-12-07 20:33:34.000000      N/A     Disabled
396     4       smss.exe        0x8a05cc2d6040  2       -       N/A     False   2023-12-07 20:33:44.000000      N/A     Disabled
504     492     csrss.exe       0x8a05cd1d3080  11      -       0       False   2023-12-07 20:33:49.000000      N/A     Disabled
580     492     wininit.exe     0x8a05cdba9080  1       -       0       False   2023-12-07 20:33:49.000000      N/A     Disabled
600     572     csrss.exe       0x8a05cdbad140  12      -       1       False   2023-12-07 20:33:49.000000      N/A     Disabled
680     572     winlogon.exe    0x8a05cdbdf080  4       -       1       False   2023-12-07 20:33:49.000000      N/A     Disabled
724     580     services.exe    0x8a05cdbeb080  8       -       0       False   2023-12-07 20:33:49.000000      N/A     Disabled
744     580     lsass.exe       0x8a05ce2dd080  9       -       0       False   2023-12-07 20:33:49.000000      N/A     Disabled
860     724     svchost.exe     0x8a05ce4d4240  15      -       0       False   2023-12-07 20:33:49.000000      N/A     Disabled
888     580     fontdrvhost.ex  0x8a05ce4de140  5       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
896     680     fontdrvhost.ex  0x8a05ce4da2c0  5       -       1       False   2023-12-07 20:33:50.000000      N/A     Disabled
976     724     svchost.exe     0x8a05ce7fb2c0  10      -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
88      724     svchost.exe     0x8a05ce404240  4       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
572     680     dwm.exe 0x8a05ce4a2080  18      -       1       False   2023-12-07 20:33:50.000000      N/A     Disabled
884     724     svchost.exe     0x8a05ce37f280  2       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1056    724     svchost.exe     0x8a05ce4bf300  0       -       0       False   2023-12-07 20:33:50.000000      2023-12-07 10:37:50.000000      Disabled
1080    724     svchost.exe     0x8a05ce3a1300  3       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1144    724     svchost.exe     0x8a05ce442300  8       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1192    724     svchost.exe     0x8a05ce4492c0  2       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1272    724     svchost.exe     0x8a05ce42f2c0  4       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1344    724     svchost.exe     0x8a05ce535240  5       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1392    724     svchost.exe     0x8a05ce547300  6       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1468    724     svchost.exe     0x8a05ce587240  13      -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1544    724     svchost.exe     0x8a05ce620300  6       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1552    724     svchost.exe     0x8a05ce617240  3       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1560    724     svchost.exe     0x8a05ce615280  6       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1568    724     svchost.exe     0x8a05ce619240  3       -       0       False   2023-12-07 20:33:50.000000      N/A     Disabled
1584    724     svchost.exe     0x8a05ce61b2c0  7       -       0       False   2023-12-07 20:33:51.000000      N/A     Disabled
1700    724     svchost.exe     0x8a05ce690300  1       -       0       False   2023-12-07 20:33:51.000000      N/A     Disabled
1756    724     svchost.exe     0x8a05ce6d0240  2       -       0       False   2023-12-07 20:33:51.000000      N/A     Disabled
1828    4       MemCompression  0x8a05ce6ce080  30      -       N/A     False   2023-12-07 20:33:51.000000      N/A     Disabled
1876    724     svchost.exe     0x8a05ce7622c0  9       -       0       False   2023-12-07 20:33:51.000000      N/A     Disabled
1912    724     svchost.exe     0x8a05ce818280  3       -       0       False   2023-12-07 20:33:51.000000      N/A     Disabled
1920    724     svchost.exe     0x8a05ce81b2c0  4       -       0       False   2023-12-07 20:33:51.000000      N/A     Disabled
```

Memory Dumps

Plugin: windows.pstree

```
└─$ python3 ~/volatility3/vol.py -f Win10.raw windows.pstree
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0×8a05cba83040  157     -       N/A     False   2023-12-07 20:33:44.000000      N/A
* 396   4       smss.exe        0×8a05cc2d6040  2       -       N/A     False   2023-12-07 20:33:44.000000      N/A
* 140   4       Registry        0×8a05cbbd9040  4       -       N/A     False   2023-12-07 20:33:34.000000      N/A
* 1828  4       MemCompression  0×8a05ce6ce080  30      -       N/A     False   2023-12-07 20:33:51.000000      N/A
504     492     csrss.exe       0×8a05cd1d3080  11      -       0       False   2023-12-07 20:33:49.000000      N/A
580     492     wininit.exe     0×8a05cdba9080  1       -       0       False   2023-12-07 20:33:49.000000      N/A
* 744   580     lsass.exe       0×8a05ce2dd080  9       -       0       False   2023-12-07 20:33:49.000000      N/A
* 724   580     services.exe    0×8a05cdbeb080  8       -       0       False   2023-12-07 20:33:49.000000      N/A
** 1544 724     svchost.exe     0×8a05ce620300  6       -       0       False   2023-12-07 20:33:50.000000      N/A
** 2572 724     spoolsv.exe     0×8a05cea070c0  9       -       0       False   2023-12-07 20:33:51.000000      N/A
** 1552 724     svchost.exe     0×8a05ce617240  3       -       0       False   2023-12-07 20:33:50.000000      N/A
** 1560 724     svchost.exe     0×8a05ce615280  6       -       0       False   2023-12-07 20:33:50.000000      N/A
** 1056 724     svchost.exe     0×8a05ce4bf300  0       -       0       False   2023-12-07 20:33:50.000000      2023-12-07 10:37:50.000000
** 1568 724     svchost.exe     0×8a05ce619240  3       -       0       False   2023-12-07 20:33:50.000000      N/A
** 3104 724     svchost.exe     0×8a05cec1f240  6       -       0       False   2023-12-07 20:33:52.000000      N/A
** 1584 724     svchost.exe     0×8a05ce61b2c0  7       -       0       False   2023-12-07 20:33:51.000000      N/A
** 4660 724     TrustedInstall  0×8a05cf626080  5       -       0       False   2023-12-07 10:38:27.000000      N/A
** 1080 724     svchost.exe     0×8a05ce3a1300  3       -       0       False   2023-12-07 20:33:50.000000      N/A
** 2620 724     svchost.exe     0×8a05cea0b0c0  13      -       0       False   2023-12-07 20:33:51.000000      N/A
** 4164 724     svchost.exe     0×8a05cf7a0080  7       -       1       False   2023-12-07 20:34:25.000000      N/A
** 6216 724     svchost.exe     0×8a05d423b300  8       -       0       False   2023-12-07 20:35:14.000000      N/A
** 4172 724     svchost.exe     0×8a05cf5ce2c0  14      -       0       False   2023-12-07 20:34:01.000000      N/A
** 4688 724     svchost.exe     0×8a05cf5aa080  1       -       0       False   2023-12-07 20:34:21.000000      N/A
** 9812 724     SgrmBroker.exe  0×8a05d532b080  6       -       0       False   2023-12-07 20:35:52.000000      N/A
** 88   724     svchost.exe     0×8a05ce404240  4       -       0       False   2023-12-07 20:33:50.000000      N/A
** 9820 724     svchost.exe     0×8a05ceac10c0  7       -       0       False   2023-12-07 10:44:02.000000      N/A
** 620  724     svchost.exe     0×8a05cfabd240  5       -       0       False   2023-12-07 20:34:20.000000      N/A
** 1144 724     svchost.exe     0×8a05ce442300  8       -       0       False   2023-12-07 20:33:50.000000      N/A
** 2184 724     svchost.exe     0×8a05ce93d2c0  10      -       0       False   2023-12-07 20:33:51.000000      N/A
**** 8764       2184    audiodg.exe     0×8a05cc3ab2c0  4       -       0       False   2023-12-07 10:46:22.000000      N/A
** 2696 724     svchost.exe     0×8a05ceacf300  5       -       0       False   2023-12-07 20:33:52.000000      N/A
** 5268 724     svchost.exe     0×8a05cf868080  3       -       0       False   2023-12-07 20:34:25.000000      N/A
**** 5360       5268    ctfmon.exe      0×8a05d0d522c0  12      -       1       False   2023-12-07 20:34:25.000000      N/A
** 4756 724     svchost.exe     0×8a05d0ef0280  7       -       0       False   2023-12-07 20:34:28.000000      N/A
** 1172 724     svchost.exe     0×8a05cea860c0  19      -       0       False   2023-12-07 10:48:54.000000      N/A
** 2204 724     svchost.exe     0×8a05ce94d300  4       -       0       False   2023-12-07 20:33:51.000000      N/A
** 4768 724     svchost.exe     0×8a05d4394300  1       -       0       False   2023-12-07 20:34:59.000000      N/A
```

Memory Dumps

Plugin: windows.cmdline

```
└─$ python3 ~/volatility3/vol.py -f Win10.raw windows.cmdline
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0×20 is not valid (process exited?)
140     Registry        Required memory at 0×20 is not valid (process exited?)
396     smss.exe        \SystemRoot\System32\smss.exe
504     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On Subs
tialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
580     wininit.exe     wininit.exe
600     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On Subs
tialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
680     winlogon.exe    winlogon.exe
724     services.exe    C:\Windows\system32\services.exe
744     lsass.exe       C:\Windows\system32\lsass.exe
860     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p
888     fontdrvhost.ex  "fontdrvhost.exe"
896     fontdrvhost.ex  "fontdrvhost.exe"
976     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS -p
88      svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
572     dwm.exe "dwm.exe"
884     svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
1056    svchost.exe     Required memory at 0×ccfd228020 is not valid (process exited?)
1080    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
1144    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
1192    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
1272    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
1344    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
1392    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
1468    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
1544    svchost.exe     C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
1552    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
1560    svchost.exe     C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain
1568    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
1584    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
1700    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
1756    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
1828    MemCompression  Required memory at 0×20 is not valid (process exited?)
1876    svchost.exe     C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
```

Thank you for your attention!!