

v1

Malware Analysis Professional

The Lab

Section 01 | Module 01 | Appendix A

<https://t.me/learningnets>

© Caendra Inc. 2020
All Rights Reserved

Table of Contents

MODULE 01 | APPENDIX A | THE LAB

A1.1 Hardware Requirements

A1.2 Operating System Requirements

A1.3 Hypervisor Requirements

A1.4 Software Requirements



Learning Objectives

By the end of this appendix module, you should have a better understanding of:

- ✓ What hardware and software is recommended to perform malware analysis
- ✓ What tools you will need and expect to be using during the course
- ✓ How to setup your network environment to perform malware analysis
- ✓ Other tools and recommendations

Hardware Requirements



A1.1 Hardware Requirements



The truth is, there is no one definite answer as to what hardware you will need. It depends on your budget. Therefore, what is recommended here, will take that into consideration.

You don't have to purchase the most expensive hardware to start your career in Malware Analysis.

```
28 def initialize(experiment, observations = [], candidates = [])
29   @experiment = experiment
30   @observations = observations
31   @control = control
32   @candidates = observations + [control]
33   evaluate_candidates
34
35   freeze
36 end
37
38 # Returns the experiment's context
39 def context
40   experiment.context
41
42   {
43     experiment_name:
44     experiment.name
45   }
46
47
48 # Returns the result a match returns
49 def matches?
50   @candidates[result.to_i]
51 end
```

A1.1 Hardware Requirements

Set up with low budget:

- Any Processor (AMD or Intel) with 4+ cores
- 16GB of Physical Memory
- Hard Disk Drive 512GB
- Network Card 1Gbps

A1.1 Hardware Requirements

Recommended setup:

- Any Processor (AMD or Intel) with 16+ cores
- 32GB/64GB of Physical Memory
- Hard Disk Drive 512GB NVMe / SSD
- Network Card 1Gbps

Operating System Requirements



A1.2 Operating System Requirements



Now that we have the hardware settled, we need an operating system to use for our analysis. This is where another question will arise: which OS should I use?

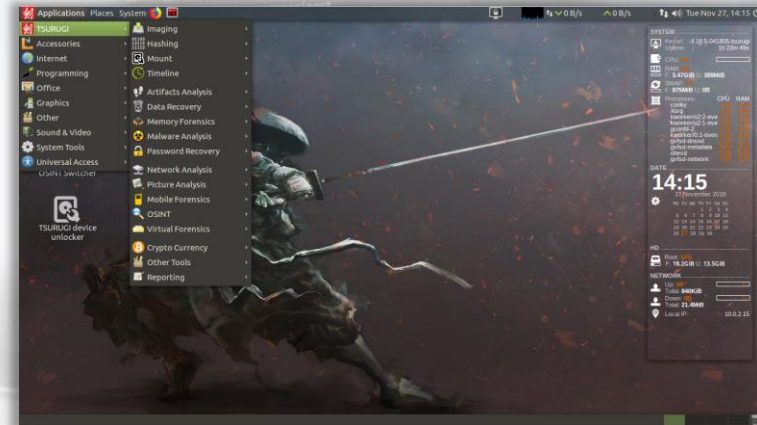
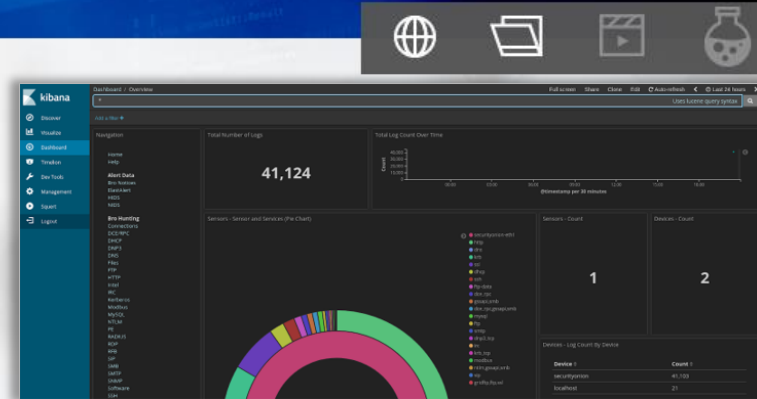
The truth again is, there is no one best system. It is best to have a diversity of systems to use and throughout the course, you will see why.

```
20 def initialize(experiment, observations = [], control = nil)
21   @experiment = experiment
22   @observations = observations
23   @control = control
24   @candidates = observations + [control]
25   evaluate_candidates
26
27   freeze
28
29   @experiment
30   experiment.context
31
32   @observations
33   experiment.observations
34   experiment.name
35
36   @control
37
38   @candidates
39   @candidates
40
41   @candidates
42   @candidates
43
44   @candidates
45   @candidates
46
47   @candidates
48   @candidates
49
50   @candidates
51   @candidates
52
53   @candidates
54   @candidates
55
56   @candidates
57   @candidates
58
59   @candidates
60   @candidates
61
62   @candidates
63   @candidates
64
65   @candidates
66   @candidates
67
68   @candidates
69   @candidates
70
71   @candidates
72   @candidates
73
74   @candidates
75   @candidates
76
77   @candidates
78   @candidates
79
80   @candidates
81   @candidates
82
83   @candidates
84   @candidates
85
86   @candidates
87   @candidates
88
89   @candidates
90   @candidates
91
92   @candidates
93   @candidates
94
95   @candidates
96   @candidates
97
98   @candidates
99   @candidates
100  @candidates
```

A1.2 Operating System Requirements

We will be using the following systems:

- [SecurityOnion](#)
- [Tsurugi Linux](#)
- [Windows 10](#)



Hypervisor Requirements



A1.3 Hypervisor Requirements



The most important part of your investigation and analysis environment is the hypervisor that will be used. There are many hypervisors out there, but the two most commonly used are [VirtualBox](#) (free) and [VMWare](#) (commercial).

We leave the choice of which one to use up to you. Regardless of which brand you go with, the outcome of using either, for this course at least, will be the same.

A1.3 Hypervisor Requirements



Other than just creating our lab using a hypervisor, we also want a way to go back when we do mistakes, and yes mistakes might happen.

Don't be worried, what we mean is, what if you were analyzing a sample and you forgot to do a specific preparation or what if you want to go back to a previous step to do it differently?

A1.3 Hypervisor Requirements



This is where using a hypervisor that allows you to take snapshots will be extremely handy and useful.

Therefore, once you finish preparing your lab, make sure to take a snapshot in a clean state before proceeding. That state is what you will go back to during the analysis, if necessary.

A1.3 Hypervisor Requirements

Before you move on to the next chapter, remember that you need to create a _____.

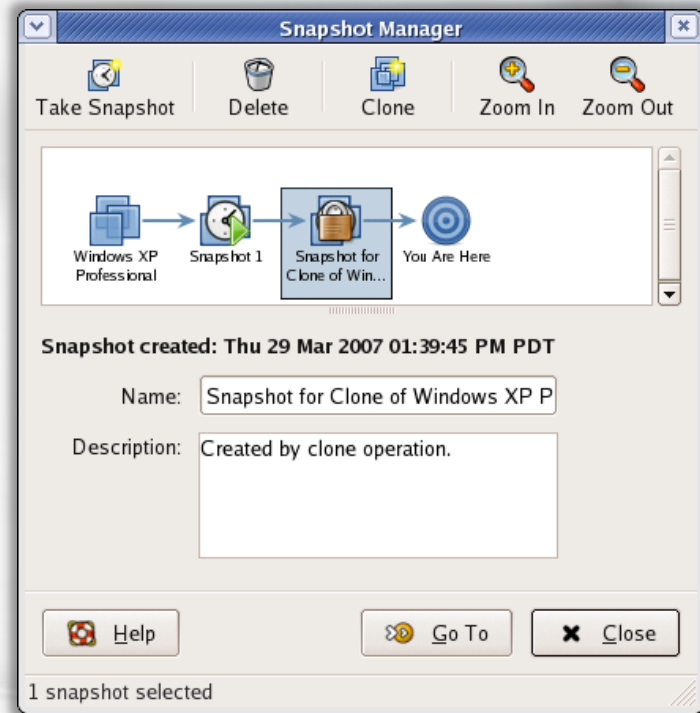
A1.3 Hypervisor Requirements

SNAPSHOT

Take a snapshot.

Take a snapshot.

We will continue to remind you.



Software Requirements



A1.4 Software Requirements



You will use many software tools in Malware Analysis. However, Malware Analysis is not about tools, but rather understanding how these tools work and the technologies behind them. The tools we need are only to simplify the dissection part of how they work, but they alone will not answer your client's questions.

A1.4 Software Requirements



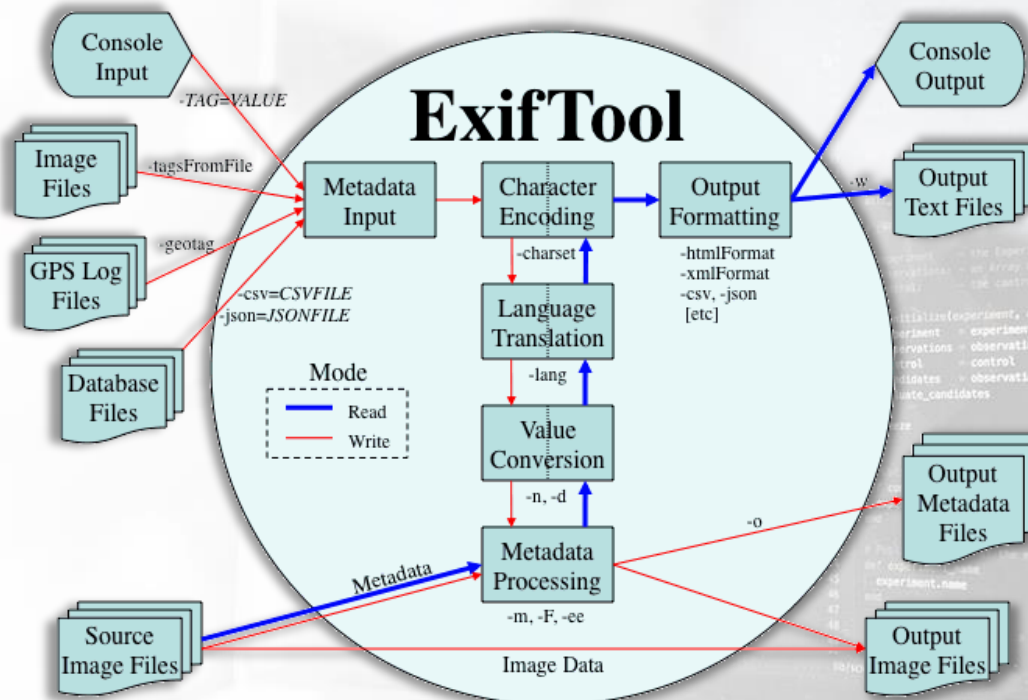
The tools we will use in this course can be divided into the following categories:

1. String and Metadata
2. Static Analysis
3. Dynamic Analysis
4. Memory Analysis
5. Incident Response
6. Network Analysis
7. Visualization
8. Frameworks

The following slides will list and link to the tools used in the above categories.

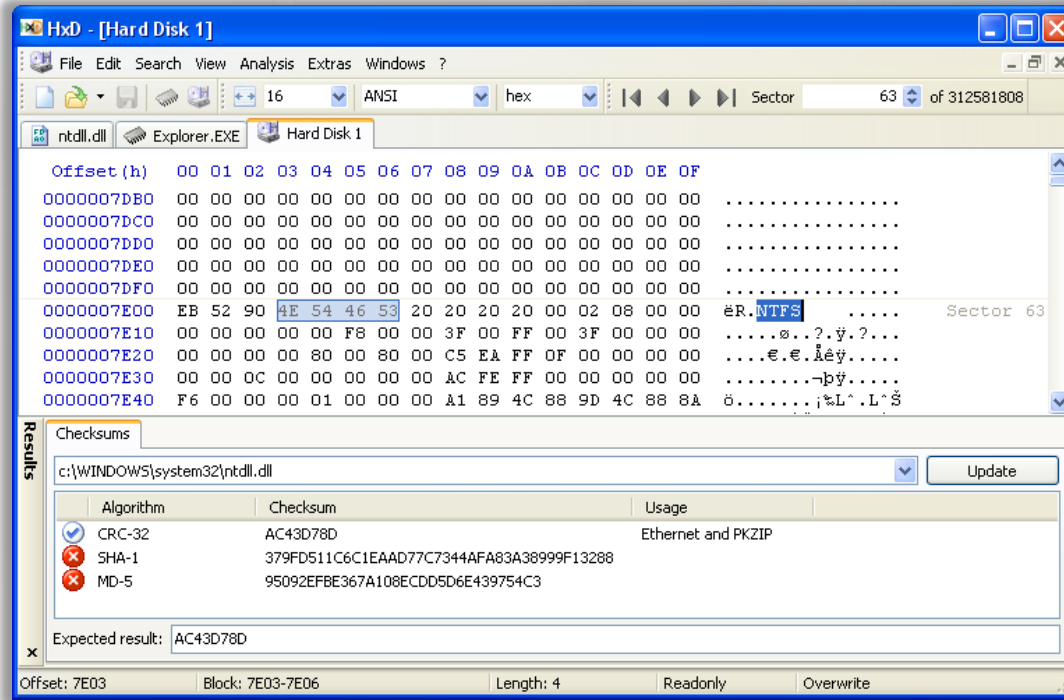
A1.4.1 String and Metadata Tools

ExifTool



A1.4.1 String and Metadata Tools

HxD Hex Editor



A1.4.1 String and Metadata Tools

Additional String and Metadata tools include:

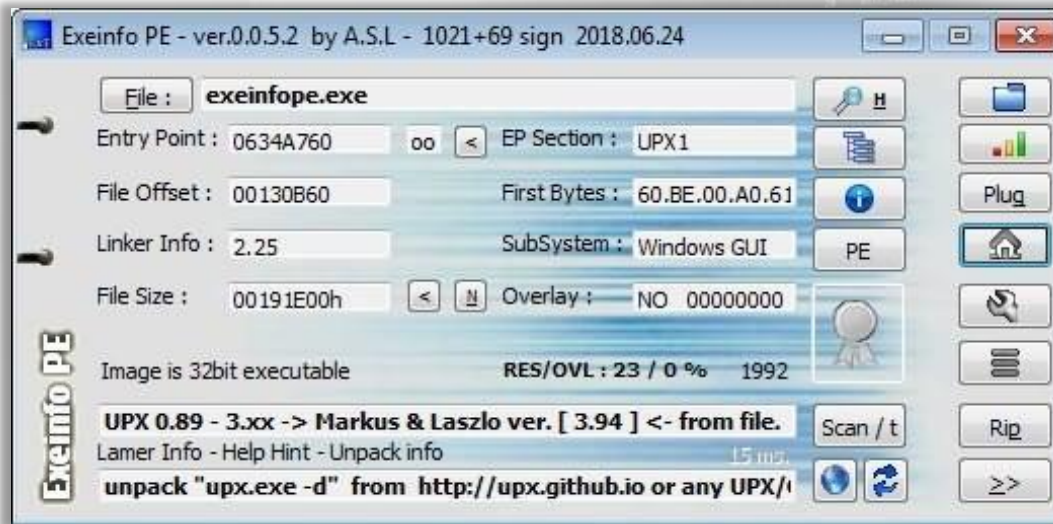
- [Free Hex Editor Neo](#)
- [bstrings](#)
- [BinText](#)
- [StringSifter](#)



A1.4.2 Static Analysis Tools



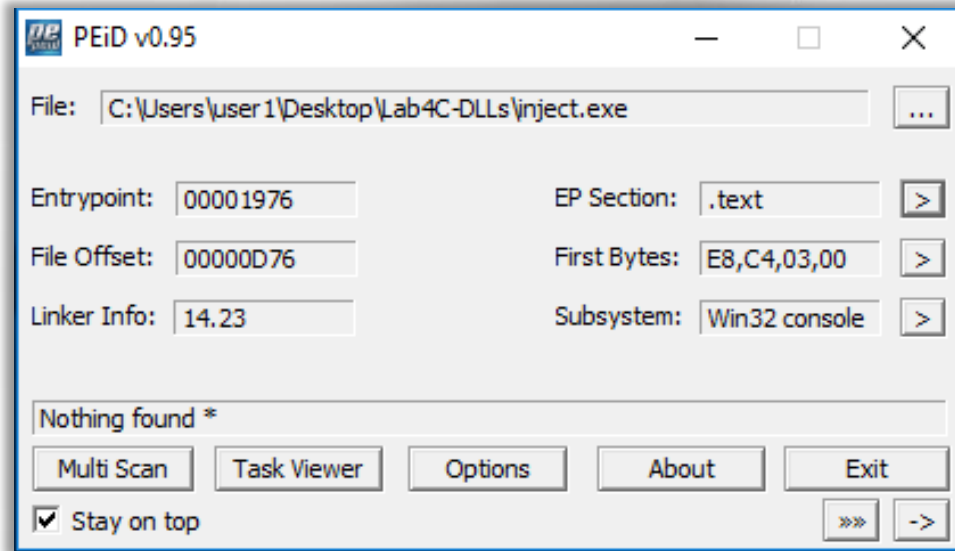
[Exeinfo PE](#) (latest version) or you can download an older version [here](#).



A1.4.2 Static Analysis Tools

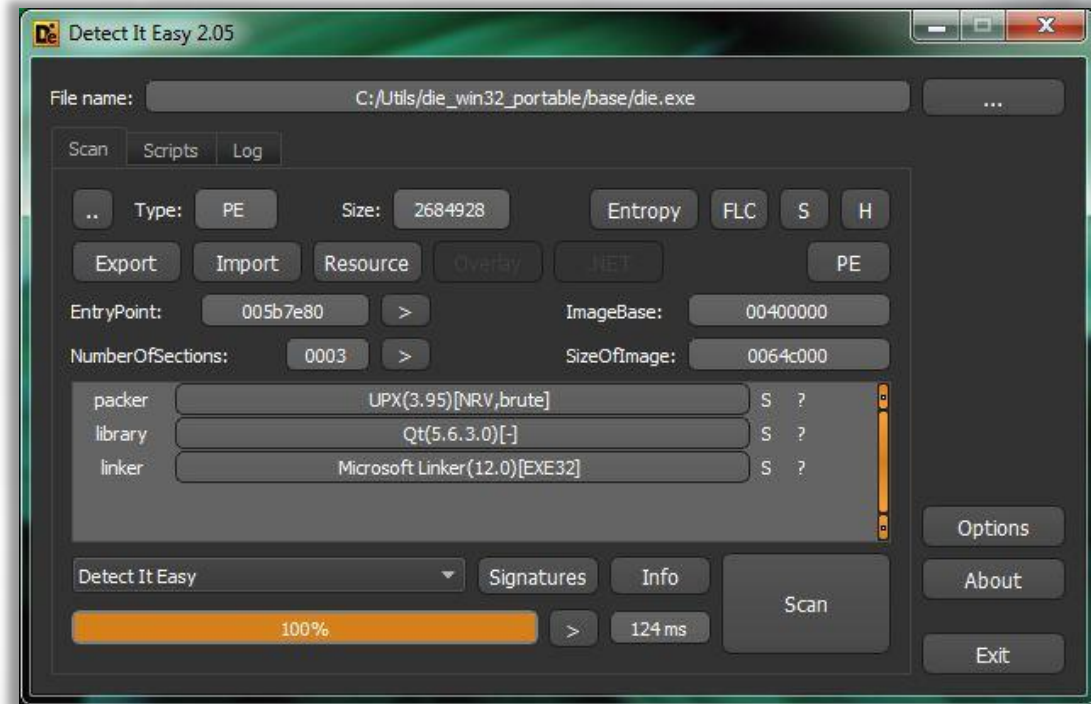


PEiD (password = tuts4you) + signatures



A1.4.2 Static Analysis Tools

Detect it Easy (DiE)



A1.4.2 Static Analysis Tools



CFF Explorer

The screenshot displays the CFF Explorer VII interface. The main window shows the file structure on the left, including sections like .text, .rdata, .data, and .rsrc. A table of sections is visible, listing Name, Virtual Size, Virtual Address, Raw Size, Raw Address, Reloc Address, Linenumbers, Relocations N., Linenumbers..., and Characteristics.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N.	Linenumbers ...	Characteristics
000001E8	000001F0	000001F4	000001F8	000001FC	00000200	00000204	00000208	0000020A	0000020C
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	001024B5	00001000	00103000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0004827A	00104000	0004C000	00104000	00000000	00000000	0000	0000	40000040
.data	000106E8	00150000	0000C000	00150000	00000000	00000000	0000	0000	C0000040
.rsrc	000A7E10	00161000	000A8000	0015C000	00000000	00000000	0000	0000	40000040

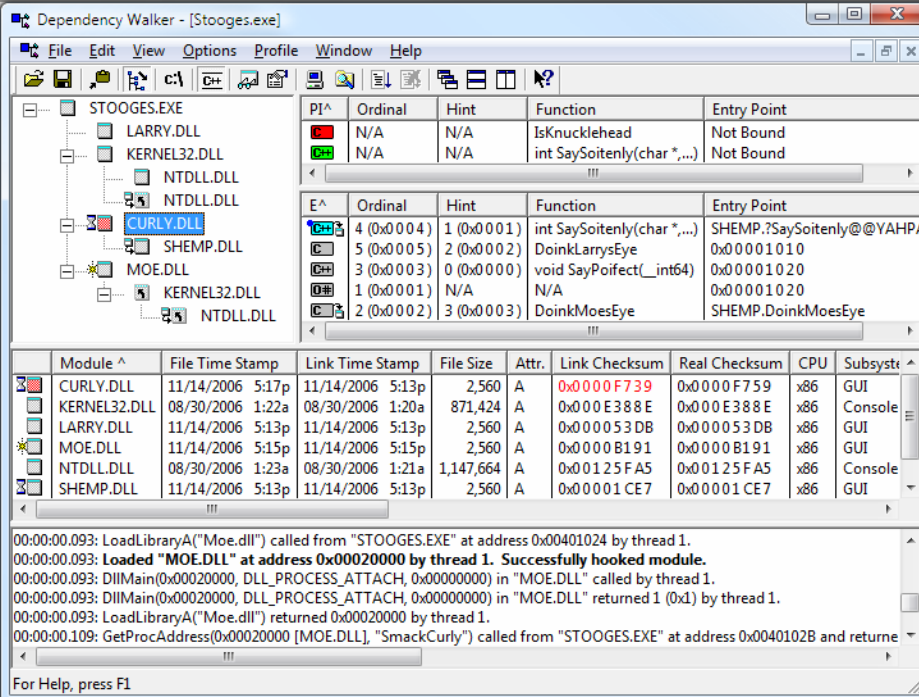
Below the table, the 'Section Headers' window is open, showing flags for the selected section. The 'Section Flags' window is also open, displaying a list of flags such as 'Is shareable', 'Is executable', 'Is readable', etc., with checkboxes.

The 'Quick Disassembler' window is open, showing disassembly parameters (Disassembler: x64, Base Address: 00000000, Offset: 1040, Size: DF) and a table of disassembly output.

Address	Opcode	Instruction
00000000	56	push rsi
00000001	8B F1	mov esi, ecx
00000003	E8 38 64 0B 00	call 0xb6440
00000008	83 F8 FF	cmp eax, -0x1
0000000B	75 06	jnz 0x13
0000000D	0B C0	or eax, eax
0000000F	5E	pop rsi
00000010	C2 04 00	ret 0x4

A1.4.2 Static Analysis Tools

Dependency Walker



The screenshot shows the Dependency Walker application window titled "Dependency Walker - [Stooges.exe]". The main window displays a dependency tree for the executable "STOOGES.EXE". The tree includes the following modules:

- STOOGES.EXE
 - LARRY.DLL
 - KERNEL32.DLL
 - NTDLL.DLL
 - CURLY.DLL (highlighted)
 - SHEMP.DLL
 - MOE.DLL
 - KERNEL32.DLL
 - NTDLL.DLL

The right-hand pane shows the details for the selected module, "CURLY.DLL". It contains two tables of function information:

PI^	Ordinal	Hint	Function	Entry Point
	N/A	N/A	IsKnucklehead	Not Bound
	N/A	N/A	int SaySoitenly(char *,...)	Not Bound

E^	Ordinal	Hint	Function	Entry Point
+	4 (0x0004)	1 (0x0001)	int SaySoitenly(char *,...)	SHEMP.?SaySoitenly@YAHP/
+	5 (0x0005)	2 (0x0002)	DoinkLarysEye	0x00001010
+	3 (0x0003)	0 (0x0000)	void SayPoifect(_int64)	0x00001020
+	1 (0x0001)	N/A	N/A	0x00001020
+	2 (0x0002)	3 (0x0003)	DoinkMoesEye	SHEMP.DoinkMoesEye

Below the function tables is a summary table of loaded modules:

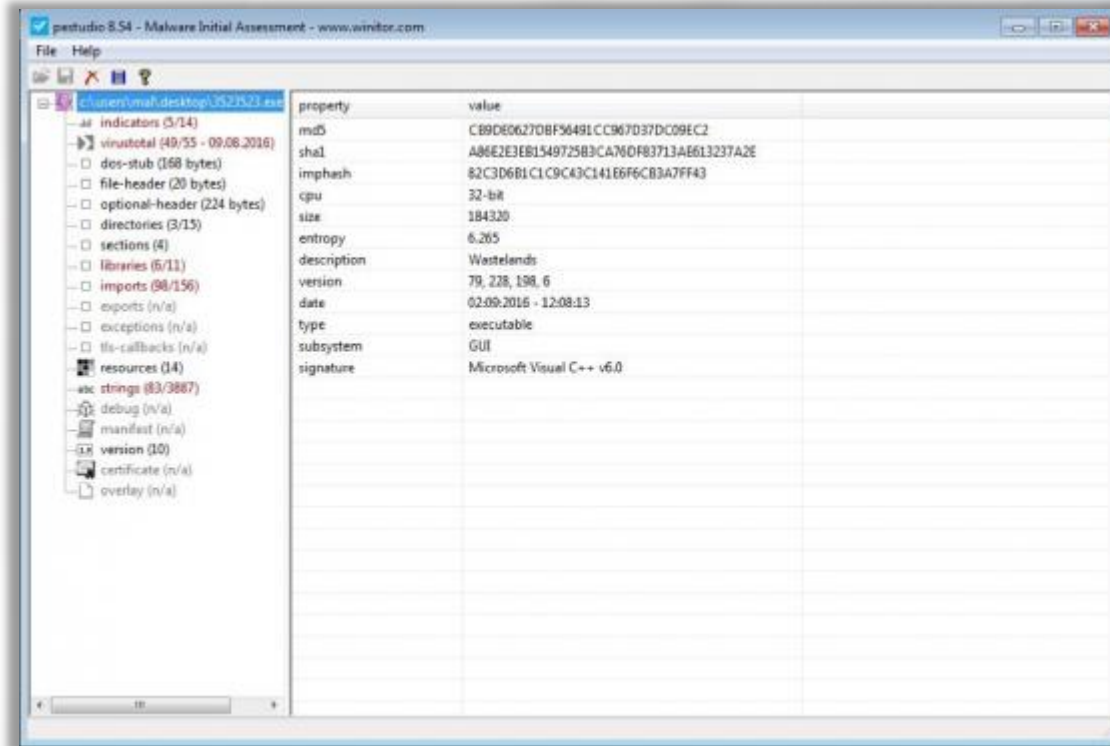
Module ^	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem
CURLY.DLL	11/14/2006 5:17p	11/14/2006 5:13p	2,560	A	0x0000F739	0x0000F759	x86	GUI
KERNEL32.DLL	08/30/2006 1:22a	08/30/2006 1:20a	871,424	A	0x000E388E	0x000E388E	x86	Console
LARRY.DLL	11/14/2006 5:13p	11/14/2006 5:13p	2,560	A	0x000053DB	0x000053DB	x86	GUI
MOE.DLL	11/14/2006 5:15p	11/14/2006 5:15p	2,560	A	0x0000B191	0x0000B191	x86	GUI
NTDLL.DLL	08/30/2006 1:23a	08/30/2006 1:21a	1,147,664	A	0x00125FA5	0x00125FA5	x86	Console
SHEMP.DLL	11/14/2006 5:13p	11/14/2006 5:13p	2,560	A	0x00001CE7	0x00001CE7	x86	GUI

The bottom pane shows a log of system events:

```
00:00:00.093: LoadLibraryA("Moe.dll") called from "STOOGES.EXE" at address 0x00401024 by thread 1.
00:00:00.093: Loaded "MOE.DLL" at address 0x00020000 by thread 1. Successfully hooked module.
00:00:00.093: DIIMain(0x00020000, DLL_PROCESS_ATTACH, 0x00000000) in "MOE.DLL" called by thread 1.
00:00:00.093: DIIMain(0x00020000, DLL_PROCESS_ATTACH, 0x00000000) in "MOE.DLL" returned 1 (0x1) by thread 1.
00:00:00.093: LoadLibraryA("Moe.dll") returned 0x00020000 by thread 1.
00:00:00.109: GetProcAddress(0x00020000 [MOE.DLL], "SmackCurly") called from "STOOGES.EXE" at address 0x0040102B and returne
```

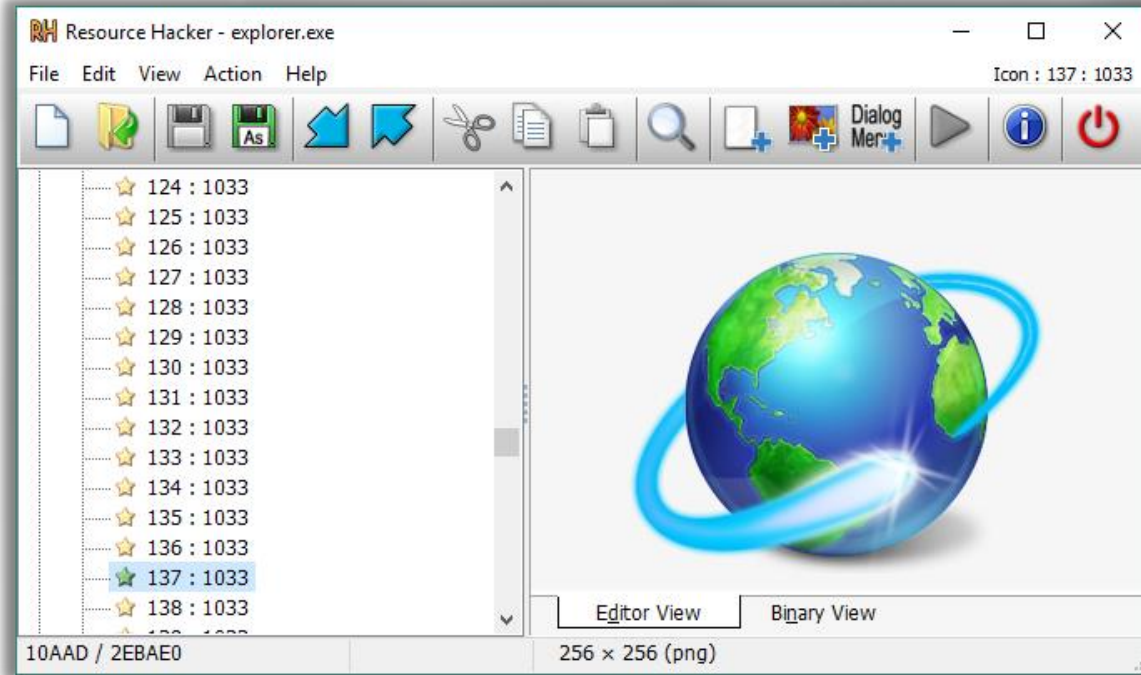
A1.4.2 Static Analysis Tools

PE Studio



A1.4.2 Static Analysis Tools

Resource Hacker



A1.4.2 Static Analysis Tools

Additional Static Analysis tools include:

- [TitanMist](#)
- [ASPack](#) (trail)
- Reflective PE Packer: [Amber](#)

A1.4.3 Dynamic Analysis Tools

Microsoft SysInternals Suite Process Explorer

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	96.14	0 K	8 K	0		
System	0.23	136 K	14,048 K	4		
smss.exe	0.83	0 K	0 K	n/a	Hardware Interrupts and DPCs	
csrss.exe		236 K	780 K	264		
csrss.exe		812 K	3,232 K	360		
wininit.exe		740 K	3,684 K	436		
csrss.exe	0.05	896 K	4,440 K	444		
winlogon.exe		1,508 K	7,480 K	560		
dwm.exe	0.13	62,800 K	64,548 K	800		
explorer.exe	1.11	38,028 K	79,564 K	2844	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.06	5,952 K	12,608 K	5340	VMware Tools Core Service	VMware, Inc.
OneDrive.exe	0.01	11,884 K	30,456 K	5376	Microsoft OneDrive	Microsoft Corporation
procexp.exe	1.29	16,504 K	24,708 K	5668	Sysinternals Process Explorer	Sysinternals - www.sysinter...

Name	Description	Company Name	Path
glib-2.0.dll	GLib	The GLib developer comm...	C:\Program Files\VMware\VMware Tools\glib-2.0.dll
glibmm-2.4.dll	The official C++ wrapper for glib	The glibmm development t...	C:\Program Files\VMware\VMware Tools\glibmm-2.4.dll
gmodule-2.0.dll	GModule	The GLib developer comm...	C:\Program Files\VMware\VMware Tools\gmodule-2.0.dll
gobject-2.0.dll	GObject	The GLib developer comm...	C:\Program Files\VMware\VMware Tools\gobject-2.0.dll
hgfs.dll	VMware Tools HGFS Library	VMware, Inc.	C:\Program Files\VMware\VMware Tools\hgfs.dll
iconv.dll	LGPLed libiconv for Windows NT/...	Free Software Foundation	C:\Program Files\VMware\VMware Tools\iconv.dll
icudt44.dat			C:\Program Files\VMware\VMware Tools\icudt44.dat
intl.dll	LGPLed libintl for Windows NT/20...	Free Software Foundation	C:\Program Files\VMware\VMware Tools\intl.dll
pcr.dll	Perl Compatible Regular Expressio...	VMware	C:\Program Files\VMware\VMware Tools\pcr.dll
hgfsServer.dll	VMware Tools HGFS Server plugin	VMware, Inc.	C:\Program Files\VMware\VMware Tools\plugins\common\...
hgfsUsability.dll	VMware Tools HGFS Usability plugin	VMware, Inc.	C:\Program Files\VMware\VMware Tools\plugins\common\...
vix.dll	VMware Tools VIX plugin	VMware, Inc.	C:\Program Files\VMware\VMware Tools\plugins\vmusd\...
desktopEvents.dll	VMware Tools Desktop Events plu...	VMware, Inc.	C:\Program Files\VMware\VMware Tools\plugins\vmusd\de...
dnDop.dll	VMware Tools DnD Copy/Paste plu...	VMware, Inc.	C:\Program Files\VMware\VMware Tools\plugins\vmusd\dn...
unity.dll	VMware Tools DnD Unity plugin	VMware, Inc.	C:\Program Files\VMware\VMware Tools\plugins\vmusd\uni...

CPU Usage: 3.86% Commit Charge: 17.13% Processes: 47 Physical Usage: 24.11%

A1.4.3 Dynamic Analysis Tools



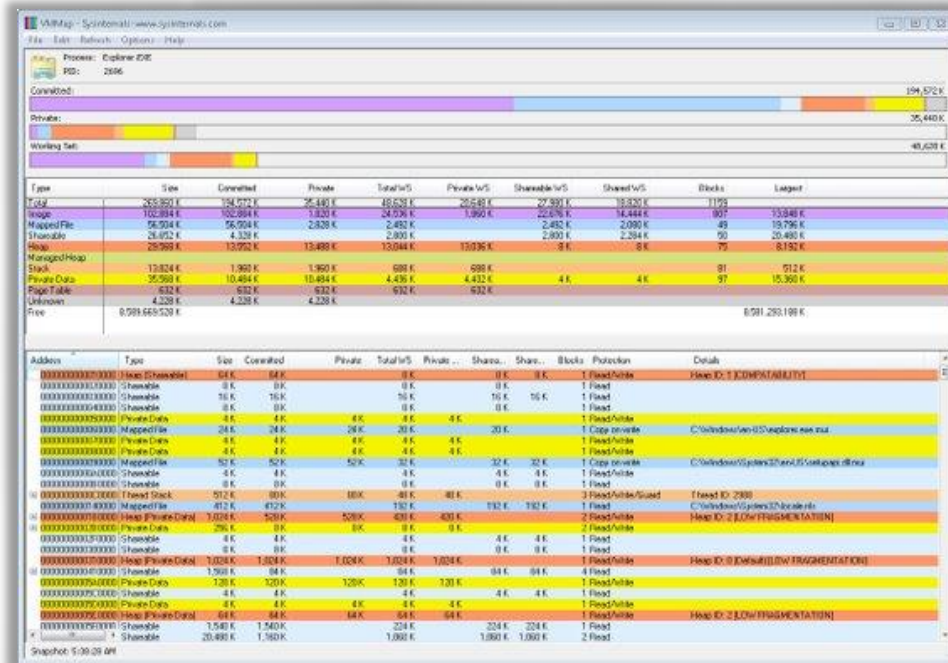
Microsoft [SysInternals](https://www.sysinternals.com) Suite Process Monitor

Time ...	Process Name	PID	Operation	Path	Result	Detail
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCR\Folder\ShellEx\IconHandler	NAME NOT FOUND	Desired Access: Q...
12:02:...	Explorer.EXE	2844	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCU\Software\Classes\AllFilesystemO...	NAME NOT FOUND	Desired Access: R...
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCR\AllFilesystemObjects	SUCCESS	Desired Access: R...
12:02:...	Explorer.EXE	2844	RegQueryKey	HKCR\AllFilesystemObjects	SUCCESS	Query: Name
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCU\Software\Classes\AllFilesystemO...	NAME NOT FOUND	Desired Access: Q...
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCR\AllFilesystemObjects\ShellEx\Ico...	NAME NOT FOUND	Desired Access: Q...
12:02:...	Explorer.EXE	2844	RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS	Query: Name
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCR\Directory	SUCCESS	Desired Access: M...
12:02:...	Explorer.EXE	2844	RegQueryValue	HKCU\Software\Classes\Directory\Doc...	NAME NOT FOUND	Length: 144
12:02:...	Explorer.EXE	2844	RegQueryValue	HKCR\Directory\DocObject	NAME NOT FOUND	Length: 144
12:02:...	Explorer.EXE	2844	RegCloseKey	HKCR\Directory	SUCCESS	
12:02:...	Explorer.EXE	2844	RegQueryKey	HKCU\Software\Classes\Directory	SUCCESS	Query: Name
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCU\Software\Classes\Directory\Doc...	NAME NOT FOUND	Desired Access: Q...
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCR\Directory\DocObject	NAME NOT FOUND	Desired Access: Q...
12:02:...	Explorer.EXE	2844	RegQueryKey	HKCR\Folder	SUCCESS	Query: Name
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCU\Software\Classes\Folder	NAME NOT FOUND	Desired Access: M...
12:02:...	Explorer.EXE	2844	RegQueryValue	HKCR\Folder\DocObject	NAME NOT FOUND	Length: 144
12:02:...	Explorer.EXE	2844	RegQueryKey	HKCR\Folder	SUCCESS	Query: Name
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCU\Software\Classes\Folder\DocOb...	NAME NOT FOUND	Desired Access: Q...
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCR\Folder\DocObject	NAME NOT FOUND	Desired Access: Q...
12:02:...	Explorer.EXE	2844	RegQueryKey	HKCR\AllFilesystemObjects	SUCCESS	Query: Name
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCU\Software\Classes\AllFilesystemO...	NAME NOT FOUND	Desired Access: M...
12:02:...	Explorer.EXE	2844	RegQueryValue	HKCR\AllFilesystemObjects\DocObject	NAME NOT FOUND	Length: 144
12:02:...	Explorer.EXE	2844	RegQueryKey	HKCR\AllFilesystemObjects	SUCCESS	Query: Name
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCU\Software\Classes\AllFilesystemO...	NAME NOT FOUND	Desired Access: Q...
12:02:...	Explorer.EXE	2844	RegOpenKey	HKCR\AllFilesystemObjects\DocObject	NAME NOT FOUND	Desired Access: Q...

Showing 24,761 of 109,183 events (22%) Backed by virtual memory

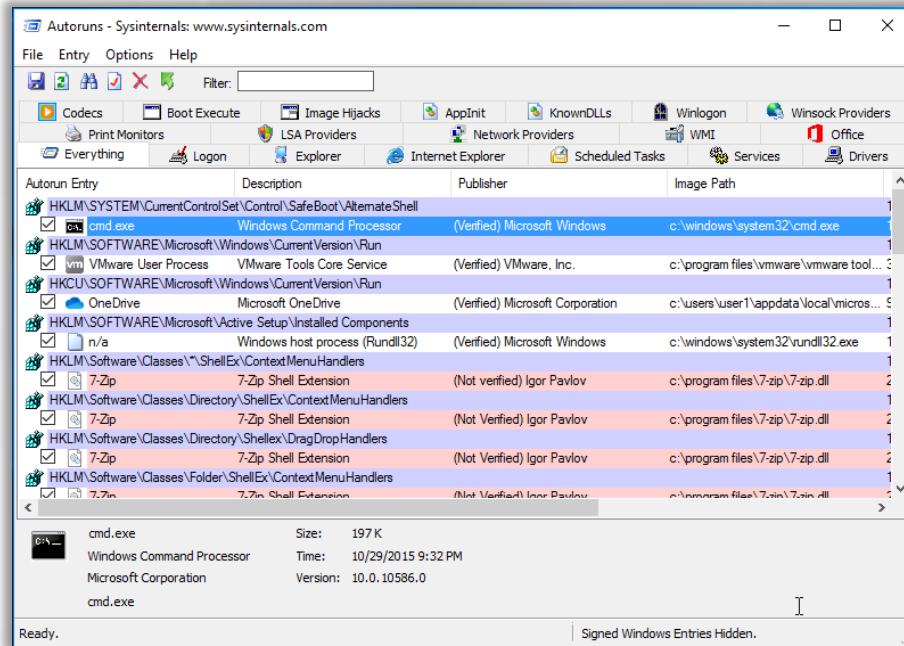
A1.4.3 Dynamic Analysis Tools

Microsoft SysInternals Suite VMMMap



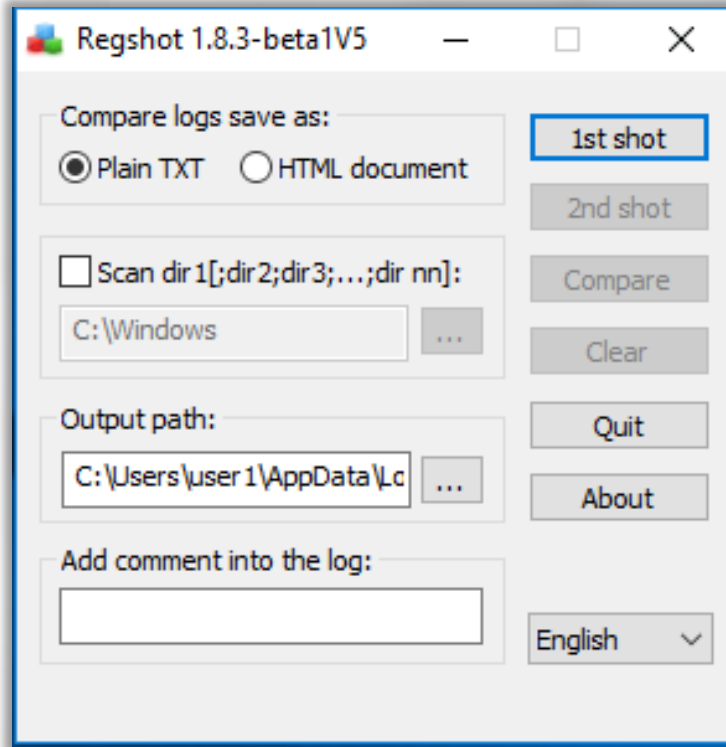
A1.4.3 Dynamic Analysis Tools

Microsoft SysInternals Suite Autoruns



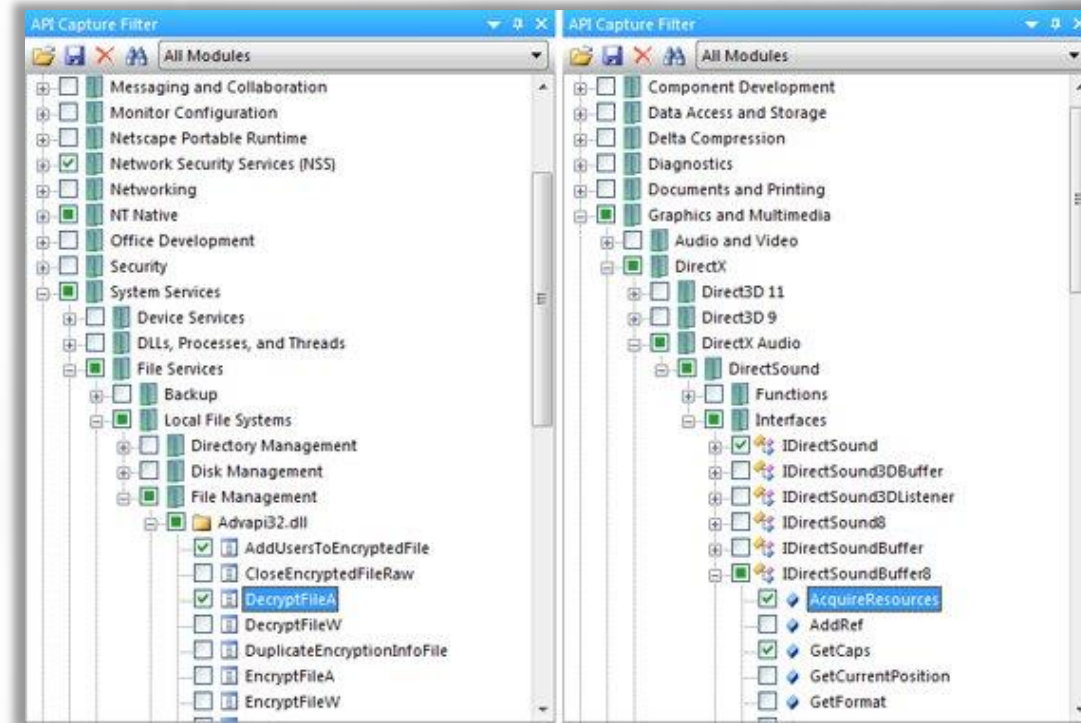
A1.4.3 Dynamic Analysis Tools

RegShot



A1.4.3 Dynamic Analysis Tools

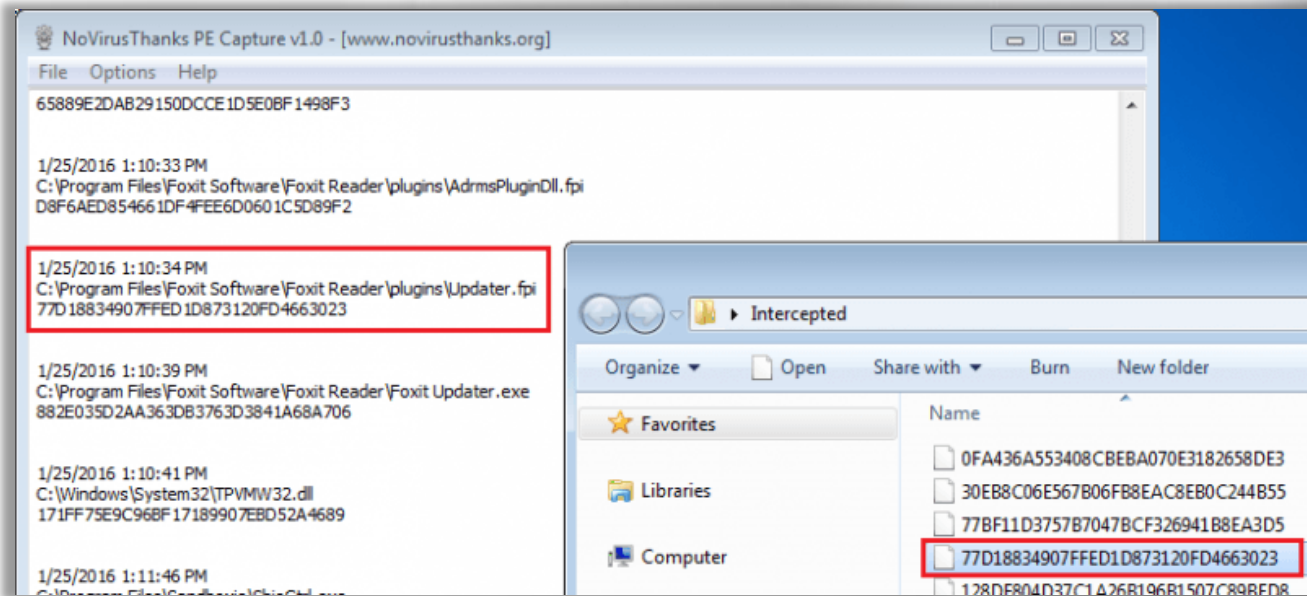
API Monitor



A1.4.3 Dynamic Analysis Tools



PE Capture



A1.4.3 Dynamic Analysis Tools

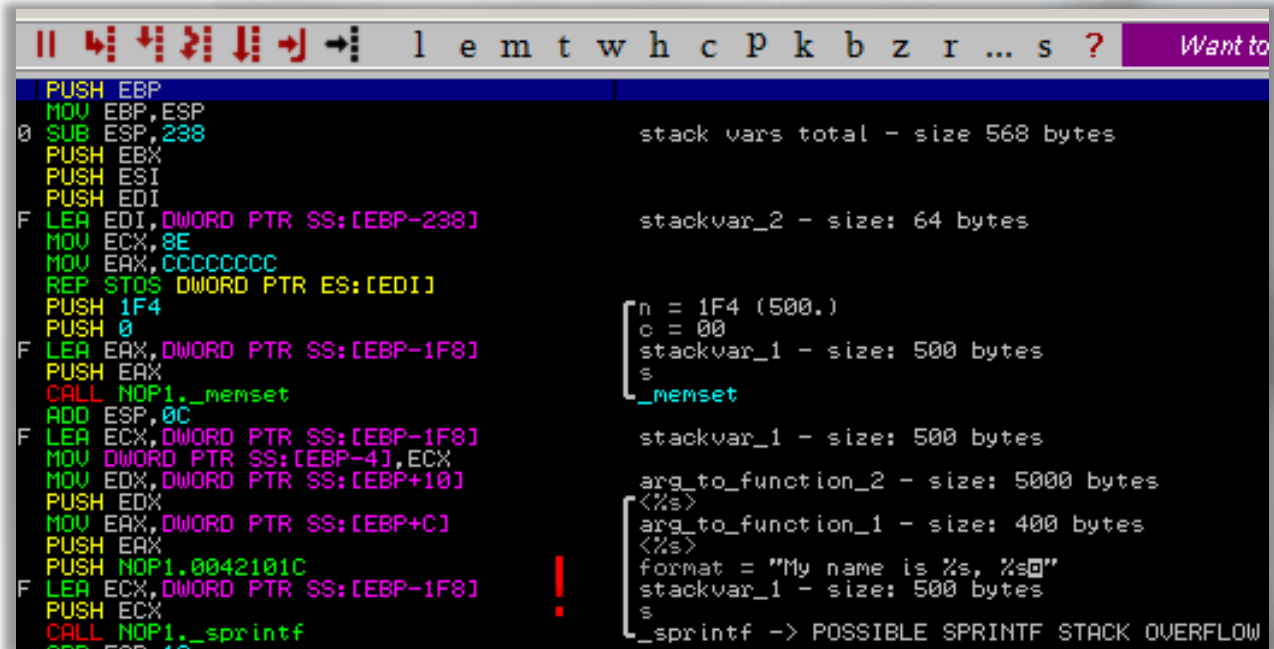


X64dbg

The screenshot displays the X64dbg debugger interface. The main window shows assembly code for a function named 'entry' at address 00000013FA01E0C0. The code includes instructions like 'pop esi', 'sub rsp, 20', 'mov eax, crackme64.13FA01E44', 'add esp, 18', 'jmp crackme64.13FA01E030', and various 'mov' and 'xor' instructions. The registers window on the right shows the 'rax' register containing the address 00000013FA01E0B8. The memory dump window at the bottom shows the memory address 0000000077551000 containing the ASCII string 'return to kernel! 0000000000000000'. The command window at the bottom shows the command 'F5: [INT3 breakpoint "entry breakpoint" at 0000000013FA01E0B8]'. The title bar of the window reads 'x64_dbg - File Crackme64.exe - 7FD:1A04 - Module crackme64.exe - Thread D74'.

A1.4.3 Dynamic Analysis Tools

Immunity Debugger



The screenshot displays the assembly view in Immunity Debugger. The assembly code on the left includes instructions like `PUSH EBP`, `MOV EBP, ESP`, `SUB ESP, 238`, `PUSH EBX`, `PUSH ESI`, `PUSH EDI`, `LEA EDI, DWORD PTR SS:[EBP-238]`, `MOV ECX, 8E`, `MOV EAX, CCCCCCCC`, `REP STOS DWORD PTR ES:[EDI]`, `PUSH 1F4`, `PUSH 0`, `LEA EAX, DWORD PTR SS:[EBP-1F8]`, `PUSH EAX`, `CALL NOP1._memset`, `ADD ESP, 0C`, `LEA ECX, DWORD PTR SS:[EBP-1F8]`, `MOV DWORD PTR SS:[EBP-4], ECX`, `MOV EDX, DWORD PTR SS:[EBP+10]`, `PUSH EDX`, `MOV EAX, DWORD PTR SS:[EBP+C]`, `PUSH EAX`, `PUSH NOP1.0042101C`, `LEA ECX, DWORD PTR SS:[EBP-1F8]`, `PUSH ECX`, and `CALL NOP1._sprintf`. The stack variables on the right include `stack vars total - size 568 bytes`, `stackvar_2 - size: 64 bytes`, `stackvar_1 - size: 500 bytes`, `arg_to_function_2 - size: 5000 bytes`, `arg_to_function_1 - size: 400 bytes`, and `format = "My name is %s, %s"`. A red exclamation mark is present next to the `CALL NOP1._sprintf` instruction, and a warning message at the bottom right reads `! _sprintf -> POSSIBLE SPRINTF STACK OVERFLOW`.

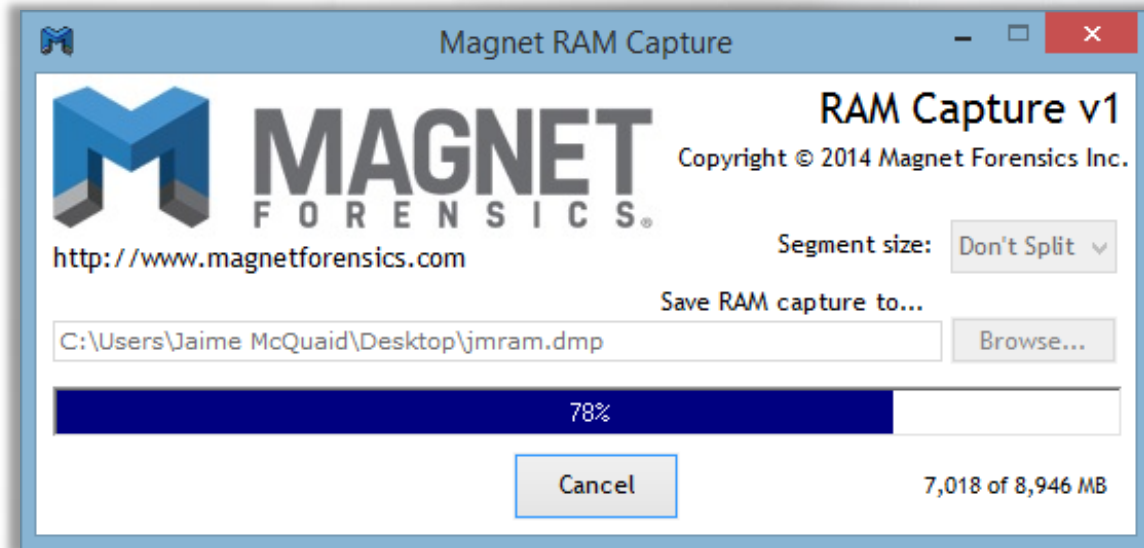
A1.4.3 Dynamic Analysis Tools

Additional Dynamic Analysis tools include:

- [Noriben](#)
- Rundll32 (LOLBin)
- Injector ([Reflective DLL Injection](#))
- [Ghidra](#)

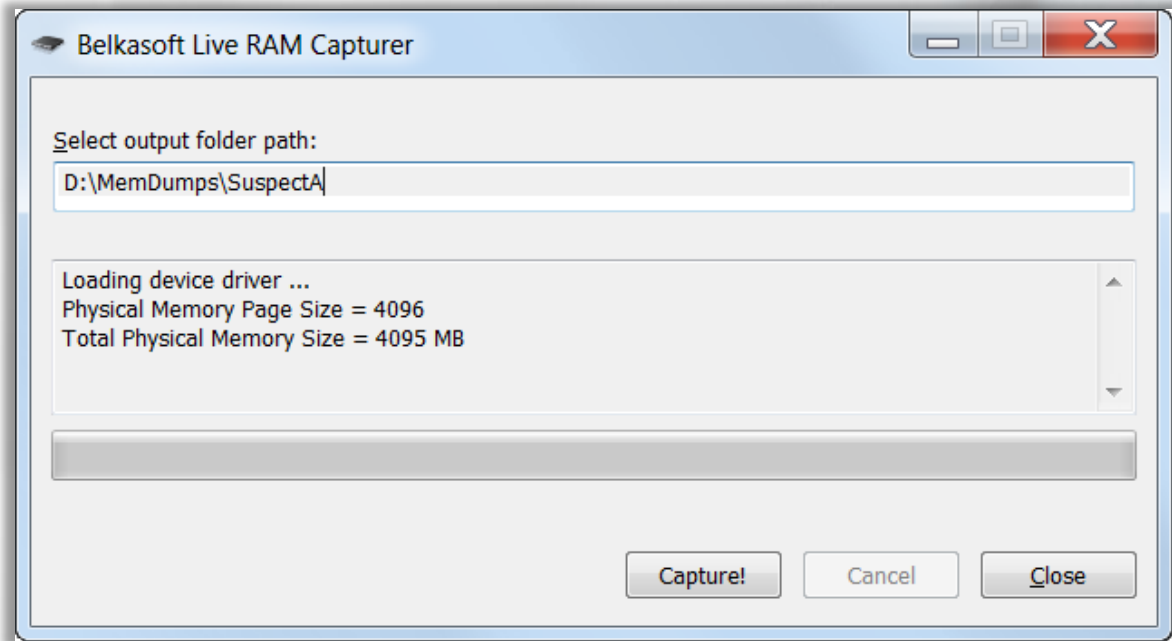
A1.4.4 Memory Forensics Tools

MagnetForensics RAM Capture



A1.4.4 Memory Forensics Tools

Belkasoft Live RAM Capture



A1.4.4 Memory Forensics Tools

Additional Memory Forensics tools include:

- Comae [DumpIt](#)
- Nirsoft [Memdump](#)
- Mandiant [Redline](#)

A1.4.4 Memory Forensics Tools

Additional Memory Forensics tools include (cont.):

- Rekal [WinPmem](#)
- [Volatility3](#), [Volatility](#) 2.6.x, [Plugins](#), etc.
 - [MalHunt](#), [AutoTimeliner](#), etc.
- [Rekal](#)

A1.4.5 Incident Response Tools

Mandiant IOC Editor

Name:	SVCHOST.EXE	T..	R..
Author:			
GUID:	658a4993-d53b-4a95-aeaa-93f0e020f		
Description:	Initial indicator of compromise for "svchost.exe" downloader		
Add:	Definition:		
<input type="button" value="Item"/>	<input type="checkbox"/> OR		
<input type="button" value="AND"/>	<input type="checkbox"/> AND	Process Name contains svchost.exe	
<input type="button" value="OR"/>		Process arguments contains not -k	
	<input type="checkbox"/> AND	File Name contains svchost.exe	
	<input type="checkbox"/> OR	File Full Path contains not system32	
		File Digital Signature Verified contains False	

A1.4.5 Incident Response Tools

GRR and Velociraptor

Velociraptor | C:388fd98a6f26e7 x +

Not secure | <https://localhost:8889/app.html#/clients/C:388fd98a6f26e7/vfs//ntfs/%255C%255C.%255C%253A/?tab=hexview>

Search Box | Velocidex-01 connected | 0 nick

file explorer: ntfs > \\.IC > \$MFT

File Name	Size	Permissions	Created	Modified	Accessed
\$Bitmap	3261744	-rwxr-xr-x	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z
\$Boot	8192	-rwxr-xr-x	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z
\$Extend	656	drwxr-xr-x	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z
\$LogFile	67108864	-rwxr-xr-x	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z
\$MFT	391643136	-rwxr-xr-x	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z
\$MFTMirr	4096	-rwxr-xr-x	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z
\$Recycle.Bin	56	drwxr-xr-x	2017-02-03T03:16:59Z	2017-02-03T03:16:59Z	2017-02-03T03:16:59Z
\$Secure.SSDH	112	drwxr-xr-x	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z	2017-02-03T03:16:54Z

> ntfs > \\.IC > \$MFT

Stats | **TextView** | HexView | CSVView | Reports

First | Previous | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... | Next | Last

```
Offset 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13
0x00000000 46 49 4c 45 30 00 03 00 3a 2c 59 fd 02 00 00 00 01 00 01 00 FILE0...Y.....
0x00000014 38 00 01 00 fd 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 8.....
0x00000028 07 00 00 00 00 00 00 00 fd 02 00 00 00 00 00 10 00 00 00 .....
0x0000003c fd 4c 12 fd fd 01 fd 4c 12 fd fd 01 fd 4c 12 fd fd 01 fd 4c 12 fd .....
0x00000054 fd 7d fd 01 fd 4c 12 fd fd 7d fd 01 06 00 00 00 00 00 00 .....
0x00000078 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 .....
0x0000008c 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 .....
0x000000a0 00 18 00 00 00 03 00 4a 00 00 00 18 00 01 00 05 00 00 00 .....
0x000000b4 00 00 05 00 fd 4c 12 fd fd 7d fd 01 fd 4c 12 fd fd 7d fd 01 .....
0x000000c8 fd 4c 12 fd fd 7d fd 01 fd 4c 12 fd fd 7d fd 01 00 40 00 00 .....
0x000000dc 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00 .....8.....
```

2019-07-23 09:30:40 UTC

A1.4.5 Incident Response Tools

Additional Incident Response tools include:

- The Yara Family:
 - [Yara](#), [Rules](#), [Yara-Merger](#), [Yara-Endpoint](#), etc.
- [Loki](#) Scanner
- Facebook [OSQuery](#)
- [ClamAV](#)

A1.4.6 Network Tools

Fiddler

The screenshot displays the Fiddler Web Debugger interface. The main window shows a list of web sessions with columns for #, Result, Protocol, Host, and URL. The right-hand pane is open to the 'Request Headers' view for a selected session.

#	Result	Protocol	Host	URL
1	200	HTTP	www.fiddler2.com	/fiddler2/updatecheck.as
2	302	HTTP	download.mozilla.org	/?product=firefox-19.0.2
3	200	HTTP	download.cdn.mozill...	/pub/mozilla.org/firefox/r
4	200	HTTP	fiddler2.com	/fiddler2/
5	200	HTTP	fiddler2.com	/Fiddler2/Fiddler.css
6	200	HTTP	www.google-analyti...	/ga.js
7	200	HTTP	fiddler2.com	/Fiddler/images/FiddlerLo
8	200	HTTP	fiddler2.com	/fiddler2/images/bookcov
9	200	HTTP	fiddler2.com	/Eric/images/rss.gif
10	200	HTTP	fiddler2.com	/images/dl-sm.png
11	200	HTTP	fiddler2.com	/fiddler2/images/tbanner
12	200	HTTP	fiddler2.com	/fiddler/images/fiddlericon
13	200	HTTP	www.google-analyti...	/__utm.gif?utmwv=5.3.9

Request Headers
GET /fiddler2/updatecheck.asp?isBeta=False HT
Cache
Pragma: no-cache
Client
Accept-Language: en-US
User-Agent: Fiddler/2.4.2.6 (.NET 2.0.50727)
Miscellaneous
Referer: http://fiddler2.com/client/2.4.2.6

A1.4.6 Network Tools

[Xplico](https://www.xplico.org/)

The screenshot displays the Xplico web interface. At the top left, it says "Xplico Interface" and "User: deft". There are "Help" and "Logout" links. A sidebar on the left contains navigation options: Cases, Sols, Email, Sip, Web, Images, Printer, Ftp, Mms, and GeoMap. The main content area is divided into several sections:

- Session Data:** Case name: case 2, Session Name: day 2, Start Time: 0000-00-00 00:00:00, End Time: 0000-00-00 00:00:00, Status: EMPTY.
- Pcap set:** A section for adding and managing PCAP files, including a "Browse..." button and an "Upload" button.
- Related HTTP:** Post: 0, Get: 0, Video: 0, Images: 0.
- Related MMS:** Number: 0, Contents: 0, Video: 0, Images: 0.
- Related SIP:** Calls: 0.
- Related RTP/VoIP:** (Empty section)
- Related Emails:** Received: 0, Sent: 0, Unread: 0/0.
- Related FTP:** Connections: 0, Downloaded: 0, Uploaded: 0.
- Related NNTP:** (Empty section)
- Related IRC:** (Empty section)
- Related Printed files:** Pdf: 0.

At the bottom, there is a footer with "Xplico.org", "CakePHP POWER", "Version: 0.5", and "© 2007-2009 Gianluca Costa & Andrea de Franceschi. All Rights Reserved."

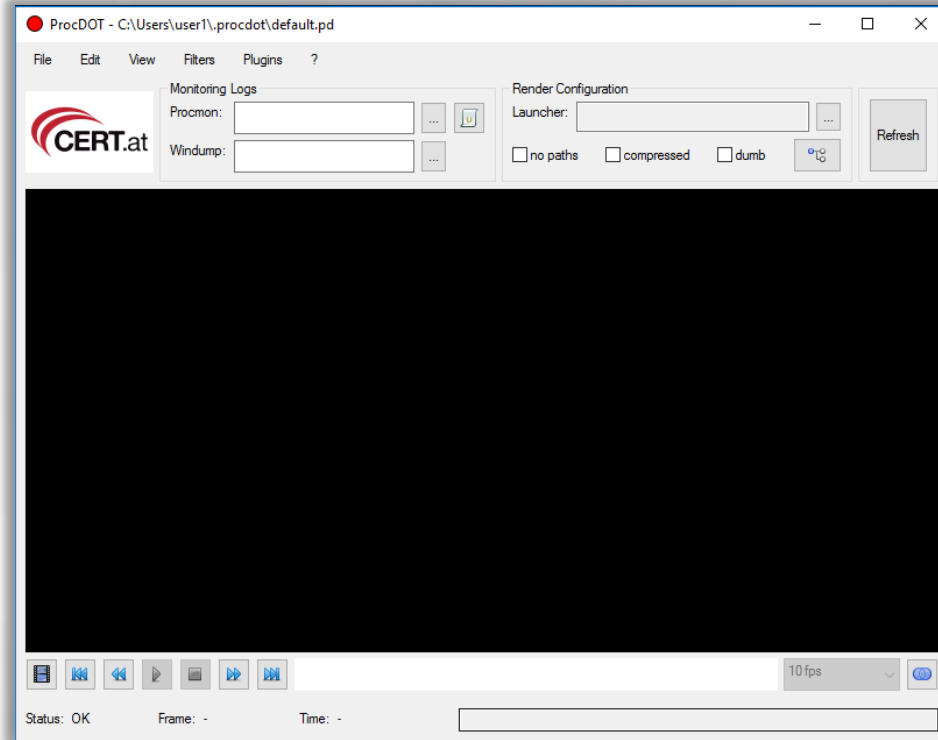
A1.4.6 Network Tools

Additional Network tools include:

- Mandiant [AptDNS](#)
- [WinDump](#)
- [CaptureBAT](#)
- [NetworkMiner](#)
- [PassiveDNS](#)
- [Stenographer](#)

A1.4.7 Visualization Tools

[ProcDOT](#) or
[here](#)

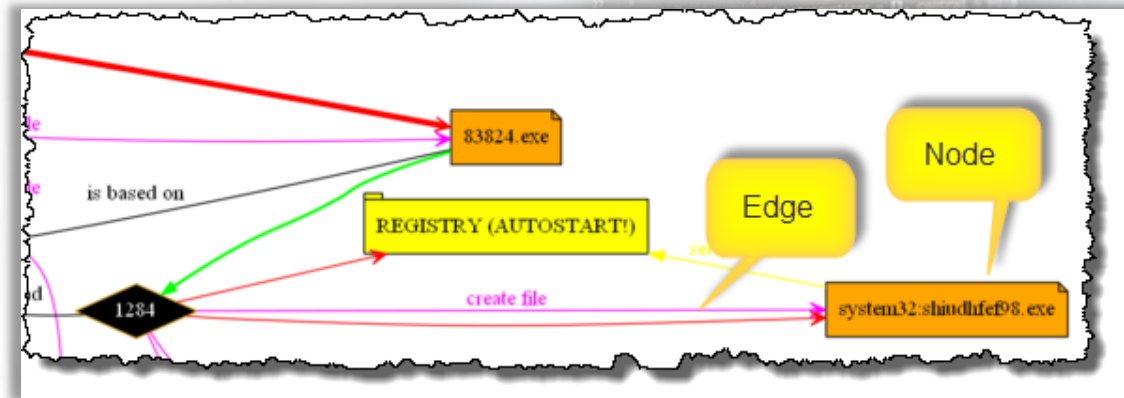


A1.4.7 Visualization Tools



Additional Visualization tools include:

- [XDot](#)
- [Graphviz](#)



A1.4.8 Framework Tools

The main Framework tool is [Viper](https://viper.li/en/latest/).



The background of the slide features a blurred image of a laptop screen displaying code. The code is in a light color against a dark background, showing various function definitions and calls. The Viper logo is prominently displayed in the center of the screen, rendered in a bold, black, stylized font.



References



References

Here's a list of all references linked or used in this course.

[Awesome Malware Analysis](#)

<https://github.com/rshipp/awesome-malware-analysis>

[Malware Analysis List of Useful Stuff](#)

<https://github.com/P3t3rp4rk3r/Malware-Analysis>

[Security Onion](#)

<https://securityonion.net/>

[Tsurugi Linux](#)

<https://tsurugi-linux.org/downloads.php>

[Windows 10](#)

<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>



References

[VMWare](https://www.vmware.com/products/workstation-pro.html)

<https://www.vmware.com/products/workstation-pro.html>

[VirtualBox](https://www.virtualbox.org/)

<https://www.virtualbox.org/>

[Exiftool](https://www.sno.phy.queensu.ca/~phil/exiftool/)

<https://www.sno.phy.queensu.ca/~phil/exiftool/>

[HxD Hex Editor](https://mh-nexus.de/en/hxd/)

<https://mh-nexus.de/en/hxd/>

[Free Hex Editor Neo](https://www.hhdsoftware.com/free-hex-editor)

<https://www.hhdsoftware.com/free-hex-editor>

[bstrings](https://ericzimmerman.github.io/#.index.md)

<https://ericzimmerman.github.io/#.index.md>

Click [HERE](#) to return to slide 22

<https://t.me/learningnets> | **NETS 1: Section 01, Module 01, Appendix A - Caendra Inc. © 2020 | p.57**



References

[Bin Text](#)

<http://b2b-download.mcafee.com/products/tools/foundstone/bintext303.zip>

[StringSifter](#)

<https://www.fireeye.com/blog/threat-research/2019/09/open-sourcing-stringsifter.html>

[Exeinfo PE \(latest version\)](#)

<http://www.exeinfo.xn.pl/>

[ExeinfoPE \(older version\)](#)

<https://tuts4you.com/download/3565/>

[PEiD](#)

https://tuts4you.com/e107_plugins/download/download.php?view.398

[signatures](#)

<https://github.com/wolfram77web/app-peid>

Click [HERE](#) to return to slide 22

<https://t.me/learningnets> | **NETS 1: Section 01, Module 01, Appendix A - Caendra Inc. © 2020 | p.58**



References

[Detect it Easy \(DiE\)](http://ntinfo.biz/index.html)

<http://ntinfo.biz/index.html>

[CFF Explorer](https://ntcore.com/?page_id=388)

https://ntcore.com/?page_id=388

[Dependency Walker](http://dependencywalker.com/)

<http://dependencywalker.com/>

[PE Studio](https://winitor.com/)

<https://winitor.com/>

[Resource Hacker](http://angusj.com/resourcehacker/)

<http://angusj.com/resourcehacker/>

[TitanMist](https://www.reversinglabs.com/open-source/titanmist)

<https://www.reversinglabs.com/open-source/titanmist>

Click [HERE](#) to return to slide 30

<https://t.me/learningnets> | **NETS 1: Section 01, Module 01, Appendix A - Caendra Inc. © 2020 | p.59**



References

[ASPack \(trail\)](#)

<http://www.aspack.com/downloads.html>

[Reflective PE Packer: Amber](#)

<https://github.com/EgeBalci/Amber>

[Microsoft SysInternals Suite](#)

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

[RegShot](#)

<https://sourceforge.net/projects/regshot/>

[API Monitor](#)

<http://www.rohitab.com/apimonitor#Download>

[PE Capture](#)

<https://www.novirusthanks.org/products/pe-capture/>

Click [HERE](#) to return to slide 30



References

[X64dbg](https://x64dbg.com/#start)

<https://x64dbg.com/#start>

[Immunity Debugger](https://www.immunityinc.com/products/debugger/)

<https://www.immunityinc.com/products/debugger/>

[IDA Pro](https://www.hex-rays.com/products/ida/)

<https://www.hex-rays.com/products/ida/>

[Noriben](https://github.com/Rurik/Noriben)

<https://github.com/Rurik/Noriben>

[Injector \(Reflective DLL Injection\)](https://github.com/stephenfewer/ReflectiveDLLInjection)

<https://github.com/stephenfewer/ReflectiveDLLInjection>

[Ghidra](https://www.ghidra-sre.org/)

<https://www.ghidra-sre.org/>

Click [HERE](#) to return to slide 41



References

[MagnetForensics RAM Capture](https://www.magnetforensics.com/resources/magnet-ram-capture/)

<https://www.magnetforensics.com/resources/magnet-ram-capture/>

[Belkasoft Live RAP Capture](https://belkasoft.com/ram-capturer)

<https://belkasoft.com/ram-capturer>

[Comae DumpIt](https://www.comae.com/dumpit/)

<https://www.comae.com/dumpit/>

[Nirsoft Memedump](https://nircmd.nirsoft.net/memdump.html)

<https://nircmd.nirsoft.net/memdump.html>

[Rekall WimPmem](https://rekall.readthedocs.io/en/gh-pages/Tools/pmem.html)

<https://rekall.readthedocs.io/en/gh-pages/Tools/pmem.html>

[Mandiant Redline](https://www.fireeye.com/services/freeware/redline.html)

<https://www.fireeye.com/services/freeware/redline.html>

Click [HERE](#) to return to slide 44.
Click [HERE](#) to return to slide 45.



References

[Volatility 3](https://github.com/volatilityfoundation/volatility3/)

<https://github.com/volatilityfoundation/volatility3/>

[Volatility 2.6.x](https://github.com/volatilityfoundation/volatility)

<https://github.com/volatilityfoundation/volatility>

[Volatility Plugins](https://github.com/volatilityfoundation)

<https://github.com/volatilityfoundation>

[MalHunt](https://github.com/andreafortuna/malhunt)

<https://github.com/andreafortuna/malhunt>

[AutoTimeliner](https://github.com/andreafortuna/autotimeliner)

<https://github.com/andreafortuna/autotimeliner>

[Rekall](http://www.rekall-forensic.com/)

<http://www.rekall-forensic.com/>

Click [HERE](#) to return to slide 45

<https://t.me/learningnets> | **ENPS 1: Section 01, Module 01, Appendix A - Caendra Inc. © 2020 | p.63**



References

[Mandiant IOC Editor](#)

<https://www.fireeye.com/services/freeware/ioc-editor.html>

[GRR](#)

<https://github.com/google/grr>

[Velociraptor](#)

<https://github.com/Velocidex/velociraptor>

[Yara](#)

<http://virustotal.github.io/yara/>

[Yara Rules](#)

<https://github.com/Yara-Rules>

[Yara-Merger](#)

https://github.com/lsoumille/Yara_Merger

Click [HERE](#) to return to slide 48



References

[Yara-Endpoint](https://github.com/Yara-Rules/yara-endpoint)

<https://github.com/Yara-Rules/yara-endpoint>

[Loki Scanner](https://github.com/Neo23x0/Loki)

<https://github.com/Neo23x0/Loki>

[Facebook OSQuery](https://osquery.io/)

<https://osquery.io/>

[ClamAV](https://www.clamav.net/)

<https://www.clamav.net/>

[Fiddler](https://www.telerik.com/fiddler)

<https://www.telerik.com/fiddler>

[Xplico](https://www.xplico.org/)

<https://www.xplico.org/>

Click [HERE](#) to return to slide 48



References

[Mandiant AptDNS](#)

<https://www.mandiant.com/assets/ApateDNS.zip>

[WinDump](#)

<https://www.winpcap.org/windump/install/default.htm>

[CaptureBAT](#)

<https://www.honeynet.org/projects/old/capture-bat/>

[NetworkMiner](#)

<https://www.netresec.com/?page=NetworkMiner>

[PassiveDNS](#)

<https://github.com/gamelinux/passivedns>

[Stenographer](#)

<https://github.com/google/stenographer>

Click [HERE](#) to return to slide 51

<https://t.me/learningnets> | **ENPTS 1: Section 01, Module 01, Appendix A - Caendra Inc. © 2020 | p.66**



References

[ProcDot](https://procdot.com/index.htm)

<https://procdot.com/index.htm>

[ProcDOT](https://www.cert.at/en/downloads/software/software-procdot)

<https://www.cert.at/en/downloads/software/software-procdot>

[XDot](http://gecos.gforge.inria.fr/doku/doku.php?id=doc:faq:opendotfiles)

<http://gecos.gforge.inria.fr/doku/doku.php?id=doc:faq:opendotfiles>

[Graphviz](https://graphviz.org/download/)

<https://graphviz.org/download/>

[Viper](https://viper.li/en/latest/)

<https://viper.li/en/latest/>

