v1

Malware Analysis Professional

The Lab

Section 01 | Module 01 | Appendix A

Table of Contents

MODULE 01 | APPENDIX A | THE LAB

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.

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

A1.2

Operating System Requirements

A1.2 Operating System Requirements

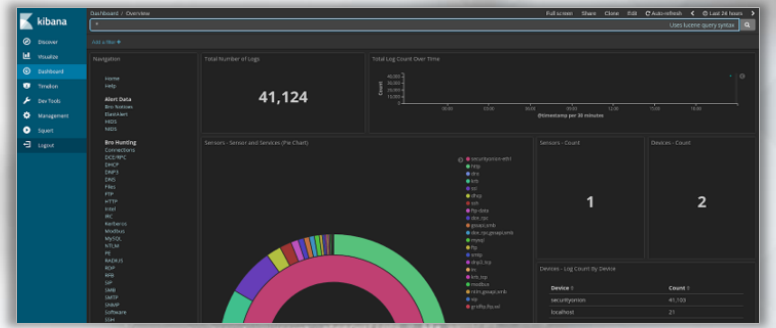
Now that we have the hardware settled, we need an operating system to use for our analysis. This is where another question will arise: which OS should I use?

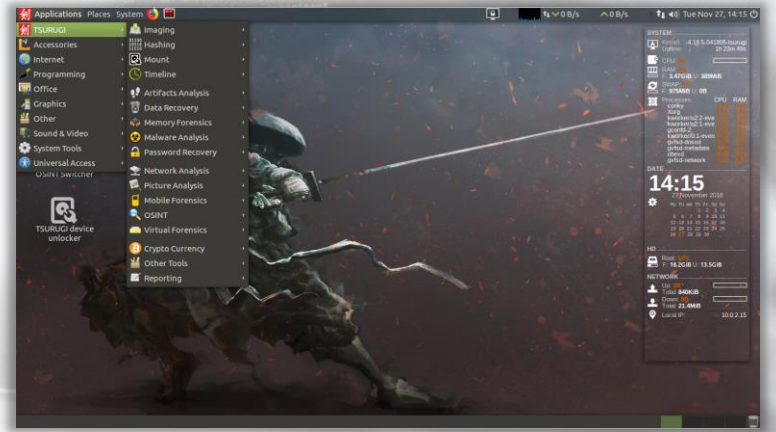
The truth again is, there is no one best system. It is best to have a diversity of systems to use and throughout the course, you will see why.

A1.2 Operating System Requirements

We will be using the following systems:

- SecurityOnion
- Tsurugi Linux
- Windows 10





Go to slide 56 to check out the full URLs

A1.3

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.

https://www.vmware.com/products/workstation-pro.html
https://www.virtualbox.org/

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.

A1.4

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

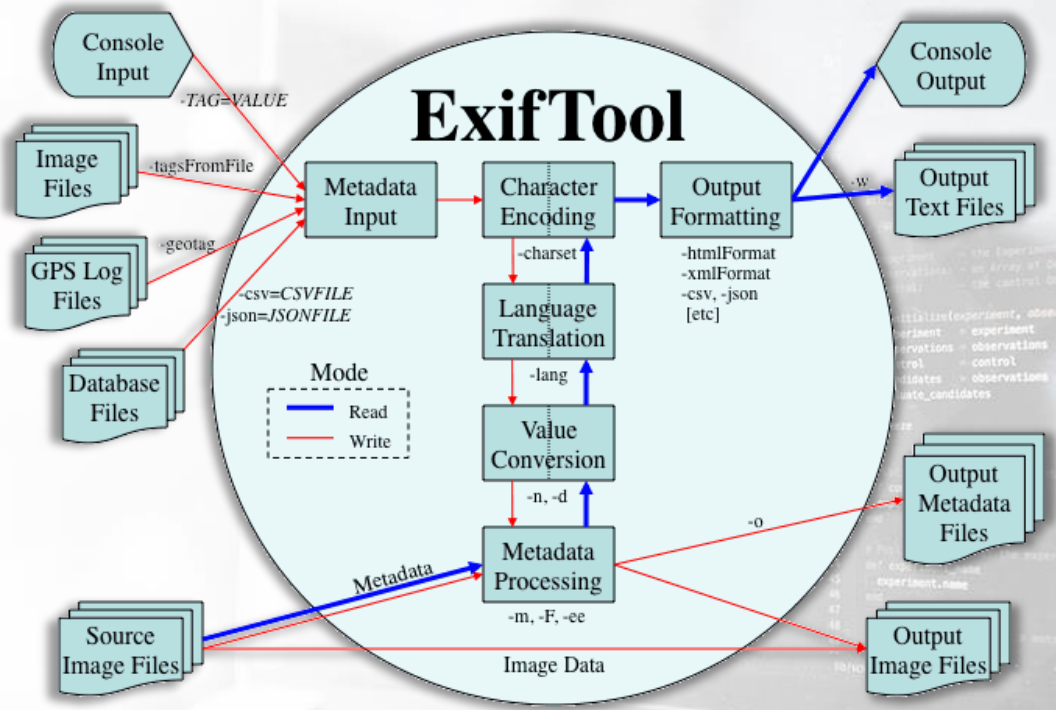
The tools we will use in this course can be divided into the following categories:

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

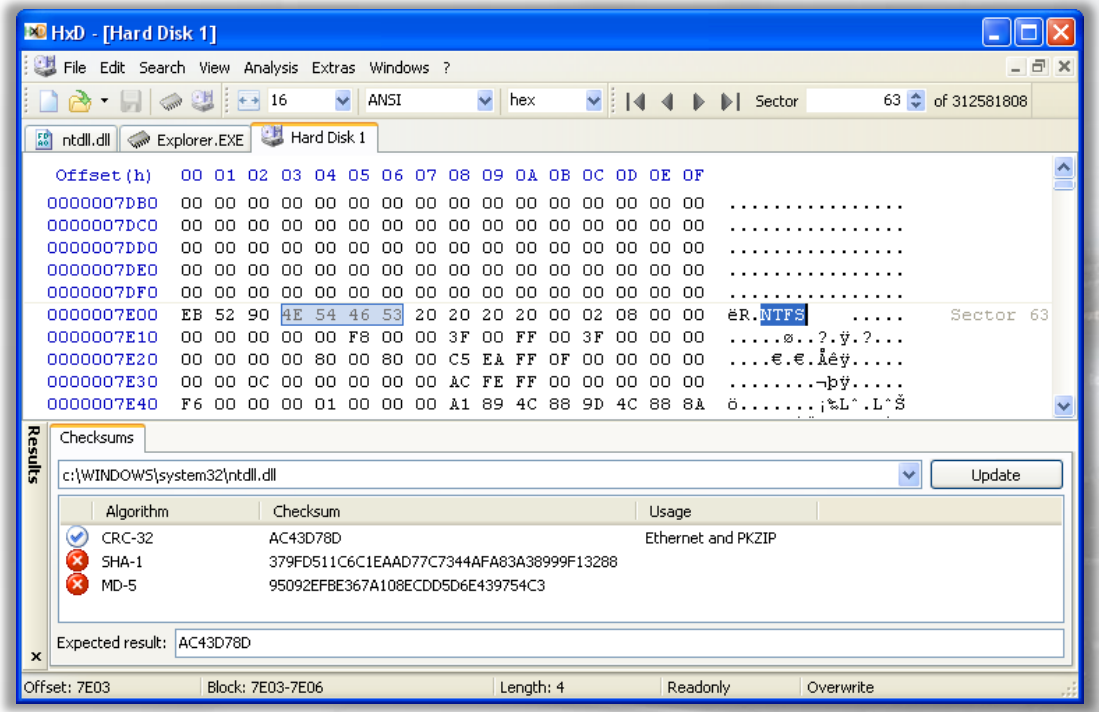
ExifTool



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

A1.4.1 String and Metadata Tools

[HxD Hex Editor]



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

A1.4.1 String and Metadata Tools

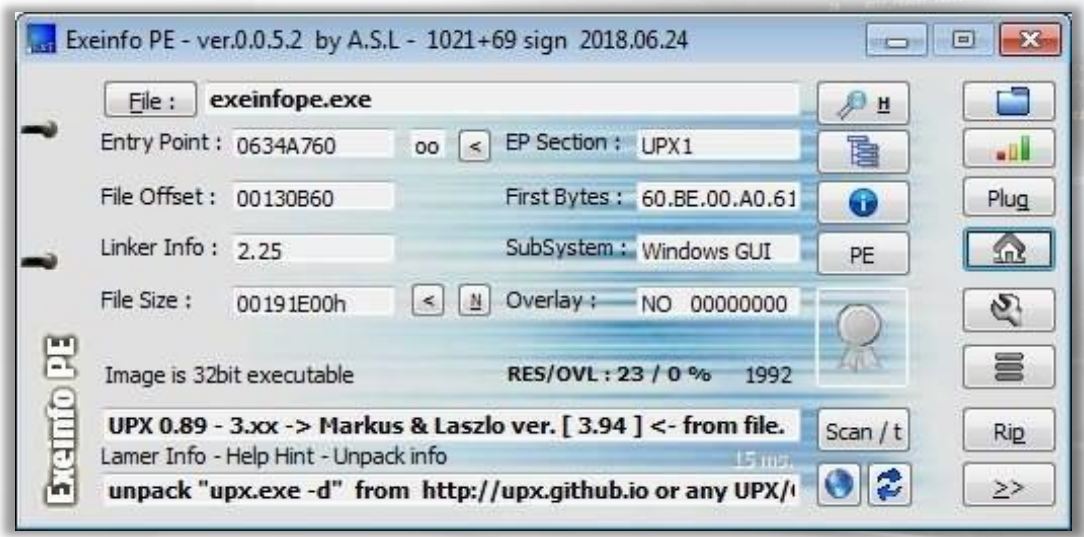
Additional String and Metadata tools include:

- Free Hex Editor Neo
- bstrings
- BinText
- StringSifter

Go to slides 57 and 58 to check out the full URLs

A1.4.2 Static Analysis Tools

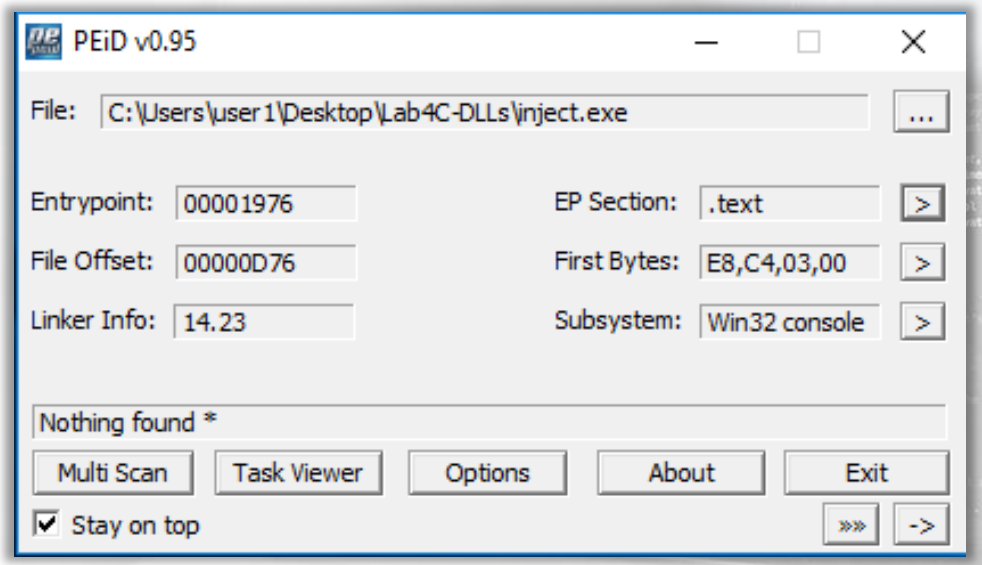
Exeinfo PE (latest version) or you can download an older version here.



http://www.exeinfo.xn.pl/
https://tuts4you.com/download/3565/

A1.4.2 Static Analysis Tools

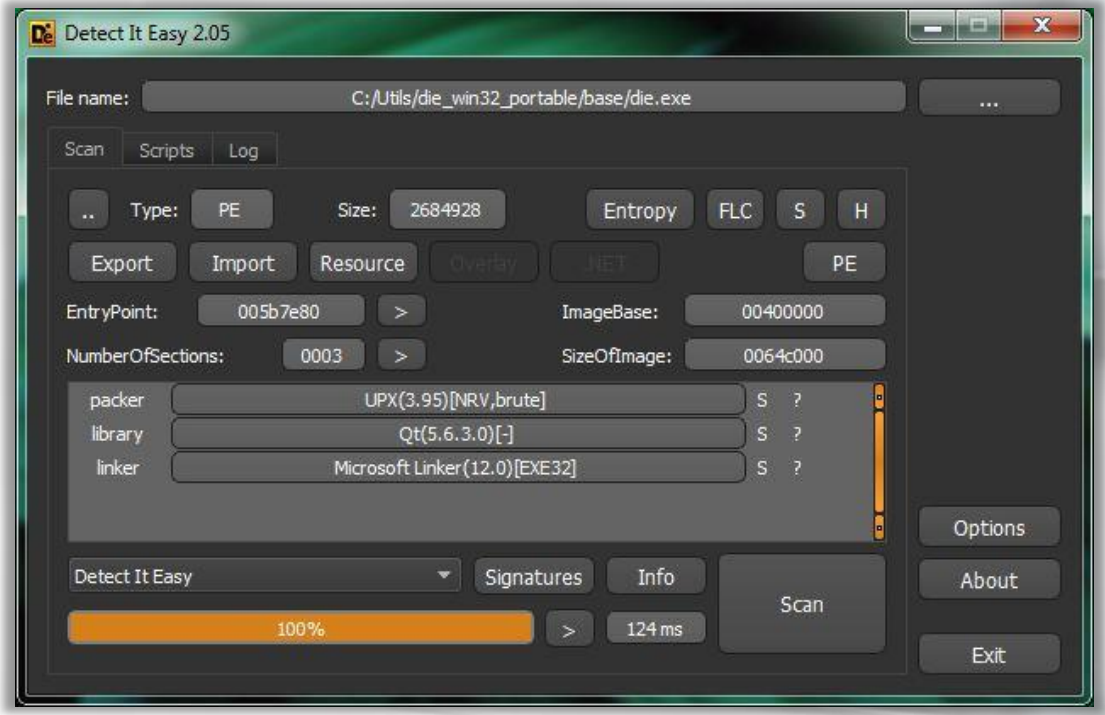
PEiD (password = tuts4you) + signatures



https://tuts4you.com/e107_plugins/download/download.php?view.21
https://github.com/wolfram77web/app-peid

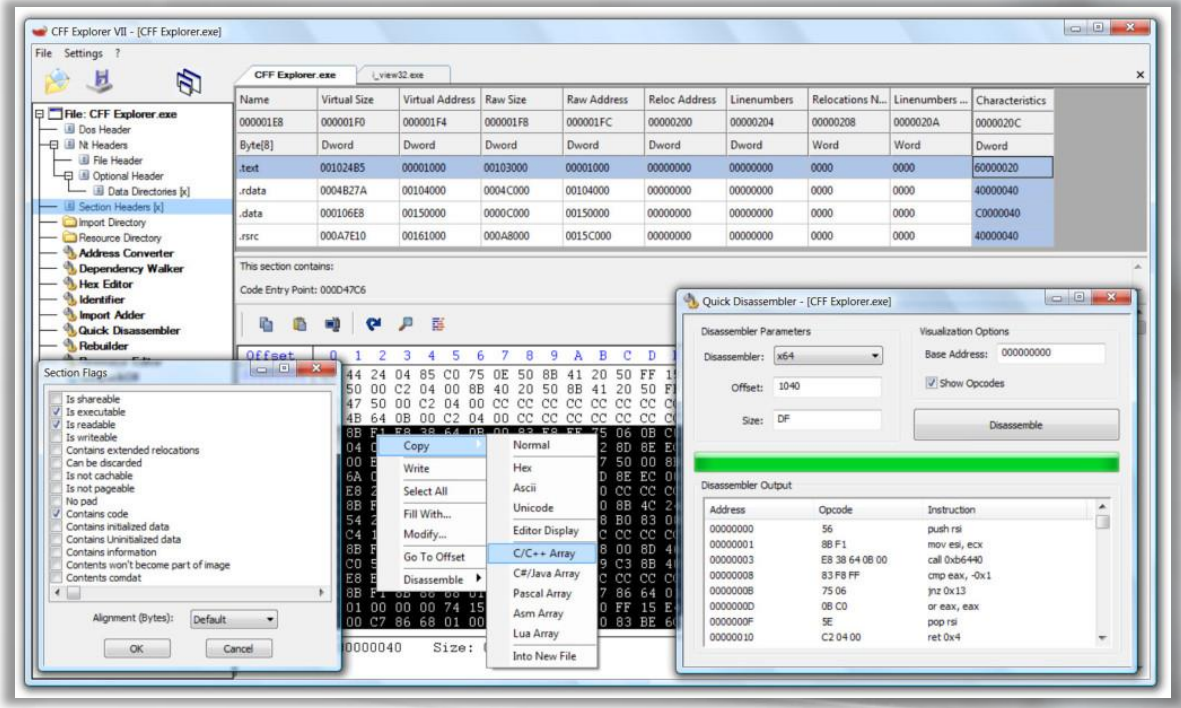
A1.4.2 Static Analysis Tools

[Detect it Easy (DiE)]



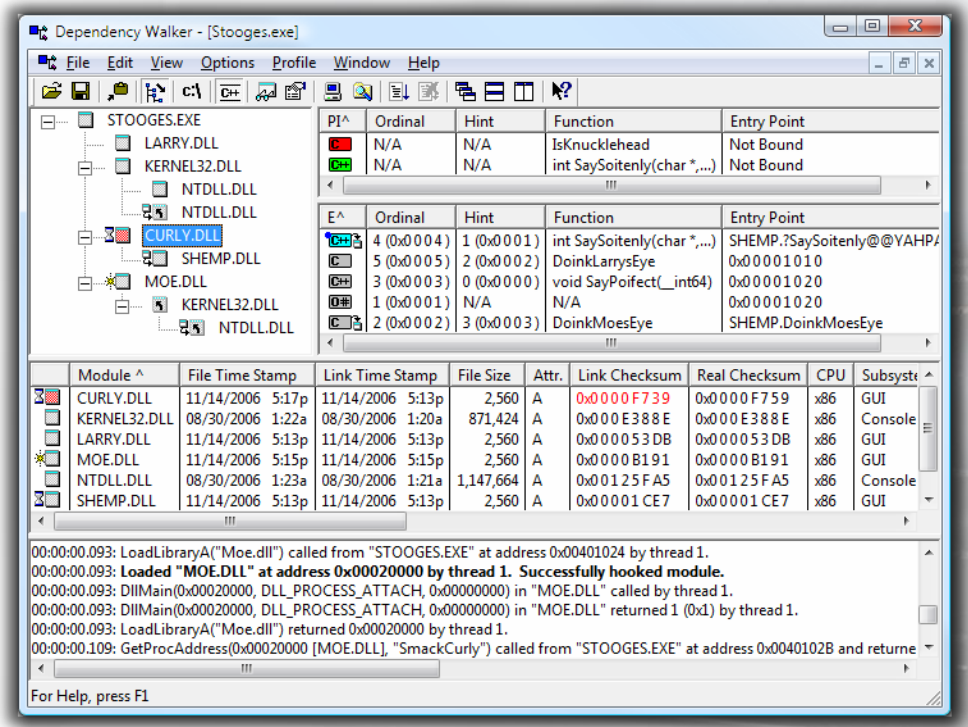
A1.4.2 Static Analysis Tools

CFF Explorer



A1.4.2 Static Analysis Tools

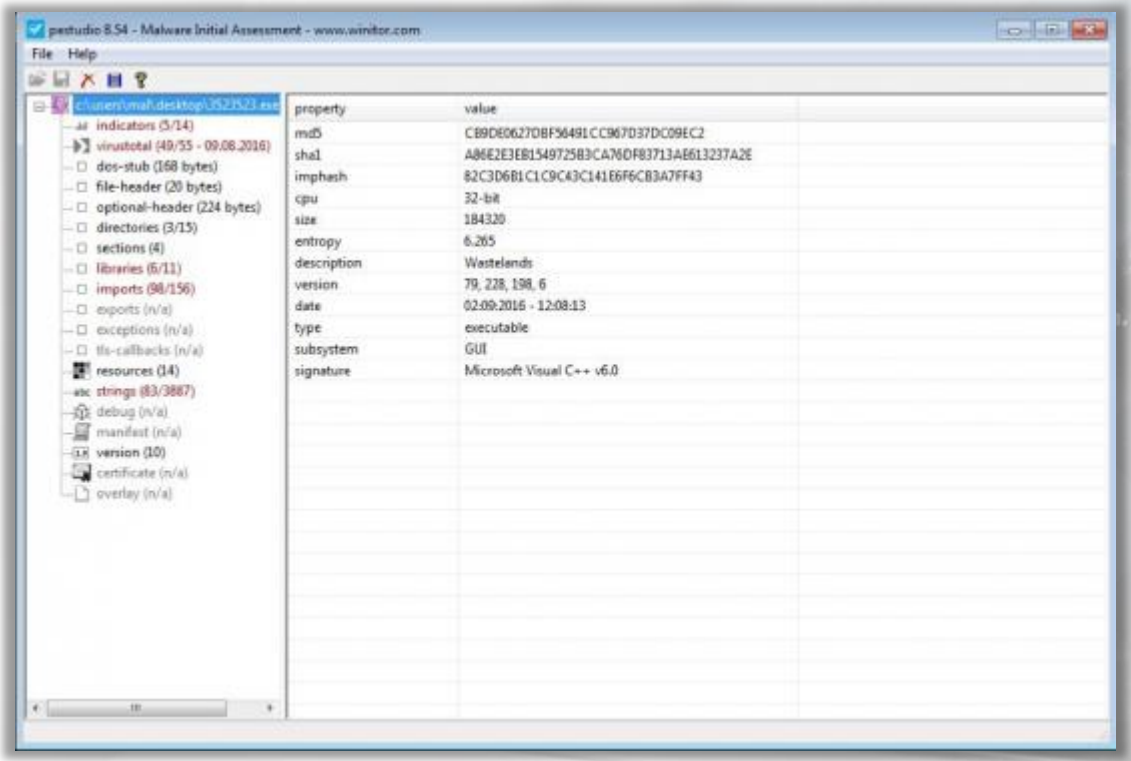
[Dependency Walker]



http://dependencywalker.com/

A1.4.2 Static Analysis Tools

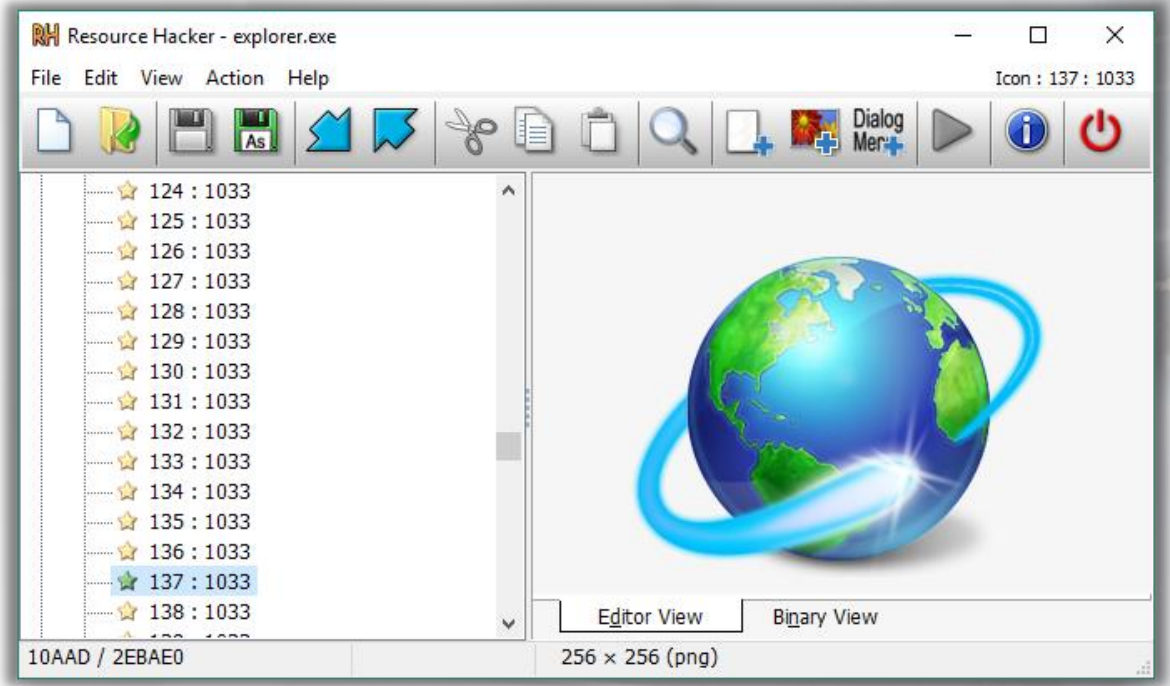
PE Studio



https://winitor.com/

A1.4.2 Static Analysis Tools

Resource Hacker



http://angusj.com/resourcehacker/

A1.4.2 Static Analysis Tools

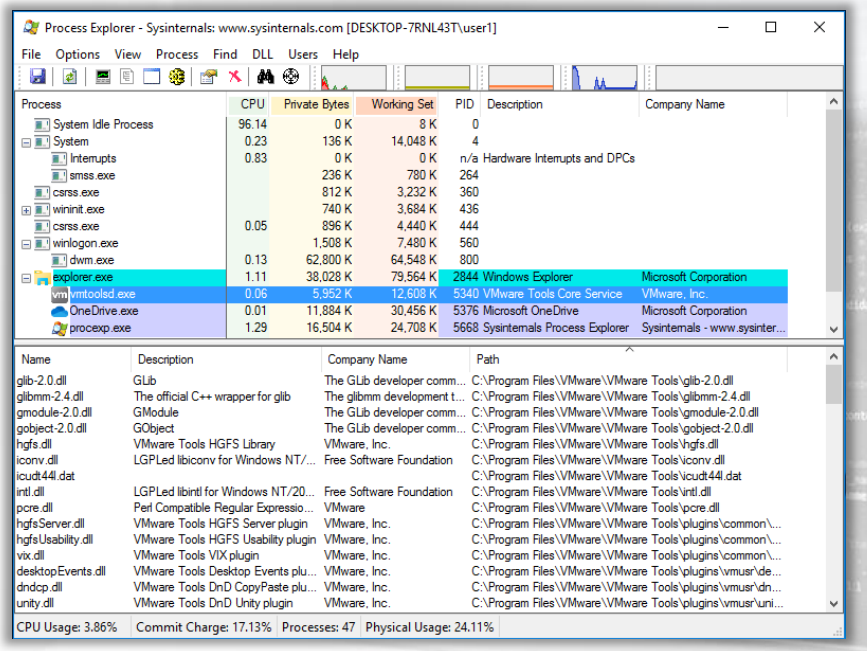
Additional Static Analysis tools include:

- TitanMist
- ASPack (trail)
- Reflective PE Packer: Amber

Go to slides 59 and 60 to check out the full URLs

A1.4.3 Dynamic Analysis Tools

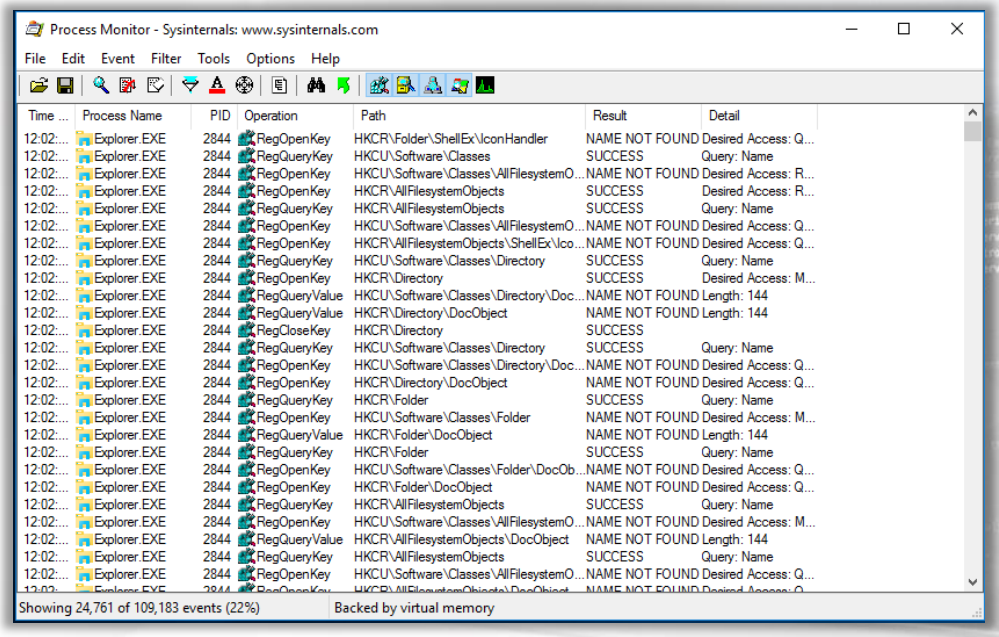
Microsoft SysInternals Suite Process Explorer



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

A1.4.3 Dynamic Analysis Tools

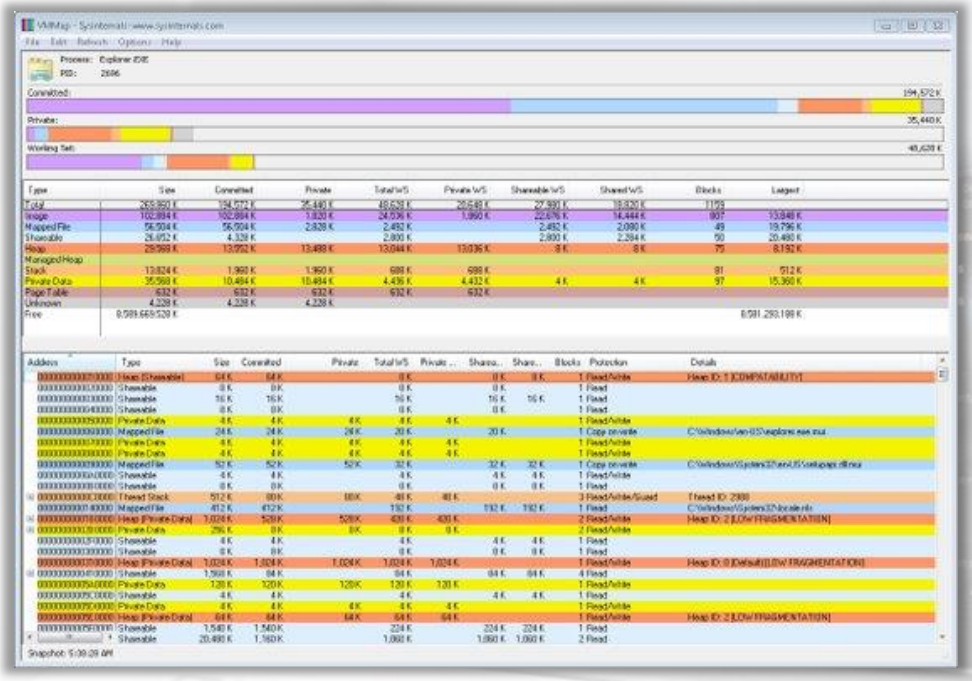
Microsoft SysInternals Suite Process Monitor



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

A1.4.3 Dynamic Analysis Tools

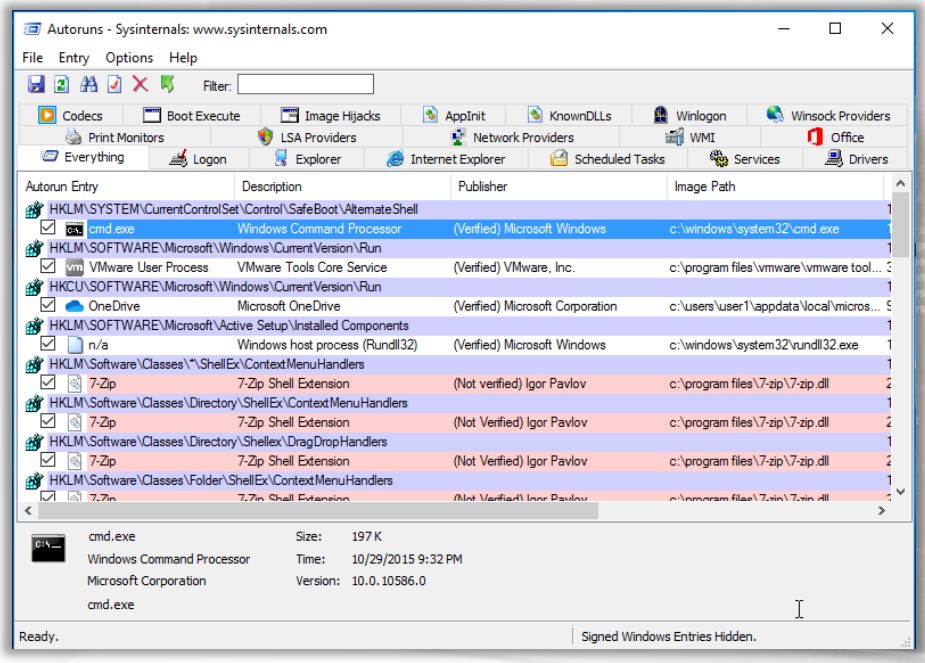
Microsoft SysInternals Suite VMMap



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

A1.4.3 Dynamic Analysis Tools

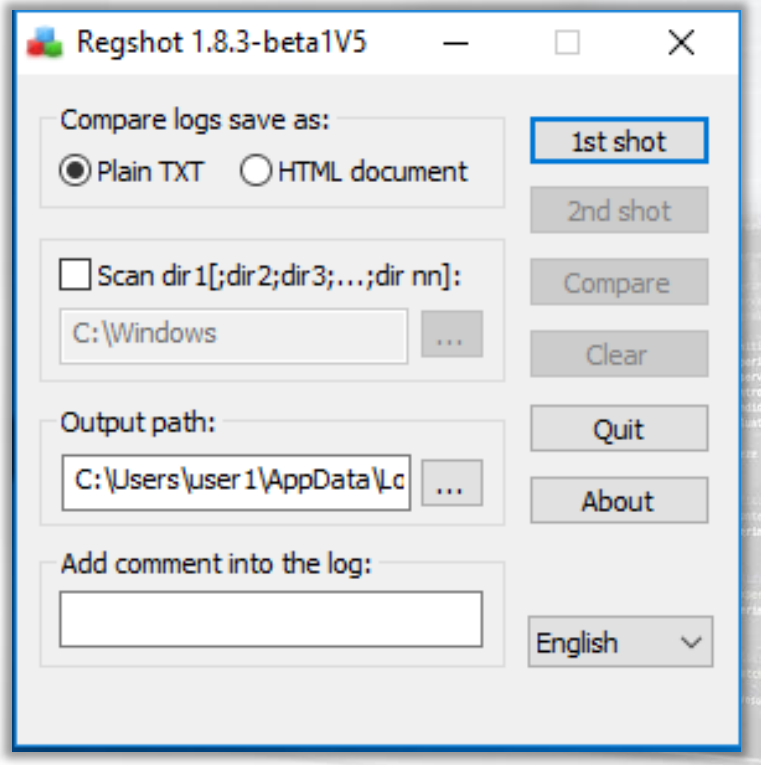
Microsoft SysInternals Suite Autoruns



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

A1.4.3 Dynamic Analysis Tools

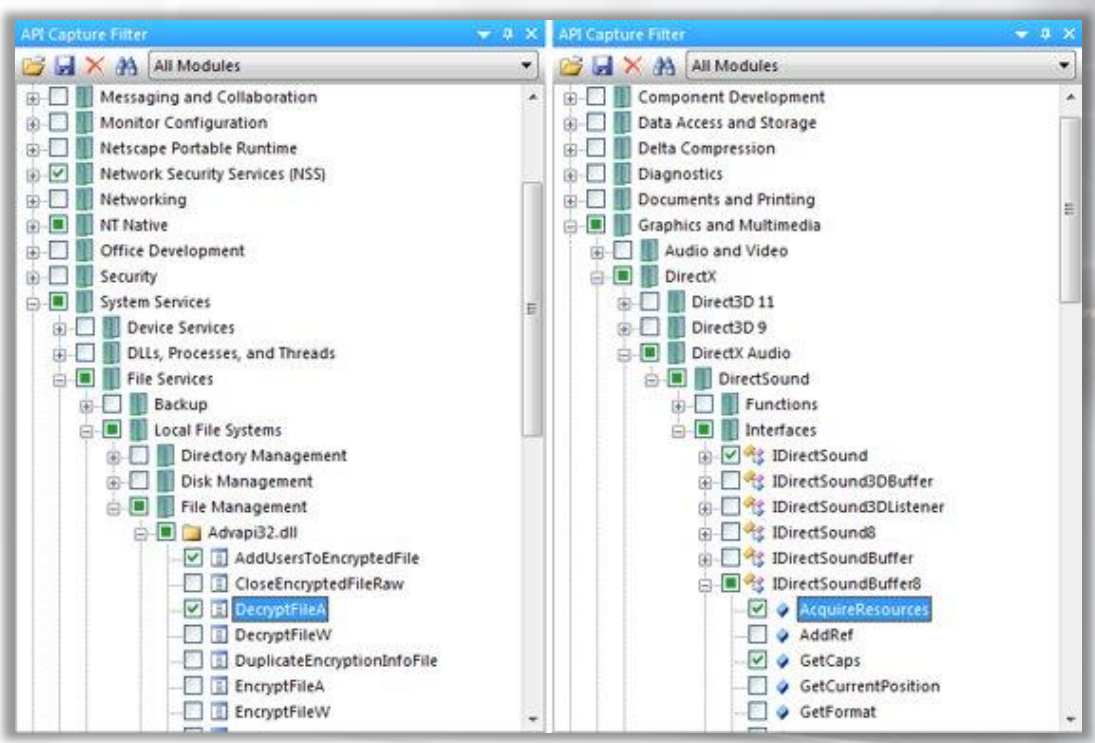
[RegShot]



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

A1.4.3 Dynamic Analysis Tools

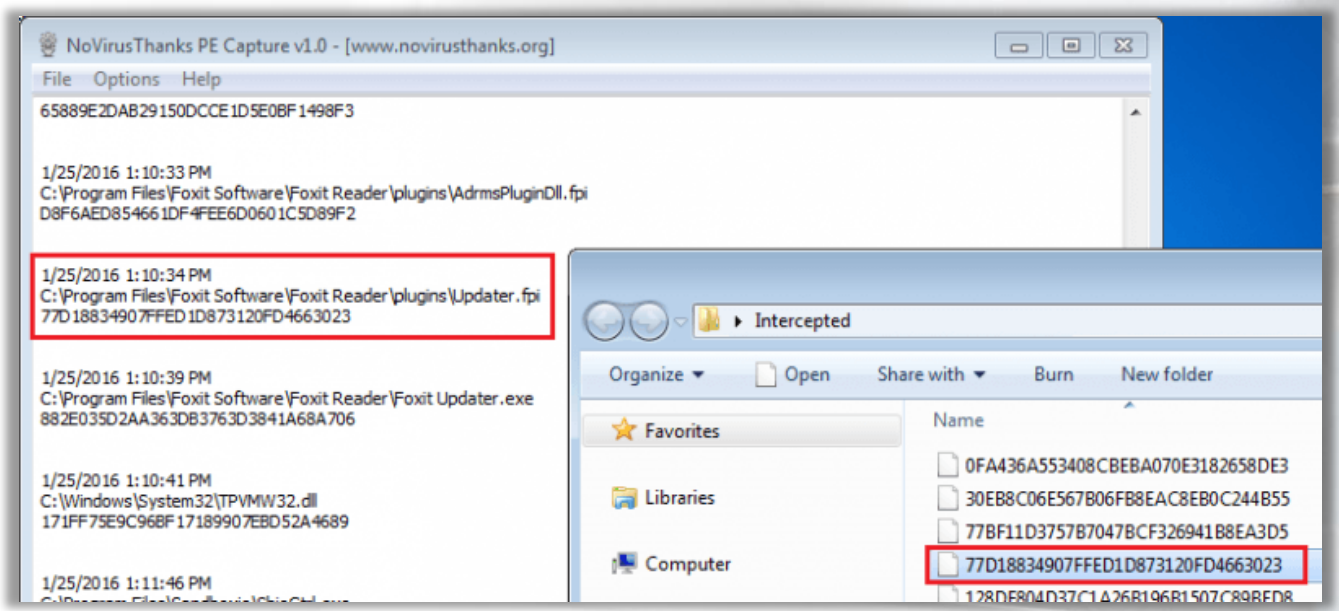
API Monitor



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

A1.4.3 Dynamic Analysis Tools

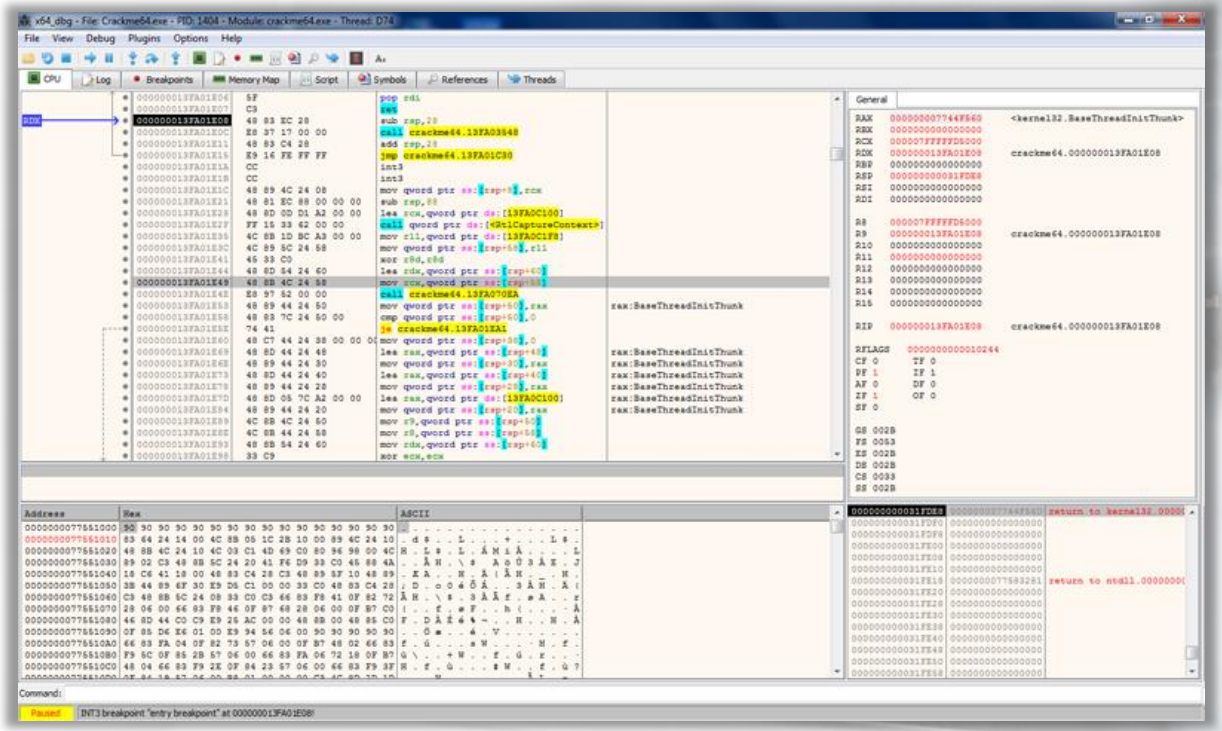
PE Capture



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

A1.4.3 Dynamic Analysis Tools

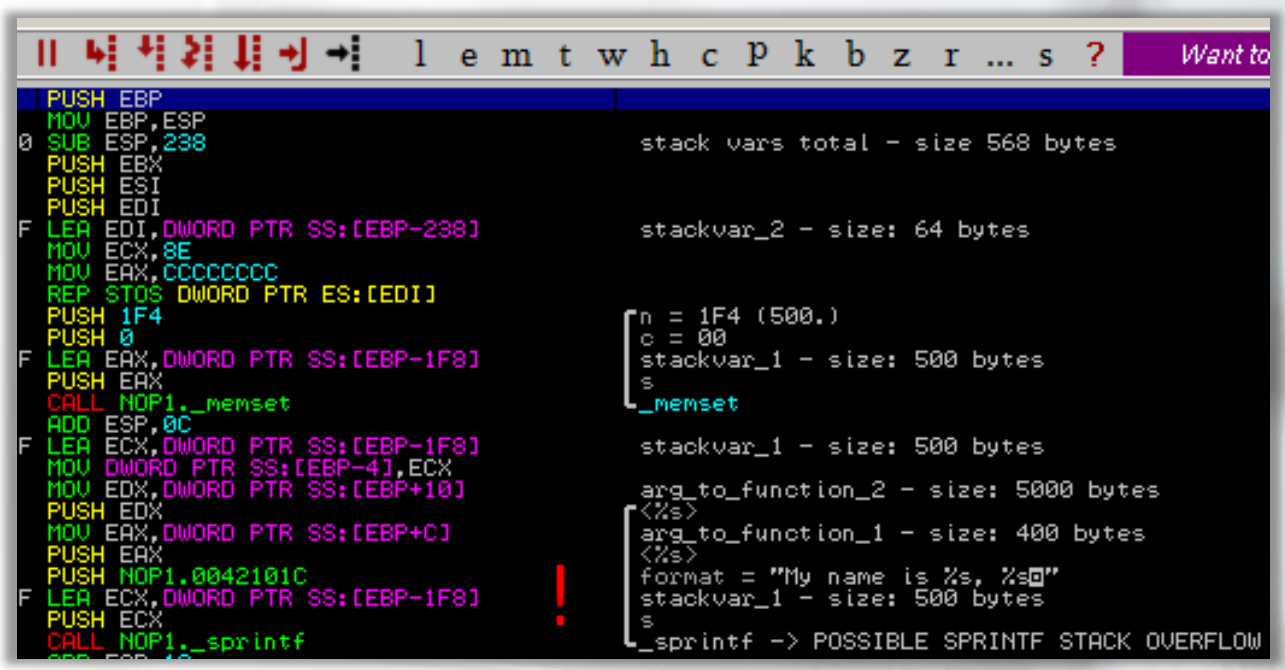
[X64dbg]



https://x64dbg.com/#start

A1.4.3 Dynamic Analysis Tools

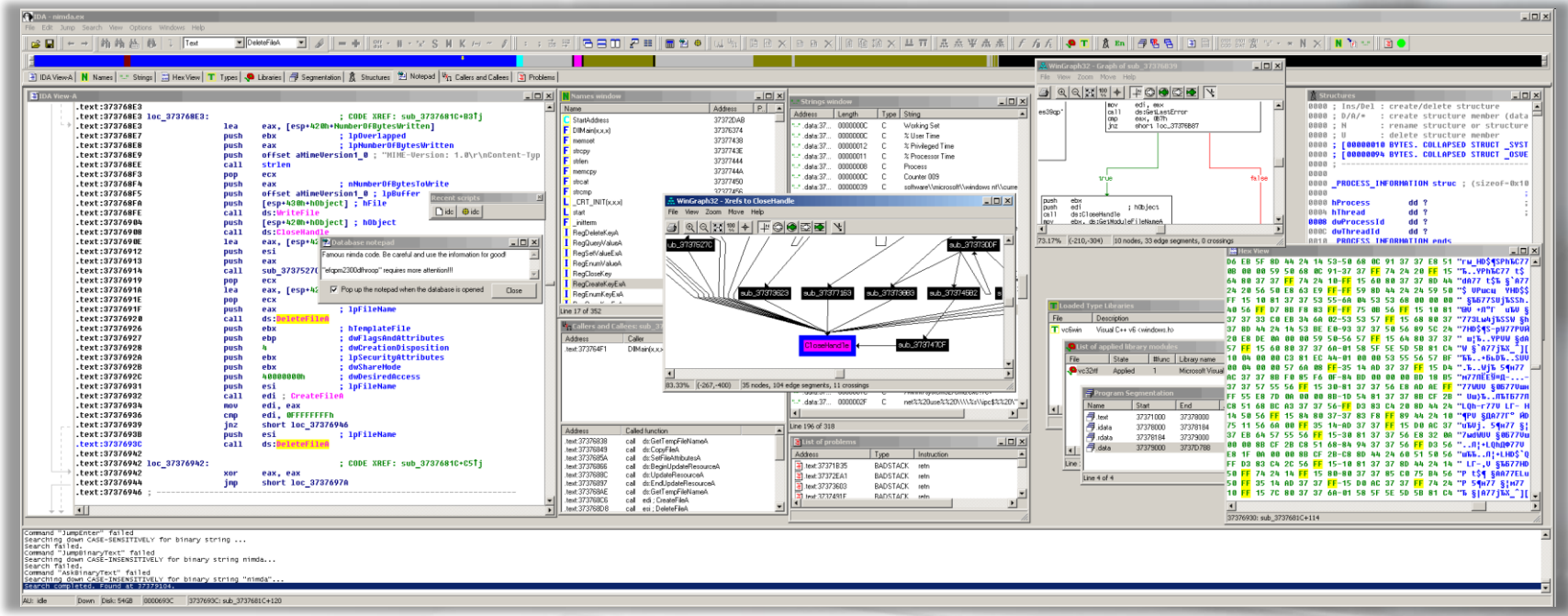
[Immunity Debugger]



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

A1.4.3 Dynamic Analysis Tools

IDA Pro



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

https://t.me/learningmalware

A1.4.3 Dynamic Analysis Tools

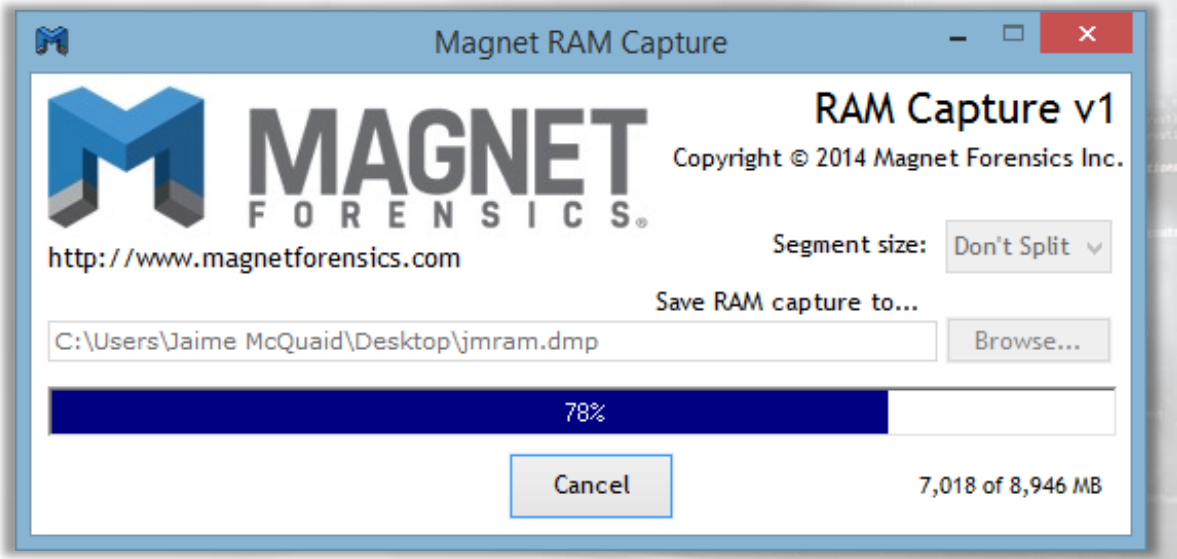
Additional Dynamic Analysis tools include:

- Noriben
- Rundll32 (LOLBin)
- Injector (Reflective DLL Injection)
- Ghidra

Go to slide 61 to check out the full URLs

A1.4.4 Memory Forensics Tools

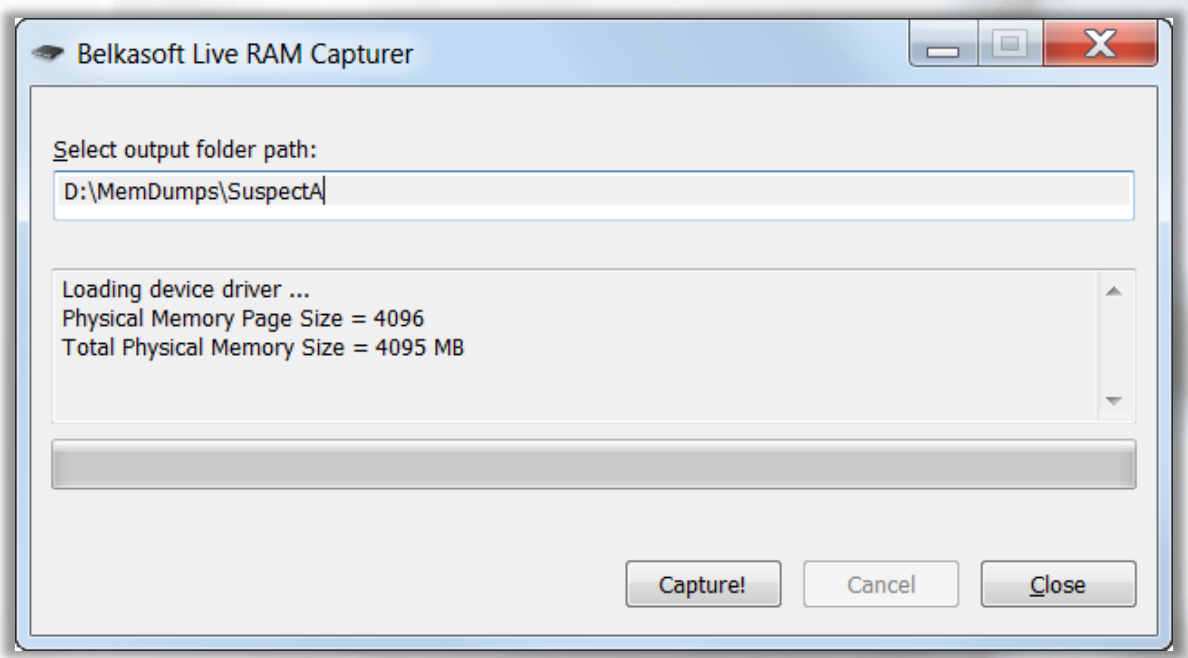
MagnetForensics RAM Capture



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

A1.4.4 Memory Forensics Tools

[Belkasoft Live RAM Capture]



https://belkasoft.com/ram-capturer

A1.4.4 Memory Forensics Tools

Additional Memory Forensics tools include:

- Comae DumpIt
- Nirsoft Memdump
- Mandiant Redline

Go to slide 62 to check out the full URLs

A1.4.4 Memory Forensics Tools

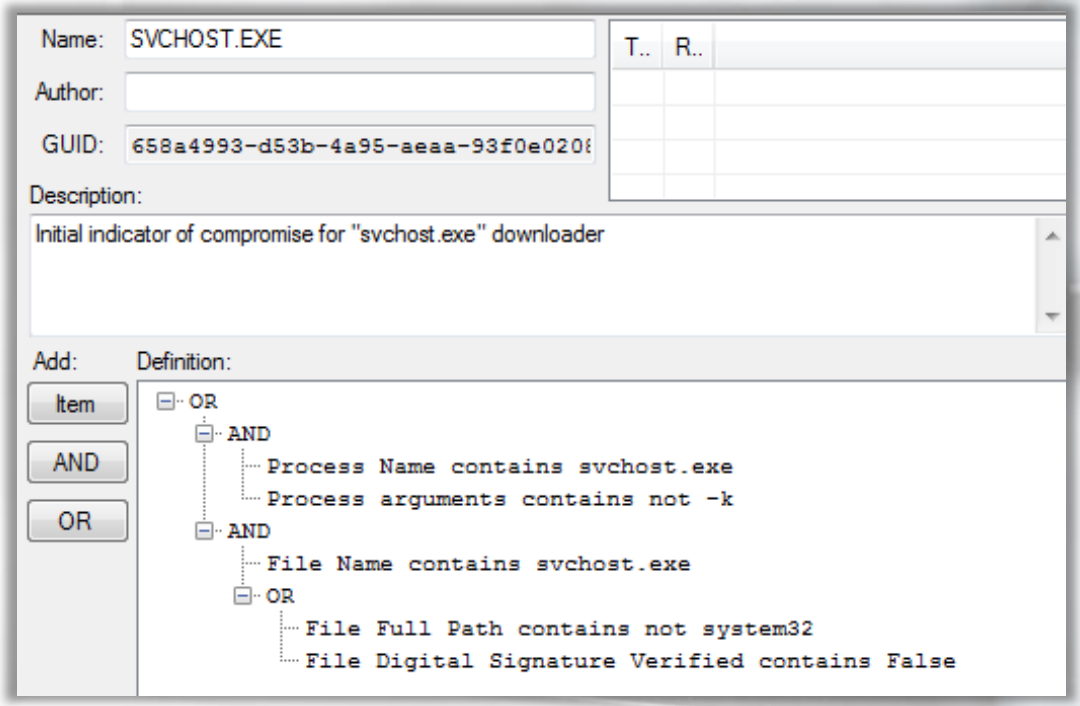
Additional Memory Forensics tools include (cont.):

- Rekall WinPmem
- Volatility3, Volatility 2.6.x, Plugins, etc.
    - MalHunt, AutoTimeliner, etc.
- Rekall

Go to slides 62 and 63 to check out the full URLs

A1.4.5 Incident Response Tools

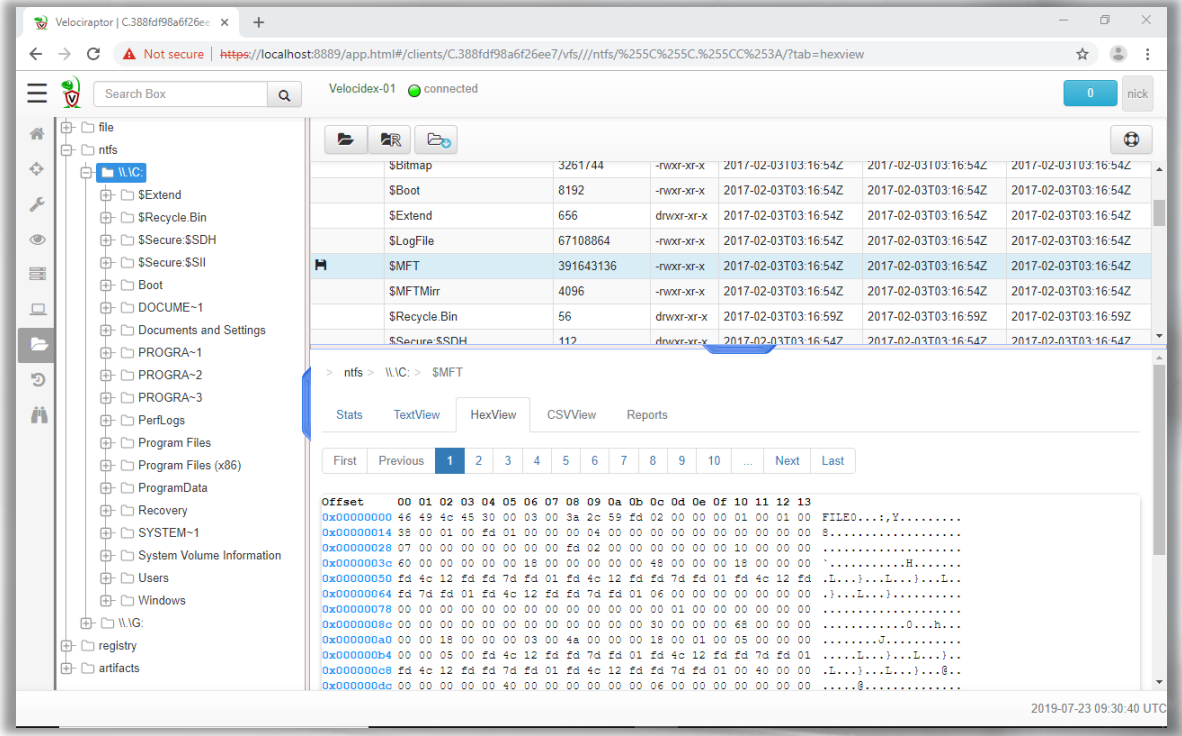
[Mandiant IOC Editor]



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

A1.4.5 Incident Response Tools

GRR and Velociraptor



https://github.com/google/grr
https://github.com/Velocidex/velociraptor

A1.4.5 Incident Response Tools

Additional Incident Response tools include:

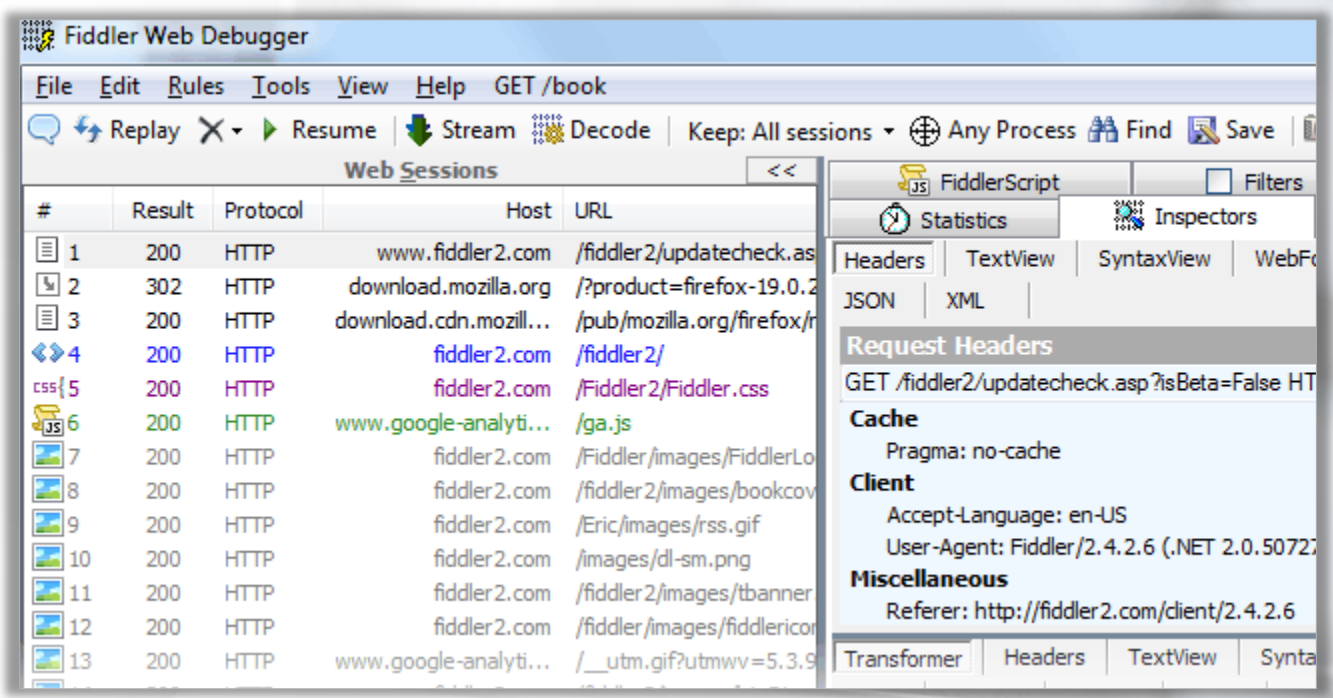
- The Yara Family:
  - Yara, Rules, Yara-Merger, Yara-Endpoint, etc.
- Loki Scanner
- Facebook OSQuery
- ClamAV

Go to slides 64 and 65 to check out the full URLs

https://t.me/learningnets

A1.4.6 Network Tools

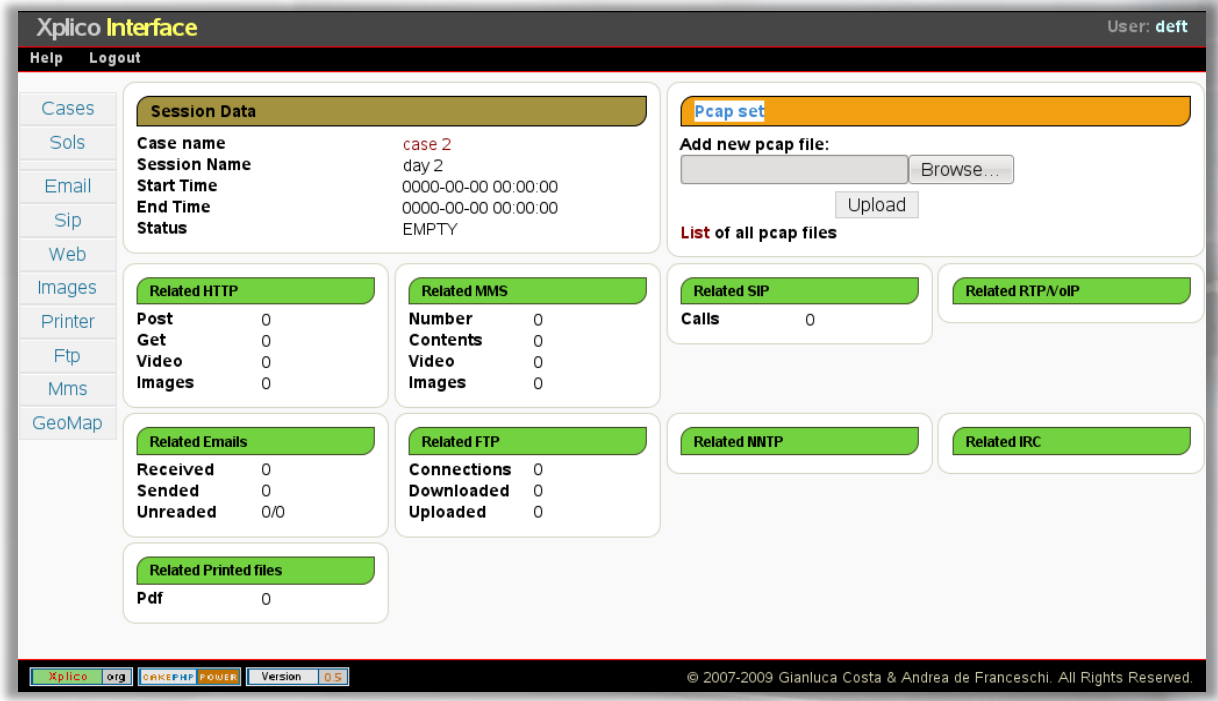
Fiddler



https://www.telerik.com/fiddler

A1.4.6 Network Tools

Xplico



https://www.xplico.org/

A1.4.6 Network Tools

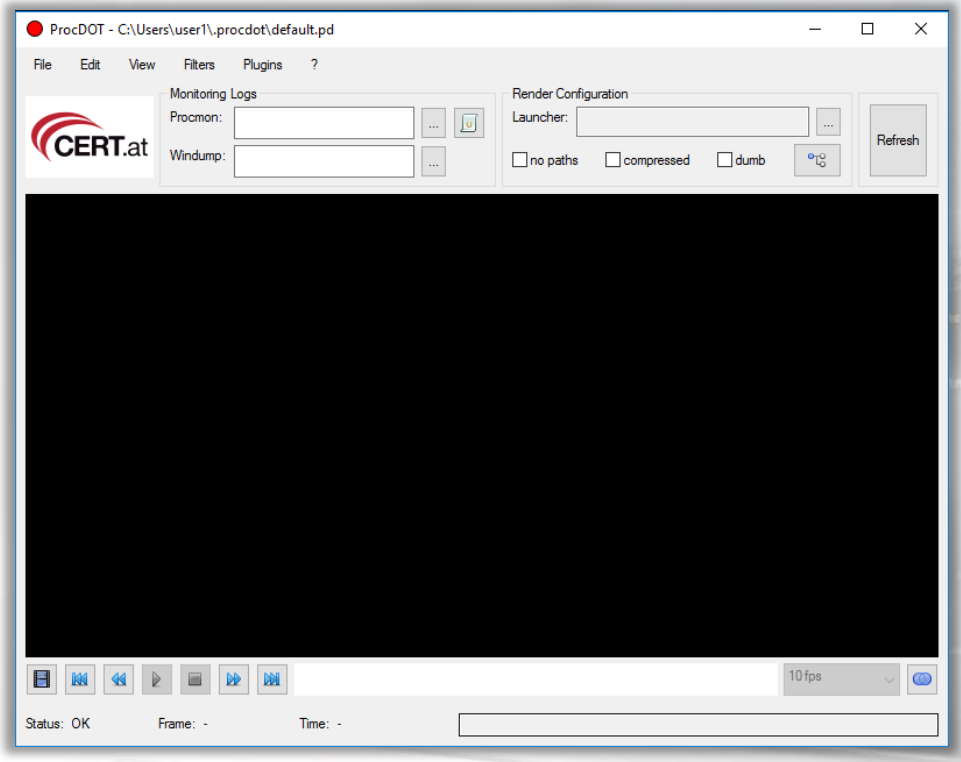
Additional Network tools include:

- Mandiant AptDNS
- WinDump
- CaptureBAT
- NetworkMiner
- PassiveDNS
- Stenographer

Go to slide 66 to check out the full URLs

A1.4.7 Visualization Tools

ProcDOT or here

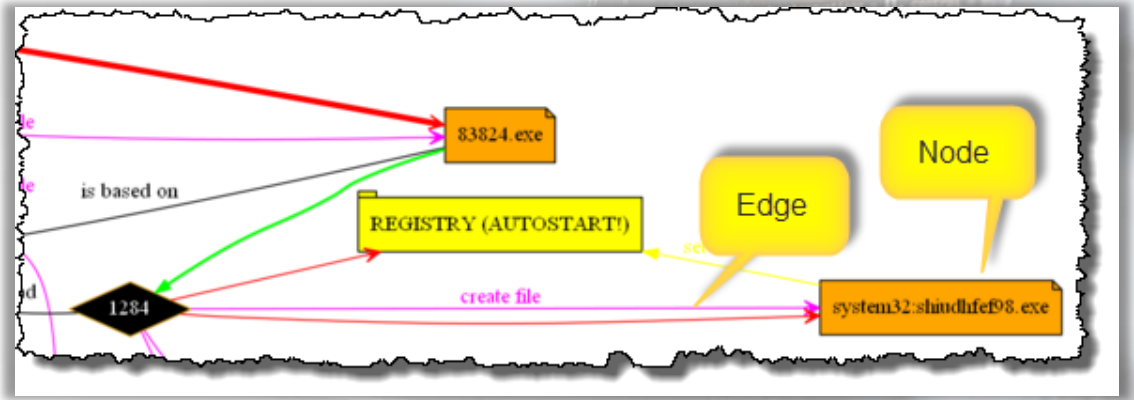


https://procdot.com/index.htm
https://www.cert.at/en/downloads/software/software-procdot

A1.4.7 Visualization Tools

Additional Visualization tools include:

- XDot
- Graphiz



http://gecos.gforge.inria.fr/doku/doku.php?id=doc:faq:opendothttps://t.me/learningnets
https://graphviz.org/download/

A1.4.8 Framework Tools

The main Framework tool is Viper.

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

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/

Click HERE to return to slide 10

References

VMWare

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

VirtualBox

https://www.virtualbox.org/

Exiftool

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

HxD Hex Editor

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

Free Hex Editor Neo

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

bstrings

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

Click HERE to return to slide 22

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

References

Detect it Easy (DiE)

http://ntinfo.biz/index.html

CFF Explorer

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

Dependency Walker

http://dependencywalker.com/

PE Studio

https://winitor.com/

Resource Hacker

http://angusj.com/resourcehacker/

TitanMist

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

Click HERE to return to slide 30

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

Immunity Debugger

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

IDA Pro

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

Noriben

https://github.com/Rurik/Noriben

Injector (Reflective DLL Injection)

https://github.com/stephenfewer/ReflectiveDLLInjection

Ghidra

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

Click HERE to return to slide 41

References

MagnetForensics RAM Capture

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

Belkasoft Live RAP Capture

https://belkasoft.com/ram-capturer

Comae DumpIt

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

Nirsoft Memedump

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

Rekall WimPmem

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

Mandiant Redline

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/

Volatility 2.6.x

https://github.com/volatilityfoundation/volatility

Volatility Plugins

https://github.com/volatilityfoundation

MalHunt

https://github.com/andreafortuna/malhunt

AutoTimeliner

https://github.com/andreafortuna/autotimeliner

Rekall

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

Click HERE to return to slide 45

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

Loki Scanner

https://github.com/Neo23x0/Loki

Facebook OSQuery

https://osquery.io/

ClamAV

https://www.clamav.net/

Fiddler

https://www.telerik.com/fiddler

Xplico

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

References

ProcDot

https://procdot.com/index.htm

ProcDOT

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

XDot

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

Graphiz

https://graphviz.org/download/

Viper

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