Introduction to Dynamic Analysis

Reverse Engineering – Introduction to Dynamic Analysis
Albert López - newlog@overflowedminds.net

Goals

What can you expect after this module?

Goals

1. Understand how binaries behave by executing them

1. Get in touch with different well-known dynamic analysis tools

Introduction

We are going to give the **first baby steps** towards dynamic analysis.

Dynamic analysis is the craft of extracting information from binaries by executing them.

Basically, we will get familiar with a couple of tools that can be used to extract information from binaries.

Warning (related to malware analysis):

Whenever you analyze malware, make sure you do so in a VM completely isolated from your day-to-day system.

This means:

- No internet connection
- No shared folders
- (...)

You can create a host-only network among VMs.

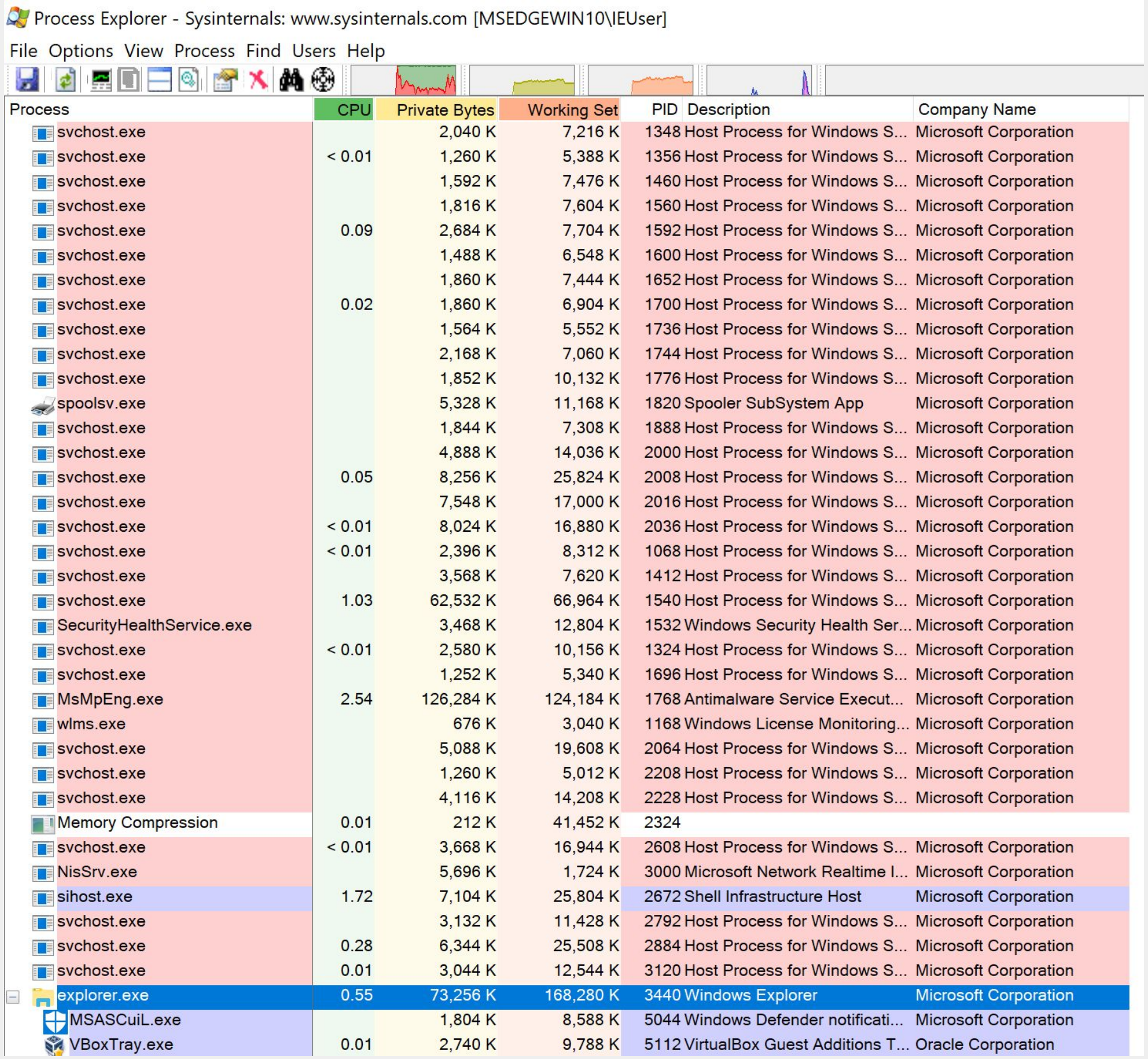
Make sure you **make an snapshot** of your VM before starting analyzing the malware sample.

The Tools

- Process Explorer: Task manager on steroids
- RegShot: Diff utility for the Windows registry
- Process Monitor: Events tracing tool
- ApateDNS: Tool to respond to any DNS request
- (...)

Inspecting Processes

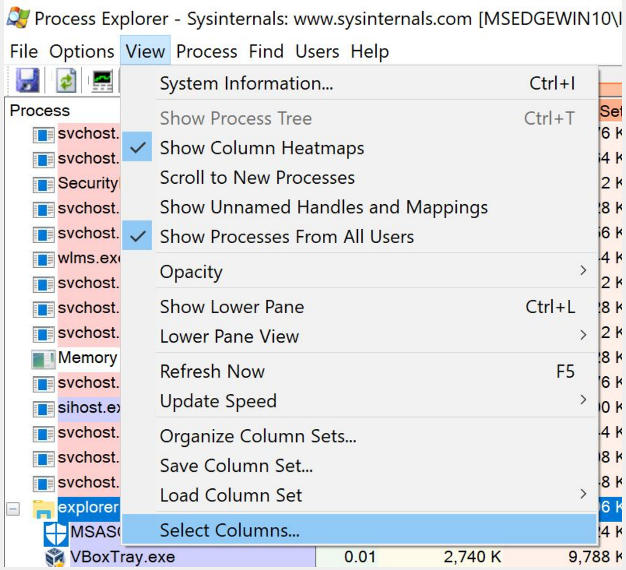
Process Explorer

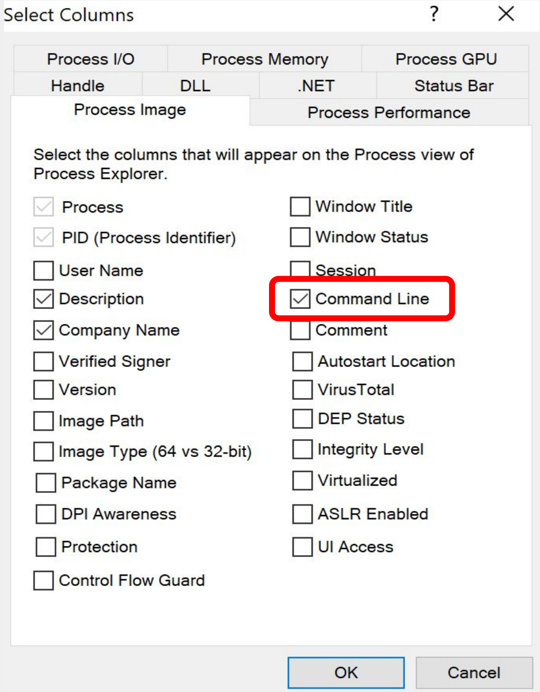


Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		2,040 K	7,216 K	1348	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	1,260 K	5,388 K	1356	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,592 K	7,476 K	1460	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,816 K	7,604 K	1560	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.09	2,684 K	7,704 K	1592	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,488 K	6,548 K	1600	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,860 K	7,444 K	1652	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.02	1,860 K	6,904 K	1700	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,564 K	5,552 K	1736	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,168 K	7,060 K	1744	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,852 K	10,132 K	1776	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		5,328 K	11,168 K	1820	Spooler SubSystem App	Microsoft Corporation
svchost.exe		1,844 K	7,308 K	1888	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,888 K	14,036 K	2000	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.05	8,256 K	25,824 K	2008	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,548 K	17,000 K	2016	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	8,024 K	16,880 K	2036	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	2,396 K	8,312 K	1068	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,568 K	7,620 K	1412	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1.03	62,532 K	66,964 K	1540	Host Process for Windows S...	Microsoft Corporation
SecurityHealthService.exe		3,468 K	12,804 K	1532	Windows Security Health Ser...	Microsoft Corporation
svchost.exe	< 0.01	2,580 K	10,156 K	1324	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,252 K	5,340 K	1696	Host Process for Windows S...	Microsoft Corporation
MsMpEng.exe	2.54	126,284 K	124,184 K	1768	Antimalware Service Execut...	Microsoft Corporation
wlms.exe		676 K	3,040 K	1168	Windows License Monitoring...	Microsoft Corporation
svchost.exe		5,088 K	19,608 K	2064	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,260 K	5,012 K	2208	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,116 K	14,208 K	2228	Host Process for Windows S...	Microsoft Corporation
Memory Compression	0.01	212 K	41,452 K	2324		
svchost.exe	< 0.01	3,668 K	16,944 K	2608	Host Process for Windows S...	Microsoft Corporation
NisSrv.exe		5,696 K	1,724 K	3000	Microsoft Network Realtime I...	Microsoft Corporation
sihost.exe	1.72	7,104 K	25,804 K	2672	Shell Infrastructure Host	Microsoft Corporation
svchost.exe		3,132 K	11,428 K	2792	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.28	6,344 K	25,508 K	2884	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	3,044 K	12,544 K	3120	Host Process for Windows S...	Microsoft Corporation
explorer.exe	0.55	73,256 K	168,280 K	3440	Windows Explorer	Microsoft Corporation
MSASCuiL.exe		1,804 K	8,588 K	5044	Windows Defender notificati...	Microsoft Corporation
VBoxTray.exe	0.01	2,740 K	9,788 K	5112	VirtualBox Guest Additions T...	Oracle Corporation

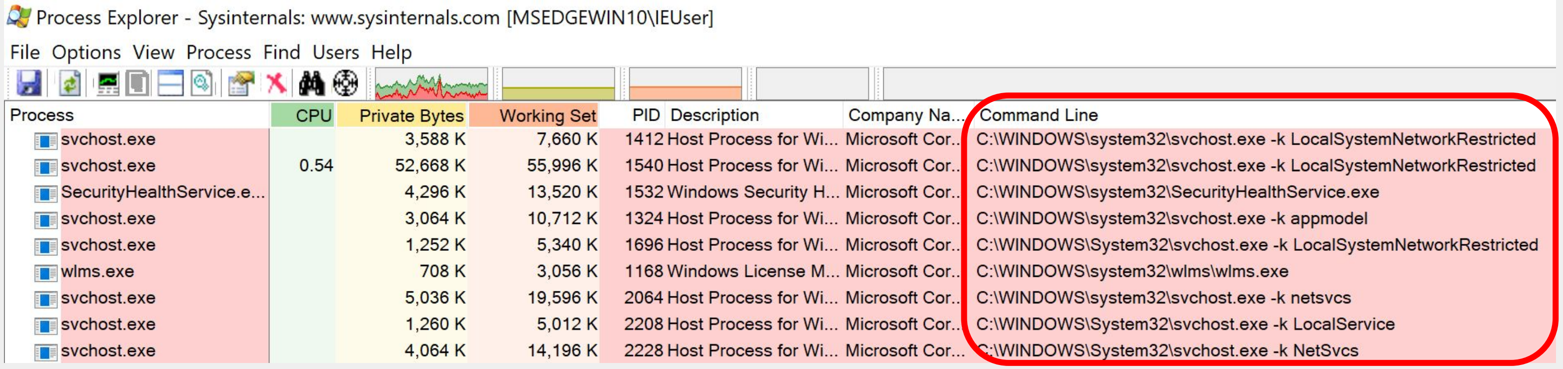
Process Explorer





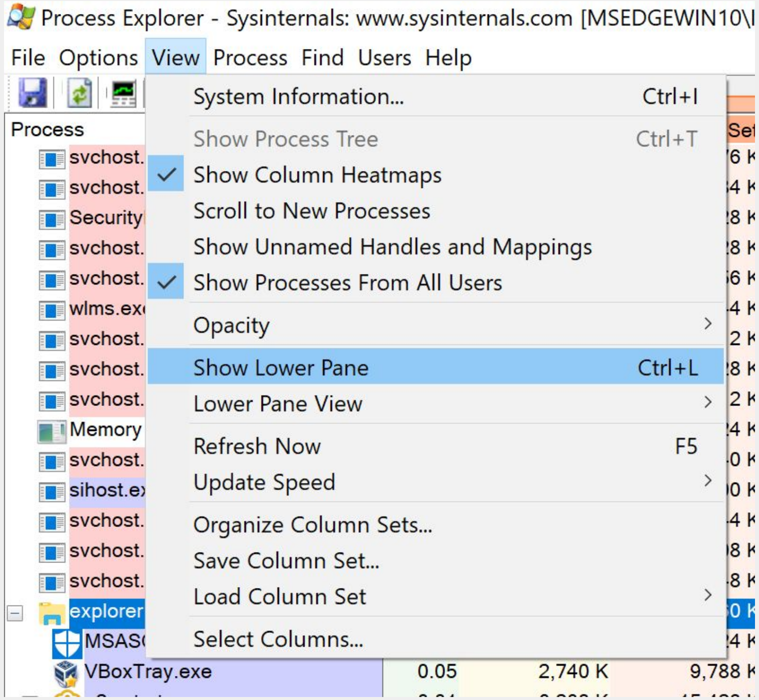
Select the columns that will appear on the Process view of Process Explorer.

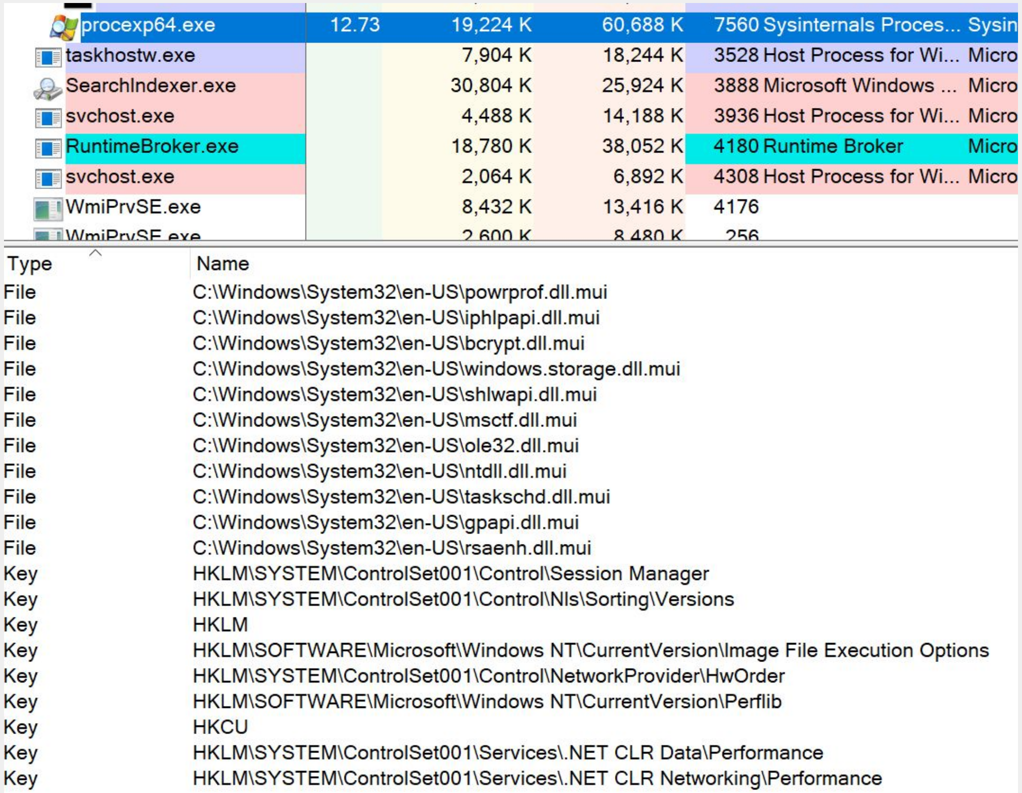
- ☑ Process
- ☑ PID (Process Identifier)
- □ User Name
- ☑ Description
- ☑ Company Name
- □ Verified Signer
- □ Version
- □ Image Path
- □ Image Type (64 vs 32-bit)
- □ Package Name
- □ DPI Awareness
- □ Protection
- □ Control Flow Guard
- □ Window Title
- □ Window Status
- □ Session
- ☑ Command Line
- □ Comment
- □ Autostart Location
- □ VirusTotal
- □ DEP Status
- □ Integrity Level
- □ Virtualized
- □ ASLR Enabled
- □ UI Access


Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Na...	Command Line
svchost.exe		3,588 K	7,660 K	1412	Host Process for Wi...	Microsoft Cor...	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted
svchost.exe	0.54	52,668 K	55,996 K	1540	Host Process for Wi...	Microsoft Cor...	C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted
SecurityHealthService.e...		4,296 K	13,520 K	1532	Windows Security H...	Microsoft Cor...	C:\WINDOWS\system32\SecurityHealthService.exe
svchost.exe		3,064 K	10,712 K	1324	Host Process for Wi...	Microsoft Cor...	C:\WINDOWS\system32\svchost.exe -k appmodel
svchost.exe		1,252 K	5,340 K	1696	Host Process for Wi...	Microsoft Cor...	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted
wlms.exe		708 K	3,056 K	1168	Windows License M...	Microsoft Cor...	C:\WINDOWS\system32\wlms\wlms.exe
svchost.exe		5,036 K	19,596 K	2064	Host Process for Wi...	Microsoft Cor...	C:\WINDOWS\system32\svchost.exe -k netsvcs
svchost.exe		1,260 K	5,012 K	2208	Host Process for Wi...	Microsoft Cor...	C:\WINDOWS\System32\svchost.exe -k LocalService
svchost.exe		4,064 K	14,196 K	2228	Host Process for Wi...	Microsoft Cor...	C:\WINDOWS\System32\svchost.exe -k NetSvcs

Process Explorer



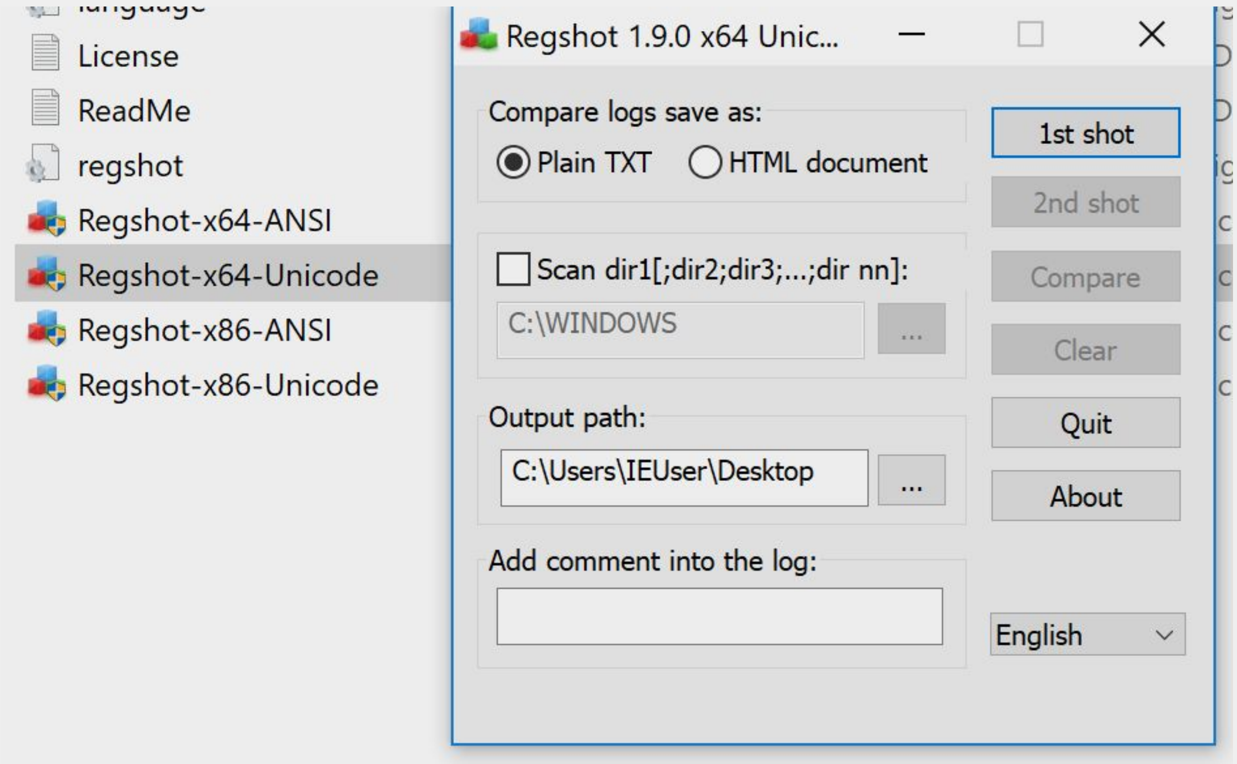


procexp64.exe	12.73	19,224 K	60,688 K	7560	Sysinternals Proces...	Sysin
taskhostw.exe		7,904 K	18,244 K	3528	Host Process for Wi...	Micro
SearchIndexer.exe		30,804 K	25,924 K	3888	Microsoft Windows ...	Micro
svchost.exe		4,488 K	14,188 K	3936	Host Process for Wi...	Micro
RuntimeBroker.exe		18,780 K	38,052 K	4180	Runtime Broker	Micro
svchost.exe		2,064 K	6,892 K	4308	Host Process for Wi...	Micro
WmiPrvSE.exe		8,432 K	13,416 K	4176		
WmiPrvSE.exe		2,600 K	8,480 K	256		

Type	Name
File	C:\Windows\System32\en-US\powrprof.dll.mui
File	C:\Windows\System32\en-US\iphlpapi.dll.mui
File	C:\Windows\System32\en-US\bcrypt.dll.mui
File	C:\Windows\System32\en-US\windows.storage.dll.mui
File	C:\Windows\System32\en-US\shlwapi.dll.mui
File	C:\Windows\System32\en-US\msctf.dll.mui
File	C:\Windows\System32\en-US\ole32.dll.mui
File	C:\Windows\System32\en-US\ntdll.dll.mui
File	C:\Windows\System32\en-US\taskschd.dll.mui
File	C:\Windows\System32\en-US\gpapi.dll.mui
File	C:\Windows\System32\en-US\rsaenh.dll.mui
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SYSTEM\ControlSet001\Control\NetworkProvider\HwOrder
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
Key	HKCU
Key	HKLM\SYSTEM\ControlSet001\Services\.NET CLR Data\Performance
Key	HKLM\SYSTEM\ControlSet001\Services\.NET CLR Networking\Performance

Registry / File Changes

RegShot



Compare logs save as:
● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:
C:\WINDOWS

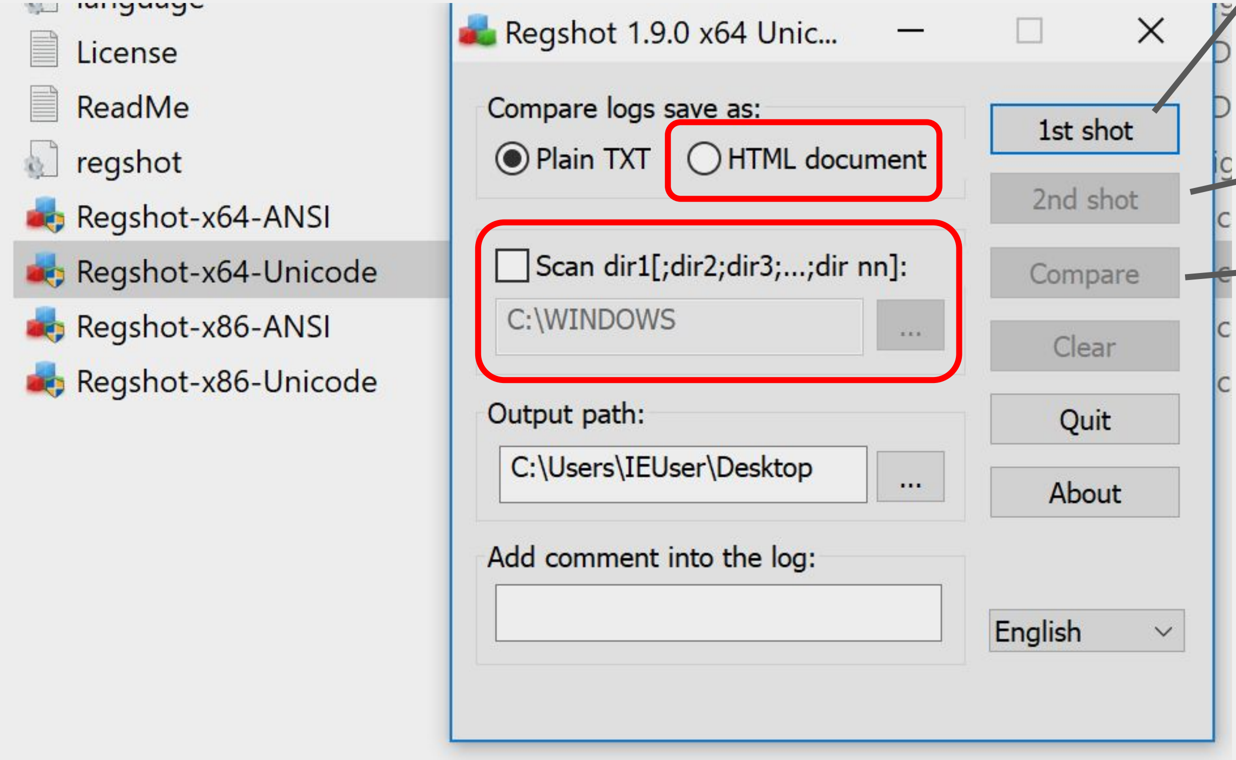
Output path:
C:\Users\IEUser\Desktop

Add comment into the log:

English

Introduction to Static Analysis → Registry / File Changes

RegShot



Regshot 1.9.0 x64 Unic...

Compare logs save as:

● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\WINDOWS

Output path:

C:\Users\IEUser\Desktop

Add comment into the log:

Click on “1st shot” before running the binary

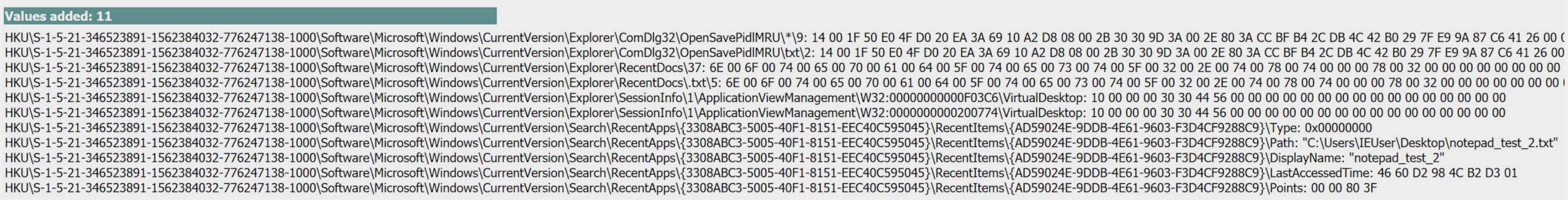
Run the binary

Click on “2nd shot”

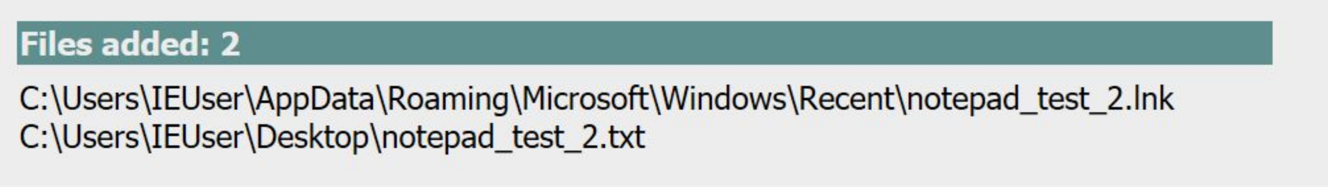
Click on “Compare”

Introduction to Static Analysis → Registry / File Changes

RegShot



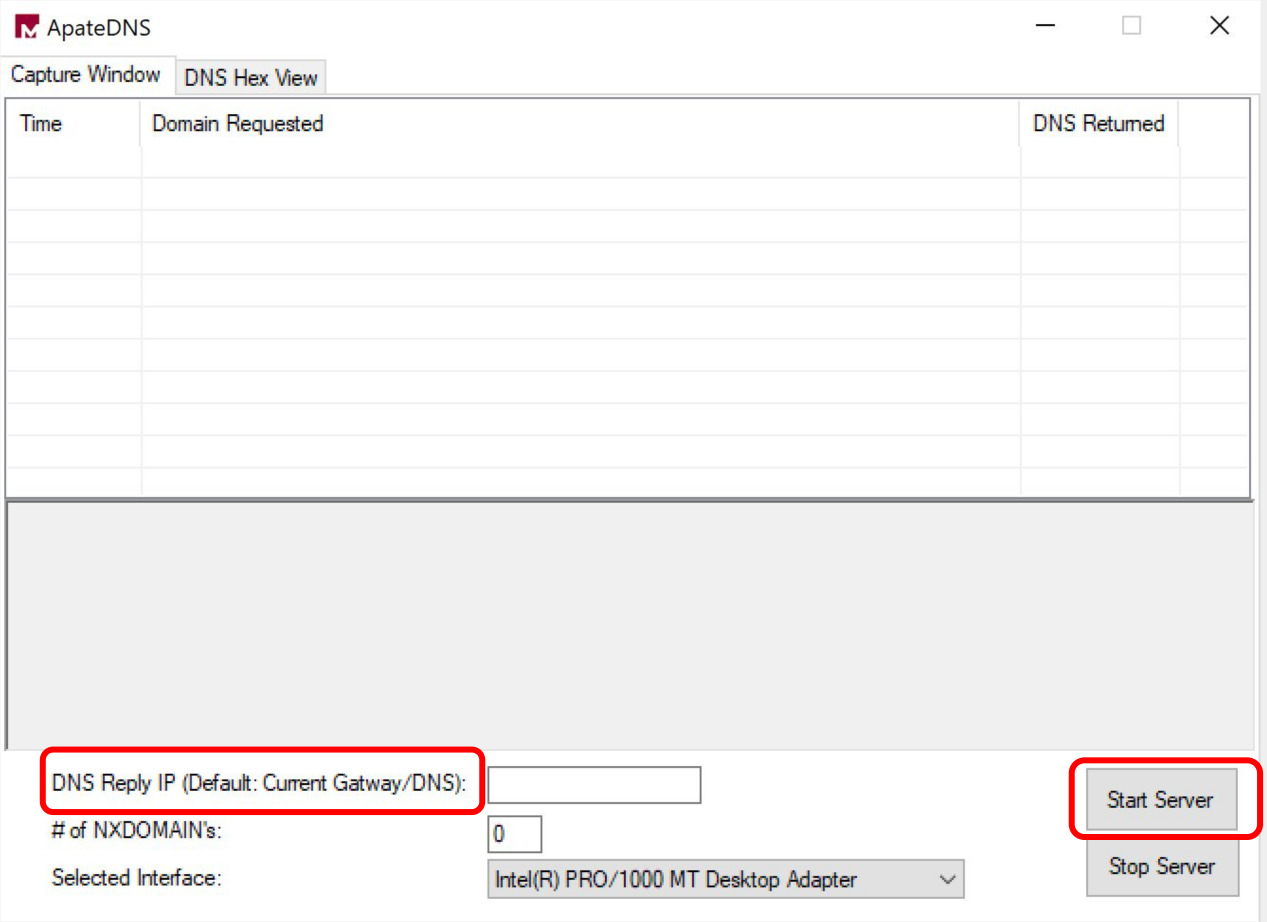
```
Values added: 11
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\*\9: 14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 3A 00 2E 80 3A CC BF B4 2C DB 4C 42 B0 29 7F E9 9A 87 C6 41 26 00
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\txt\2: 14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 3A 00 2E 80 3A CC BF B4 2C DB 4C 42 B0 29 7F E9 9A 87 C6 41 26 00
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\37: 6E 00 6F 00 74 00 65 00 70 00 61 00 64 00 5F 00 74 00 65 00 73 00 74 00 5F 00 32 00 2E 00 74 00 78 00 74 00 00 00 78 00 32 00 00 00 00 00 00 00 00
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt\5: 6E 00 6F 00 74 00 65 00 70 00 61 00 64 00 5F 00 74 00 65 00 73 00 74 00 5F 00 32 00 2E 00 74 00 78 00 74 00 00 00 78 00 32 00 00 00 00 00 00 00 00
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000F03C6\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000200774\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{3308ABC3-5005-40F1-8151-EEC40C595045}\RecentItems\{AD59024E-9DDB-4E61-9603-F3D4CF9288C9}\Type: 0x00000000
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{3308ABC3-5005-40F1-8151-EEC40C595045}\RecentItems\{AD59024E-9DDB-4E61-9603-F3D4CF9288C9}\Path: "C:\Users\IEUser\Desktop\notepad_test_2.txt"
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{3308ABC3-5005-40F1-8151-EEC40C595045}\RecentItems\{AD59024E-9DDB-4E61-9603-F3D4CF9288C9}\DisplayName: "notepad_test_2"
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{3308ABC3-5005-40F1-8151-EEC40C595045}\RecentItems\{AD59024E-9DDB-4E61-9603-F3D4CF9288C9}\LastAccessedTime: 46 60 D2 98 4C B2 D3 01
HKU\S-1-5-21-346523891-1562384032-776247138-1000\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{3308ABC3-5005-40F1-8151-EEC40C595045}\RecentItems\{AD59024E-9DDB-4E61-9603-F3D4CF9288C9}\Points: 00 00 80 3F
```



```
Files added: 2
C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\notepad_test_2.lnk
C:\Users\IEUser\Desktop\notepad_test_2.txt
```

DNS Resolution

ApateDNS

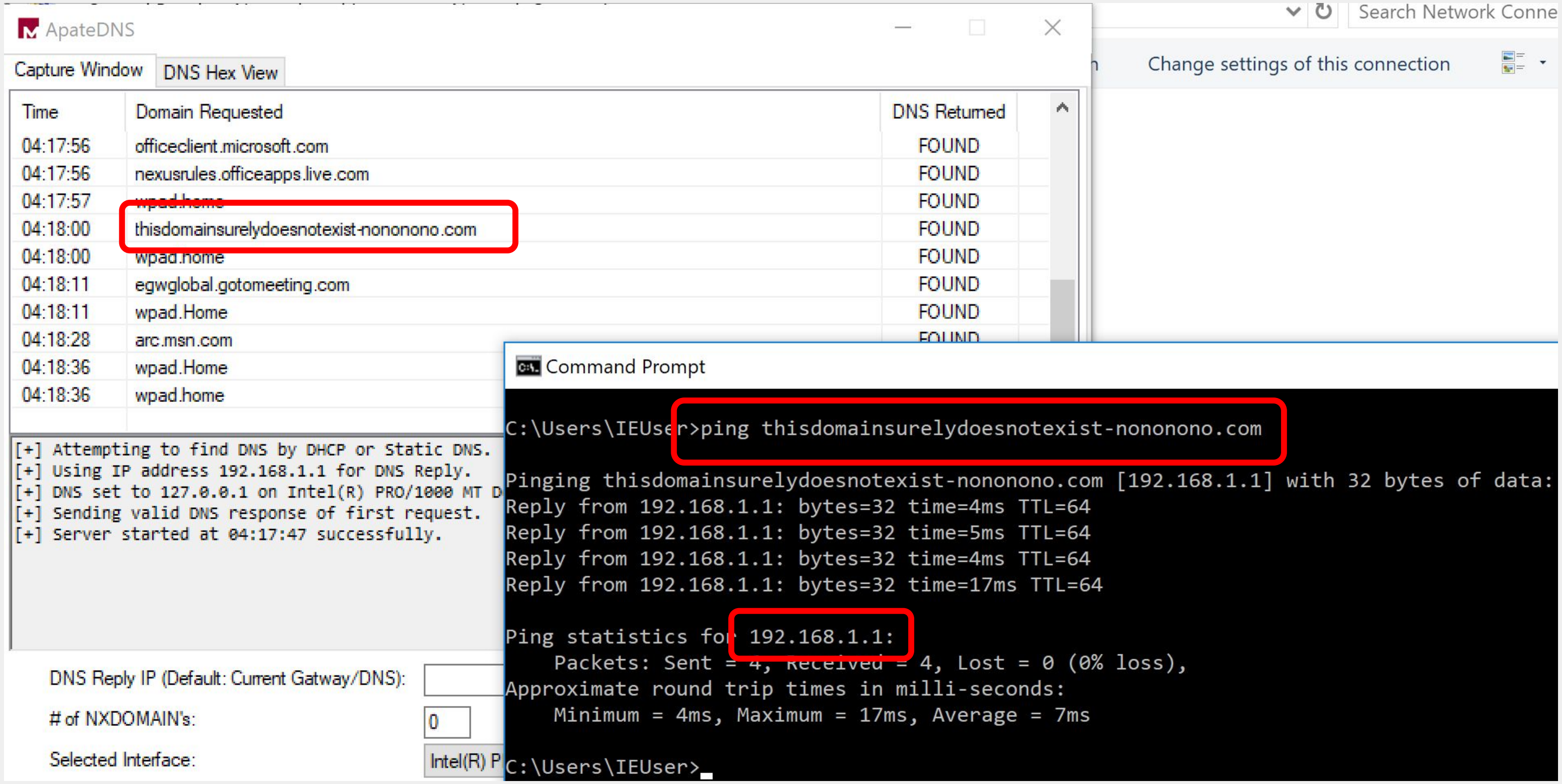


DNS Reply IP (Default: Current Gatway/DNS):

# of NXDOMAIN's: 0

Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter

ApateDNS



Time	Domain Requested	DNS Returned
04:17:56	officeclient.microsoft.com	FOUND
04:17:56	nexusrules.officeapps.live.com	FOUND
04:17:57	wpad.home	FOUND
04:18:00	thisdomainsurelydoesnotexist-nonono.com	FOUND
04:18:00	wpad.home	FOUND
04:18:11	egwglobal.gotomeeting.com	FOUND
04:18:11	wpad.Home	FOUND
04:18:28	arc.msn.com	FOUND
04:18:36	wpad.Home	
04:18:36	wpad.home	

```
[+] Attempting to find DNS by DHCP or Static DNS.
[+] Using IP address 192.168.1.1 for DNS Reply.
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT D
[+] Sending valid DNS response of first request.
[+] Server started at 04:17:47 successfully.
```

DNS Reply IP (Default: Current Gatway/DNS):

# of NXDOMAIN's: 0

Selected Interface: Intel(R) P

```
C:\Users\IEUser>ping thisdomainsurelydoesnotexist-nonono.com

Pinging thisdomainsurelydoesnotexist-nonono.com [192.168.1.1] with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=17ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 17ms, Average = 7ms

C:\Users\IEUser>_
```

Extra Ball: InetSim (Internet Services Simulation Suite)

- http://www.inetsim.org/index.html

With these tool you can simulate many services such as DNS, HTTP/S, FTP, etc.

Written in Perl, it needs to be executed from a Linux system.

The idea is to execute it in a Linux system with which you VM can communicate with. Then set the DNS server of the VM to the IP of the system running InetSim.

Extra Ball: InetSim (Internet Services Simulation Suite)

- Install InetSim in Ubuntu:

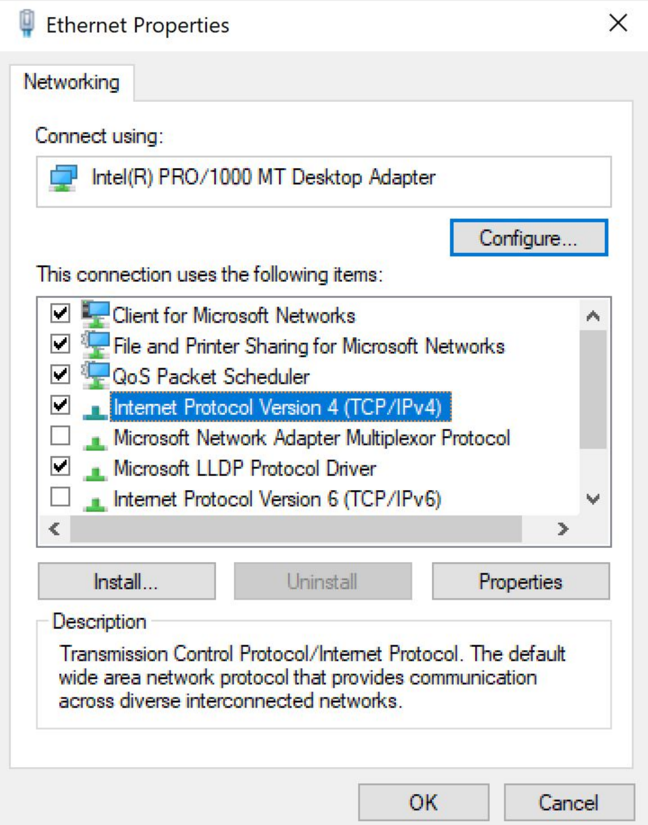
1. sudo apt-get install libnet-server-perl libnet-dns-perl libipc-shareable-perl libdigest-sha-perl libio-socket-ssl-perl
2. sudo groupadd inetsim
3. cd <inetsim_directory>

In <inetsim_directory>/conf/inetsim.conf, uncomment the following lines and set their values to the Ubuntu system private IP.

```
service_bind_address    192.168.1.34
dns_default_ip          192.168.1.34
```

1. ./setup.sh
2. ./inetsim

Extra Ball: InetSim (Internet Services Simulation Suite)



Ethernet Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

Configure...

This connection uses the following items:

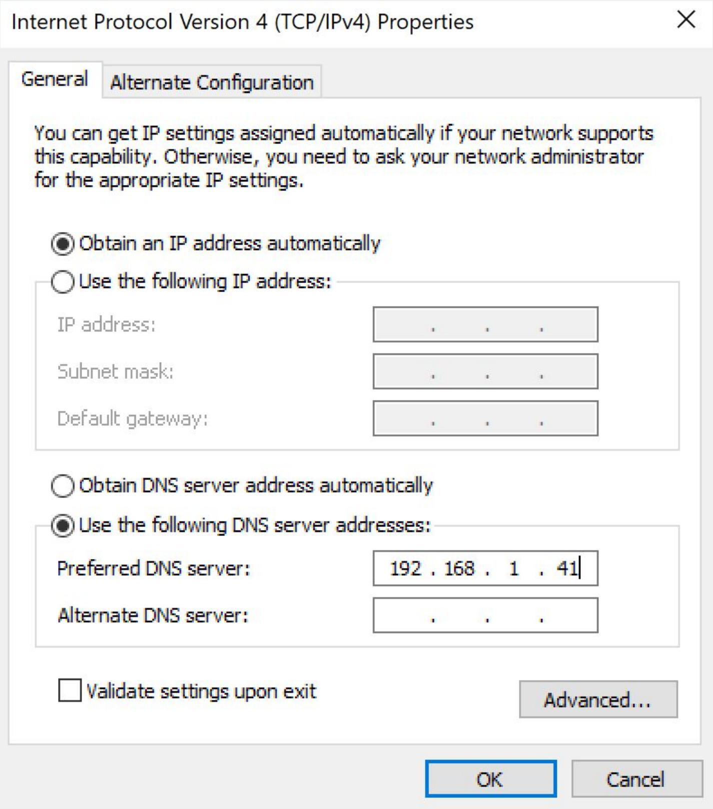
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- □ Internet Protocol Version 6 (TCP/IPv6)

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 41

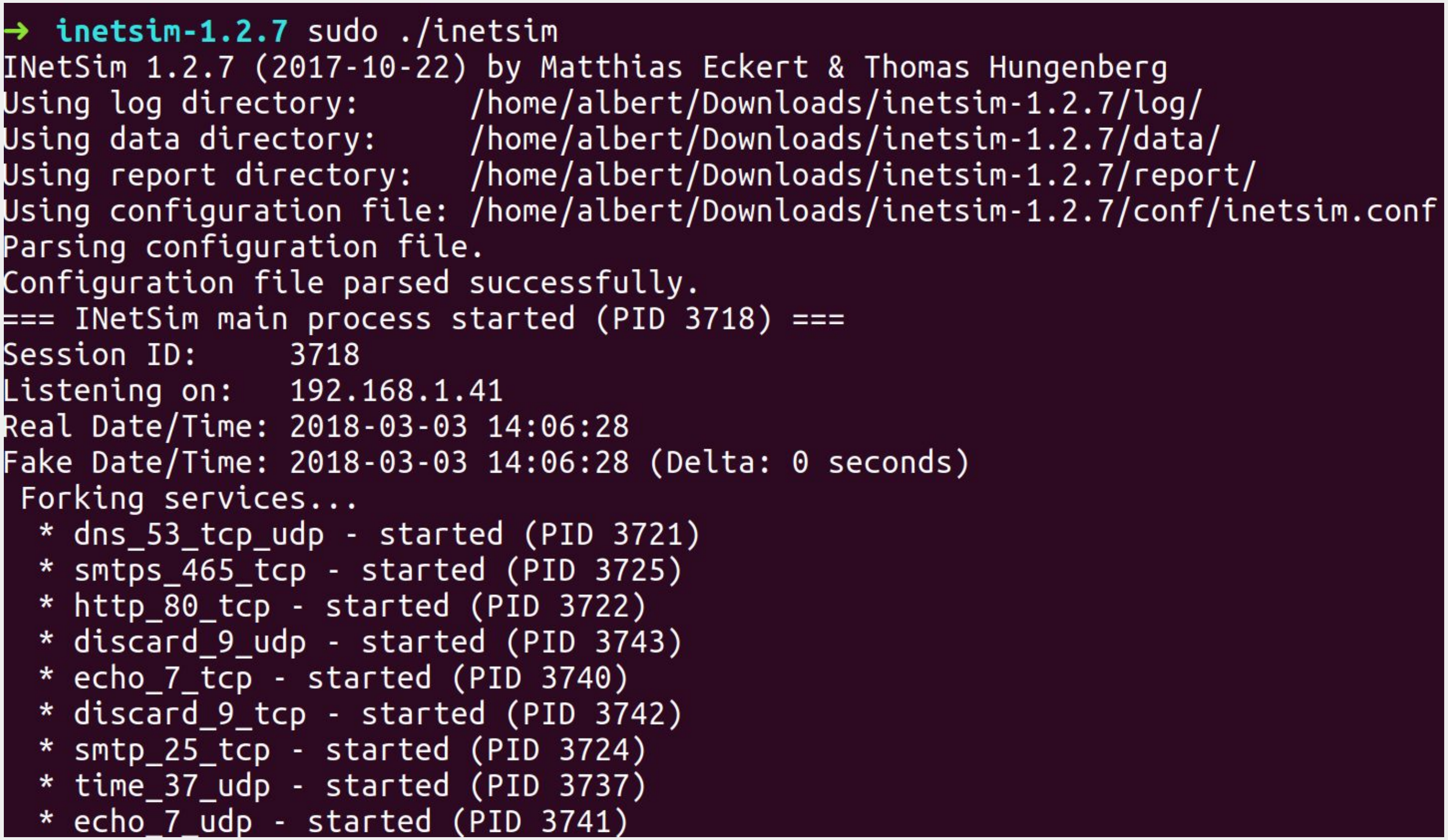
Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

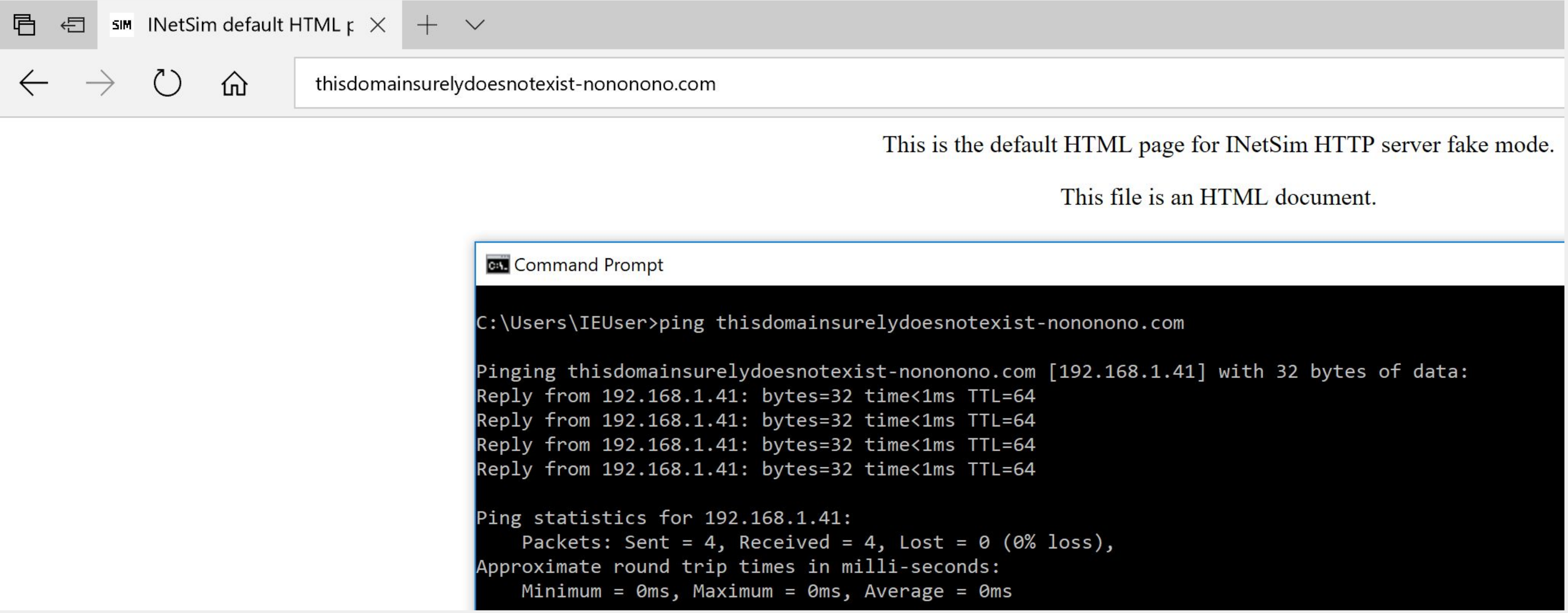
OK Cancel

Extra Ball: InetSim (Internet Services Simulation Suite)



```
➜  inetsim-1.2.7 sudo ./inetsim
INetSim 1.2.7 (2017-10-22) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /home/albert/Downloads/inetsim-1.2.7/log/
Using data directory:     /home/albert/Downloads/inetsim-1.2.7/data/
Using report directory:   /home/albert/Downloads/inetsim-1.2.7/report/
Using configuration file: /home/albert/Downloads/inetsim-1.2.7/conf/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 3718) ===
Session ID:     3718
Listening on:   192.168.1.41
Real Date/Time: 2018-03-03 14:06:28
Fake Date/Time: 2018-03-03 14:06:28 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 3721)
  * smtps_465_tcp - started (PID 3725)
  * http_80_tcp - started (PID 3722)
  * discard_9_udp - started (PID 3743)
  * echo_7_tcp - started (PID 3740)
  * discard_9_tcp - started (PID 3742)
  * smtp_25_tcp - started (PID 3724)
  * time_37_udp - started (PID 3737)
  * echo_7_udp - started (PID 3741)
```

Extra Ball: InetSim (Internet Services Simulation Suite)



thisdomainsurelydoesnotexist-nonono.com

This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

Command Prompt

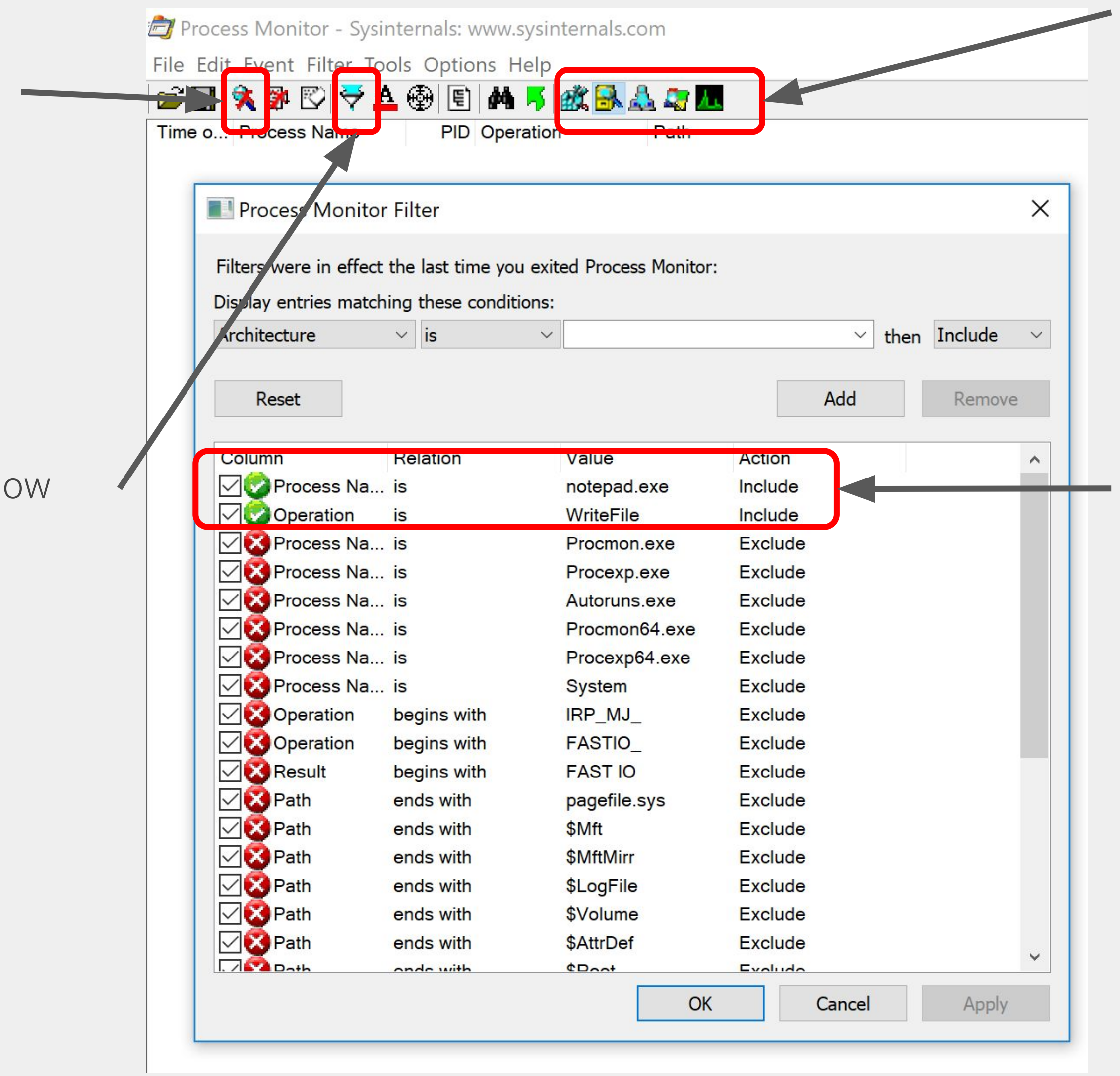
```
C:\Users\IEUser>ping thisdomainsurelydoesnotexist-nonono.com

Pinging thisdomainsurelydoesnotexist-nonono.com [192.168.1.41] with 32 bytes of data:
Reply from 192.168.1.41: bytes=32 time<1ms TTL=64
Reply from 192.168.1.41: bytes=32 time<1ms TTL=64
Reply from 192.168.1.41: bytes=32 time<1ms TTL=64
Reply from 192.168.1.41: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.41:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Monitor All The Things

Process Monitor


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path
Process Monitor Filter
Reset
Add
Remove
OK
Cancel
Apply

Filters were in effect the last time you exited Process Monitor:

Display entries matching these conditions:

Architecture | is | | then Include

Column	Relation	Value	Action
☑ ✓ Process Na...	is	notepad.exe	Include
☑ ✓ Operation	is	WriteFile	Include
☑ ✗ Process Na...	is	Procmon.exe	Exclude
☑ ✗ Process Na...	is	Procexp.exe	Exclude
☑ ✗ Process Na...	is	Autoruns.exe	Exclude
☑ ✗ Process Na...	is	Procmon64.exe	Exclude
☑ ✗ Process Na...	is	Procexp64.exe	Exclude
☑ ✗ Process Na...	is	System	Exclude
☑ ✗ Operation	begins with	IRP_MJ_	Exclude
☑ ✗ Operation	begins with	FASTIO_	Exclude
☑ ✗ Result	begins with	FAST IO	Exclude
☑ ✗ Path	ends with	pagefile.sys	Exclude
☑ ✗ Path	ends with	$Mft	Exclude
☑ ✗ Path	ends with	$MftMirr	Exclude
☑ ✗ Path	ends with	$LogFile	Exclude
☑ ✗ Path	ends with	$Volume	Exclude
☑ ✗ Path	ends with	$AttrDef	Exclude
☑ ✗ Path	ends with	$Root	Exclude

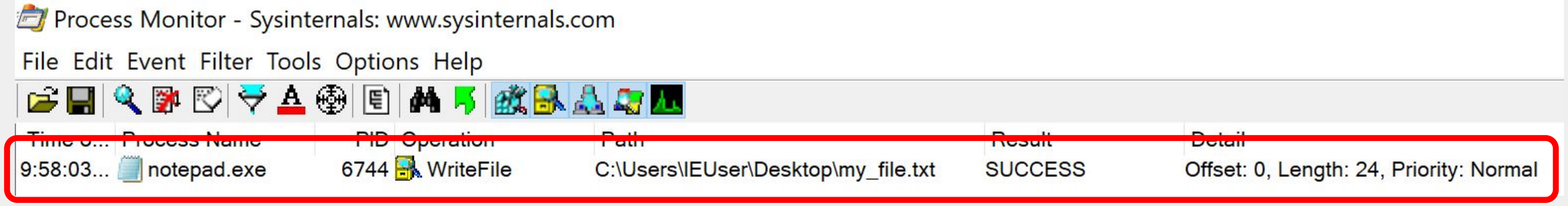
Start monitoring

Filter by event types

Open filters window

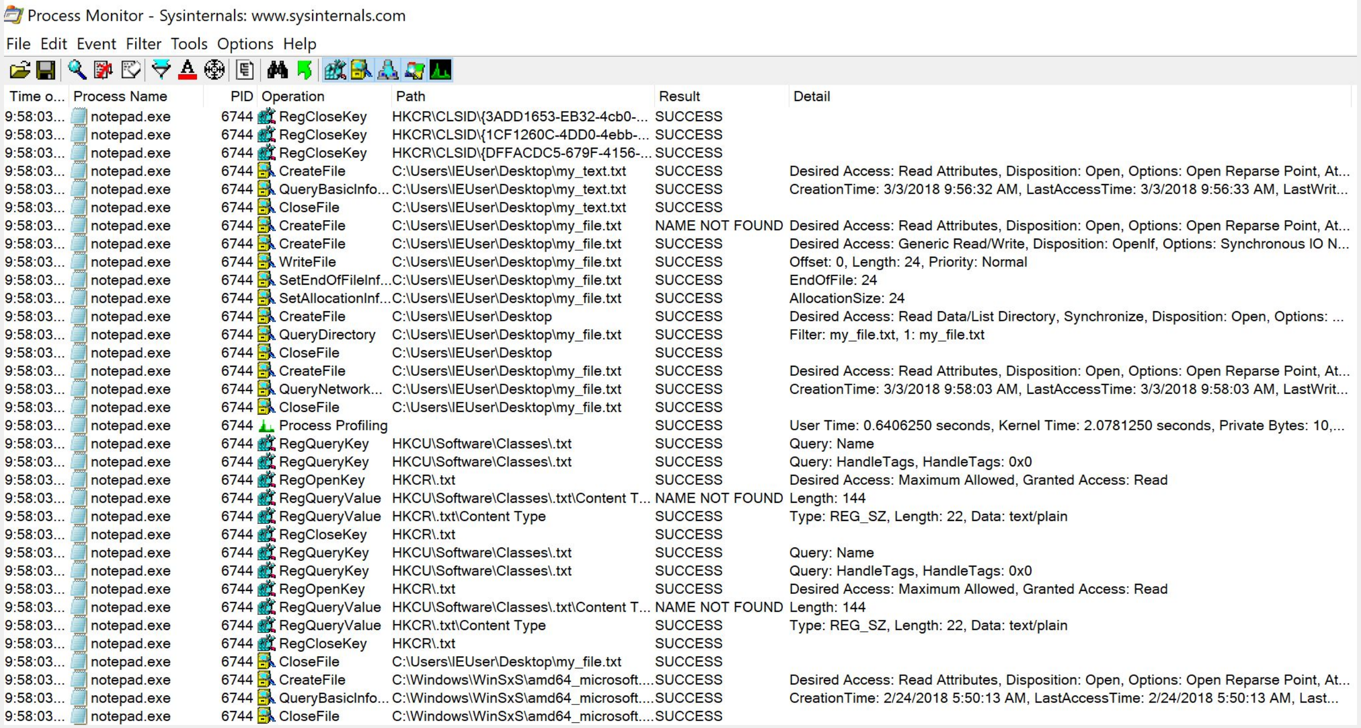
Custom filters

Process Monitor



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
9:58:03...	notepad.exe	6744	WriteFile	C:\Users\IEUser\Desktop\my_file.txt	SUCCESS	Offset: 0, Length: 24, Priority: Normal



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
9:58:03...	notepad.exe	6744	RegCloseKey	HKCR\CLSID\{3ADD1653-EB32-4cb0-...	SUCCESS	
9:58:03...	notepad.exe	6744	RegCloseKey	HKCR\CLSID\{1CF1260C-4DD0-4ebb-...	SUCCESS	
9:58:03...	notepad.exe	6744	RegCloseKey	HKCR\CLSID\{DFFACDC5-679F-4156-...	SUCCESS	
9:58:03...	notepad.exe	6744	CreateFile	C:\Users\IEUser\Desktop\my_text.txt	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, At...
9:58:03...	notepad.exe	6744	QueryBasicInfo...	C:\Users\IEUser\Desktop\my_text.txt	SUCCESS	CreationTime: 3/3/2018 9:56:32 AM, LastAccessTime: 3/3/2018 9:56:33 AM, LastWrit...
9:58:03...	notepad.exe	6744	CloseFile	C:\Users\IEUser\Desktop\my_text.txt	SUCCESS	
9:58:03...	notepad.exe	6744	CreateFile	C:\Users\IEUser\Desktop\my_file.txt	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, At...
9:58:03...	notepad.exe	6744	CreateFile	C:\Users\IEUser\Desktop\my_file.txt	SUCCESS	Desired Access: Generic Read/Write, Disposition: OpenIf, Options: Synchronous IO N...
9:58:03...	notepad.exe	6744	WriteFile	C:\Users\IEUser\Desktop\my_file.txt	SUCCESS	Offset: 0, Length: 24, Priority: Normal
9:58:03...	notepad.exe	6744	SetEndOfFileInf...	C:\Users\IEUser\Desktop\my_file.txt	SUCCESS	EndOfFile: 24
9:58:03...	notepad.exe	6744	SetAllocationInf...	C:\Users\IEUser\Desktop\my_file.txt	SUCCESS	AllocationSize: 24
9:58:03...	notepad.exe	6744	CreateFile	C:\Users\IEUser\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: ...
9:58:03...	notepad.exe	6744	QueryDirectory	C:\Users\IEUser\Desktop\my_file.txt	SUCCESS	Filter: my_file.txt, 1: my_file.txt
9:58:03...	notepad.exe	6744	CloseFile	C:\Users\IEUser\Desktop	SUCCESS	
9:58:03...	notepad.exe	6744	CreateFile	C:\Users\IEUser\Desktop\my_file.txt	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, At...
9:58:03...	notepad.exe	6744	QueryNetwork...	C:\Users\IEUser\Desktop\my_file.txt	SUCCESS	CreationTime: 3/3/2018 9:58:03 AM, LastAccessTime: 3/3/2018 9:58:03 AM, LastWrit...
9:58:03...	notepad.exe	6744	CloseFile	C:\Users\IEUser\Desktop\my_file.txt	SUCCESS	
9:58:03...	notepad.exe	6744	Process Profiling		SUCCESS	User Time: 0.6406250 seconds, Kernel Time: 2.0781250 seconds, Private Bytes: 10,...
9:58:03...	notepad.exe	6744	RegQueryKey	HKCU\Software\Classes\.txt	SUCCESS	Query: Name
9:58:03...	notepad.exe	6744	RegQueryKey	HKCU\Software\Classes\.txt	SUCCESS	Query: HandleTags, HandleTags: 0x0
9:58:03...	notepad.exe	6744	RegOpenKey	HKCR\.txt	SUCCESS	Desired Access: Maximum Allowed, Granted Access: Read
9:58:03...	notepad.exe	6744	RegQueryValue	HKCU\Software\Classes\.txt\Content T...	NAME NOT FOUND	Length: 144
9:58:03...	notepad.exe	6744	RegQueryValue	HKCR\.txt\Content Type	SUCCESS	Type: REG_SZ, Length: 22, Data: text/plain
9:58:03...	notepad.exe	6744	RegCloseKey	HKCR\.txt	SUCCESS	
9:58:03...	notepad.exe	6744	RegQueryKey	HKCU\Software\Classes\.txt	SUCCESS	Query: Name
9:58:03...	notepad.exe	6744	RegQueryKey	HKCU\Software\Classes\.txt	SUCCESS	Query: HandleTags, HandleTags: 0x0
9:58:03...	notepad.exe	6744	RegOpenKey	HKCR\.txt	SUCCESS	Desired Access: Maximum Allowed, Granted Access: Read
9:58:03...	notepad.exe	6744	RegQueryValue	HKCU\Software\Classes\.txt\Content T...	NAME NOT FOUND	Length: 144
9:58:03...	notepad.exe	6744	RegQueryValue	HKCR\.txt\Content Type	SUCCESS	Type: REG_SZ, Length: 22, Data: text/plain
9:58:03...	notepad.exe	6744	RegCloseKey	HKCR\.txt	SUCCESS	
9:58:03...	notepad.exe	6744	CloseFile	C:\Users\IEUser\Desktop\my_file.txt	SUCCESS	
9:58:03...	notepad.exe	6744	CreateFile	C:\Windows\WinSxS\amd64_microsoft....	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, At...
9:58:03...	notepad.exe	6744	QueryBasicInfo...	C:\Windows\WinSxS\amd64_microsoft....	SUCCESS	CreationTime: 2/24/2018 5:50:13 AM, LastAccessTime: 2/24/2018 5:50:13 AM, Last...
9:58:03...	notepad.exe	6744	CloseFile	C:\Windows\WinSxS\amd64_microsoft....	SUCCESS	

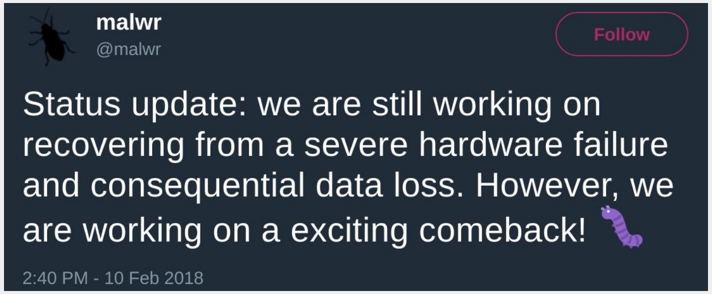
Ready to Use Solutions

Introduction to Static Analysis → Ready to Use Solutions

There are some built-in ready to use sandboxes that will do the analysis for you.

- Hybrid Analysis

- malwr.com



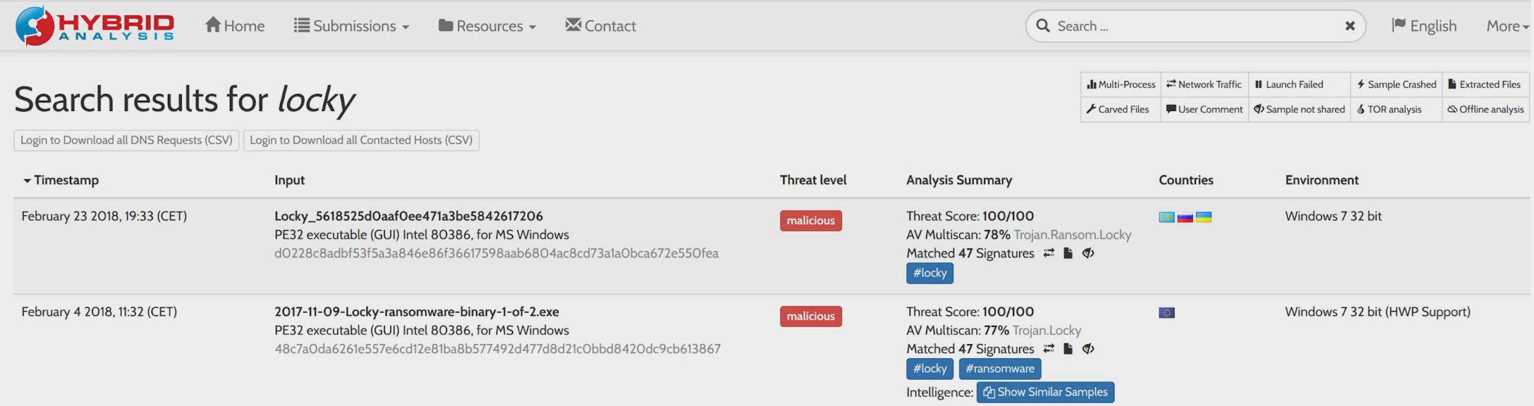
malwr
@malwr

Follow

Status update: we are still working on recovering from a severe hardware failure and consequential data loss. However, we are working on a exciting comeback! 🐛

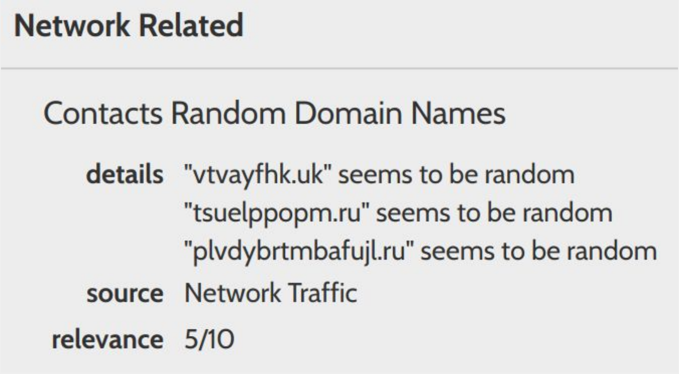
2:40 PM - 10 Feb 2018

Hybrid Analysis



Search results for *locky*

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment
February 23 2018, 19:33 (CET)	**Locky_5618525d0aaf0ee471a3be5842617206** PE32 executable (GUI) Intel 80386, for MS Windows d0228c8adbf53f5a3a846e86f36617598aab6804ac8cd73a1a0bca672e550fea	malicious	Threat Score: **100/100** AV Multiscan: **78%** Trojan.Ransom.Locky Matched **47** Signatures #locky		Windows 7 32 bit
February 4 2018, 11:32 (CET)	**2017-11-09-Locky-ransomware-binary-1-of-2.exe** PE32 executable (GUI) Intel 80386, for MS Windows 48c7a0da6261e557e6cd12e81ba8b577492d477d8d21c0bbd8420dc9cb613867	malicious	Threat Score: **100/100** AV Multiscan: **77%** Trojan.Locky Matched **47** Signatures #locky #ransomware Intelligence: Show Similar Samples		Windows 7 32 bit (HWP Support)



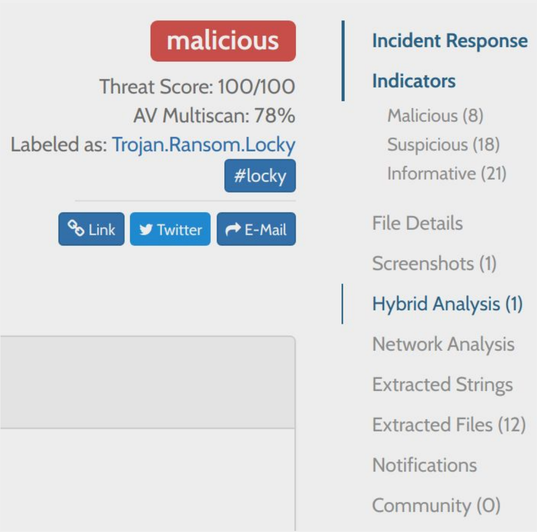
Network Related

Contacts Random Domain Names

details "vtvayfhk.uk" seems to be random
"tsuelppopm.ru" seems to be random
"plvdybrtmbafujl.ru" seems to be random

source Network Traffic

relevance 5/10



malicious

Threat Score: 100/100
AV Multiscan: 78%
Labeled as: Trojan.Ransom.Locky
#locky

~~Home~~Classwork

~~Home~~Classwork

Let’s analyze the following samples. What do they do?

- Lab03_01.exe

- second_mine.exe

Bibliography

Introduction to Static Analysis → Bibliography

- Installing and Configuring InetSim
- InetSim installation of Ubuntu 12.10