

## LAB 3: Basic Dynamic Techniques

**Course Name:** Malware Analysis and Reverse Engineering (IAM302)

**Student Name:** Nguyễn Trần Vinh – SE160258

**Instructor Name:** Mai Hoàng Đình

**Lab Due Date:** 14/1/2023

### Purpose

You will practice the techniques in chapter 3.

This project follows Lab 3-1 in the textbook. There are more detailed solutions in the back of the book

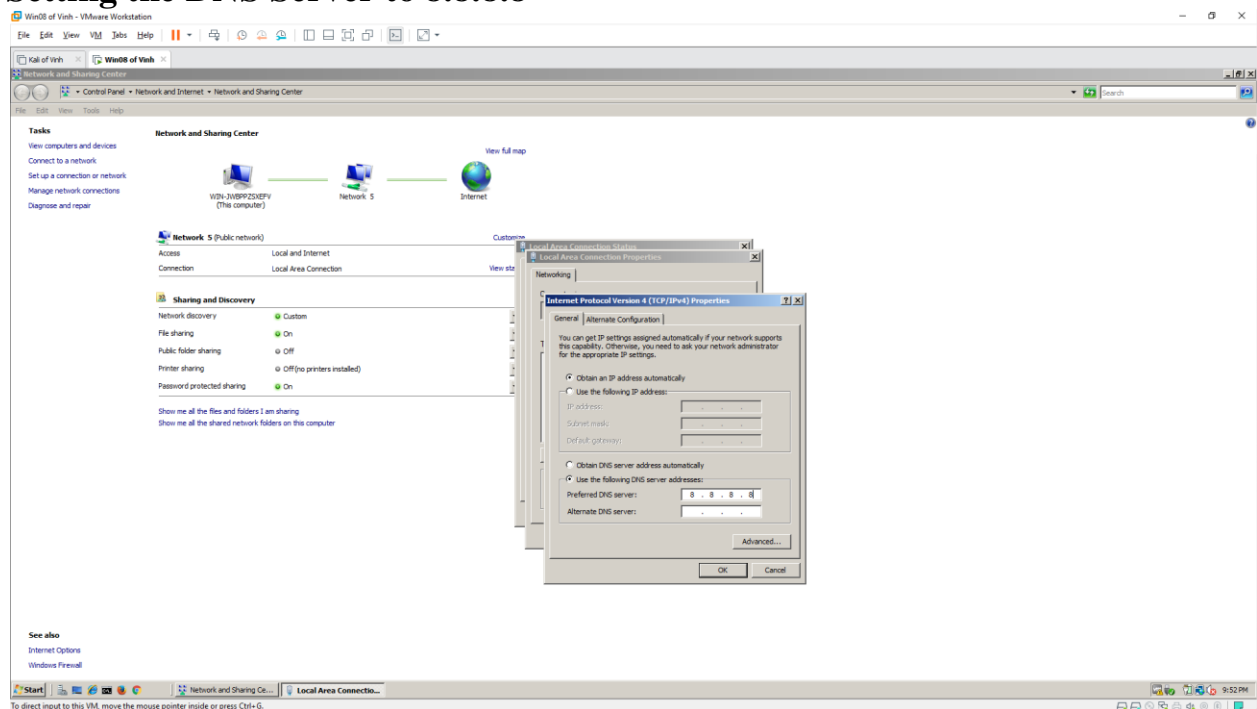
What you need:

- A Windows 2008 Server virtual machine with a Kali virtual machine running INetSim, which you prepared in the previous project.

**NOTE: Windows 7 will not work for this project!**

- Recommended: the textbook: "Practical Malware Analysis"

### Setting the DNS Server to 8.8.8.8



### Using PEvent



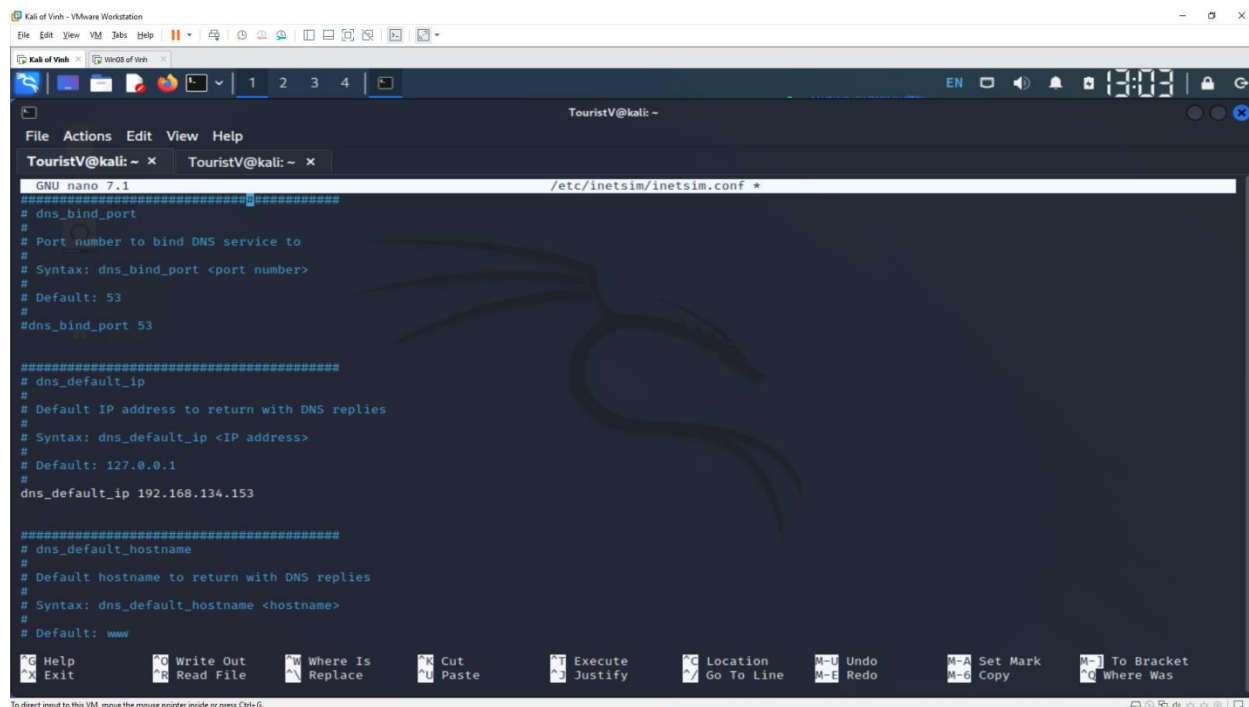
```
Kali of Vinh - VMware Workstation
File Edit View VM Tools Help
Kali of Vinh
1 2 3 4
EN 13:01
TouristV@kali: ~
File Actions Edit View Help
(TouristV@kali)-[~]
└─$ dhclient -v
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

can't create /var/lib/dhcp/dhclient.leases: Permission denied
RTNETLINK answers: Operation not permitted
RTNETLINK answers: Operation not permitted
Open a socket for LPF: Operation not permitted

If you think you have received this message due to a bug rather
than a configuration issue please read the section on submitting
bugs on either our web page at www.isc.org or in the README file
before submitting a bug. These pages explain the proper
process and the information we find helpful for debugging.

exiting.
(TouristV@kali)-[~]
└─$ ifconfig -i :80
(TouristV@kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:65:8a:b0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.123/24 brd 192.168.122.255 scope global dynamic noprefixroute eth0
        valid_lft 1591sec preferred_lft 1591sec
    inet6 fe80::8788:6ffa:9029:c782/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
```

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

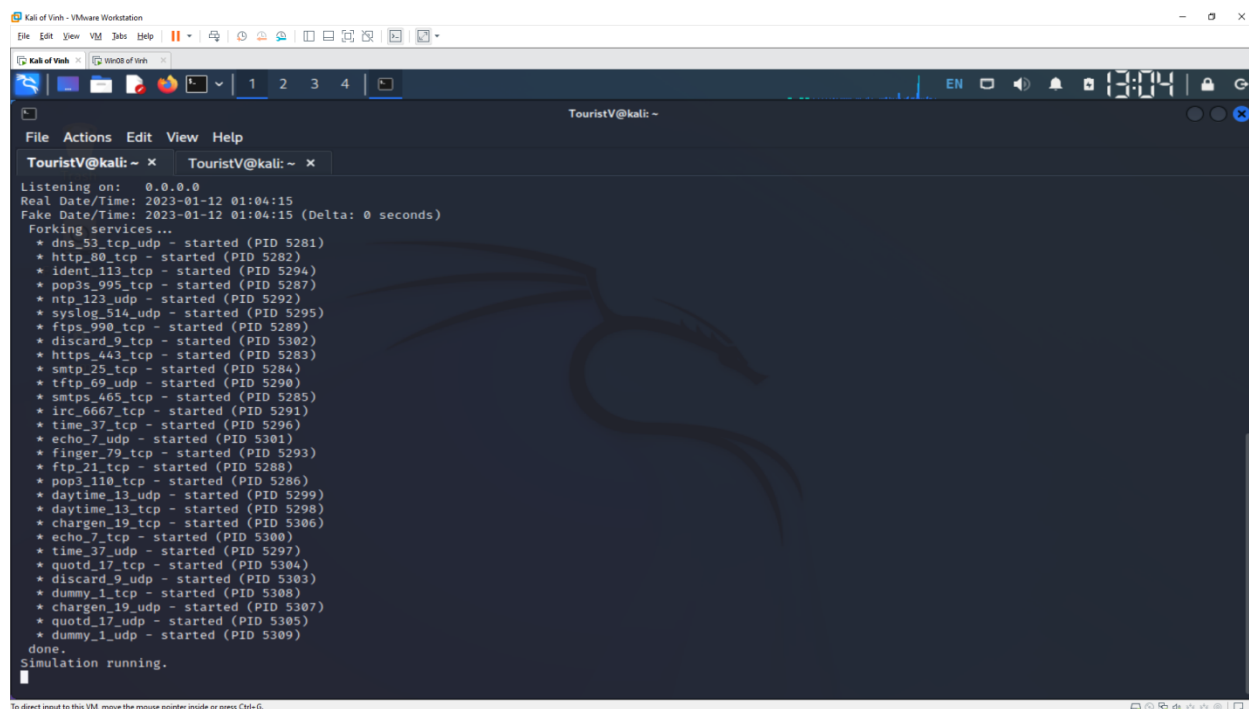


```
GNU nano 7.1 /etc/inetsim/inetsim.conf
#####
# dns_bind_port
#
# Port number to bind DNS service to
#
# Syntax: dns_bind_port <port number>
#
# Default: 53
#dns_bind_port 53

#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip 192.168.134.153

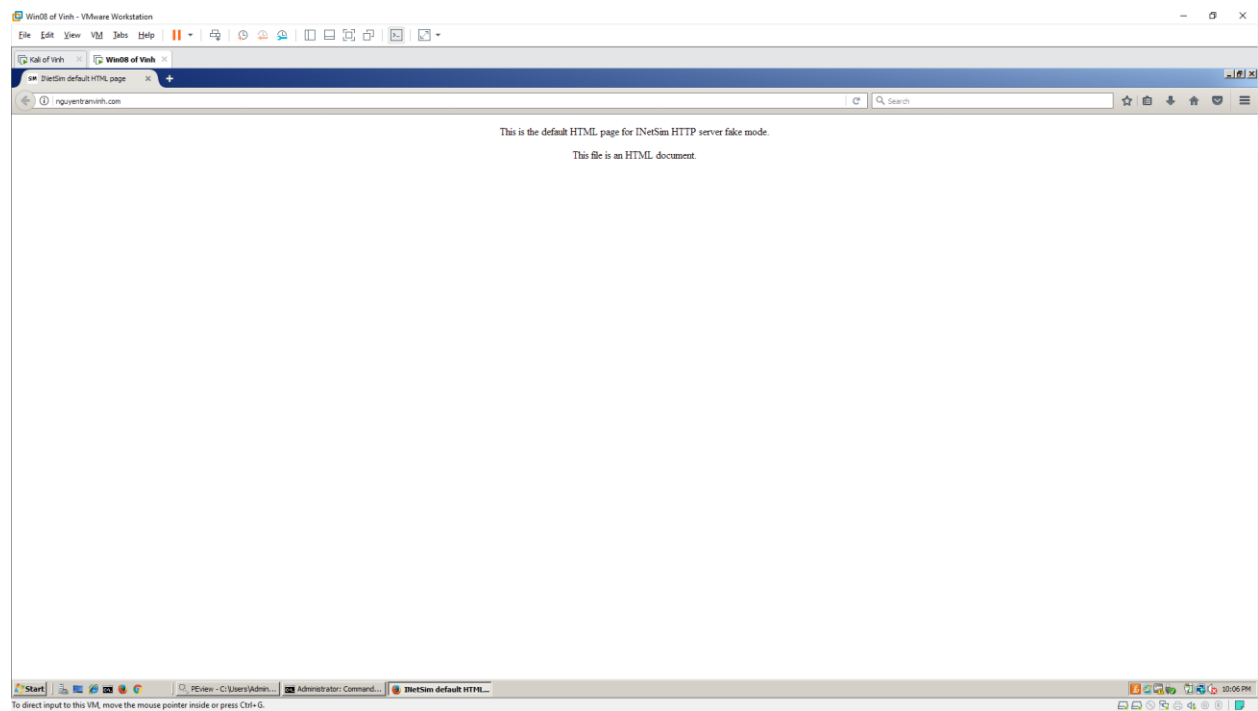
#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www

Help      Write Out  Where Is  Cut       Execute   Location  M-U      M-A      M-]
Exit      Read File  Replace  Paste     Justify   Go To Line Undo      Copy     To Bracket
Where Was
```

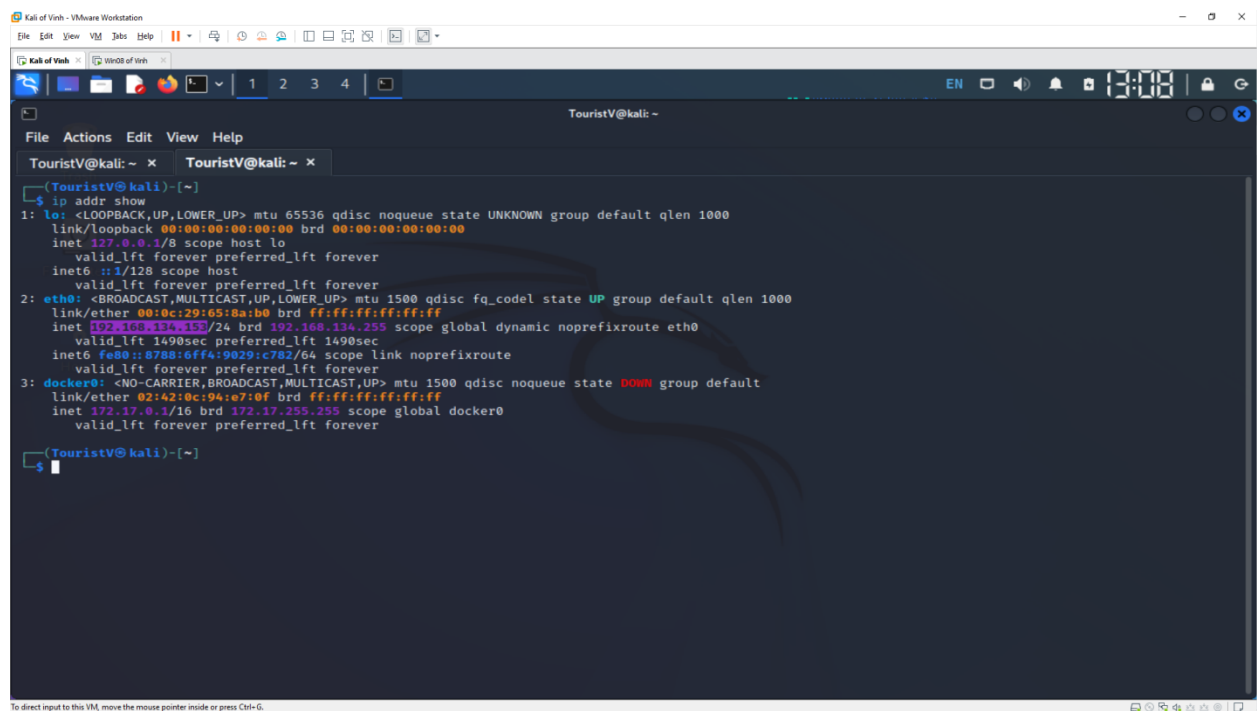
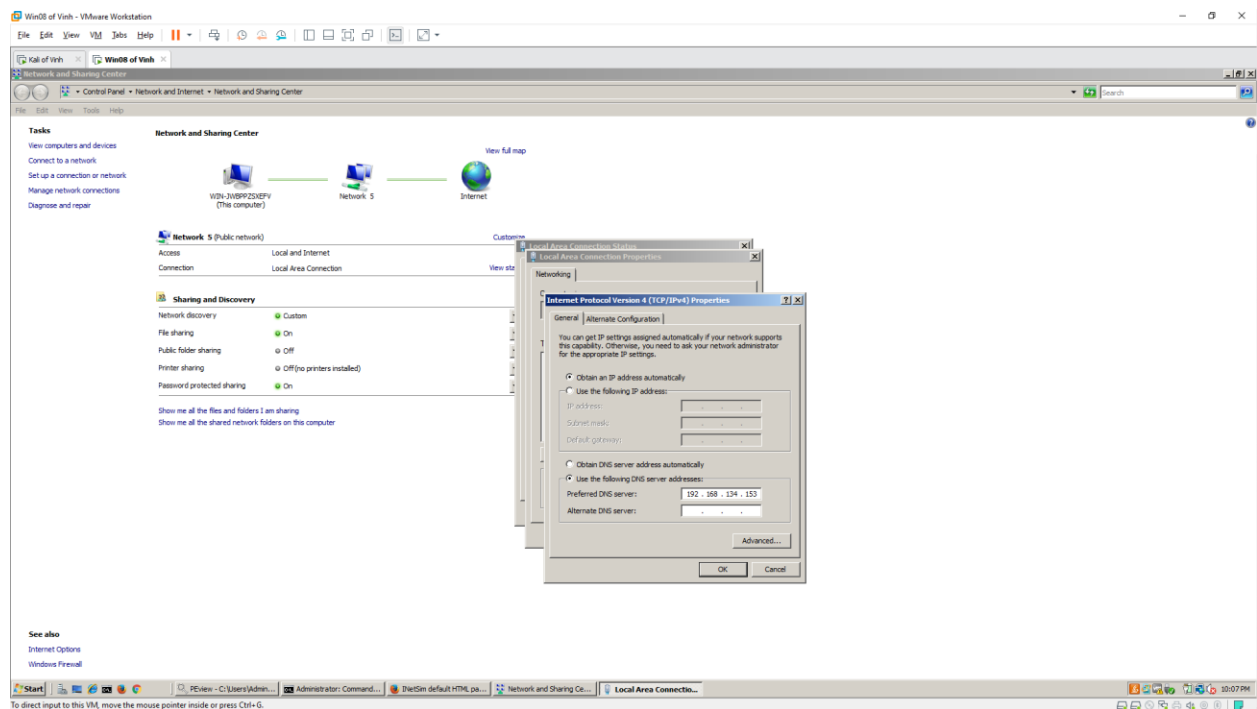


```
Listening on:  0.0.0.0
Real Date/Time: 2023-01-12 01:04:15
Fake Date/Time: 2023-01-12 01:04:15 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 5281)
* http_80_tcp - started (PID 5282)
* ident_113_tcp - started (PID 5294)
* pop3s_995_tcp - started (PID 5287)
* ntp_123_udp - started (PID 5292)
* syslog_514_udp - started (PID 5295)
* ftps_990_tcp - started (PID 5289)
* discard_9_tcp - started (PID 5302)
* https_443_tcp - started (PID 5283)
* smtp_25_tcp - started (PID 5284)
* tftp_69_udp - started (PID 5290)
* smtps_465_tcp - started (PID 5285)
* irc_6667_tcp - started (PID 5291)
* time_37_tcp - started (PID 5296)
* echo_7_udp - started (PID 5301)
* finger_79_tcp - started (PID 5293)
* ftp_21_tcp - started (PID 5280)
* pop3_110_tcp - started (PID 5286)
* daytime_13_udp - started (PID 5299)
* daytime_13_tcp - started (PID 5298)
* chargen_19_tcp - started (PID 5306)
* echo_7_tcp - started (PID 5300)
* time_37_udp - started (PID 5297)
* quotd_17_tcp - started (PID 5304)
* discard_9_udp - started (PID 5303)
* dummy_1_tcp - started (PID 5308)
* chargen_19_udp - started (PID 5307)
* quotd_17_udp - started (PID 5305)
* dummy_1_udp - started (PID 5309)
done.
Simulation running.
```

- Windows Machine



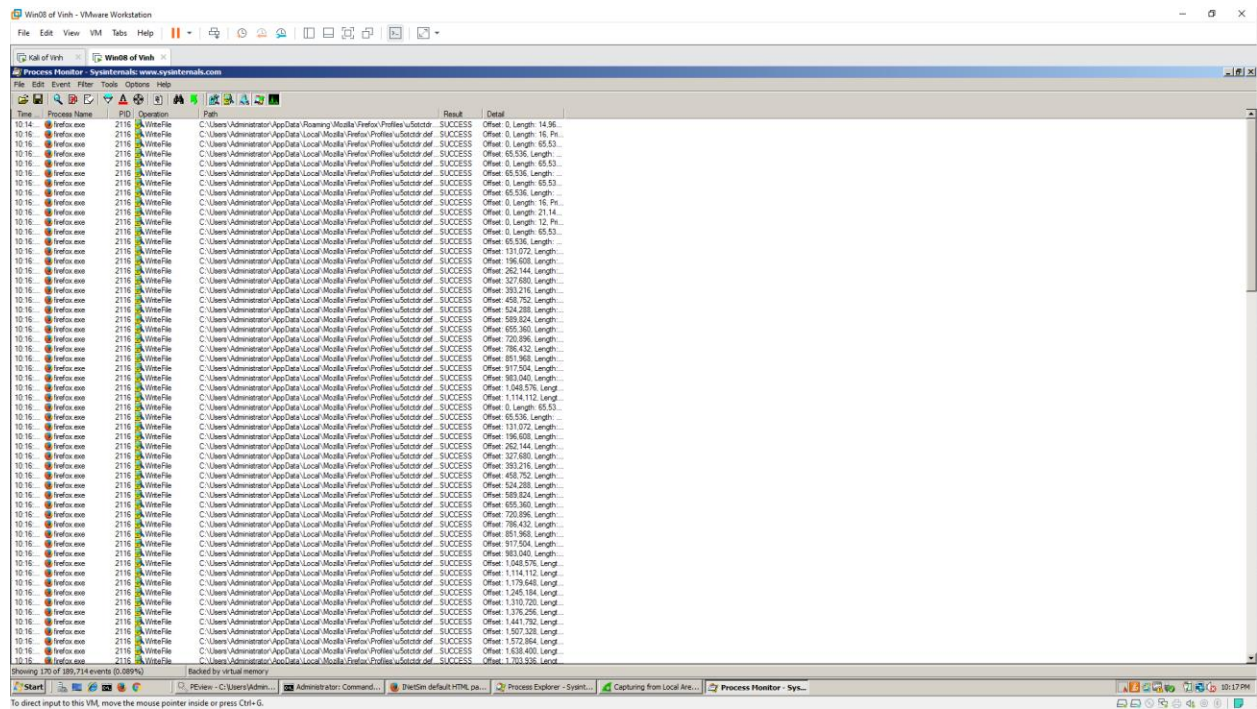
## 2. Setting the DNS Server



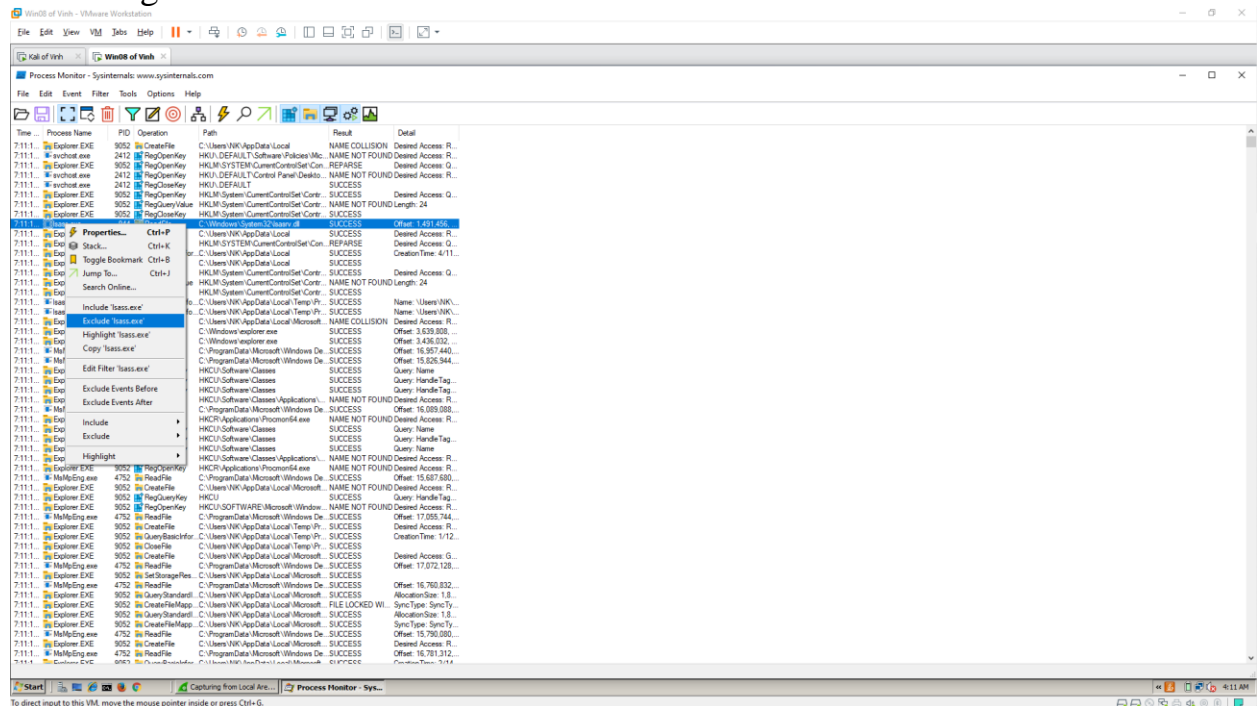
### 3. Run Process Explorer







# Excluding Harmless Processes





Win10 of Vm - VMware Workstation

File Edit View VM Tools Help

Process Monitor - Sysinternals www.sysinternals.com

File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
7111..	Explorer.exe	9052	CreateFile	C:\Users\NVR\AppData\Local\...	NAME COLLISION	Desired Access: R...
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT\Software\Policies\Mc...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPAIRER	Desired Access: Q...
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT\Control Panel\Desktop...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT	SUCCESS	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	Desired Access: Q...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	NAME NOT FOUND Length: 24	
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	Offset: 1,481,456
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR\AppData\Local\...	SUCCESS	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPAIRER	Desired Access: Q...
7111..	svchost.exe	9052	QueryBatchInfo	C:\Users\NVR\AppData\Local\...	SUCCESS	CreationTime: 4/11...
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR\AppData\Local\...	SUCCESS	
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	Desired Access: Q...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	NAME NOT FOUND Length: 24	
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	
7111..	svchost.exe	9052	RegOpenKey	C:\Users\NVR\AppData\Local\Temp\Pr...	SUCCESS	Name: Users\NVR...
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR\AppData\Local\Temp\Pr...	NAME COLLISION	Desired Access: R...
7111..	svchost.exe	9052	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 3,639,808...
7111..	svchost.exe	9052	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 3,438,532...
7111..	svchost.exe	4752	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 16,957,440...
7111..	svchost.exe	4752	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15,826,344...
7111..	svchost.exe	9052	RegOpenKey	HCU\Software\Classes	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU\Software\Classes	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	4752	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 16,089,088...
7111..	svchost.exe	9052	RegOpenKey	HCU\Applications\Photoresizer.exe	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HCU\Software\Classes	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU\Software\Classes	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU\Software\Classes	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HCU\Applications\Photoresizer.exe	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	4752	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15,687,680...
7111..	svchost.exe	9052	ReadFile	C:\Users\NVR\AppData\Local\Microsoft...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HCU	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU\SOFTWARE\Microsoft\Windows De...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	4752	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 17,055,744...
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR\AppData\Local\Temp\Pr...	SUCCESS	Desired Access: R...
7111..	svchost.exe	9052	QueryBatchInfo	C:\Users\NVR\AppData\Local\Temp\Pr...	SUCCESS	CreationTime: 7/12...
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR\AppData\Local\Temp\Pr...	SUCCESS	
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR\AppData\Local\Microsoft...	SUCCESS	Desired Access: G...
7111..	svchost.exe	4752	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 17,072,128...
7111..	svchost.exe	9052	ReadFile	C:\Users\NVR\AppData\Local\Microsoft...	SUCCESS	Offset: 16,760,832...
7111..	svchost.exe	9052	QueryBatchInfo	C:\Users\NVR\AppData\Local\Microsoft...	SUCCESS	AllocationSize: 1.0...
7111..	svchost.exe	9052	CreateFileMap	C:\Users\NVR\AppData\Local\Microsoft...	FILE LOCKED WI...	SynType: SynType...
7111..	svchost.exe	9052	CreateFileMap	C:\Users\NVR\AppData\Local\Microsoft...	SUCCESS	AllocationSize: 1.0...
7111..	svchost.exe	9052	CreateFileMap	C:\Users\NVR\AppData\Local\Microsoft...	SUCCESS	SynType: SynType...
7111..	svchost.exe	4752	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15,790,080...
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR\AppData\Local\Microsoft...	Desired Access: R...	
7111..	svchost.exe	4752	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 16,781,312...
7111..	svchost.exe	9052	ReadFile	C:\Users\NVR\AppData\Local\Microsoft...	SUCCESS	CreationTime: 7/12...

Showing 446,469 of 884,253 events (50%) Backed by virtual memory

Start [Icons] [Capturing from Local Area...] [Process Monitor - Sys...

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Win10 of Vm - VMware Workstation

File Edit View VM Tools Help

Process Monitor - Sysinternals www.sysinternals.com

File Edit Event Filter Tools Options Help

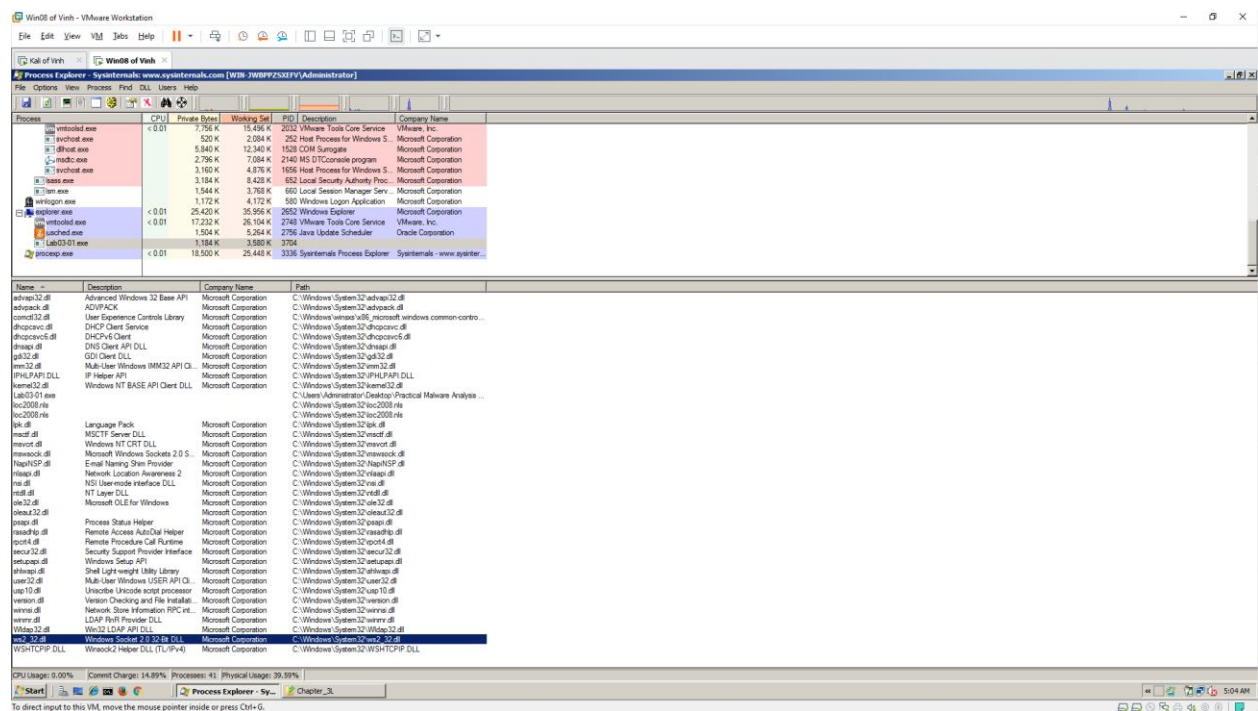
Time	Process Name	PID	Operation	Path	Result	Detail
7111..	svchost.exe	2412	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 650,080 Le...
7111..	svchost.exe	2412	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 672,480 Le...
7111..	svchost.exe	2412	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 635,904 Le...
7111..	svchost.exe	2412	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 623,616 Le...
7111..	svchost.exe	9052	RegOpenKey	HCU	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU\SOFTWARE\Microsoft\Tablet Ti...	NAME NOT FOUND	Desired Access: Q...
7111..	svchost.exe	9052	RegOpenKey	HCU	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU\SOFTWARE\Microsoft\Tablet Ti...	NAME NOT FOUND	Desired Access: Q...
7111..	svchost.exe	9052	RegOpenKey	HCU	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HCU\SOFTWARE\Microsoft\Tablet Ti...	NAME NOT FOUND	Desired Access: Q...
7111..	svchost.exe	9052	RegOpenKey	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Exclusive: False, O...
7111..	svchost.exe	2412	QueryBatchInfo	C:\ProgramData\Microsoft\Windows A...	SUCCESS	AllocationSize: 5.2...
7111..	svchost.exe	2412	Unhook/Redirge	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Offset: 123, Length...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPAIRER	Desired Access: Q...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	Desired Access: Q...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	NAME NOT FOUND Length: 24	
7111..	svchost.exe	2412	RegOpenKey	HKLM\Software\Policies\Microsoft\MI...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	
7111..	svchost.exe	2412	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows De...	REPAIRER	Desired Access: M...
7111..	svchost.exe	2412	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows De...	SUCCESS	Desired Access: M...
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT\Software\Policies\Mc...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT\Software\Policies\Mc...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT\Control Panel\Desktop...	REPAIRER	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	NAME NOT FOUND Length: 24	
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT\Control Panel\Desktop...	SUCCESS	Query Name
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT\Control Panel\Desktop...	SUCCESS	NAME NOT FOUND
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	Offset: 1,504,256...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPAIRER	Desired Access: Q...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	Desired Access: Q...
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR	NAME COLLISION	Desired Access: R...
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR	SUCCESS	Desired Access: R...
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR	SUCCESS	CreationTime: 4/11...
7111..	svchost.exe	9052	CreateFile	C:\Users\NVR	SUCCESS	
7111..	svchost.exe	2412	RegOpenKey	HKLM\Software\Policies\Microsoft\MI...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	2412	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows De...	REPAIRER	Desired Access: M...
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT	SUCCESS	Desired Access: M...
7111..	svchost.exe	2412	RegOpenKey	C:\Users\NVR\AppData\Local\...	NAME COLLISION	Desired Access: R...
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT\Software\Policies\Mc...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPAIRER	Desired Access: Q...
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT\Control Panel\Desktop...	NAME NOT FOUND	Desired Access: R...
7111..	svchost.exe	2412	RegOpenKey	HKLM\DEFAULT	SUCCESS	Desired Access: Q...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	NAME NOT FOUND Length: 24
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	SUCCESS	
7111..	svchost.exe	9052	RegOpenKey	C:\Users\NVR\AppData\Local\...	SUCCESS	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	C:\Users\NVR\AppData\Local\...	SUCCESS	Desired Access: R...
7111..	svchost.exe	9052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPAIRER	Desired Access: Q...

Showing 475,919 of 5,965,188 events (80%) Backed by virtual memory

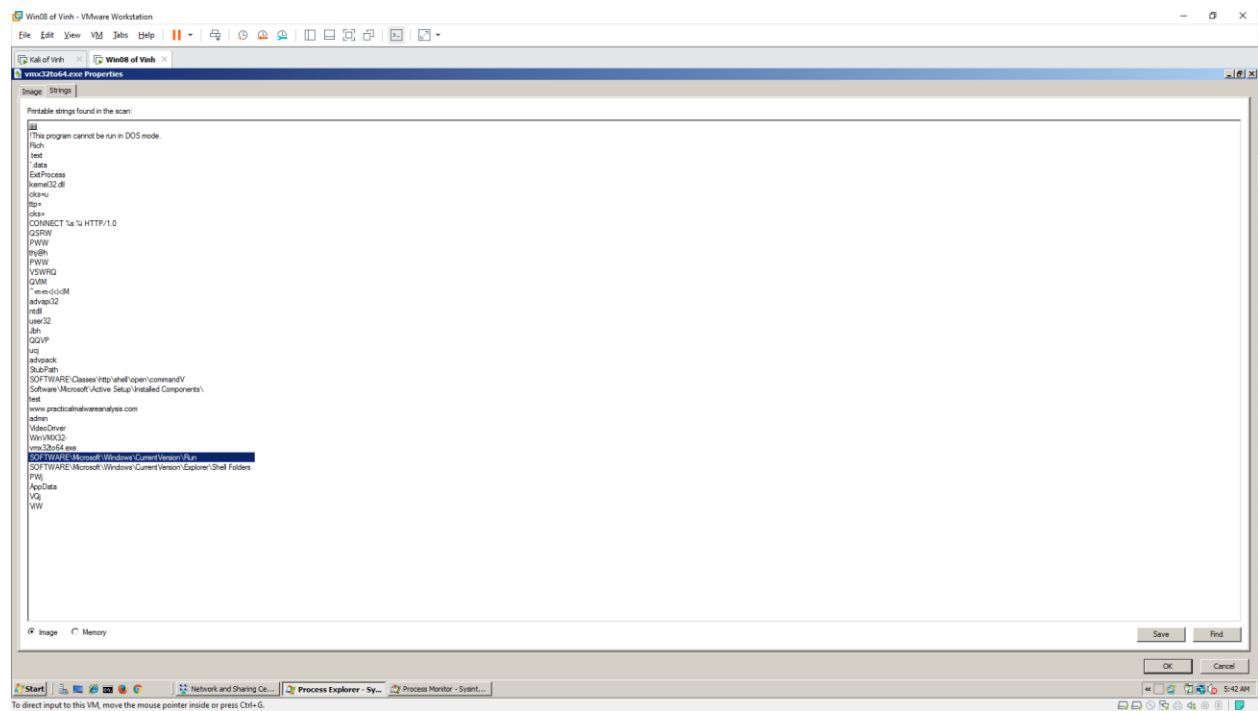
Start [Icons] [Capturing from Local Area...] [Process Monitor - Sys...

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Run the Lab03-01.exe File



## Viewing the Malicious Process's Events in Process Monitor



## Viewing INetSim Logs

```
Kali of Vinh - VMware Workstation
File Edit View VM Jobs Help
Kali of Vinh x1 x2 x3 x4 x5
TouristV@kali: ~
File Actions Edit View Help
TouristV@kali: ~ x TouristV@kali: ~ x
^C * https_443_tcp - stopped (PID 5283)
* http_80_tcp - stopped (PID 5282)
* ident_113_tcp - stopped (PID 5294)
* ntp_123_udp - stopped (PID 5292)
* dummy_1_udp - stopped (PID 5309)
* pop3s_995_tcp - stopped (PID 5287)
* daytime_13_tcp - stopped (PID 5298)
* discard_9_udp - stopped (PID 5303)
* dns_53_tcp_udp - stopped (PID 5281)
* daytime_13_udp - stopped (PID 5299)
* smtps_465_tcp - stopped (PID 5285)
* quotd_17_udp - stopped (PID 5305)
* chargen_19_udp - stopped (PID 5307)
* finger_79_tcp - stopped (PID 5293)
* quotd_17_tcp - stopped (PID 5304)
* echo_7_udp - stopped (PID 5301)
* chargen_19_tcp - stopped (PID 5306)
* time_37_tcp - stopped (PID 5296)
* discard_9_tcp - stopped (PID 5302)
* ftps_990_tcp - stopped (PID 5289)
* time_37_udp - stopped (PID 5297)
* smtp_25_tcp - stopped (PID 5284)
* ftp_21_tcp - stopped (PID 5288)
* echo_7_tcp - stopped (PID 5300)
* pop3_110_tcp - stopped (PID 5286)
* dummy_1_tcp - stopped (PID 5308)
* syslog_514_udp - stopped (PID 5295)
* tftp_69_udp - stopped (PID 5290)
* irc_6667_tcp - stopped (PID 5291)
Simulation stopped.
Report written to '/var/log/inetsim/report/report.5279.txt' (1460 lines)
== Inetsim main process stopped (PID 5279) ==
.
(TouristV@kali)-[~]
$
```

```
Kali of Vinh - VMware Workstation
File Edit View VM Jobs Help
Kali of Vinh x1 x2 x3 x4 x5
root@kali: /var/log/inetsim/report Usage: 2%
File Actions Edit View Help
root@kali: /var/log/inetsim/report x TouristV@kali: ~ x
$ cd /var
(TouristV@kali)-[/var]
$ cd log/inetsim
cd: permission denied: log/inetsim
(TouristV@kali)-[/var]
$ ls
backups cache lib local lock log mail opt run spool tmp
(TouristV@kali)-[/var]
$ sudo -i
[sudo] password for TouristV:
(root@kali)-[~]
# cd /var/log
(root@kali)-[/var/log]
# cd inetsim
(root@kali)-[/var/log/inetsim]
# cd report
(root@kali)-[/var/log/inetsim/report]
# nano report.5279.txt
(root@kali)-[/var/log/inetsim/report]
# cat report.5279.txt | grep prac
2023-01-12 08:02:50 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2023-01-12 08:03:20 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2023-01-12 08:03:50 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2023-01-12 08:04:20 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2023-01-12 08:20:31 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2023-01-12 08:39:31 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
(root@kali)-[/var/log/inetsim/report]
#
```

## Viewing the Network Request in Wireshark

WinBox of Vmsh - VMware Workstation

File Edit View VM Jobs Help

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp stream eq 11

Wireshark - Follow TCP Stream (tcp.stream eq 11) - wireshark\_64f8b6-8a57-E1AB3302BCAS...

178 26.011... 192.168...  
179 26.012... 192.168...  
180 26.012... 192.168...  
181 26.012... 192.168...  
182 26.013... 192.168...  
186 26.051... 192.168...  
187 26.061... 192.168...  
188 26.061... 192.168...  
189 26.063... 192.168...  
190 26.064... 192.168...  
191 26.064... 192.168...

Filter Out This Stream Print Save as Back Close Help

Frame 191: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
Ethernet II, Src: VMware\_adf3:3e (00:0c:29:ad:f3:3e), Dst: VMware\_65:8a:b8 (00:0c:29:65:8a:b8)  
Internet Protocol Version 4, Src: 192.168.134.156, Dst: 192.168.134.153  
Transmission Control Protocol, Src Port: 3070, Dst Port: 443, Seq: 337, Ack: 1491, Len: 0

0000 00 0c 29 65 8a b8 00 0c 29 ad f3 3e 00 00 45 00 ...  
0010 00 28 01 97 40 00 00 00 00 c0 a8 86 9c c0 a8 ...  
0020 86 99 04 2e 01 b0 f8 ae 1c 0c 24 36 1f f3 50 14 ...  
0030 00 00 8e a1 00 00 .....

Wireshark\_64f8b6-8a57-E1AB3302BCAS\_20230112054659\_jd01932

Start Process Monitor - Sysint... Local Area Connection Wireshark - Follow TC... ZNetSim default HTML pa... Process Explorer - Sysint...

Packets: 758 - Displayed: 11 (1.5%)

Profile: Default

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.