Lab 5: Keylogger

Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 8/2/2023

Purpose

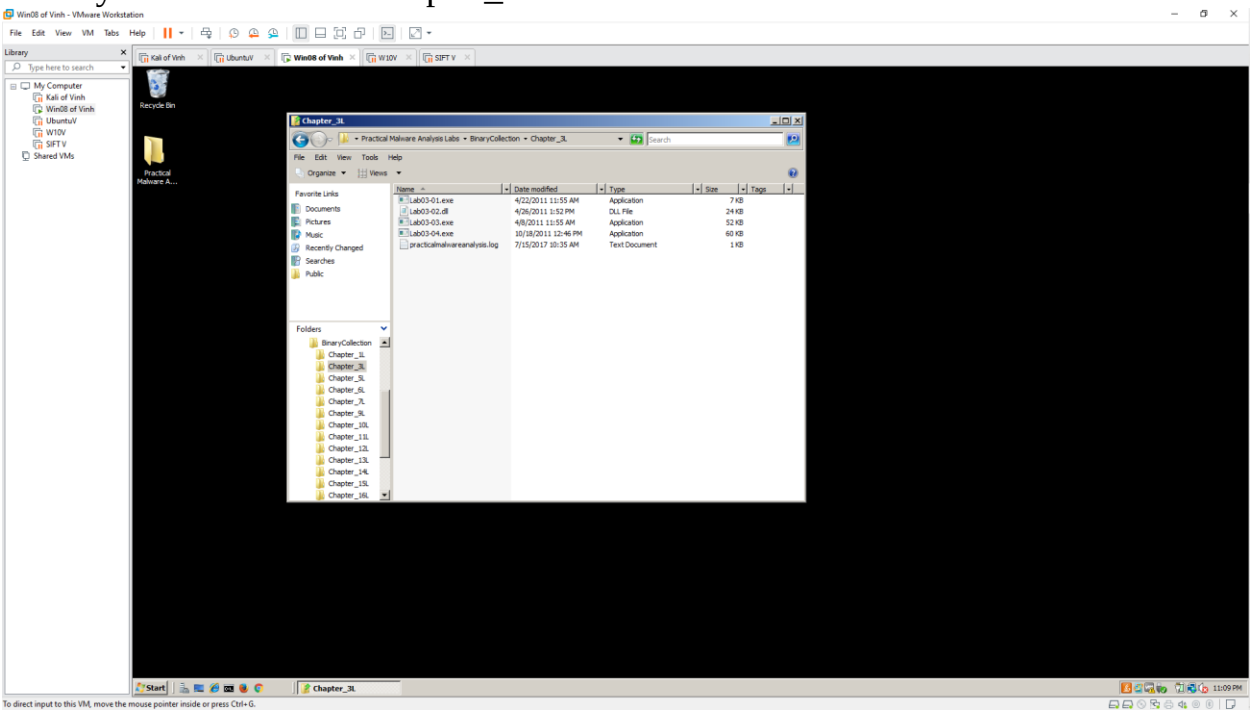
You will practice the techniques in chapter 3.
This project follows Lab 3-3 in the textbook.

What you need:

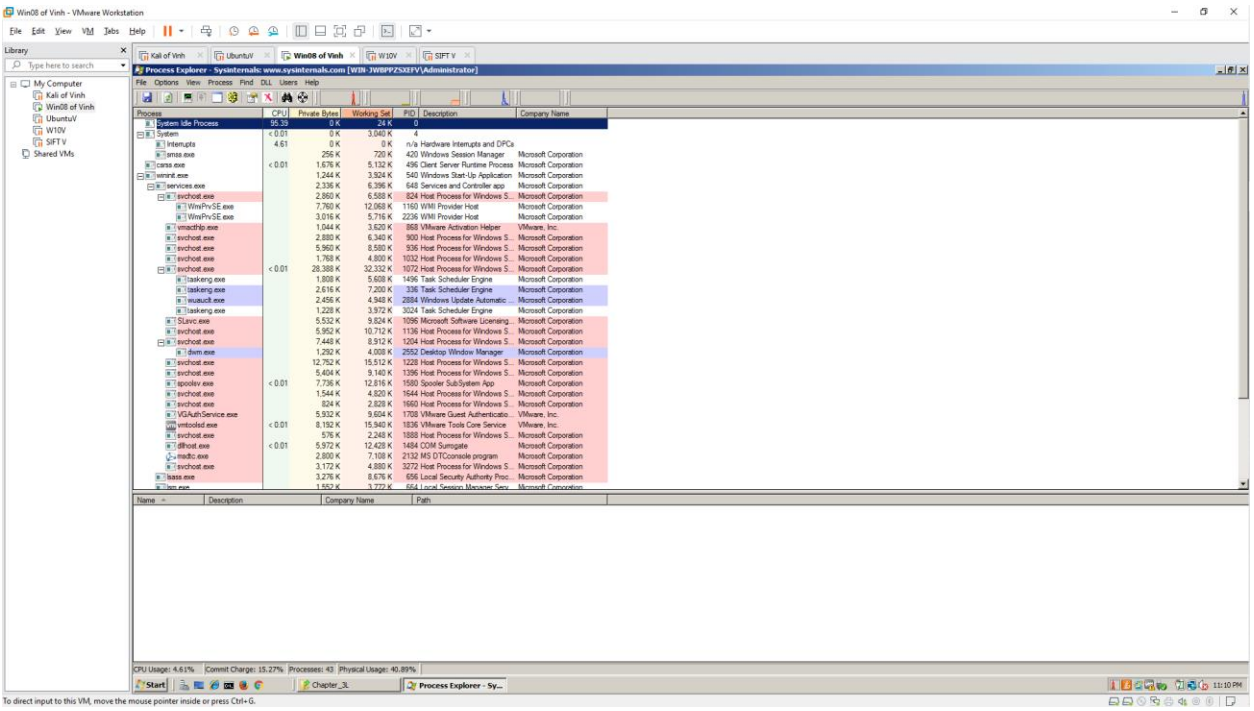
The Windows 2008 Server virtual machine we have been using

Preparing Windows

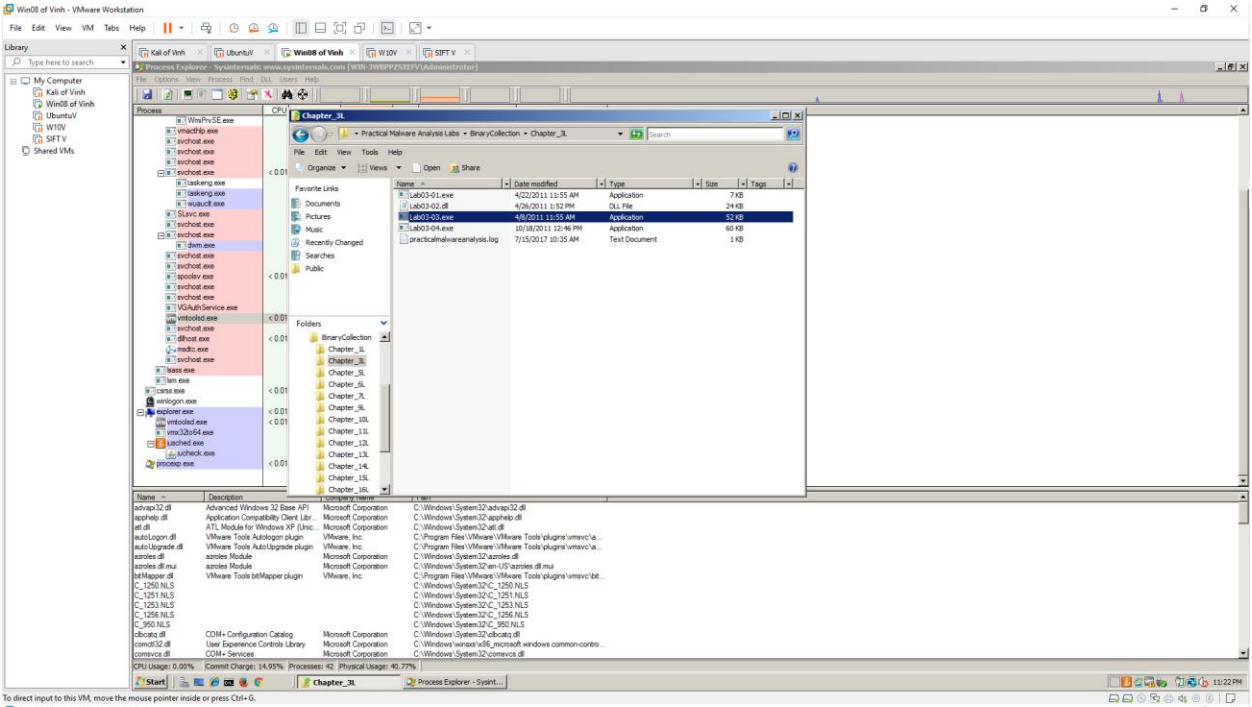
On your desktop, open the "Practical Malware Analysys Labs" folder. Open the "Binary Collection" and Chapter_3L folders.

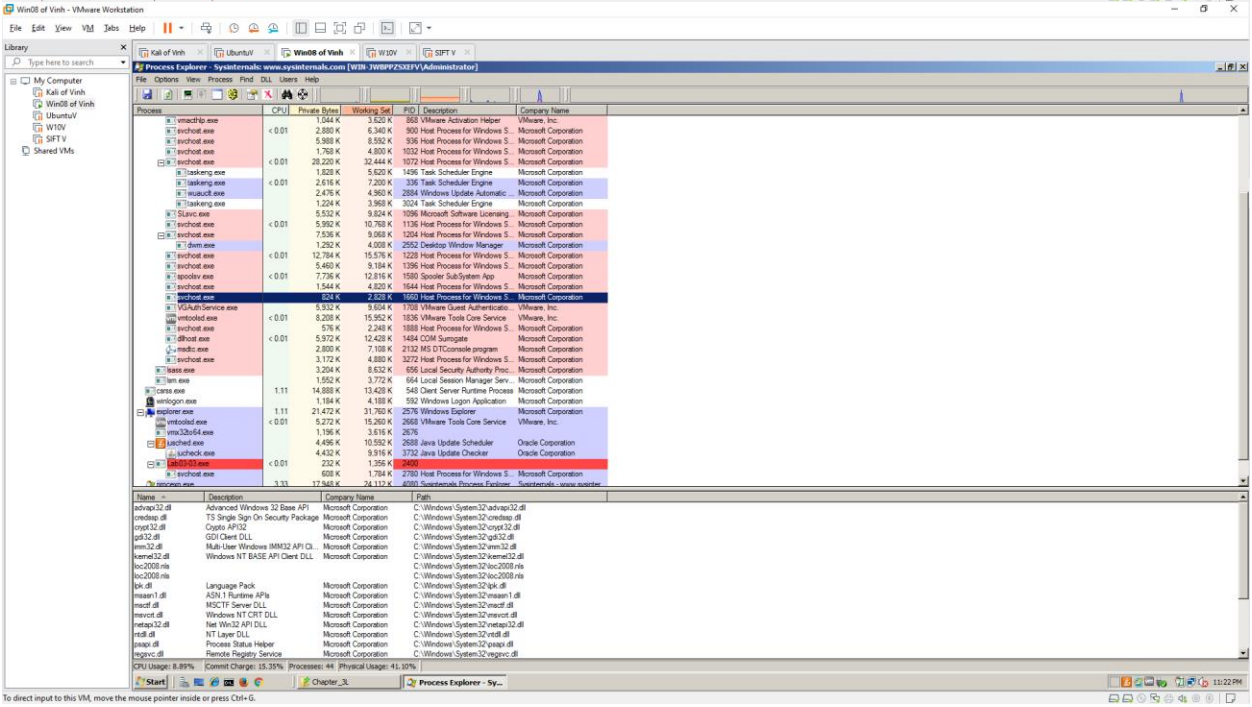


Open Process Explorer and move it so you can see it at the same time as the Explorer window. Scroll to the bottom to show explorer.exe (your desktop) and its children, which are processes launched by the currently logged-in user, as shown below.

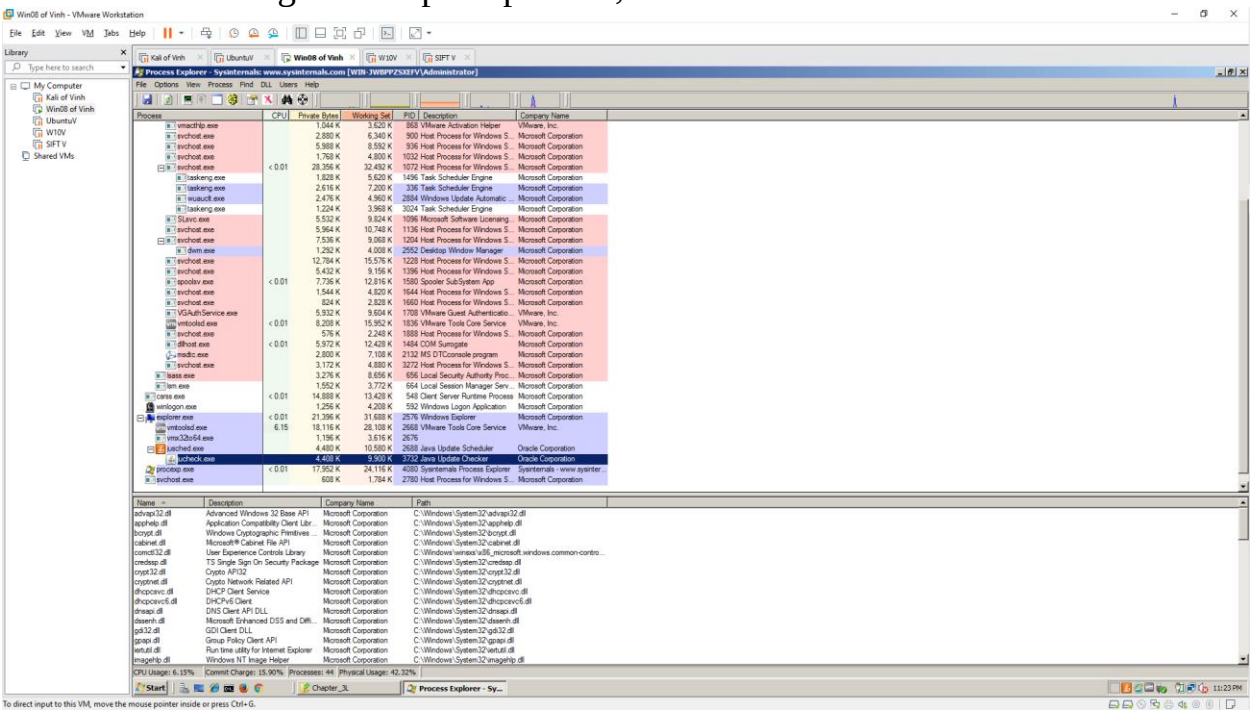


Launch the Malware


Win08 of Vinh - VMware Workstation
Chapter_3L
Process Explorer - Sysinternals: www.sysinternals.com [WIN-JWBPPZS3EFV\Administrator]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Win08 of Vinh - VMware Workstation
Process Explorer - Sysinternals: www.sysinternals.com [WIN-JWBPPZS3EFV\Administrator]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

After a second or two, the Lab03-03.exe process terminates, leaving the svchost.exe running as an orphan process, as shown below



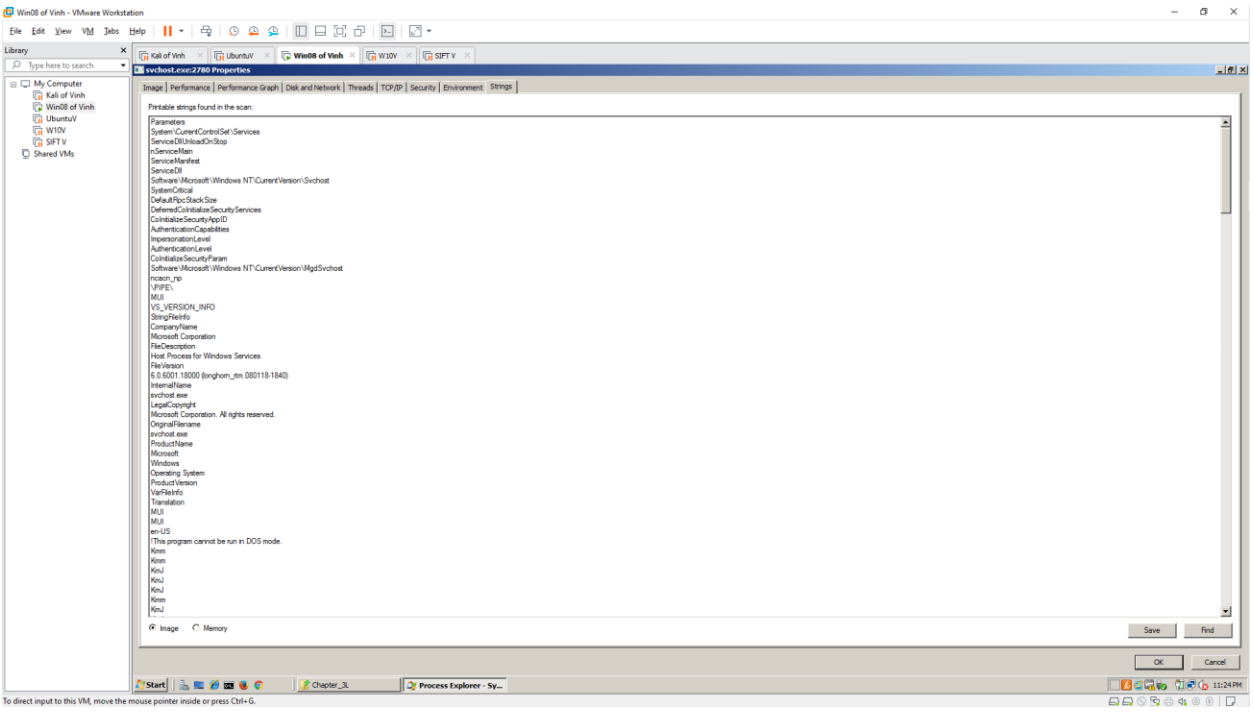
Observing Process Replacement

This svchost process is strange in another way: the code running in RAM does not match the code on the disk.

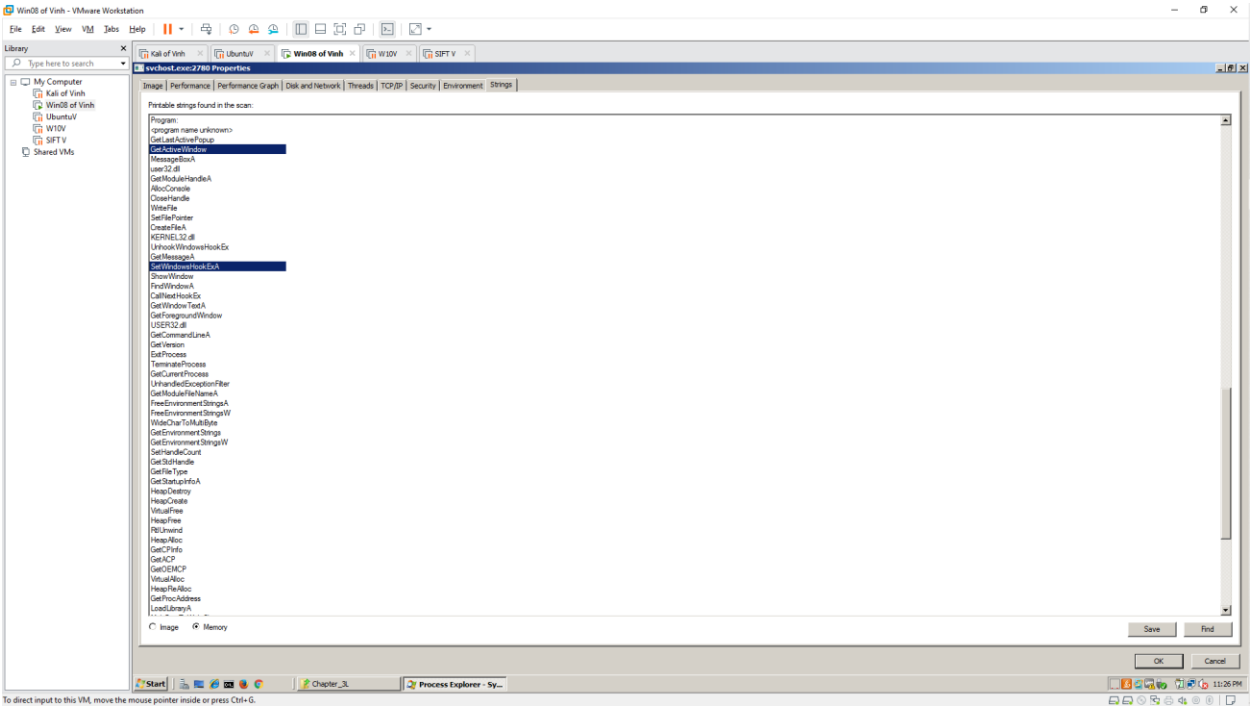
To see that, in Process Explorer, right-click svchost.exe and click Properties.

Click the Strings tab. At the bottom, make sure Image is selected, as shown below.

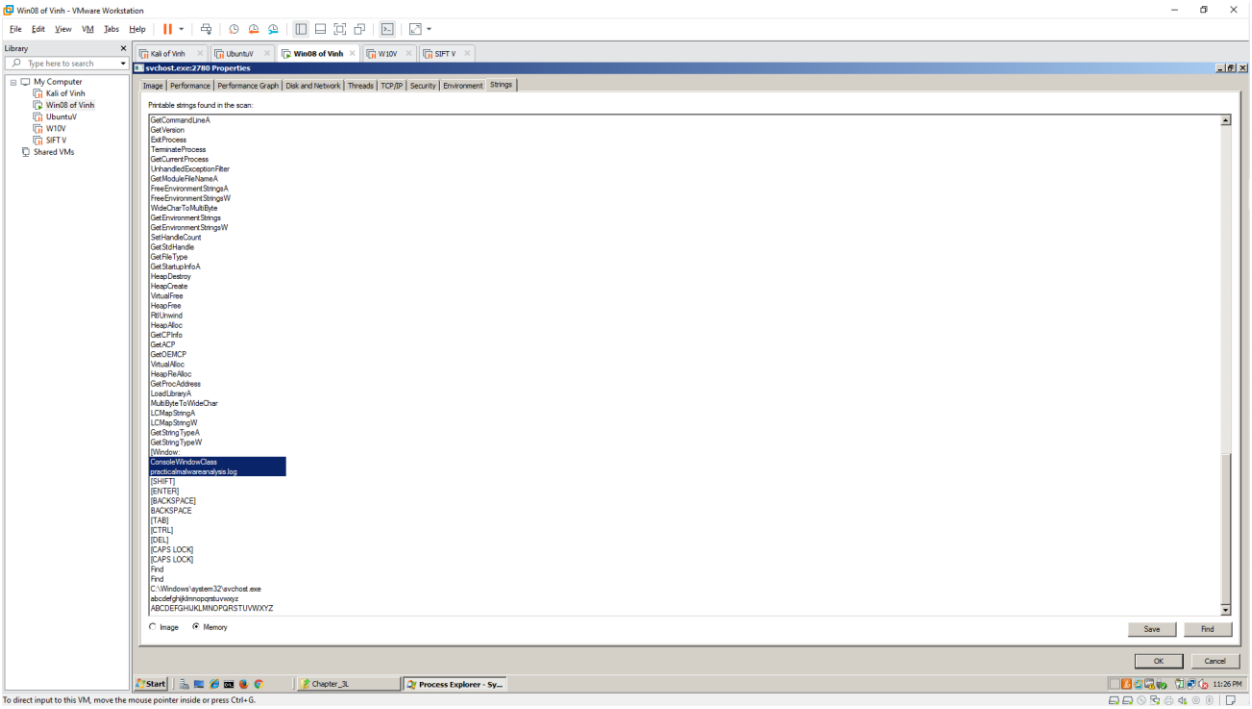
These are the strings on the disk, in the real svchost.exe file



At the bottom of the box, click the Memory button. Now the strings are completely different, and contain these suspicious items: GetActiveWindow and SetWindowsHookExA.

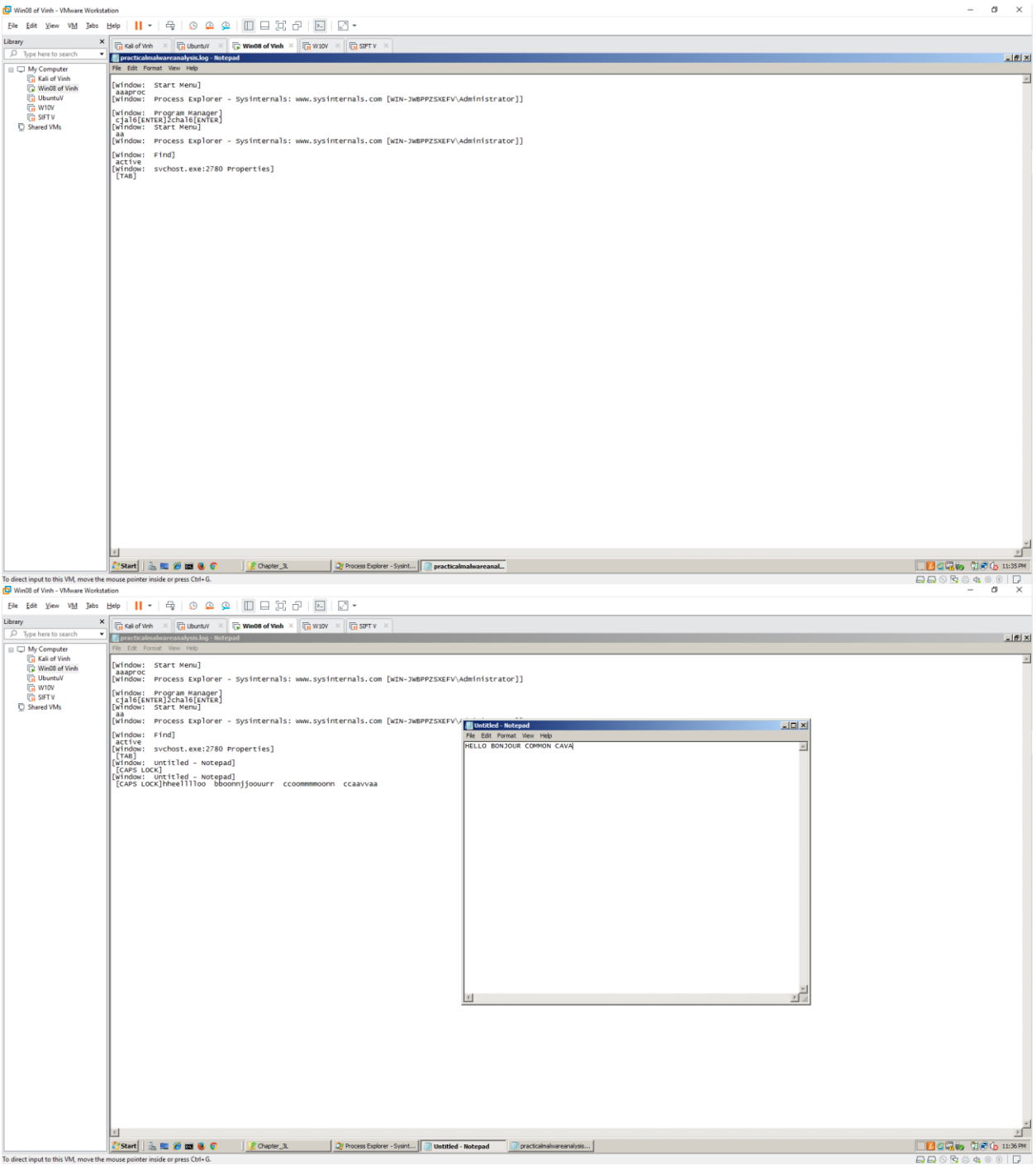


Scroll down and find the string practicalmalwareanalysis.log, as shown below. This may be the filename used to store the keypresses

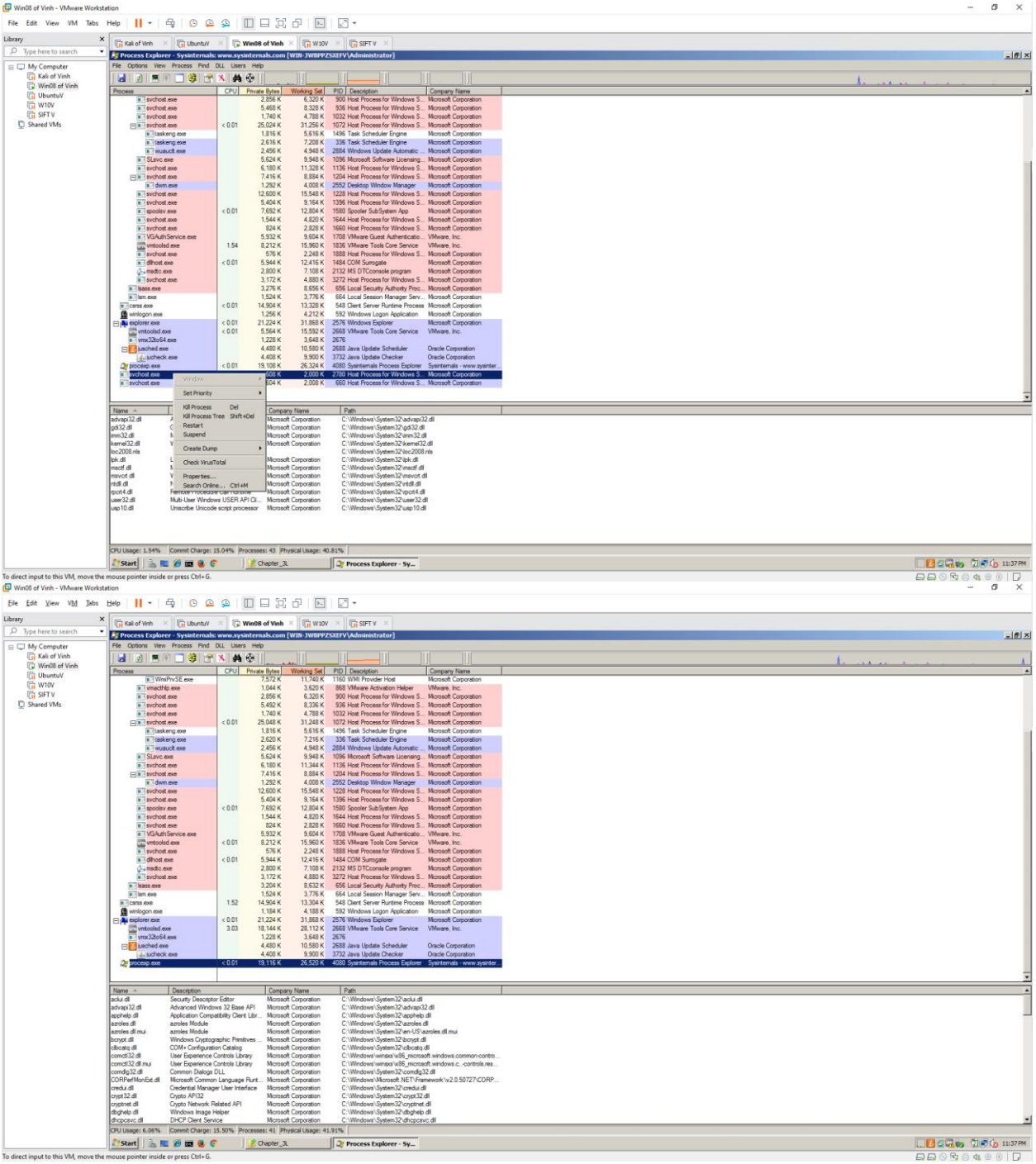


5.1: Recording Your Success

Testing the Keylogger

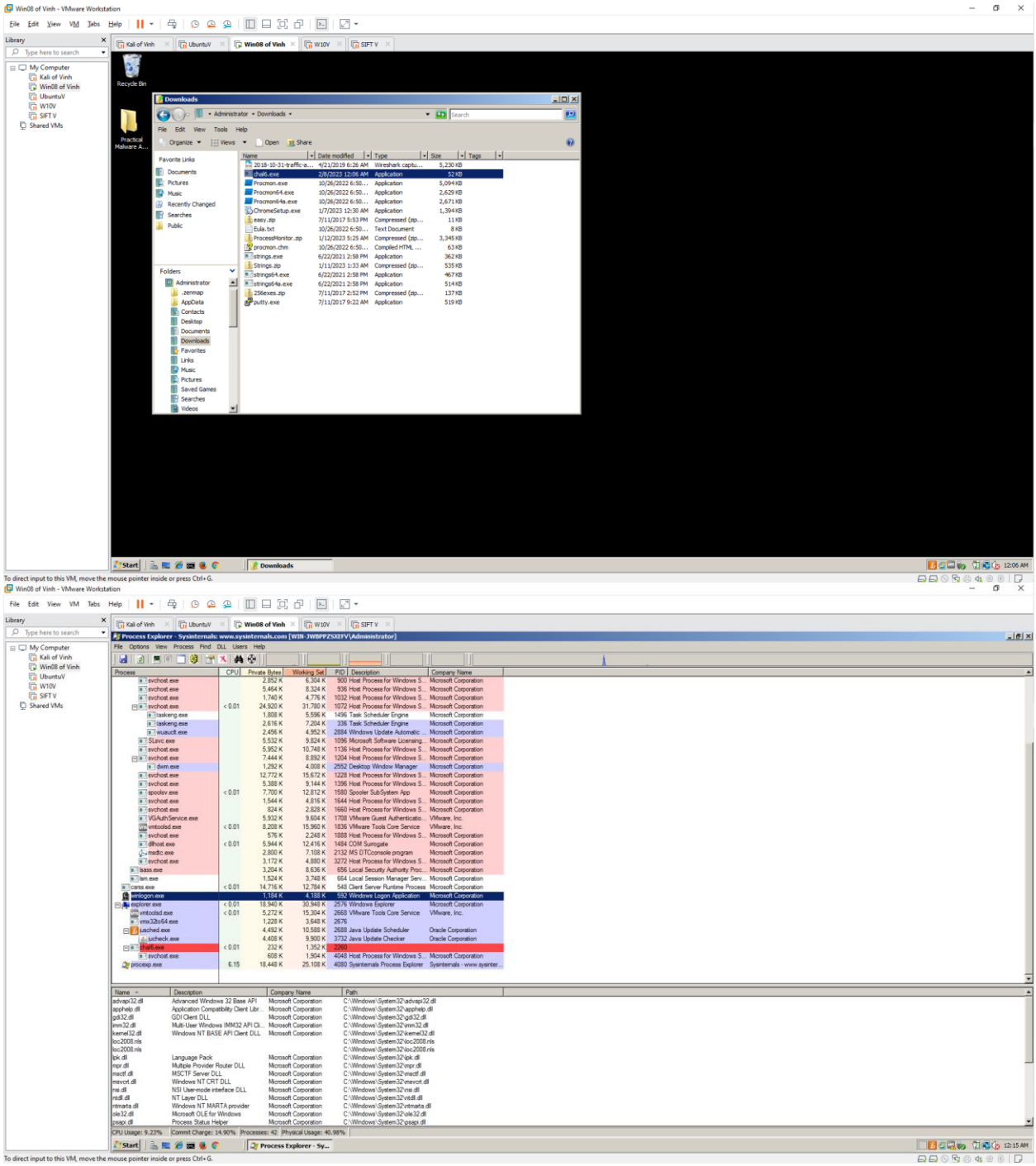


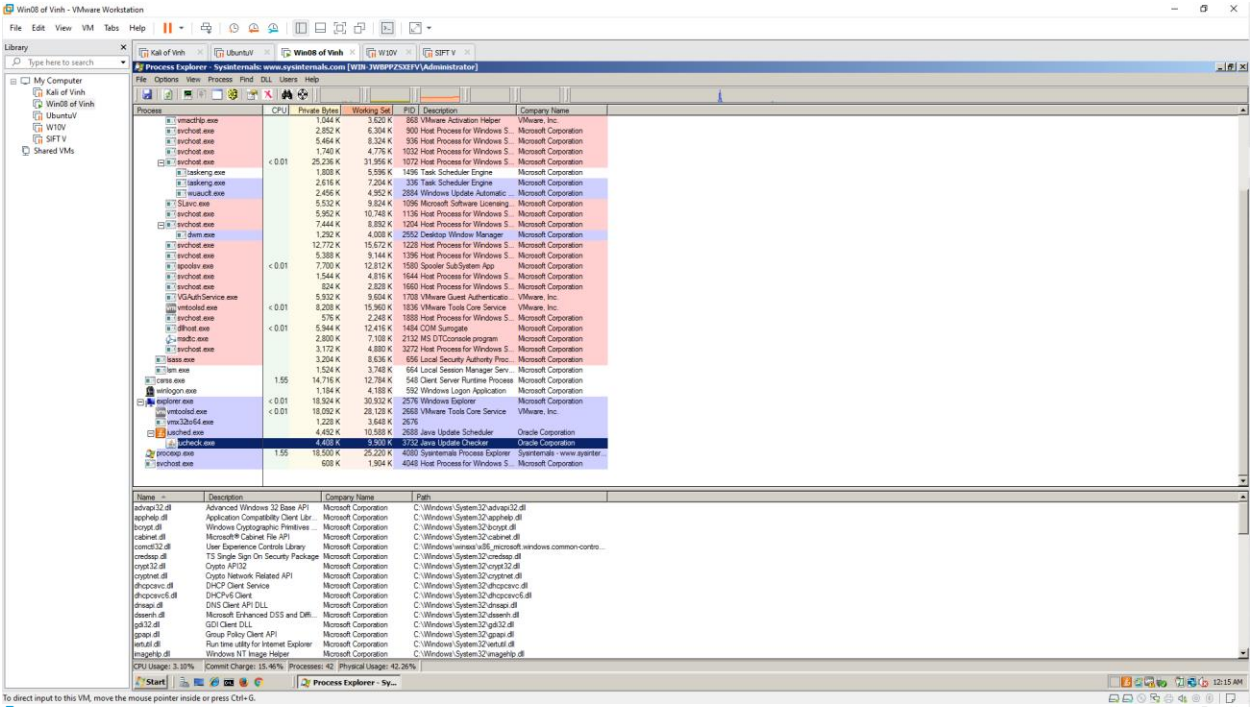
Killing the Keylogger Process

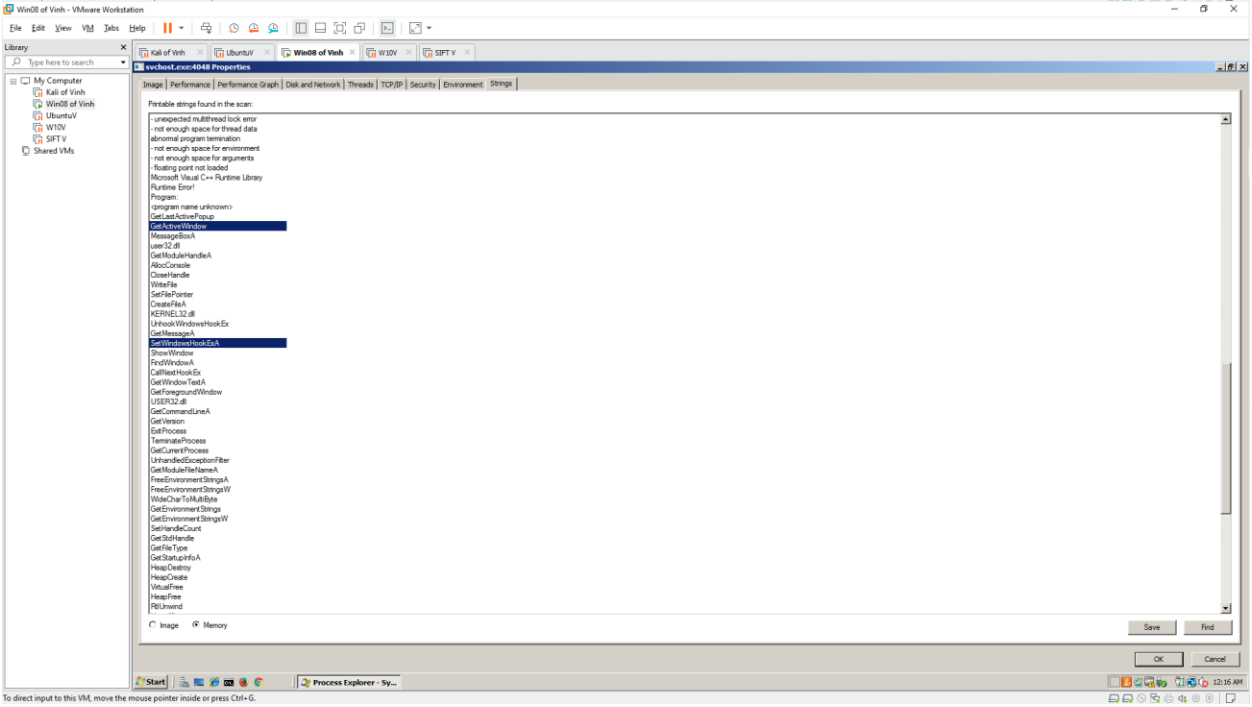


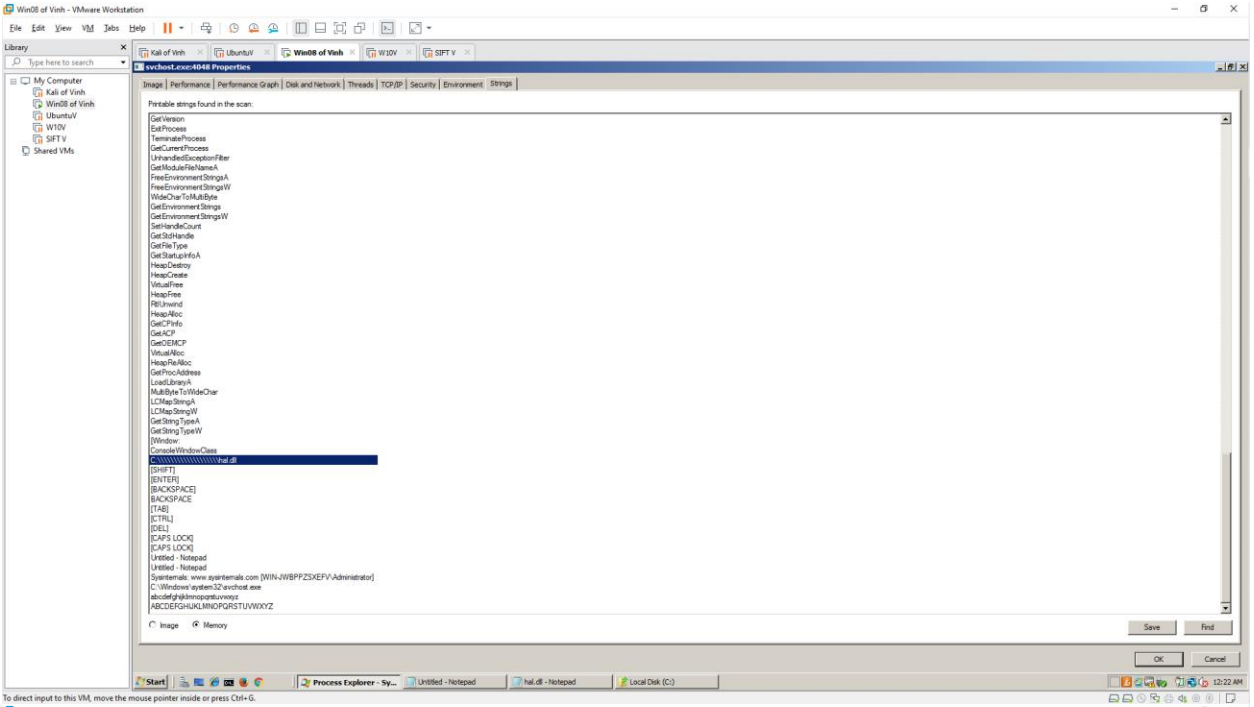
Challenge 5.2: Find the Logfile

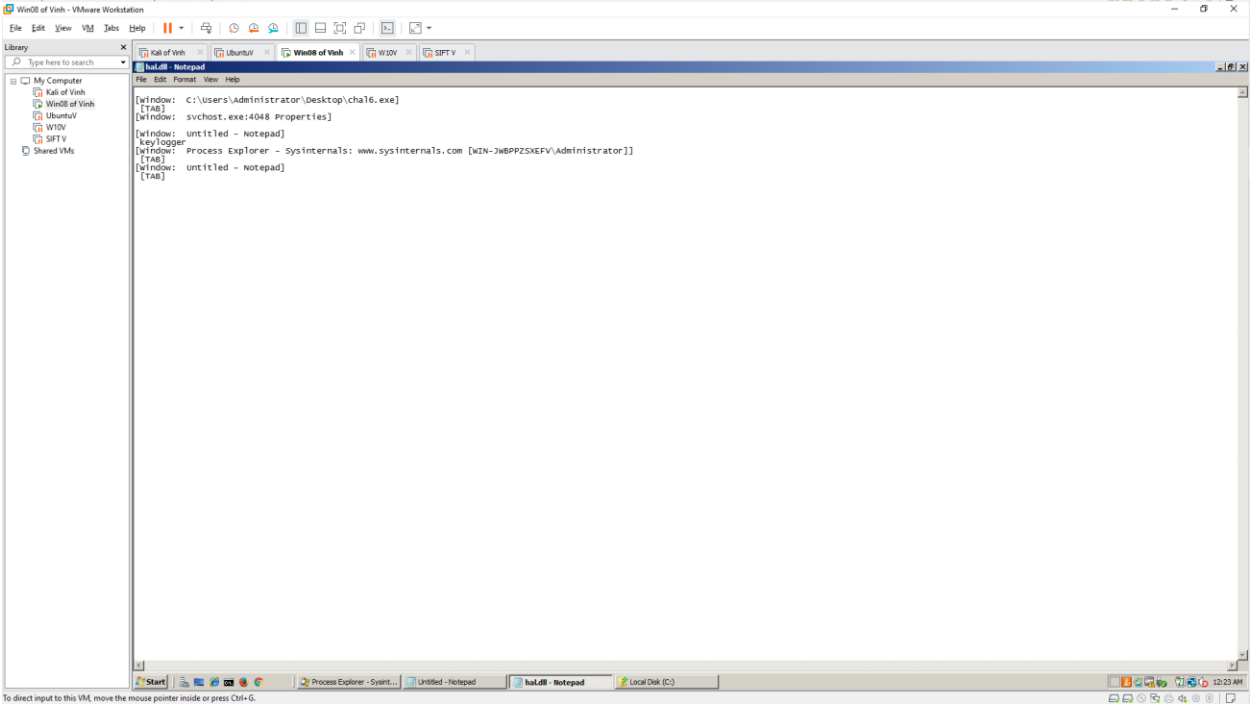
In your Documents folder, find the file chal6.exe

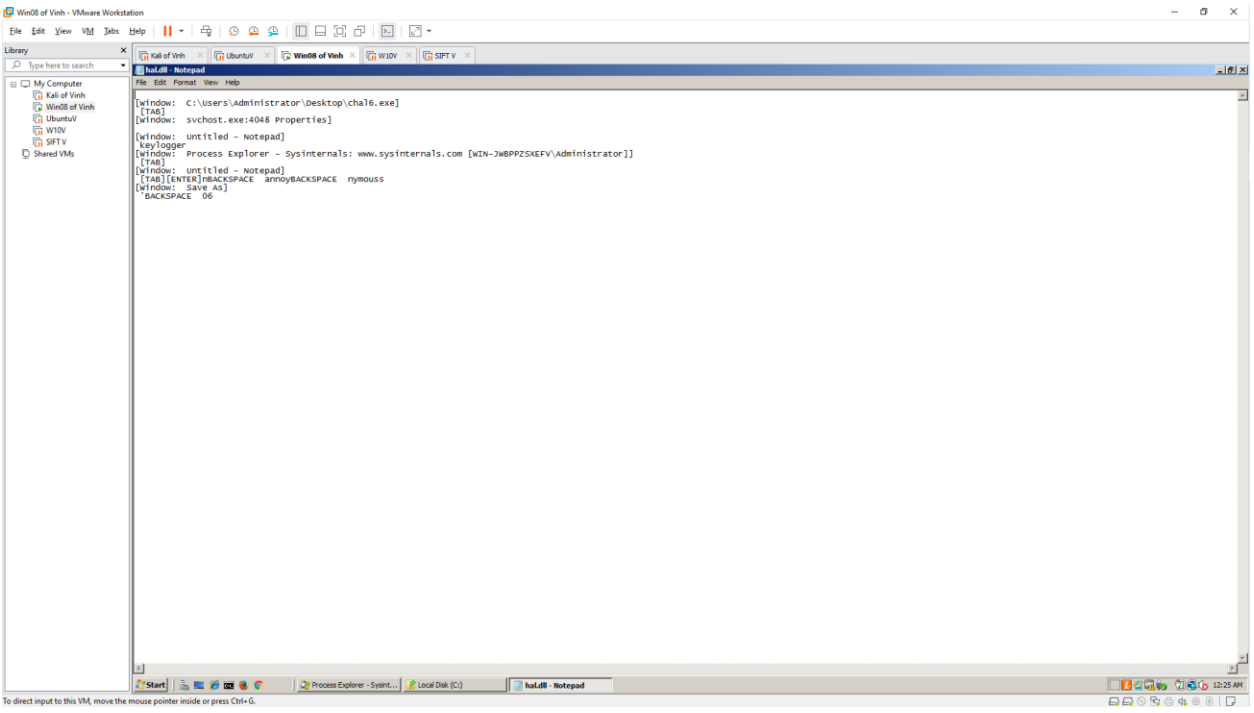



Win08 of Vinh - VMware Workstation
Process Explorer - Sysinternals: www.sysinternals.com [WIN-JWBPPZS3EFV\Administrator]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Win08 of Vinh - VMware Workstation
svchost.exe:4048 Properties
Printable strings found in the scan:
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
svchost.exe:4048 Properties
Image Performance Performance Graph Disk and Network Threads TCP/IP Security Environment Strings
Printable strings found in the scan:
GetVersion
ExitProcess
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
GetModuleFileNameA
FreeEnvironmentStringsA
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStrings
GetEnvironmentStringsW
SetHandleCount
GetStdHandle
GetFileType
GetStartupInfoA
HeapDestroy
HeapCreate
VirtualFree
HeapFree
RtlUnwind
HeapAlloc
GetCPInfo
GetACP
GetOEMCP
VirtualAlloc
HeapReAlloc
GetProcAddress
LoadLibraryA
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
[Window
ConsoleWindowClass
C:\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\hal.dll
[SHIFT]
[ENTER]
[BACKSPACE]
BACKSPACE
[TAB]
[CTRL]
[DEL]
[CAPS LOCK]
[CAPS LOCK]
Untitled - Notepad
Untitled - Notepad
Sysinternals: www.sysinternals.com [WIN-JWBPPZSXEFV\Administrator]
C:\Windows\system32\svchost.exe
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Image
Memory
Save
Find
OK
Cancel
Start
Process Explorer - Sy...
Untitled - Notepad
hal.dll - Notepad
Local Disk (C:)
12:22 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
hal.dll - Notepad
File Edit Format View Help
[window: C:\Users\Administrator\Desktop\chal6.exe]
[TAB]
[window: svchost.exe:4048 Properties]
[window: Untitled - Notepad]
keylogger
[window: Process Explorer - Sysinternals: www.sysinternals.com [WIN-JWBPPZSXEFV\Administrator]]
[TAB]
[window: Untitled - Notepad]
[TAB]
Start
Process Explorer - Sysint...
Untitled - Notepad
hal.dll - Notepad
Local Disk (C:)
12:23 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
hal.dll - Notepad
File Edit Format View Help
[window: C:\Users\Administrator\Desktop\chal6.exe]
[TAB]
[window: svchost.exe:4048 Properties]
[window: untitled - Notepad]
keylogger
[window: Process Explorer - Sysinternals: www.sysinternals.com [WIN-JWBPPZSXEFV\Administrator]]
[TAB]
[window: untitled - Notepad]
[TAB][ENTER]mBACKSPACE annoyBACKSPACE nymouss
[window: Save As]
BACKSPACE 06
Start
Process Explorer - Sysint...
Local Disk (C:)
hal.dll - Notepad
12:25 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.