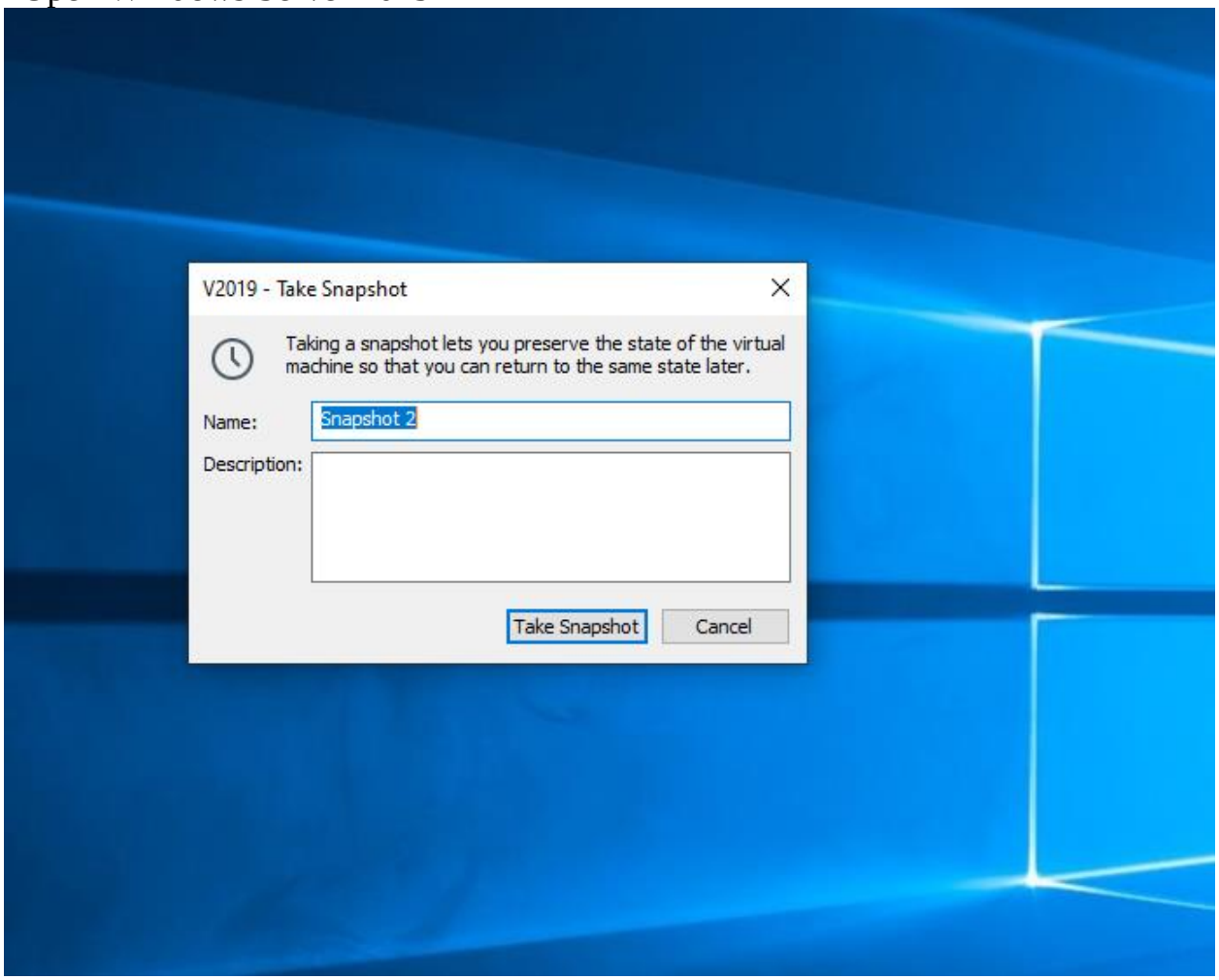
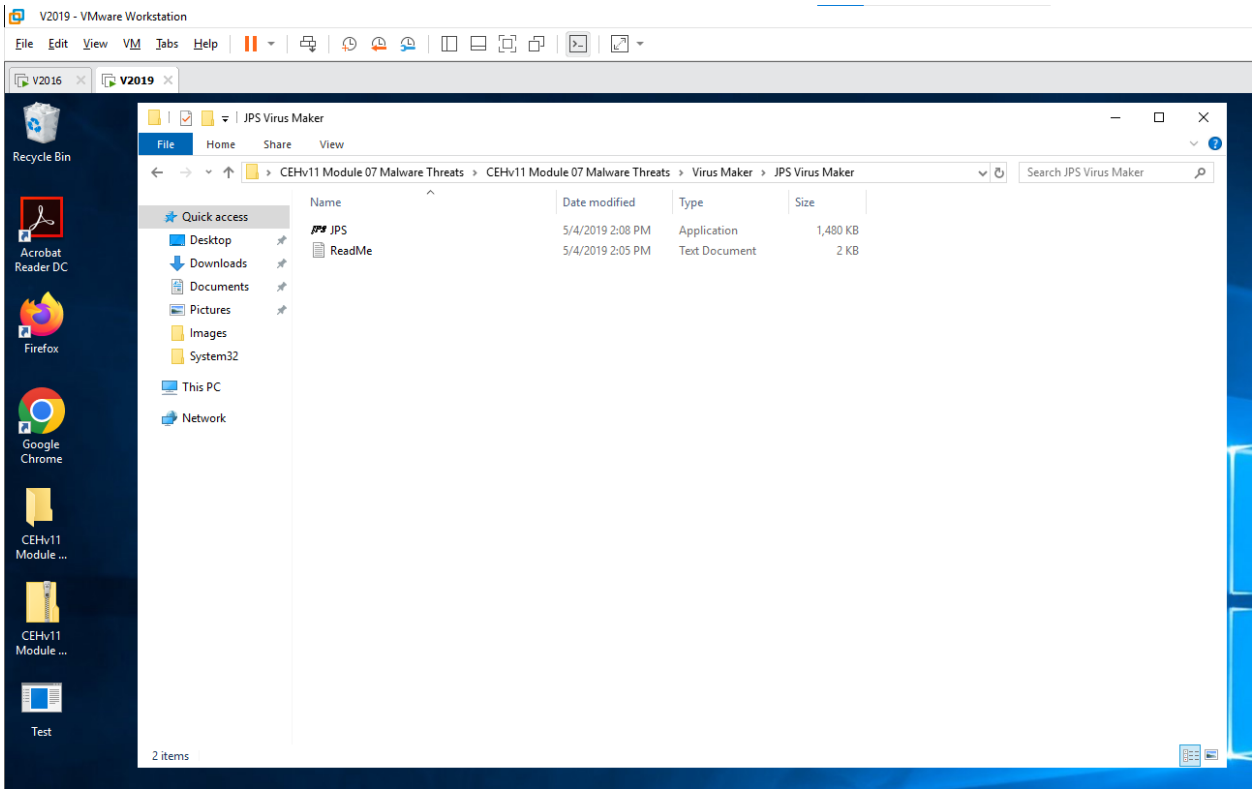
Lab 9: Malware Threats

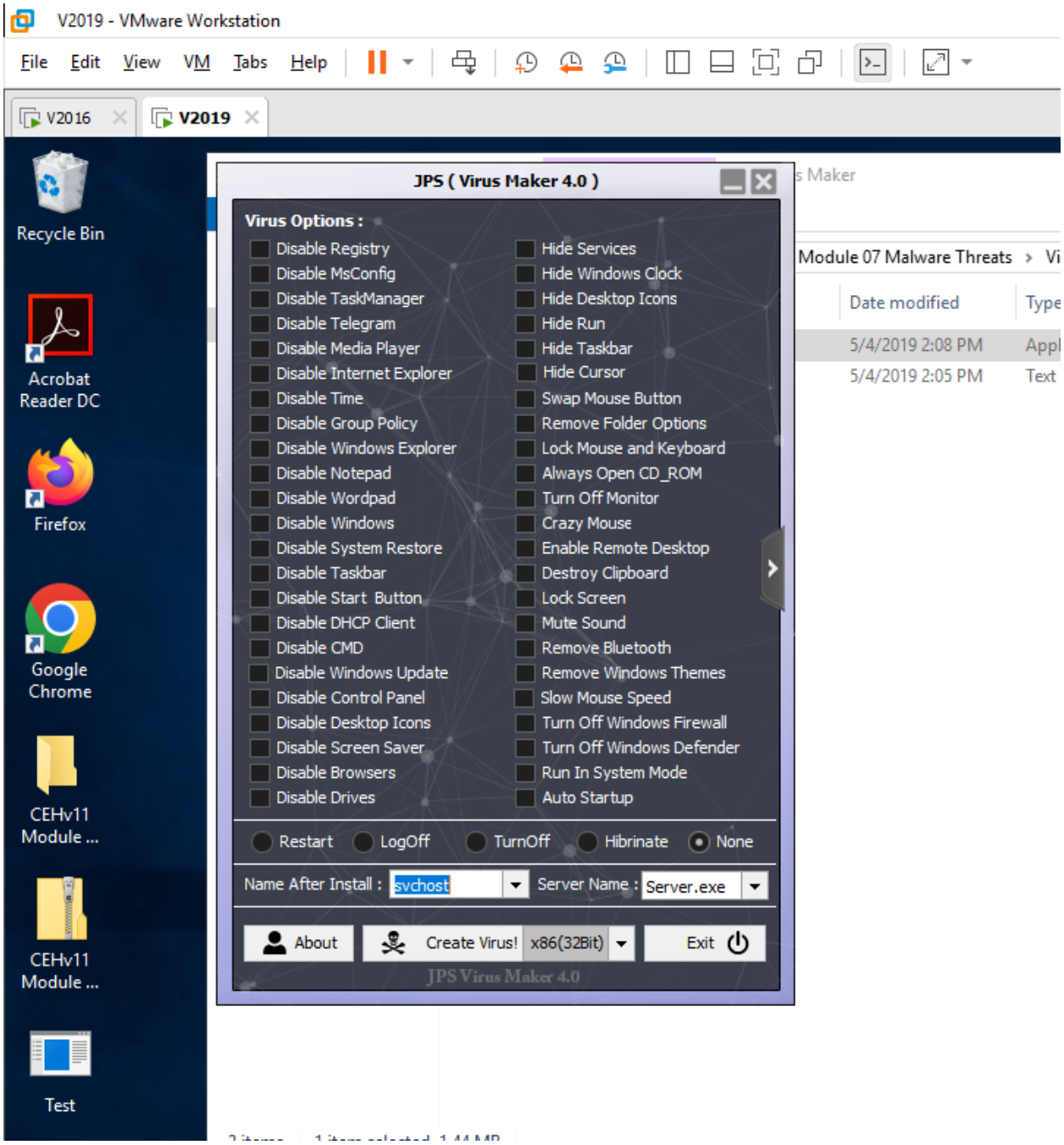
Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 07/10/2023

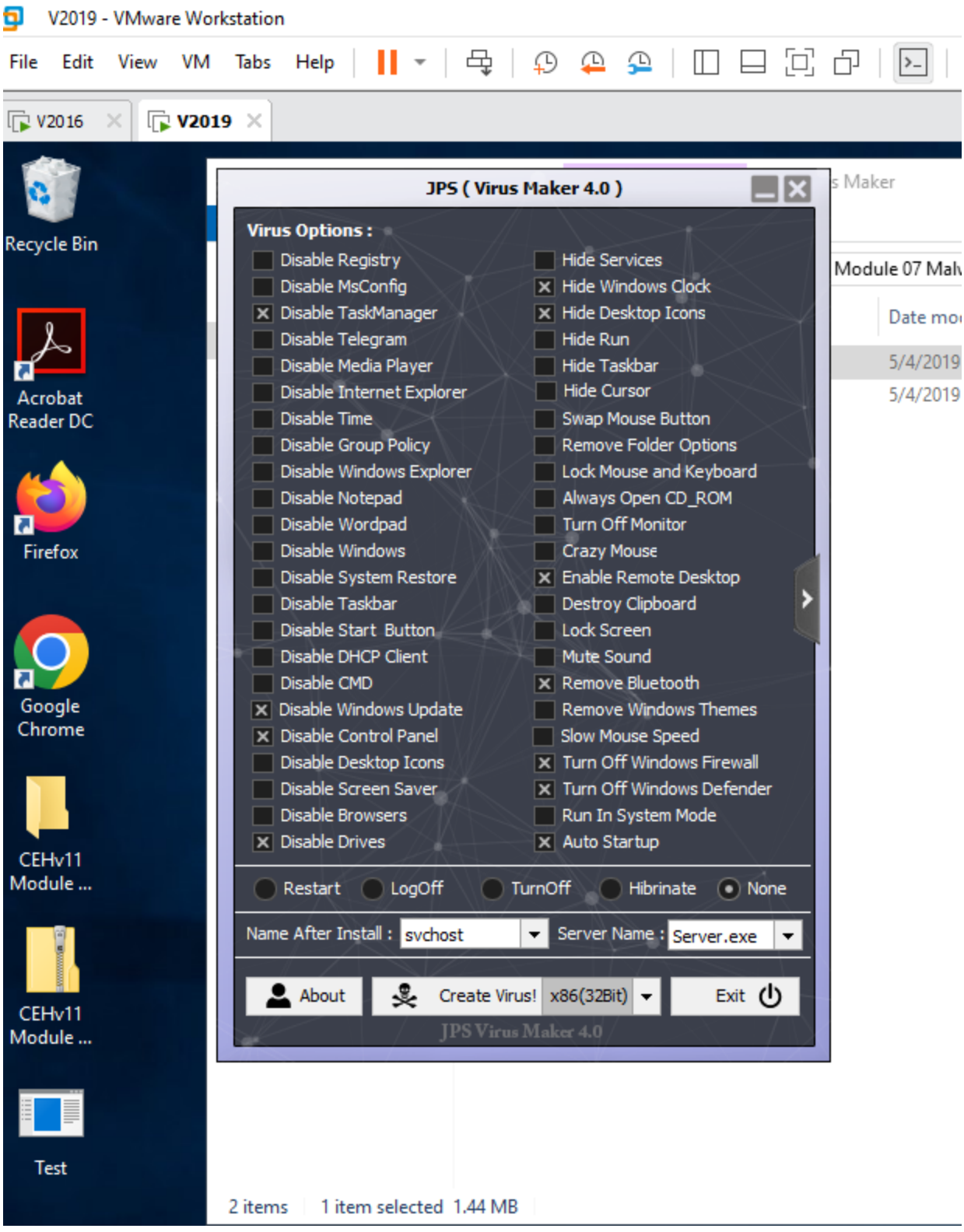
2. Infect the Target System using a Virus

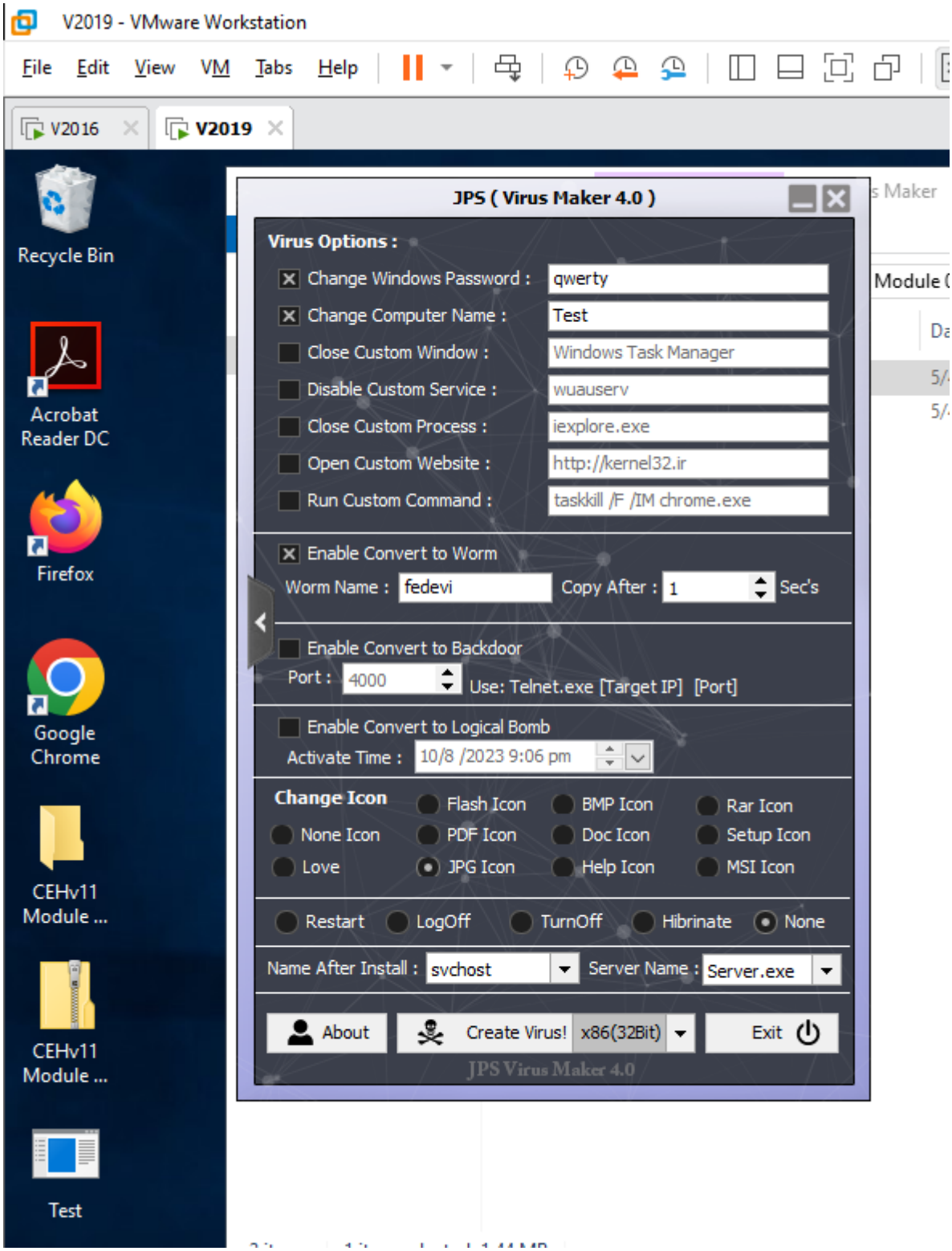
2.1 Create a Virus using the JPS Virus Maker Tool and Infect the Target System
- Open Windows Server 2019

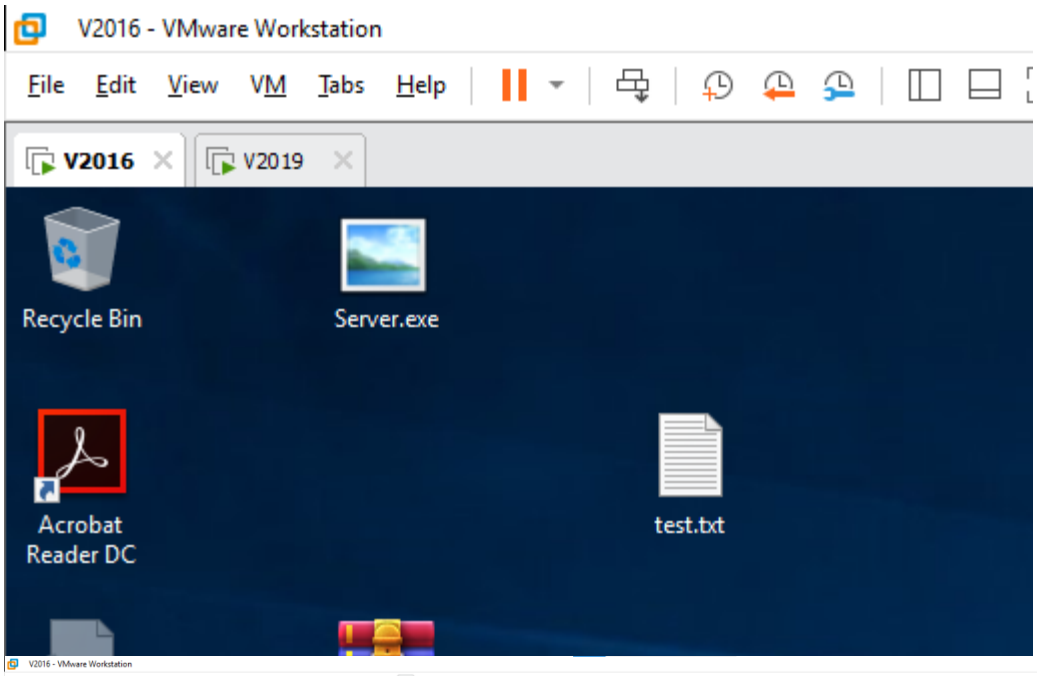


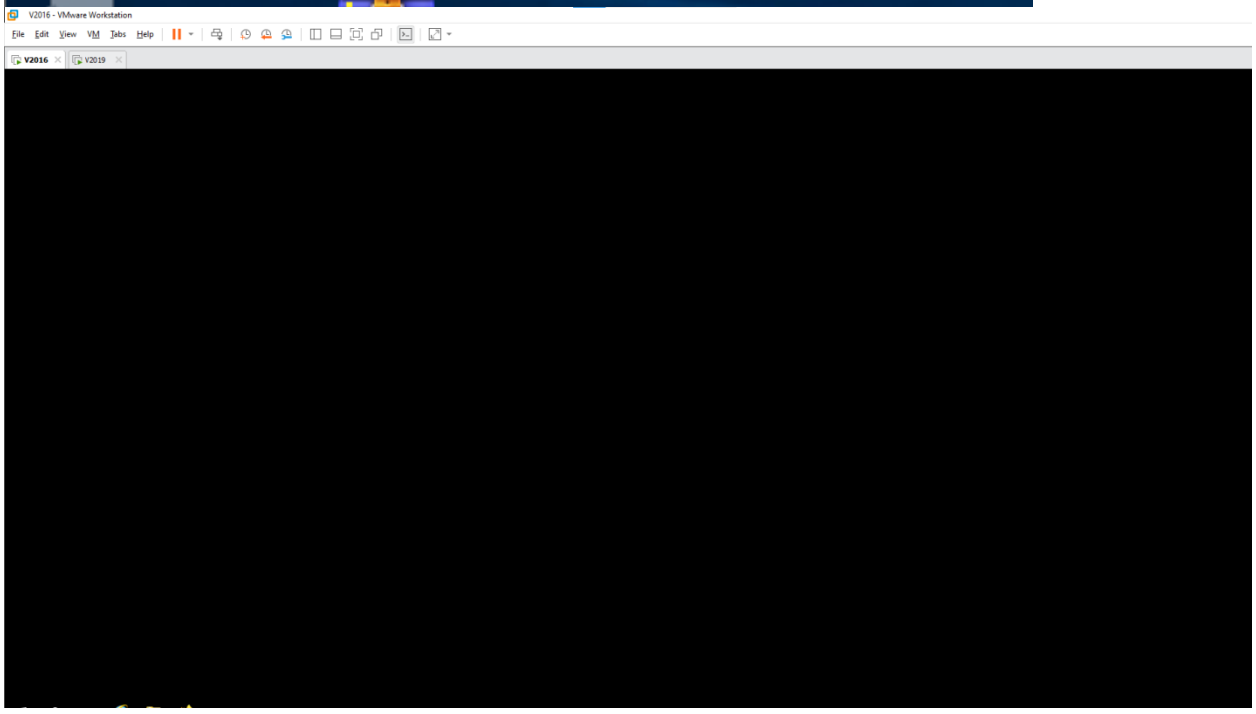

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
JPS Virus Maker
File Home Share View
CEHv11 Module 07 Malware Threats › CEHv11 Module 07 Malware Threats › Virus Maker › JPS Virus Maker
Search JPS Virus Maker
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
JPS
5/4/2019 2:08 PM
Application
1,480 KB
ReadMe
5/4/2019 2:05 PM
Text Document
2 KB
2 items

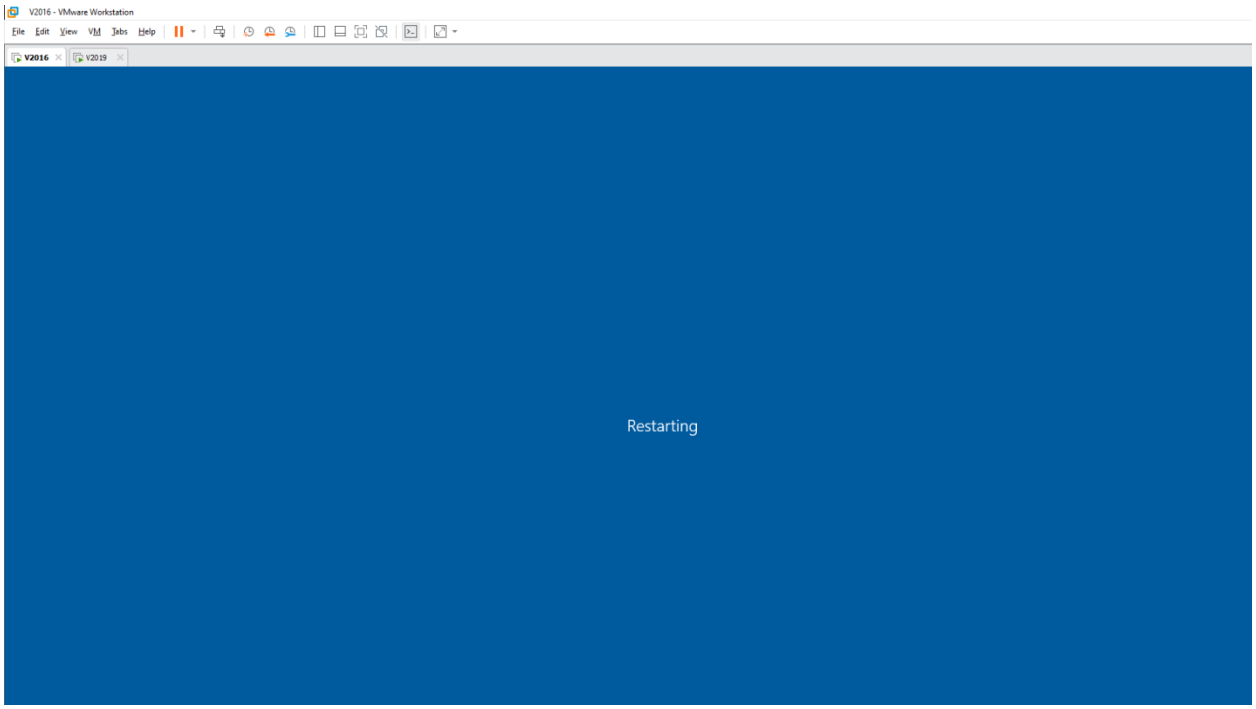

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
JPS (Virus Maker 4.0)
Virus Options :
Disable Registry
Disable MsConfig
Disable TaskManager
Disable Telegram
Disable Media Player
Disable Internet Explorer
Disable Time
Disable Group Policy
Disable Windows Explorer
Disable Notepad
Disable Wordpad
Disable Windows
Disable System Restore
Disable Taskbar
Disable Start Button
Disable DHCP Client
Disable CMD
Disable Windows Update
Disable Control Panel
Disable Desktop Icons
Disable Screen Saver
Disable Browsers
Disable Drives
Hide Services
Hide Windows Clock
Hide Desktop Icons
Hide Run
Hide Taskbar
Hide Cursor
Swap Mouse Button
Remove Folder Options
Lock Mouse and Keyboard
Always Open CD_ROM
Turn Off Monitor
Crazy Mouse
Enable Remote Desktop
Destroy Clipboard
Lock Screen
Mute Sound
Remove Bluetooth
Remove Windows Themes
Slow Mouse Speed
Turn Off Windows Firewall
Turn Off Windows Defender
Run In System Mode
Auto Startup
Restart LogOff TurnOff Hibrinate None
Name After Install : svchost
Server Name : Server.exe
About
Create Virus!
x86(32Bit)
Exit
JPS Virus Maker 4.0
Module 07 Malware Threats
Date modified
5/4/2019 2:08 PM
5/4/2019 2:05 PM


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
JPS (Virus Maker 4.0)
Virus Options :
Disable Registry
Disable MsConfig
Disable TaskManager
Disable Telegram
Disable Media Player
Disable Internet Explorer
Disable Time
Disable Group Policy
Disable Windows Explorer
Disable Notepad
Disable Wordpad
Disable Windows
Disable System Restore
Disable Taskbar
Disable Start Button
Disable DHCP Client
Disable CMD
Disable Windows Update
Disable Control Panel
Disable Desktop Icons
Disable Screen Saver
Disable Browsers
Disable Drives
Hide Services
Hide Windows Clock
Hide Desktop Icons
Hide Run
Hide Taskbar
Hide Cursor
Swap Mouse Button
Remove Folder Options
Lock Mouse and Keyboard
Always Open CD_ROM
Turn Off Monitor
Crazy Mouse
Enable Remote Desktop
Destroy Clipboard
Lock Screen
Mute Sound
Remove Bluetooth
Remove Windows Themes
Slow Mouse Speed
Turn Off Windows Firewall
Turn Off Windows Defender
Run In System Mode
Auto Startup
Restart LogOff TurnOff Hibrinate None
Name After Install : svchost
Server Name : Server.exe
About
Create Virus! x86(32Bit)
Exit
JPS Virus Maker 4.0
Module 07 Mal
Date mo
5/4/2019
5/4/2019
2 items 1 item selected 1.44 MB


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
JPS (Virus Maker 4.0)
Virus Options :
Change Windows Password : qwerty
Change Computer Name : Test
Close Custom Window : Windows Task Manager
Disable Custom Service : wuauserv
Close Custom Process : iexplore.exe
Open Custom Website : http://kernel32.ir
Run Custom Command : taskkill /F /IM chrome.exe
Enable Convert to Worm
Worm Name : fedevi
Copy After : 1 Sec's
Enable Convert to Backdoor
Port : 4000
Use: Telnet.exe [Target IP] [Port]
Enable Convert to Logical Bomb
Activate Time : 10/8 /2023 9:06 pm
Change Icon
Flash Icon
BMP Icon
Rar Icon
None Icon
PDF Icon
Doc Icon
Setup Icon
Love
JPG Icon
Help Icon
MSI Icon
Restart
LogOff
TurnOff
Hibrinate
None
Name After Install : svchost
Server Name : Server.exe
About
Create Virus!
x86(32Bit)
Exit
JPS Virus Maker 4.0


V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Server.exe
Acrobat Reader DC
test.txt

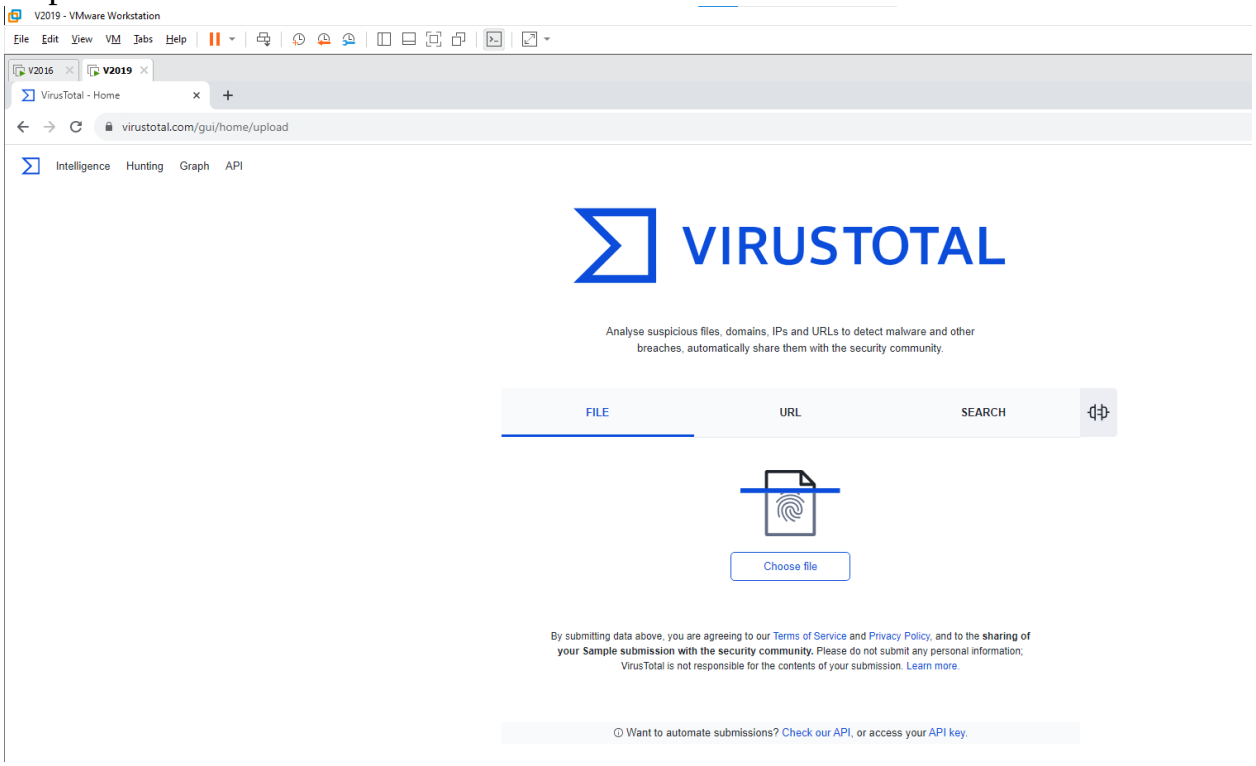


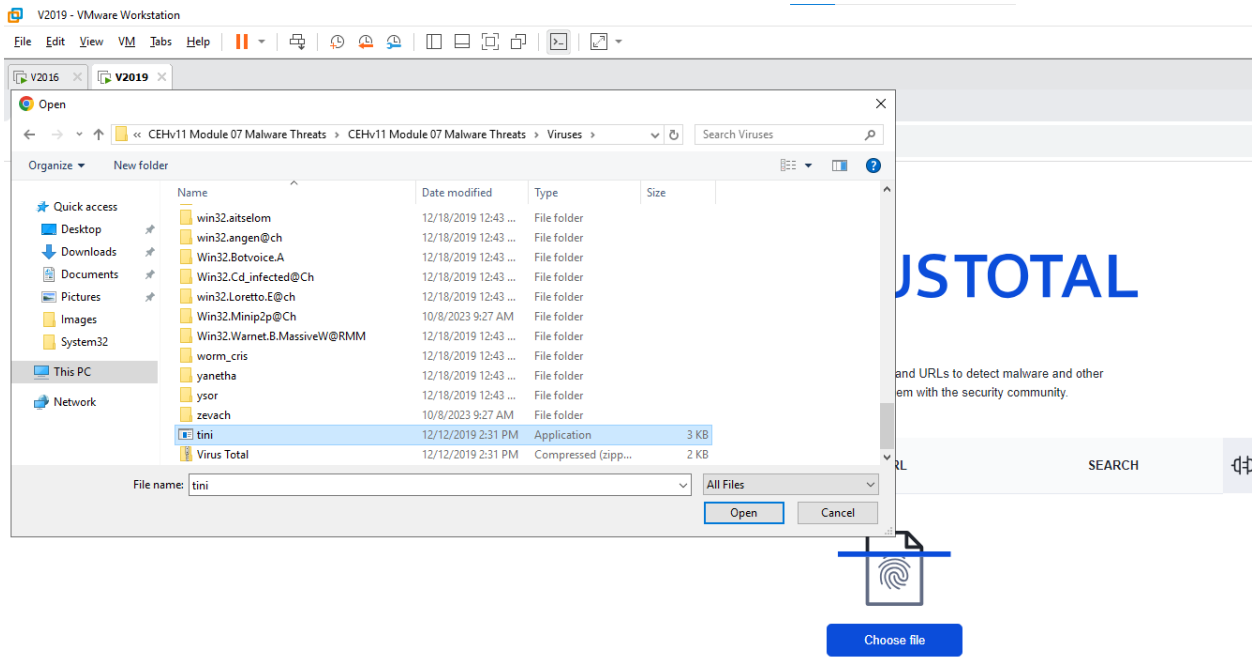


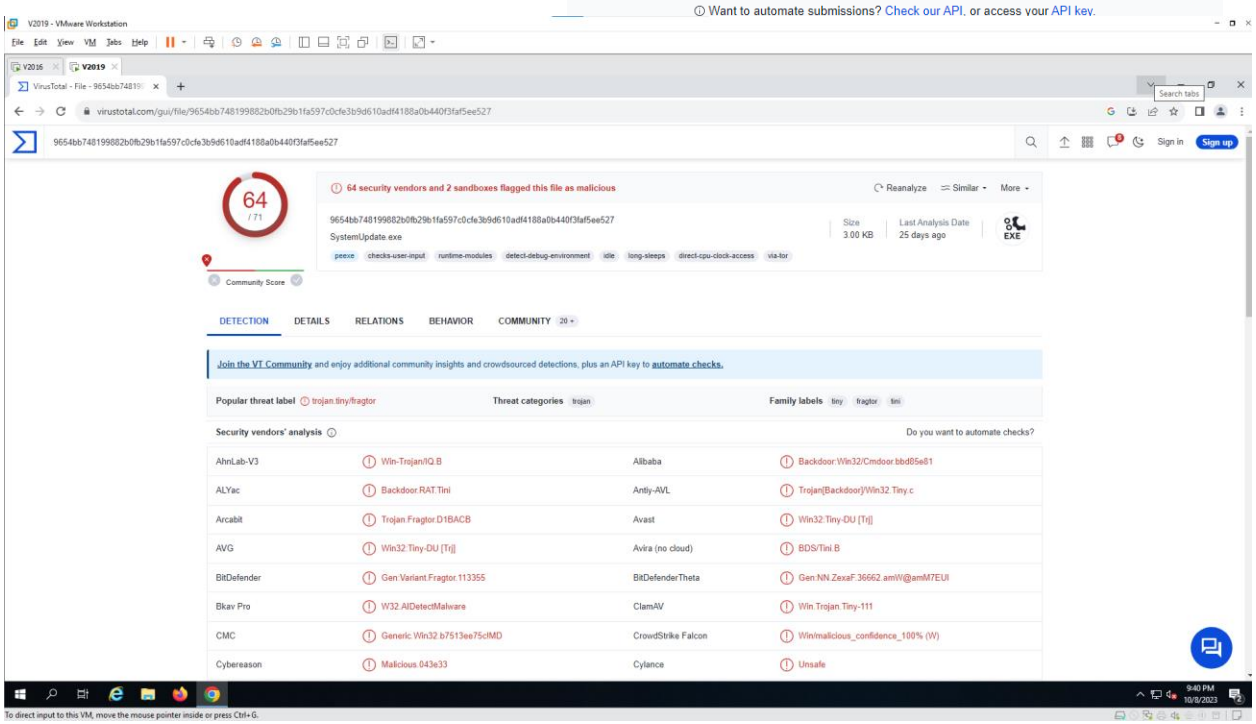
3. Perform Static Malware Analysis

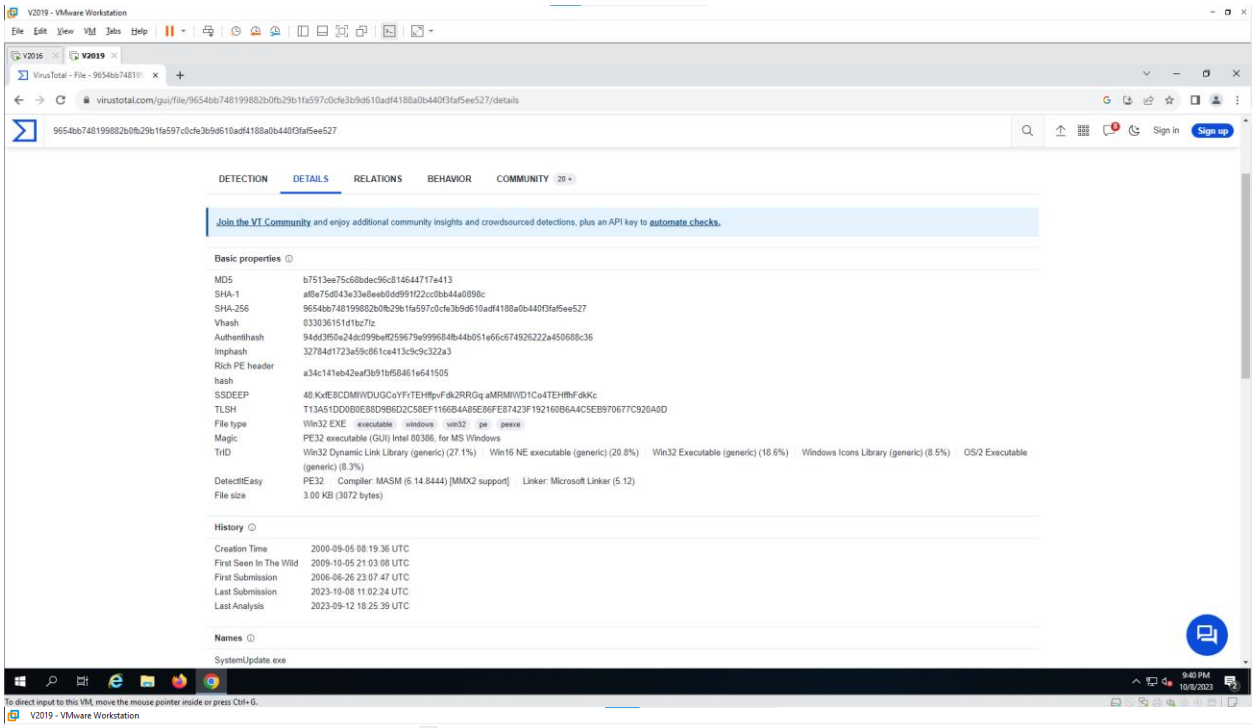
3.1 Perform Online Malware Scanning using VirusTotal

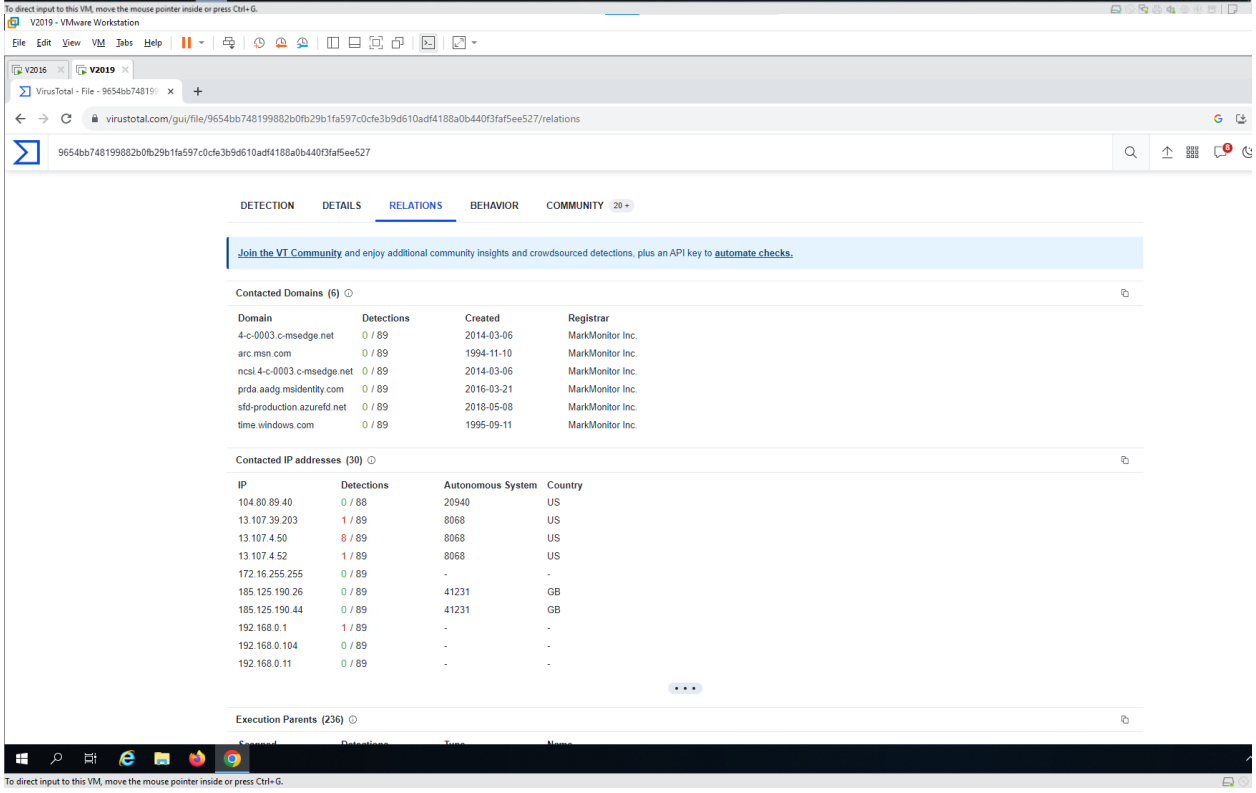
- Open Windows 10

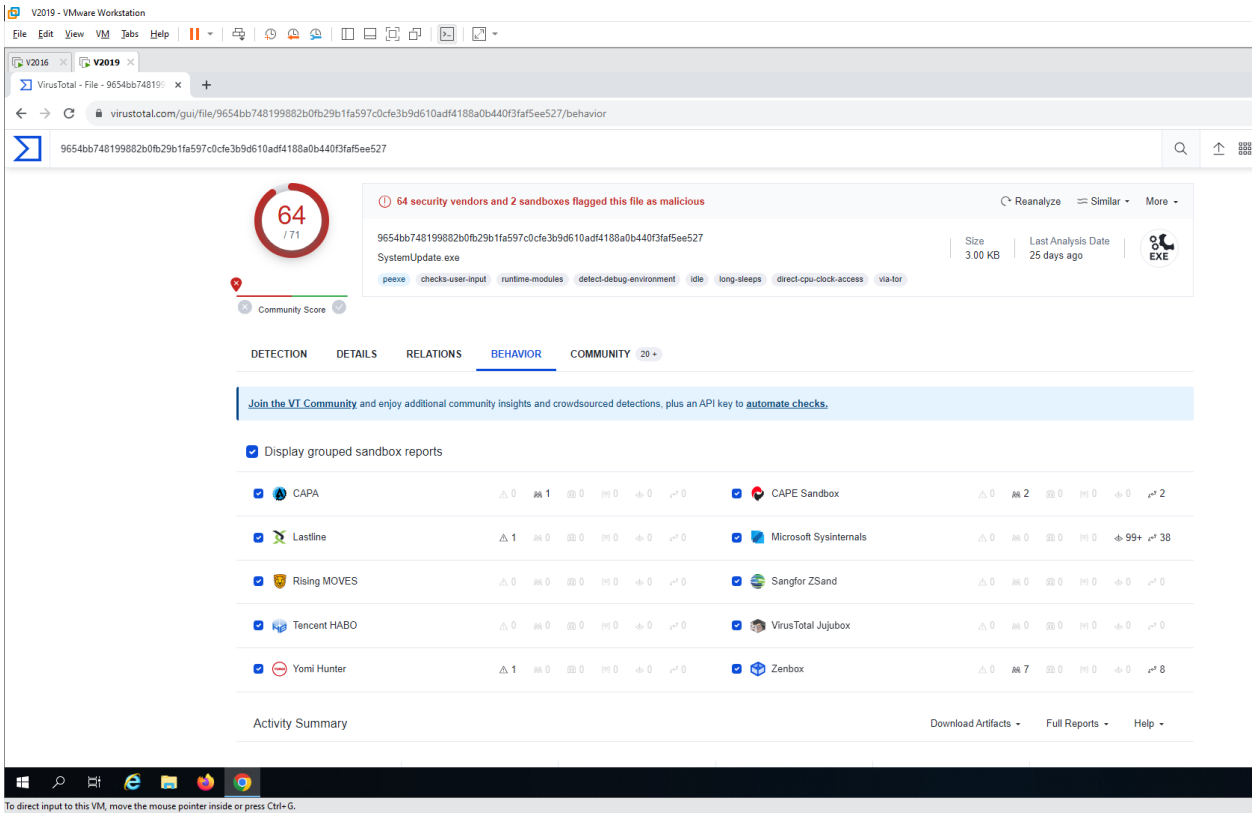



V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Open
CEHv11 Module 07 Malware Threats › CEHv11 Module 07 Malware Threats › Viruses ›
Search Viruses
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
win32.aitselom 12/18/2019 12:43 ... File folder
win32.angen@ch 12/18/2019 12:43 ... File folder
Win32.Botvoice.A 12/18/2019 12:43 ... File folder
Win32.Cd_infected@Ch 12/18/2019 12:43 ... File folder
win32.Loretto.E@ch 12/18/2019 12:43 ... File folder
Win32.Minip2p@Ch 10/8/2023 9:27 AM File folder
Win32.Warnet.B.MassiveW@RMM 12/18/2019 12:43 ... File folder
worm_cris 12/18/2019 12:43 ... File folder
yanetha 12/18/2019 12:43 ... File folder
ysor 12/18/2019 12:43 ... File folder
zevach 10/8/2023 9:27 AM File folder
tini 12/12/2019 2:31 PM Application 3 KB
Virus Total 12/12/2019 2:31 PM Compressed (zipp... 2 KB
File name: tini
All Files
Open
Cancel
USTOTAL
and URLs to detect malware and other
em with the security community.
SEARCH
Choose file
By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.


Want to automate submissions? Check our API, or access your API key.
V2019 - VMware Workstation
9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527
Sign in
Sign up
64
/ 71
64 security vendors and 2 sandboxes flagged this file as malicious
Reanalyze
Similar
More
9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527
SystemUpdate.exe
Size
3.00 KB
Last Analysis Date
25 days ago
EXE
peexe
checks-user-input
runtime-modules
detect-debug-environment
idle
long-sleeps
direct-cpu-clock-access
via-tor
Community Score
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 20 +
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label
trojan.tiny/fragtor
Threat categories
trojan
Family labels
tiny
fragtor
tini
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3
Win-Trojan/IQ.B
Alibaba
Backdoor:Win32/Cmdoor.bbd85e81
ALYac
Backdoor.RAT.Tini
Antiy-AVL
Trojan[Backdoor]/Win32.Tiny.c
Arcabit
Trojan.Fragtor.D1BACB
Avast
Win32:Tiny-DU [Trj]
AVG
Win32:Tiny-DU [Trj]
Avira (no cloud)
BDS/Tini.B
BitDefender
Gen:Variant.Fragtor.113355
BitDefenderTheta
Gen:NN.ZexaF.36662.amW@amM7EUI
Bkav Pro
W32.AIDetectMalware
ClamAV
Win.Trojan.Tiny-111
CMC
Generic.Win32.b7513ee75cfMD
CrowdStrike Falcon
Win/malicious_confidence_100% (W)
Cybereason
Malicious.043e33
Cylance
Unsafe
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

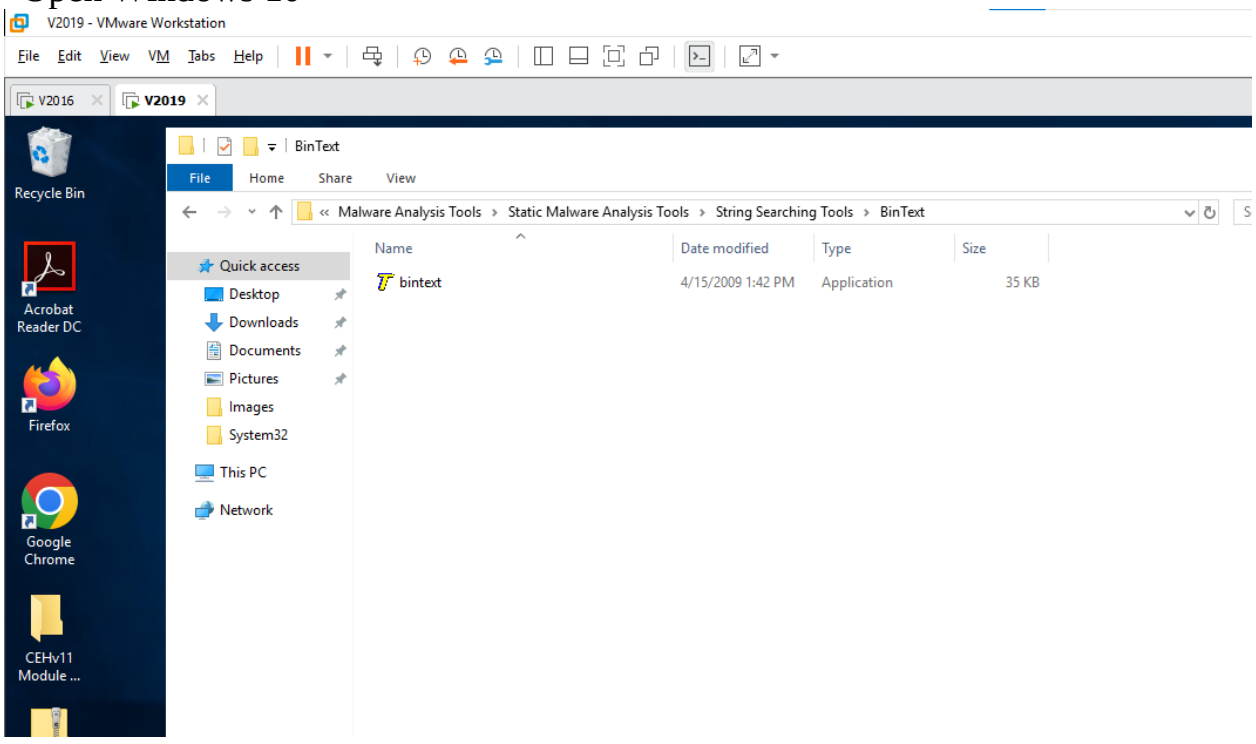

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
VirusTotal - File - 9654bb74819
virustotal.com/gui/file/9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527/details
9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527
Sign in
Sign up
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 20+
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Basic properties
MD5 b7513ee75c68bdec96c814644717e413
SHA-1 af8e75d043e33e8eeb0dd991f22cc0bb44a0898c
SHA-256 9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527
Vhash 033036151d1bz7lz
Authentihash 94dd3f50e24dc099beff259679e999684fb44b051e66c674926222a450688c36
Imphash 32784d1723a59c861ce413c9c9c322a3
Rich PE header hash a34c141eb42eaf3b91bf58461e641505
SSDEEP 48:KxfE8CDMlWDUGCoYFrTEHffpvFdk2RRGq:aMRMlWD1Co4TEHffhFdkKc
TLSH T13A51DD0B0E88D9B6D2C58EF1166B4A85E86FE87423F192160B6A4C5EB970677C920A0D
File type Win32 EXE executable windows win32 pe peexe
Magic PE32 executable (GUI) Intel 80386, for MS Windows
TrID Win32 Dynamic Link Library (generic) (27.1%) Win16 NE executable (generic) (20.8%) Win32 Executable (generic) (18.6%) Windows Icons Library (generic) (8.5%) OS/2 Executable (generic) (8.3%)
DetectItEasy PE32 Compiler: MASM (6.14.8444) [MMX2 support] Linker: Microsoft Linker (5.12)
File size 3.00 KB (3072 bytes)
History
Creation Time 2000-09-05 08:19:36 UTC
First Seen In The Wild 2009-10-05 21:03:08 UTC
First Submission 2006-06-26 23:07:47 UTC
Last Submission 2023-10-08 11:02:24 UTC
Last Analysis 2023-09-12 18:25:39 UTC
Names
SystemUpdate.exe
9:40 PM
10/8/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

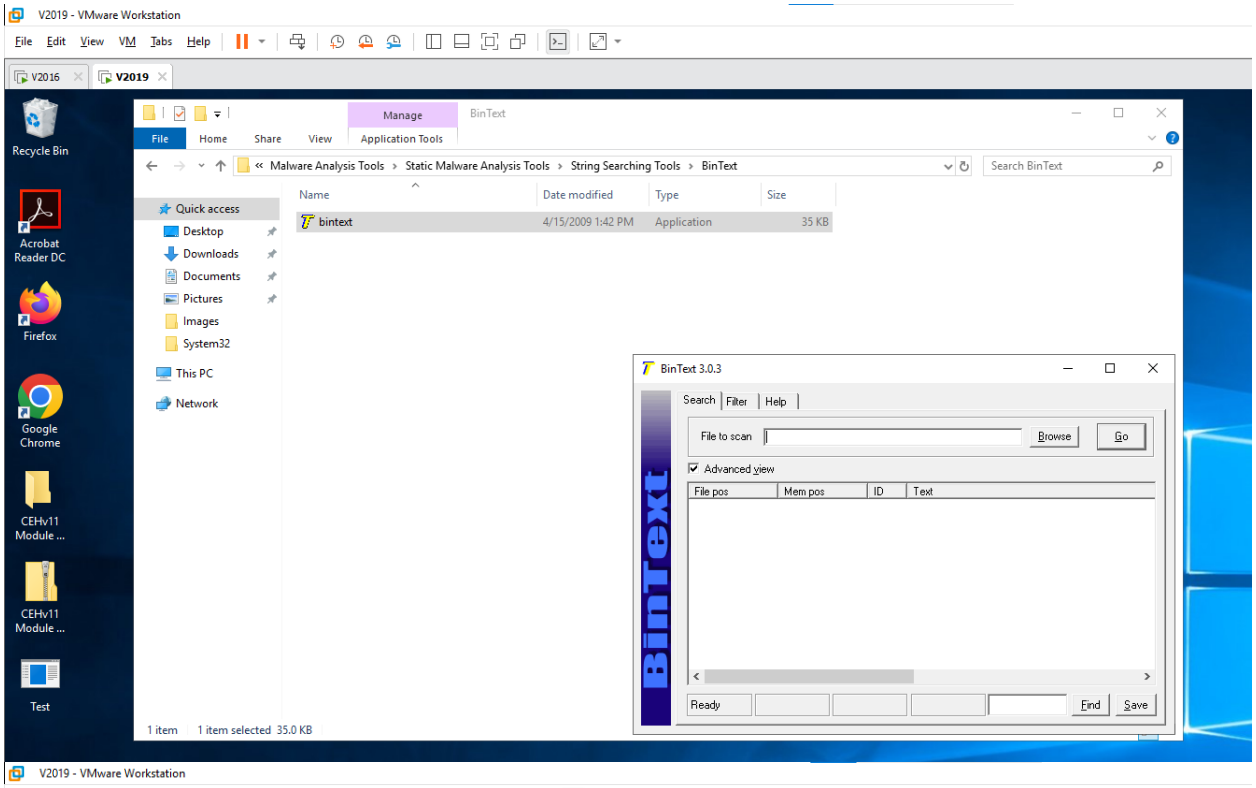

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
VirusTotal - File - 9654bb74819
virustotal.com/gui/file/9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527/relations
9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 20+
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Contacted Domains (6)
Domain Detections Created Registrar
4-c-0003.c-msedge.net 0 / 89 2014-03-06 MarkMonitor Inc.
arc.msn.com 0 / 89 1994-11-10 MarkMonitor Inc.
ncsi.4-c-0003.c-msedge.net 0 / 89 2014-03-06 MarkMonitor Inc.
prda.aadg.msidentity.com 0 / 89 2016-03-21 MarkMonitor Inc.
sfd-production.azurefd.net 0 / 89 2018-05-08 MarkMonitor Inc.
time.windows.com 0 / 89 1995-09-11 MarkMonitor Inc.
Contacted IP addresses (30)
IP Detections Autonomous System Country
104.80.89.40 0 / 88 20940 US
13.107.39.203 1 / 89 8068 US
13.107.4.50 8 / 89 8068 US
13.107.4.52 1 / 89 8068 US
172.16.255.255 0 / 89 - -
185.125.190.26 0 / 89 41231 GB
185.125.190.44 0 / 89 41231 GB
192.168.0.1 1 / 89 - -
192.168.0.104 0 / 89 - -
192.168.0.11 0 / 89 - -
Execution Parents (236)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

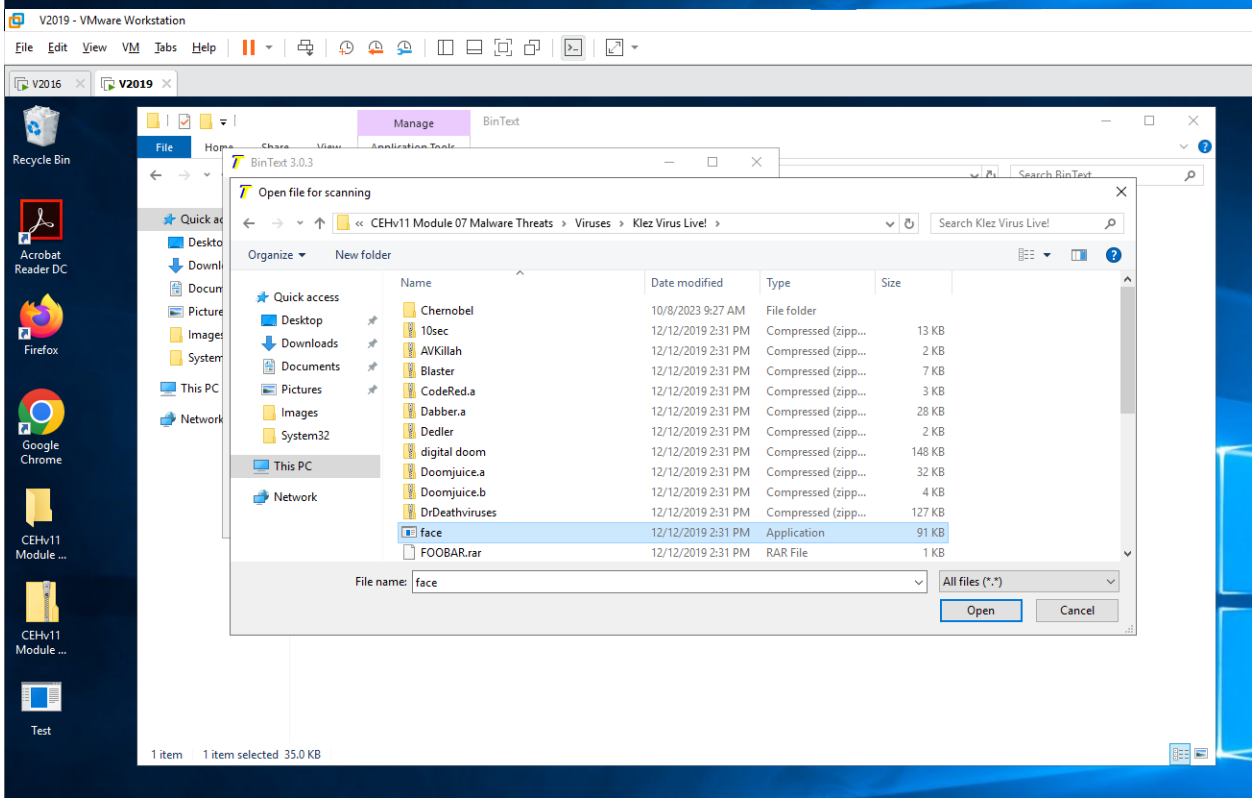


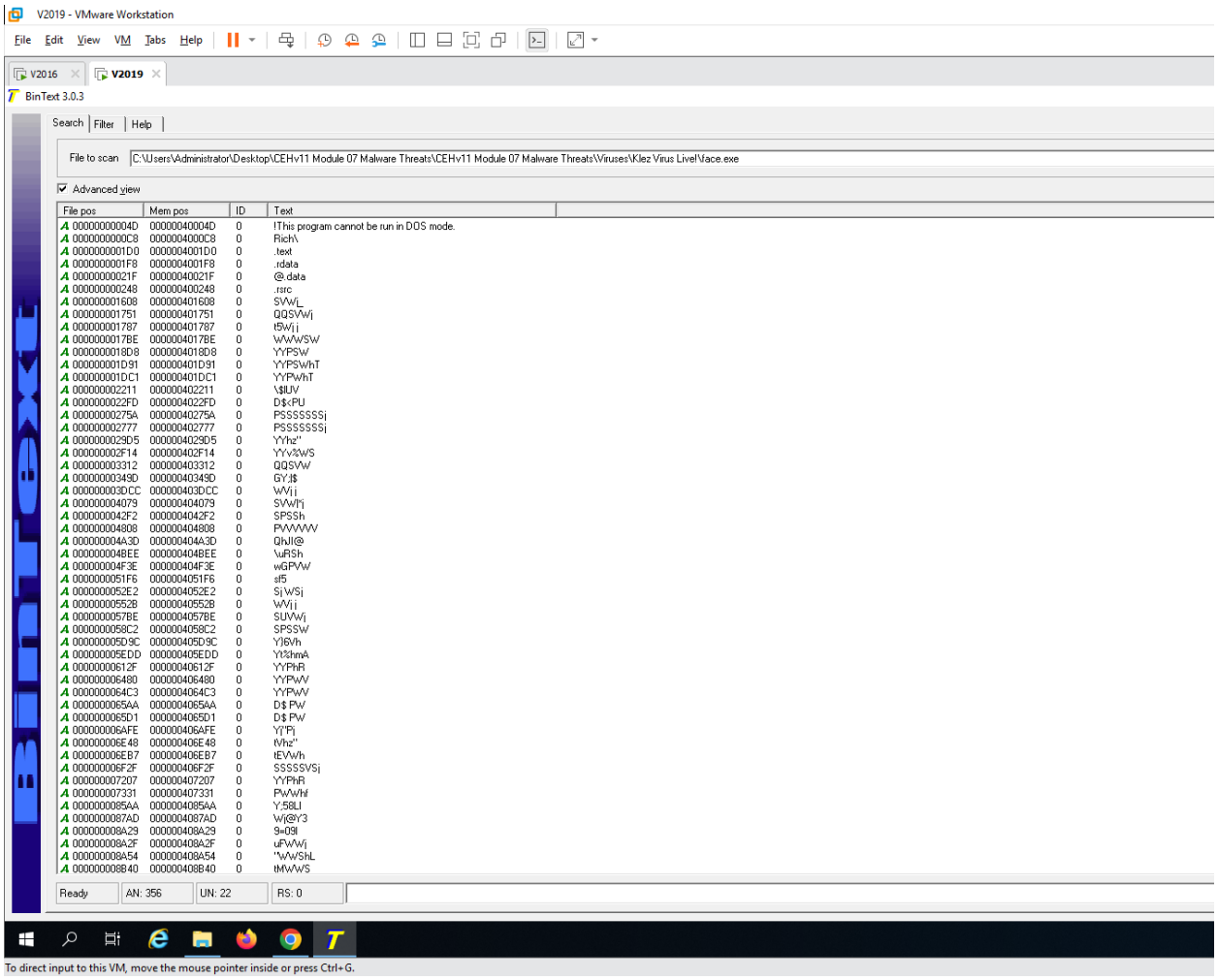
3.2 Perform a Strings Search using BinText

- Open Windows 10



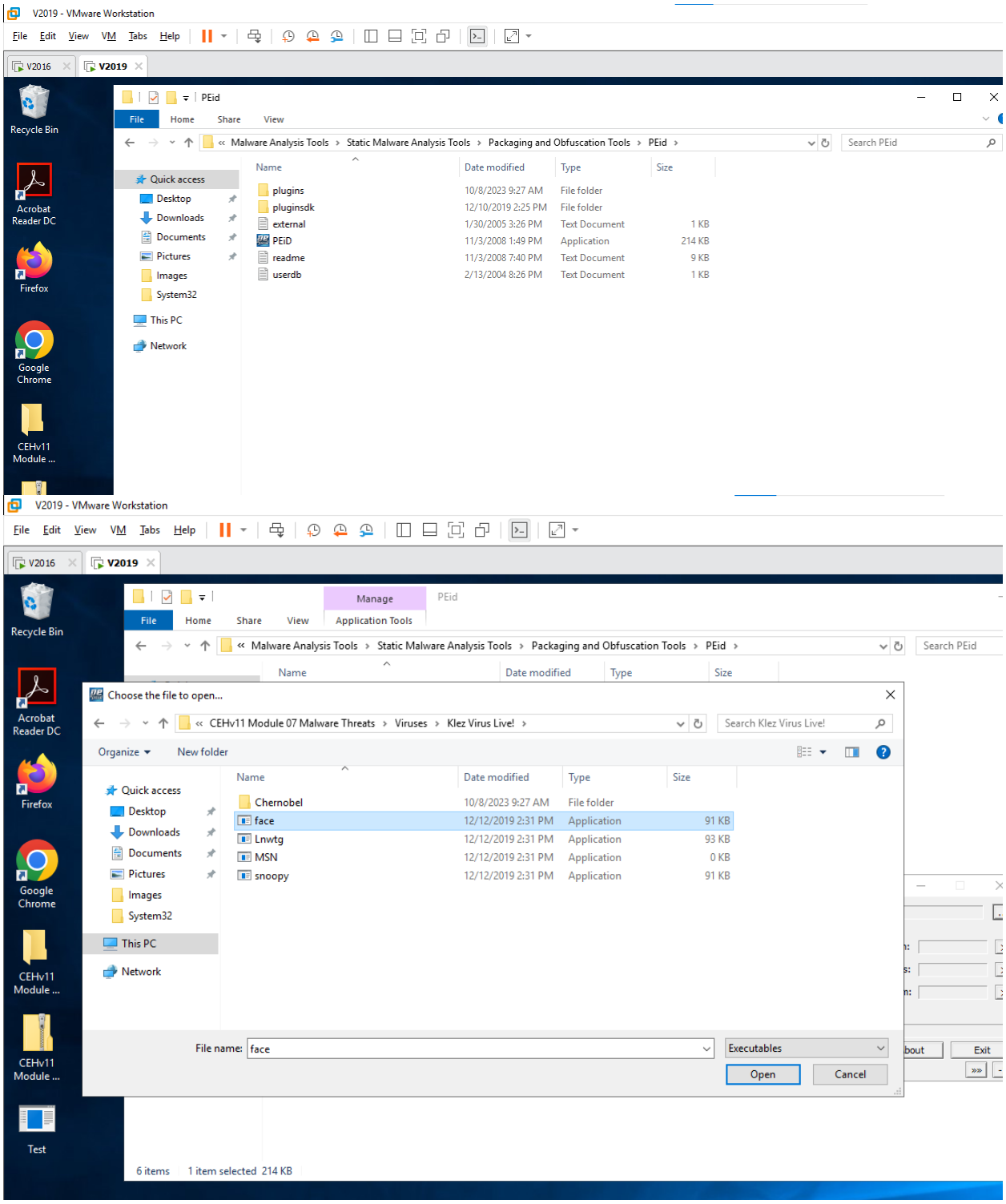

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
Manage
BinText
File Home Share View Application Tools
Malware Analysis Tools › Static Malware Analysis Tools › String Searching Tools › BinText
Search BinText
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
bintext
4/15/2009 1:42 PM
Application
35 KB
1 item
1 item selected 35.0 KB
BinText 3.0.3
Search Filter Help
File to scan
Browse
Go
Advanced view
File pos
Mem pos
ID
Text
Ready
Find
Save

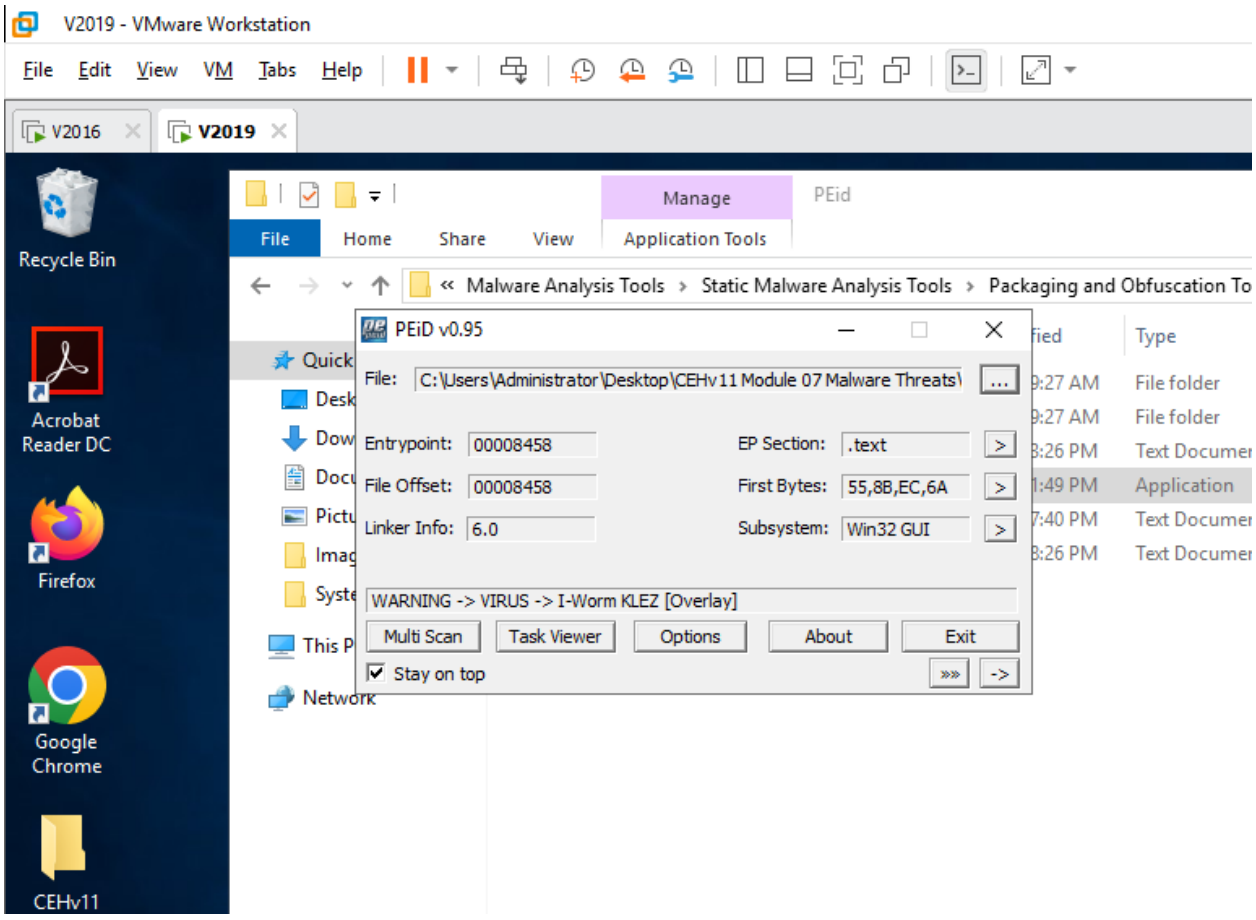

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
BinText 3.0.3
Open file for scanning
CEHv11 Module 07 Malware Threats › Viruses › Klez Virus Live! ›
Search Klez Virus Live!
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
Chernobel 10/8/2023 9:27 AM File folder
10sec 12/12/2019 2:31 PM Compressed (zipp... 13 KB
AVKillah 12/12/2019 2:31 PM Compressed (zipp... 2 KB
Blaster 12/12/2019 2:31 PM Compressed (zipp... 7 KB
CodeRed.a 12/12/2019 2:31 PM Compressed (zipp... 3 KB
Dabber.a 12/12/2019 2:31 PM Compressed (zipp... 28 KB
Dedler 12/12/2019 2:31 PM Compressed (zipp... 2 KB
digital doom 12/12/2019 2:31 PM Compressed (zipp... 148 KB
Doomjuice.a 12/12/2019 2:31 PM Compressed (zipp... 32 KB
Doomjuice.b 12/12/2019 2:31 PM Compressed (zipp... 4 KB
DrDeathviruses 12/12/2019 2:31 PM Compressed (zipp... 127 KB
face 12/12/2019 2:31 PM Application 91 KB
FOOBAR.rar 12/12/2019 2:31 PM RAR File 1 KB
File name: face
All files (*.*)
Open
Cancel
1 item
1 item selected 35.0 KB



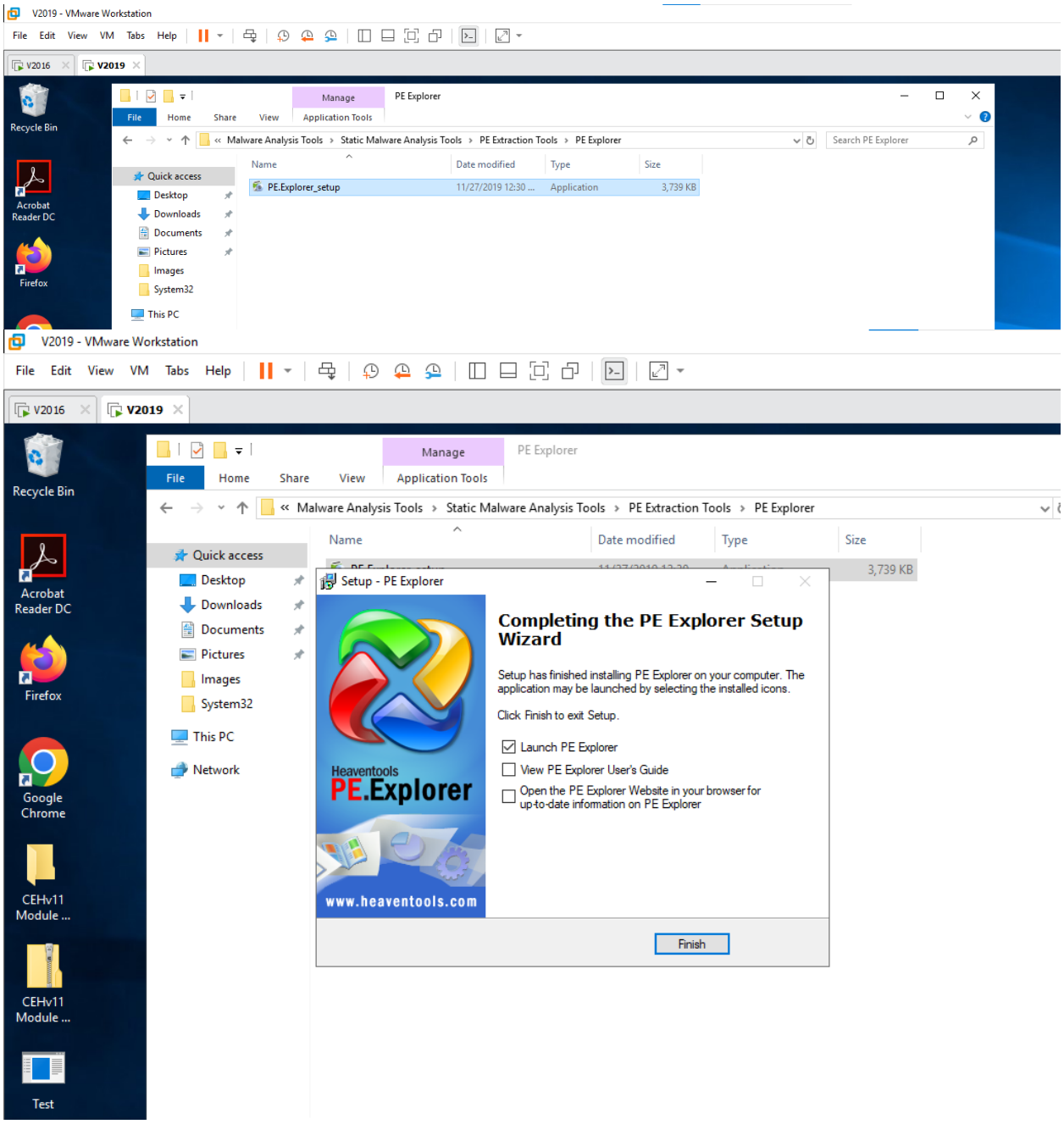
3.3 Identify Packaging and Obfuscation Methods using PEid

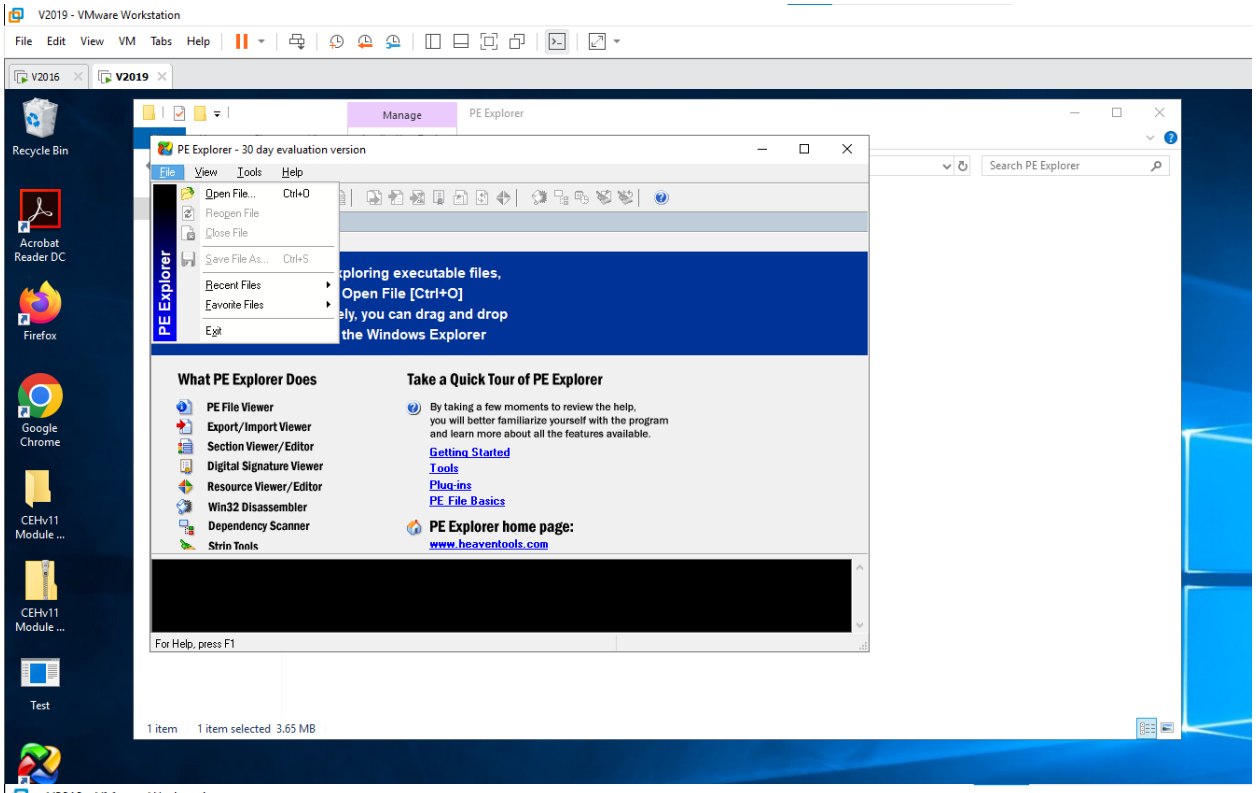
- Open Windows 10

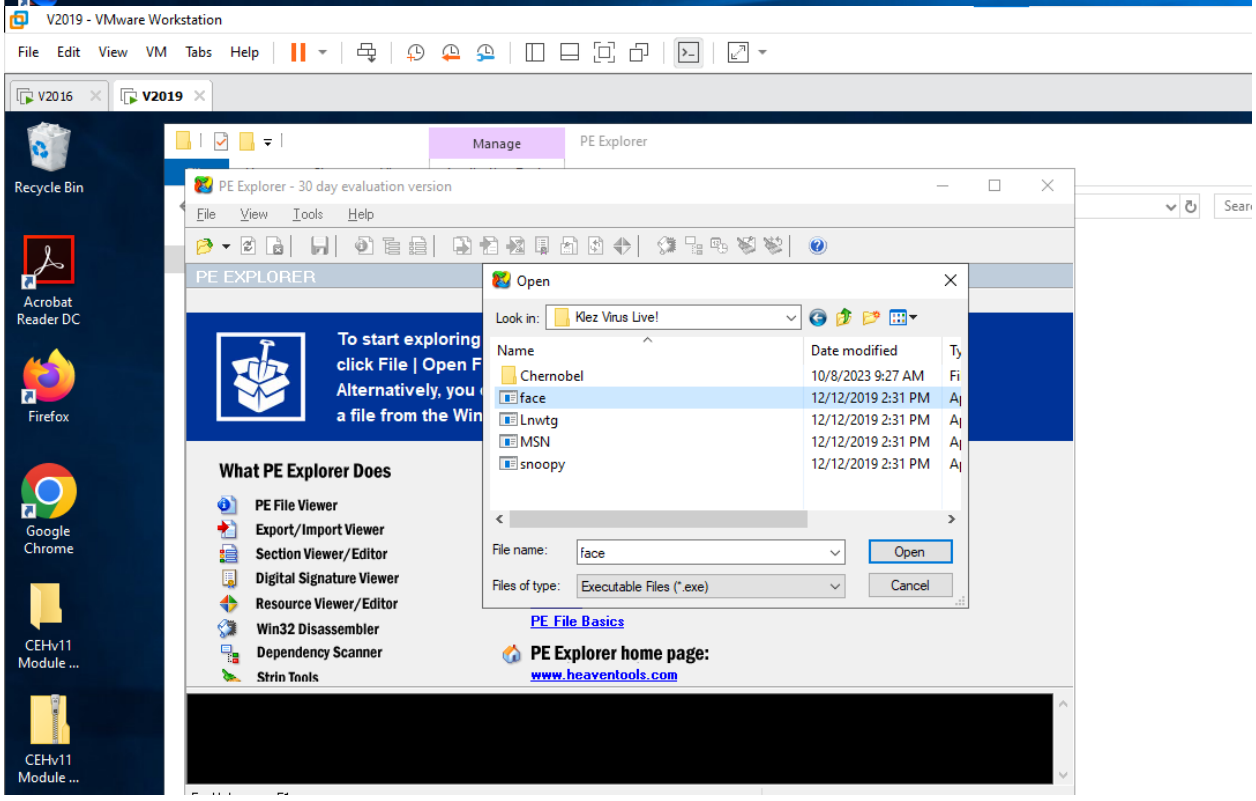

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
PEid
File Home Share View
Malware Analysis Tools › Static Malware Analysis Tools › Packaging and Obfuscation Tools › PEid ›
Search PEid
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name Date modified Type Size
plugins 10/8/2023 9:27 AM File folder
pluginsdk 12/10/2019 2:25 PM File folder
external 1/30/2005 3:26 PM Text Document 1 KB
PEiD 11/3/2008 1:49 PM Application 214 KB
readme 11/3/2008 7:40 PM Text Document 9 KB
userdb 2/13/2004 8:26 PM Text Document 1 KB
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
Manage
PEid
File Home Share View Application Tools
Malware Analysis Tools › Static Malware Analysis Tools › Packaging and Obfuscation Tools › PEid ›
Search PEid
Choose the file to open...
CEHv11 Module 07 Malware Threats › Viruses › Klez Virus Live! ›
Search Klez Virus Live!
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name Date modified Type Size
Chernobel 10/8/2023 9:27 AM File folder
face 12/12/2019 2:31 PM Application 91 KB
Lnwtg 12/12/2019 2:31 PM Application 93 KB
MSN 12/12/2019 2:31 PM Application 0 KB
snoopy 12/12/2019 2:31 PM Application 91 KB
File name: face
Executables
Open
Cancel
Exit
6 items
1 item selected 214 KB

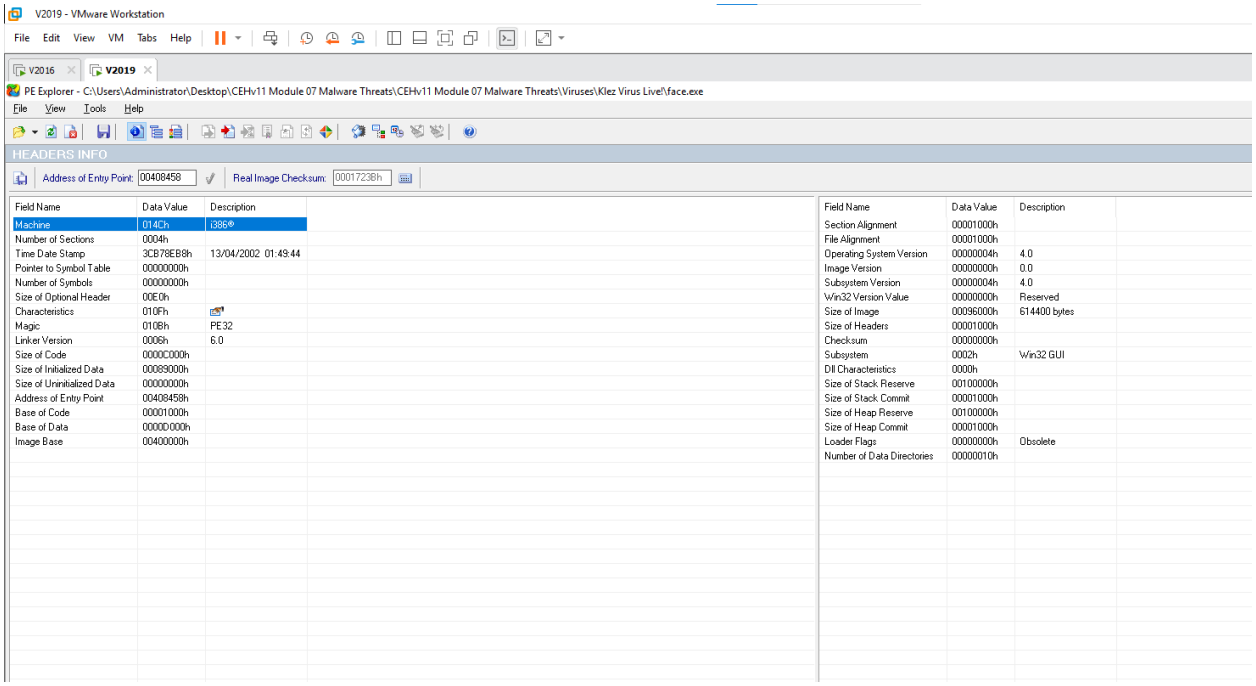


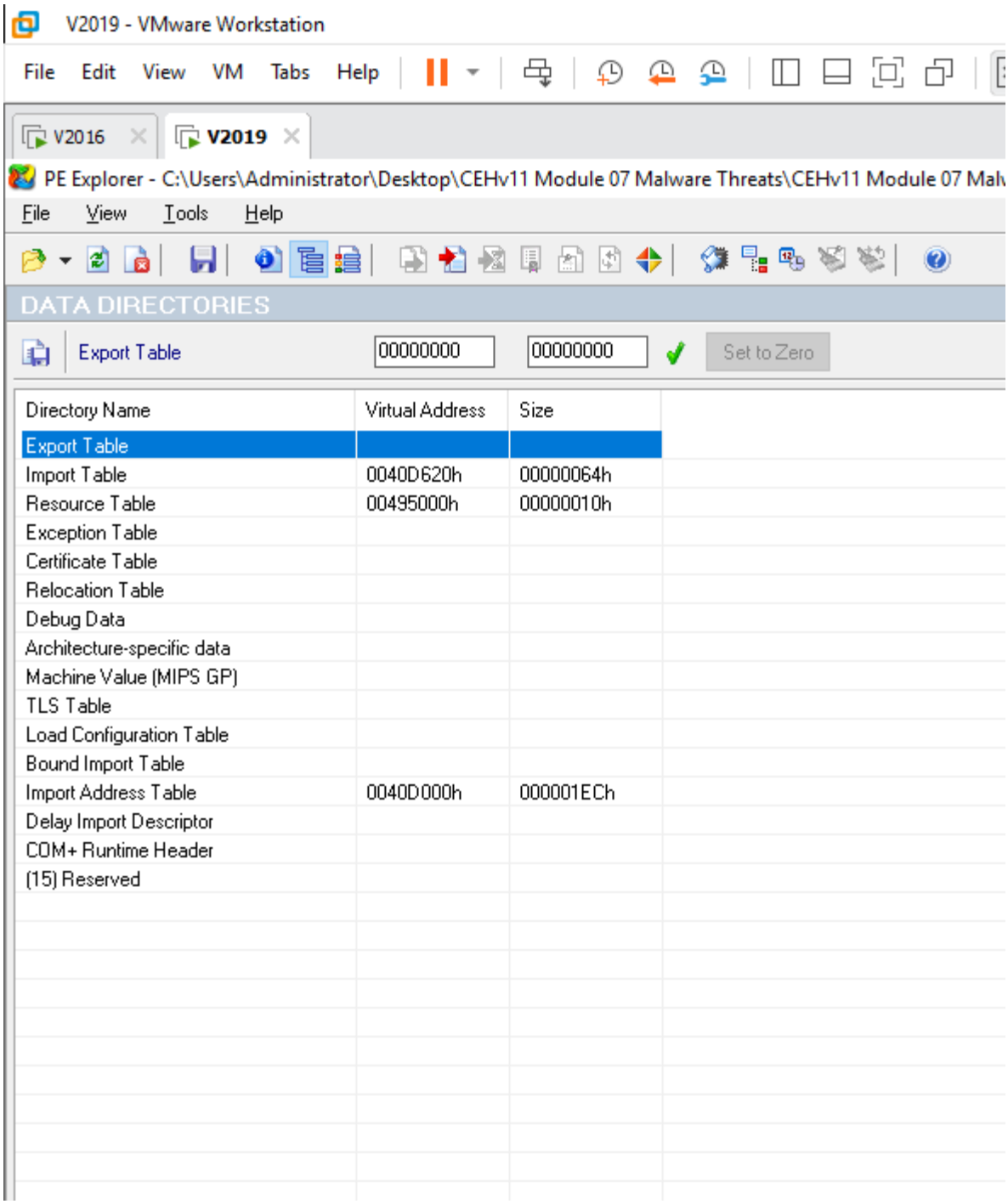
3.4 Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer

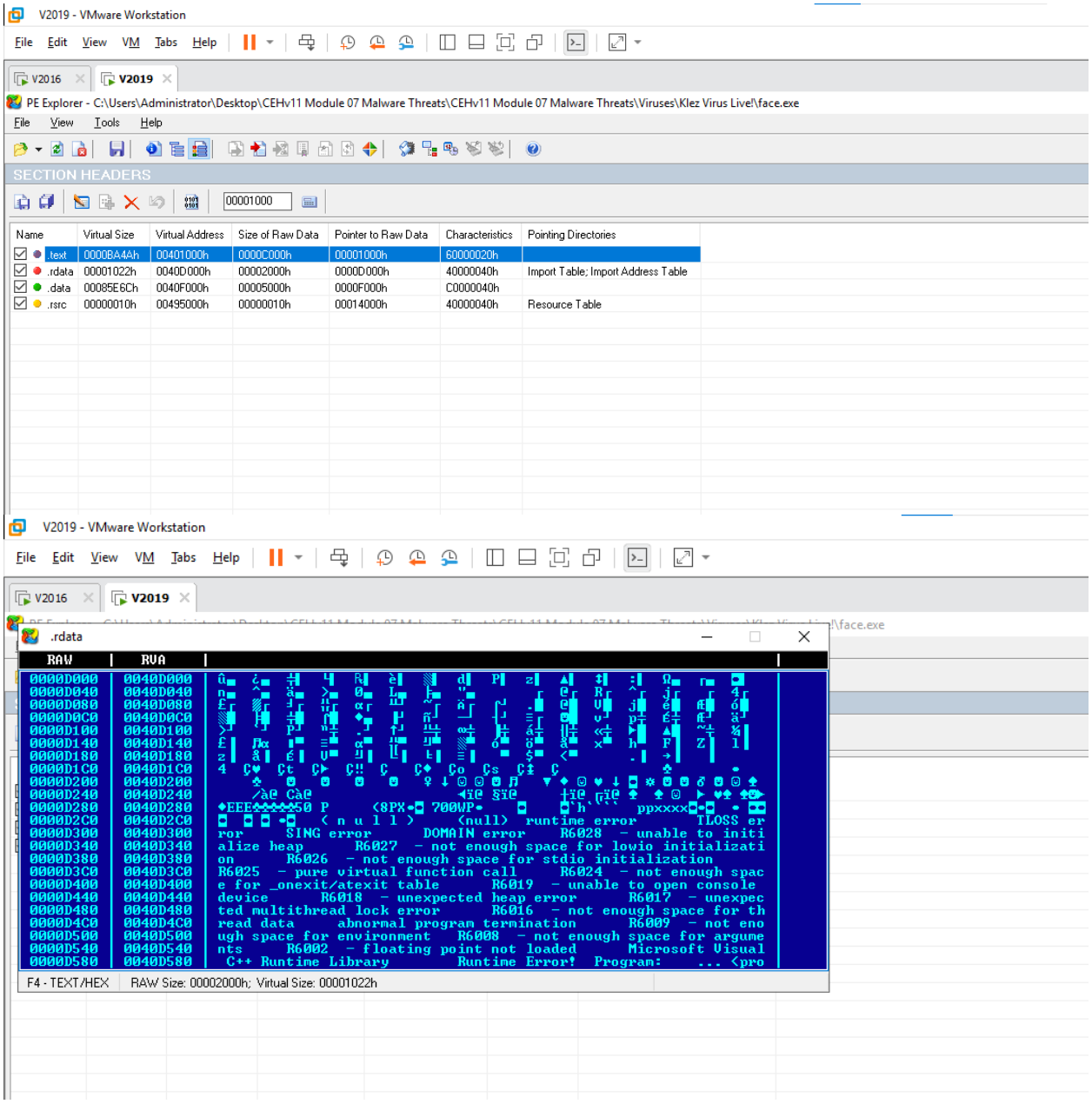

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
Manage
PE Explorer
File Home Share View Application Tools
« Malware Analysis Tools › Static Malware Analysis Tools › PE Extraction Tools › PE Explorer
Search PE Explorer
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
PE.Explorer_setup
11/27/2019 12:30 ...
Application
3,739 KB
Setup - PE Explorer
Completing the PE Explorer Setup Wizard
Setup has finished installing PE Explorer on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch PE Explorer
View PE Explorer User's Guide
Open the PE Explorer Website in your browser for up-to-date infomation on PE Explorer
Heaventools
PE.Explorer
www.heaventools.com
Finish


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
Manage
PE Explorer
PE Explorer - 30 day evaluation version
File View Tools Help
Open File... Ctrl+O
Reopen File
Close File
Save File As... Ctrl+S
Recent Files
Favorite Files
Exit
PE Explorer
oring executable files,
Open File [Ctrl+O]
ly, you can drag and drop
the Windows Explorer
What PE Explorer Does
PE File Viewer
Export/Import Viewer
Section Viewer/Editor
Digital Signature Viewer
Resource Viewer/Editor
Win32 Disassembler
Dependency Scanner
Strin Tools
Take a Quick Tour of PE Explorer
By taking a few moments to review the help, you will better familiarize yourself with the program and learn more about all the features available.
Getting Started
Tools
Plug-ins
PE File Basics
PE Explorer home page:
www.heaventools.com
For Help, press F1
Search PE Explorer
1 item
1 item selected 3.65 MB

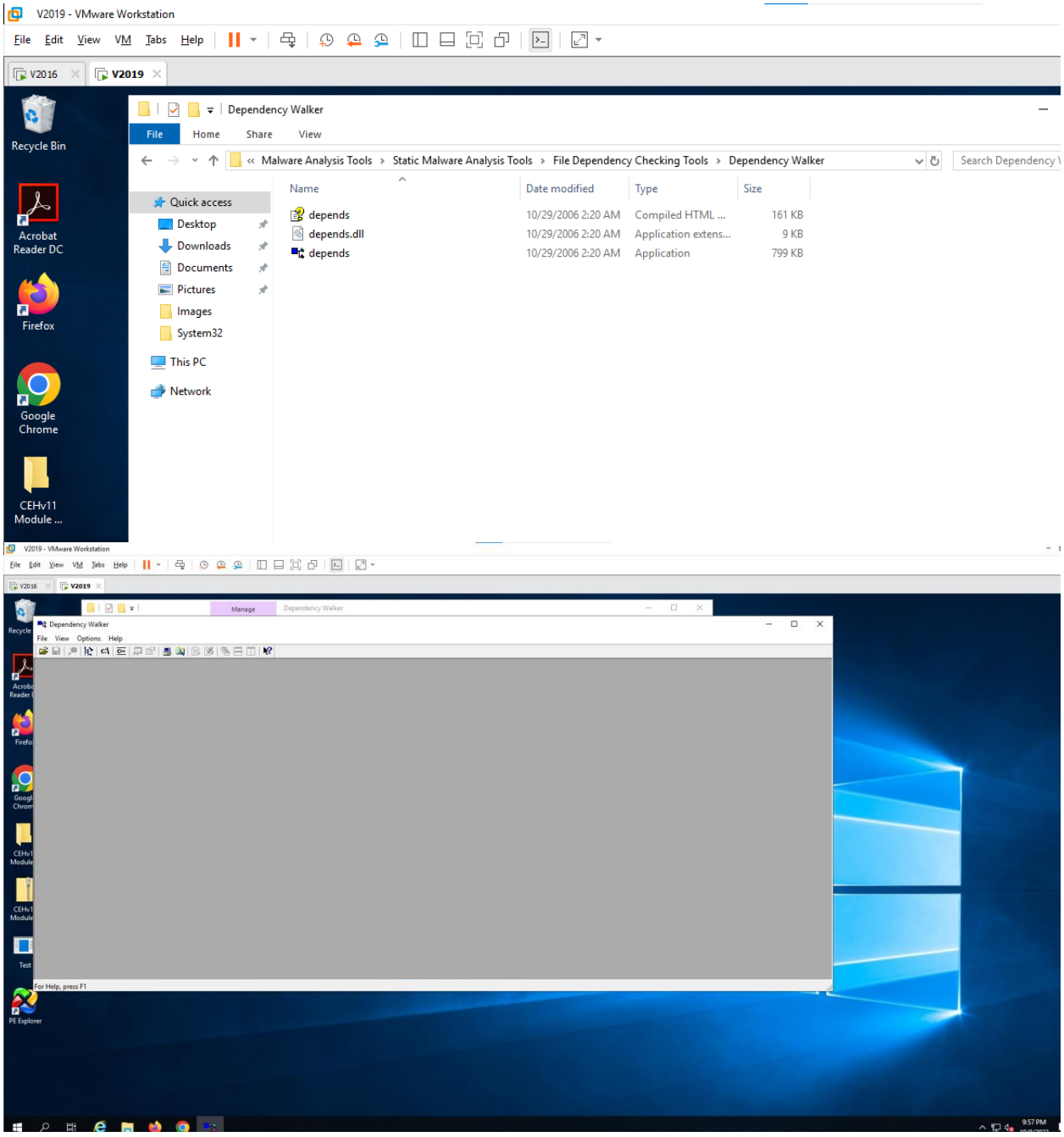

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Manage
PE Explorer
PE Explorer - 30 day evaluation version
File View Tools Help
PE EXPLORER
To start exploring
click File | Open F
Alternatively, you
a file from the Win
What PE Explorer Does
PE File Viewer
Export/Import Viewer
Section Viewer/Editor
Digital Signature Viewer
Resource Viewer/Editor
Win32 Disassembler
Dependency Scanner
Strin Tools
Open
Look in: Klez Virus Live!
Name
Date modified
Chernobel 10/8/2023 9:27 AM
face 12/12/2019 2:31 PM
Lnwtg 12/12/2019 2:31 PM
MSN 12/12/2019 2:31 PM
snoopy 12/12/2019 2:31 PM
File name: face
Open
Files of type: Executable Files (*.exe)
Cancel
PE File Basics
PE Explorer home page:
www.heaventools.com

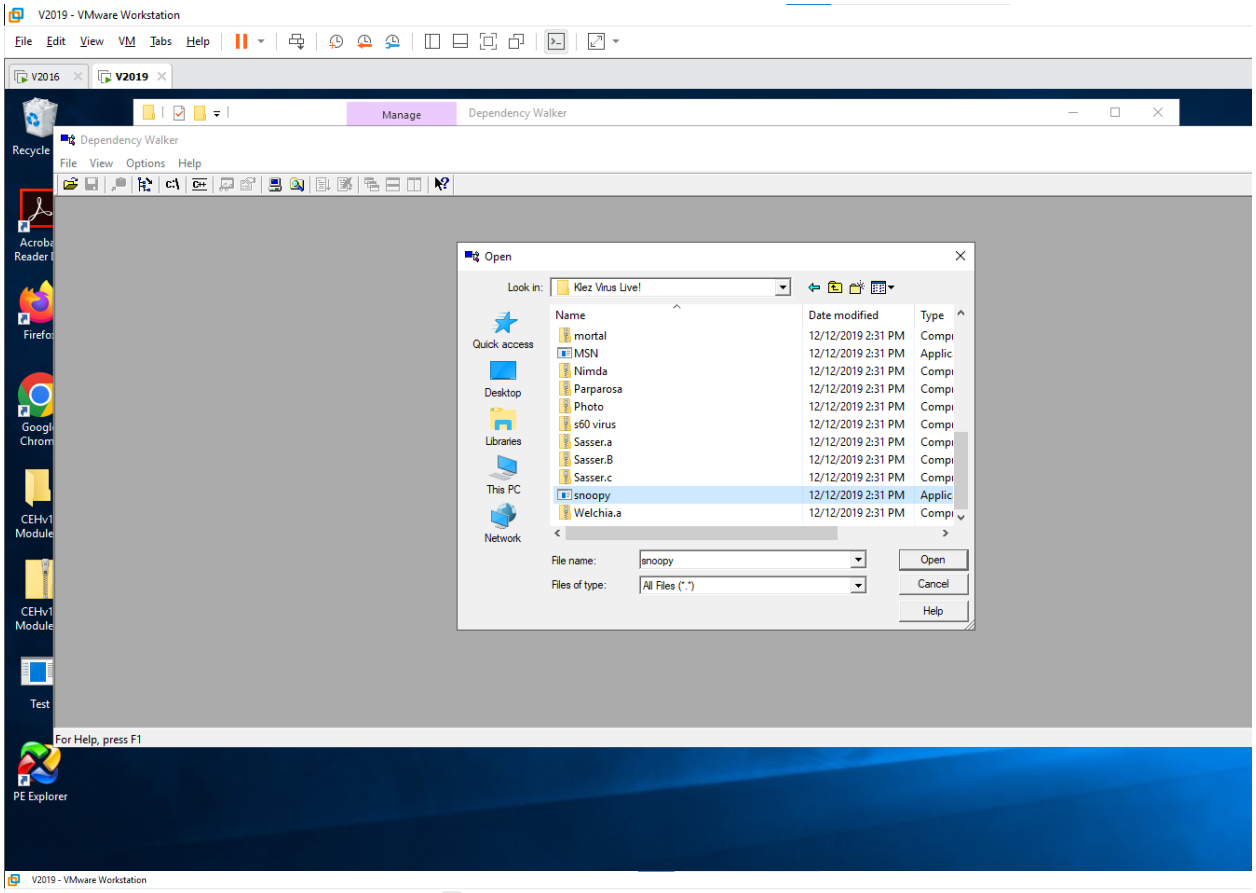

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
PE Explorer - C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware Threats\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!\face.exe
File View Tools Help
HEADERS INFO
Address of Entry Point: 00408458
Real Image Checksum: 00017238h
Field Name | Data Value | Description
Machine | 014Ch | i386®
Number of Sections | 0004h |
Time Date Stamp | 3CB78EB8h | 13/04/2002 01:49:44
Pointer to Symbol Table | 00000000h |
Number of Symbols | 00000000h |
Size of Optional Header | 00E0h |
Characteristics | 010Fh |
Magic | 010Bh | PE32
Linker Version | 0006h | 6.0
Size of Code | 0000C000h |
Size of Initialized Data | 00089000h |
Size of Uninitialized Data | 00000000h |
Address of Entry Point | 00408458h |
Base of Code | 00001000h |
Base of Data | 0000D000h |
Image Base | 00400000h |
Field Name | Data Value | Description
Section Alignment | 00001000h |
File Alignment | 00001000h |
Operating System Version | 00000004h | 4.0
Image Version | 00000000h | 0.0
Subsystem Version | 00000004h | 4.0
Win32 Version Value | 00000000h | Reserved
Size of Image | 00096000h | 614400 bytes
Size of Headers | 00001000h |
Checksum | 00000000h |
Subsystem | 0002h | Win32 GUI
Dll Characteristics | 0000h |
Size of Stack Reserve | 00100000h |
Size of Stack Commit | 00001000h |
Size of Heap Reserve | 00100000h |
Size of Heap Commit | 00001000h |
Loader Flags | 00000000h | Obsolete
Number of Data Directories | 00000010h

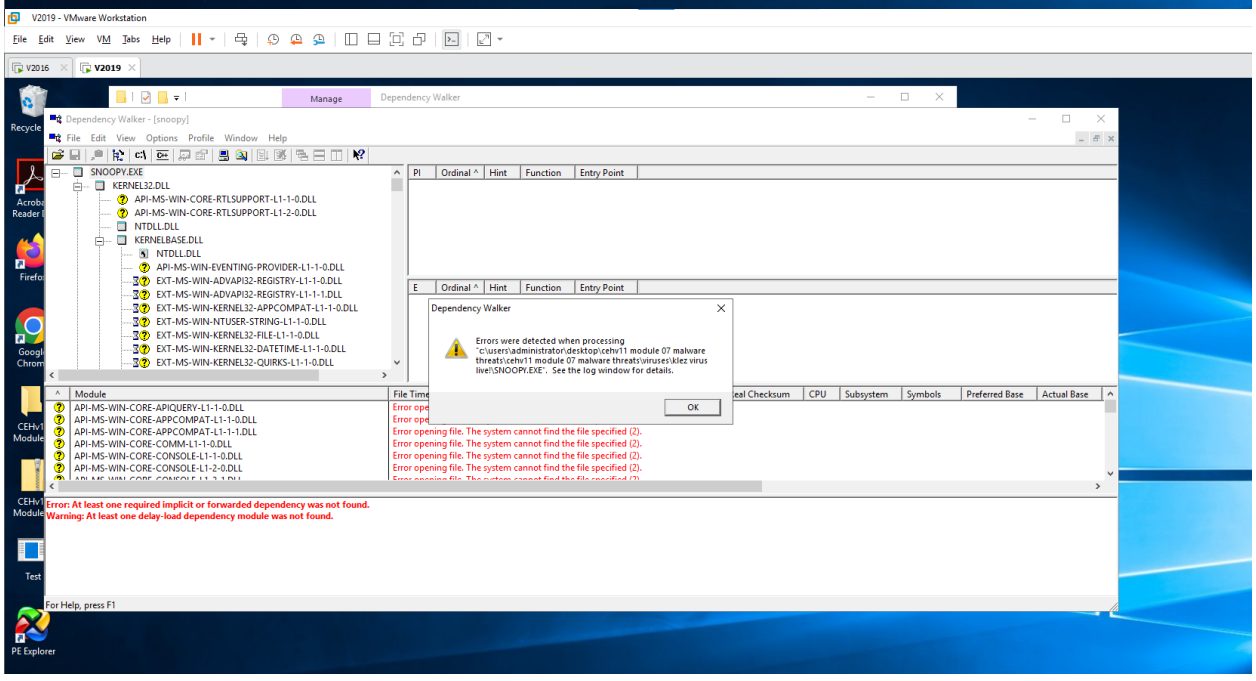

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
PE Explorer - C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware Threats\CEHv11 Module 07 Mal
File View Tools Help
DATA DIRECTORIES
Export Table
00000000
00000000
Set to Zero
Directory Name
Virtual Address
Size
Export Table
Import Table 0040D620h 00000064h
Resource Table 00495000h 00000010h
Exception Table
Certificate Table
Relocation Table
Debug Data
Architecture-specific data
Machine Value (MIPS GP)
TLS Table
Load Configuration Table
Bound Import Table
Import Address Table 0040D000h 000001ECh
Delay Import Descriptor
COM+ Runtime Header
(15) Reserved

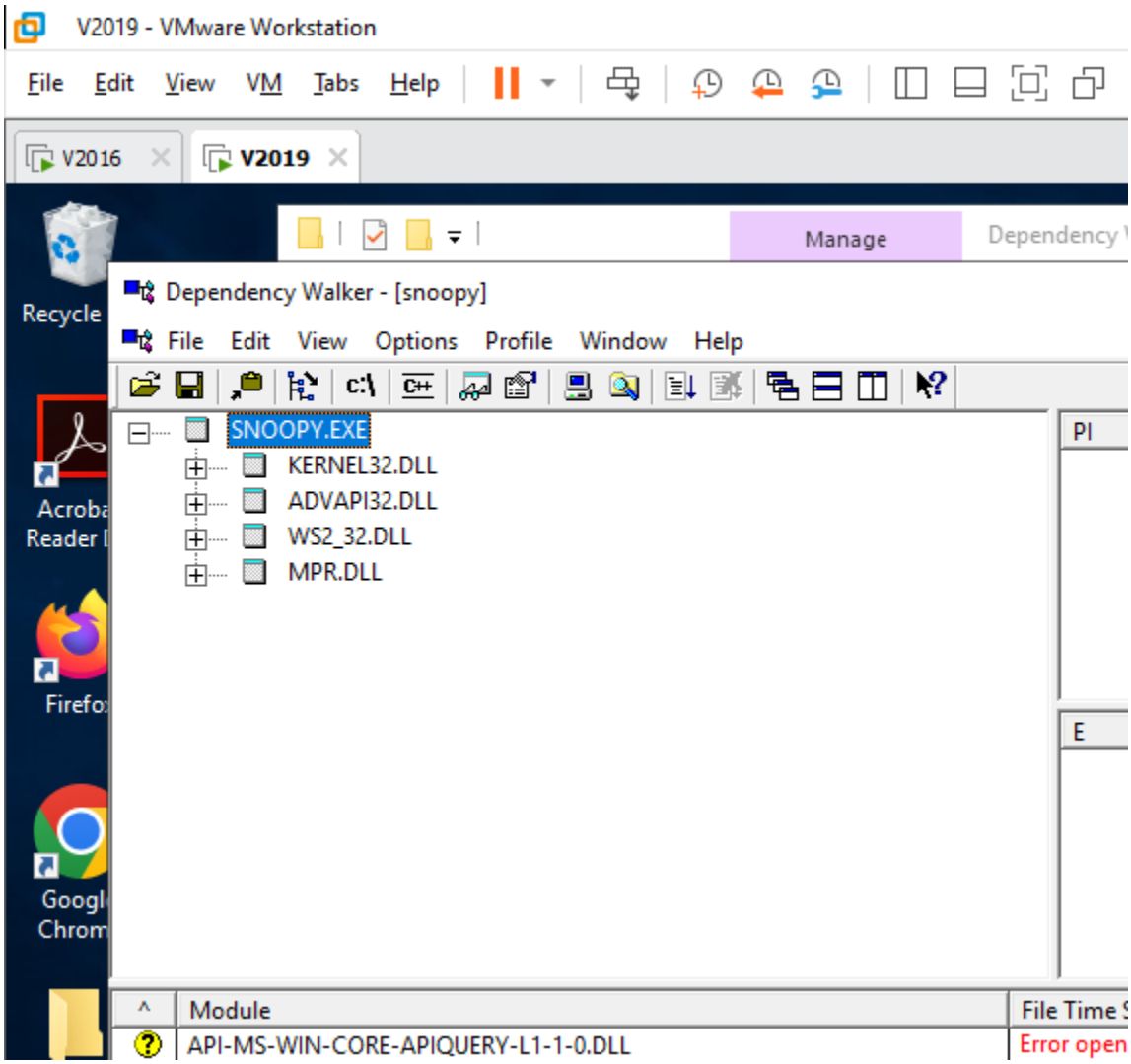


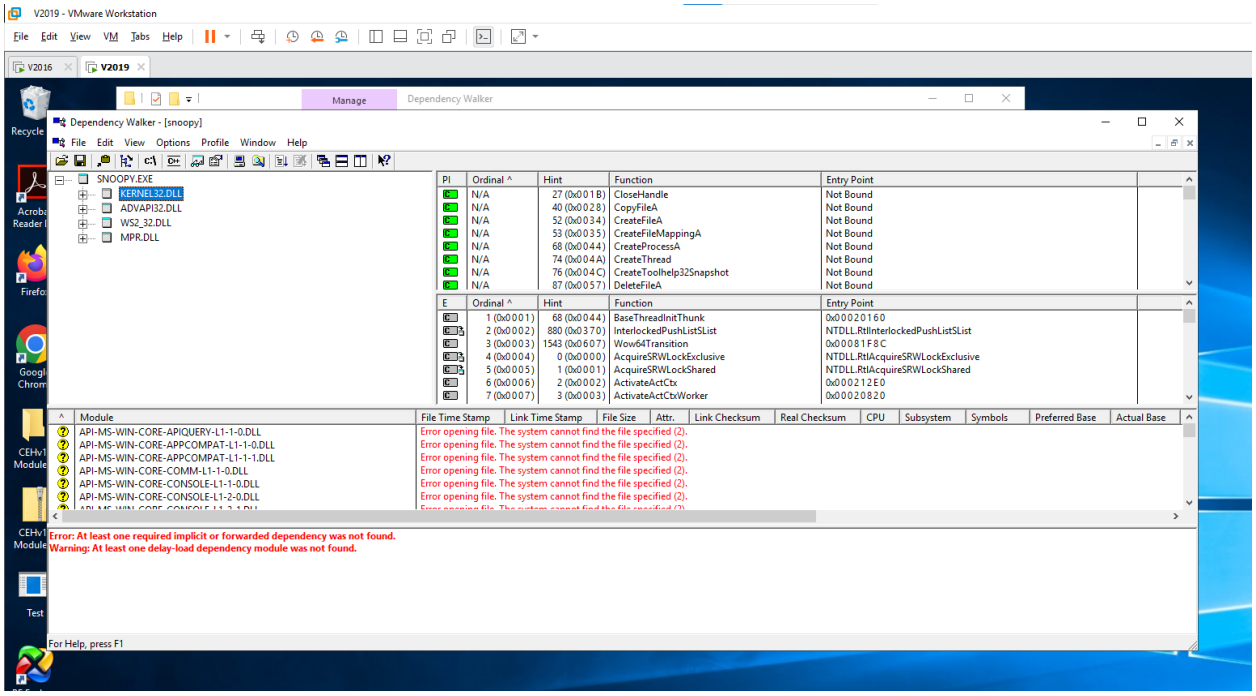
3.5 Identify File Dependencies using Dependency Walker
- Open Windows 10


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
Dependency Walker
File Home Share View
Malware Analysis Tools › Static Malware Analysis Tools › File Dependency Checking Tools › Dependency Walker
Search Dependency
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
depends
10/29/2006 2:20 AM
Compiled HTML ...
161 KB
depends.dll
10/29/2006 2:20 AM
Application extens...
9 KB
depends
10/29/2006 2:20 AM
Application
799 KB
Manage
Dependency Walker
File View Options Help
For Help, press F1
PE Explorer
9:57 PM

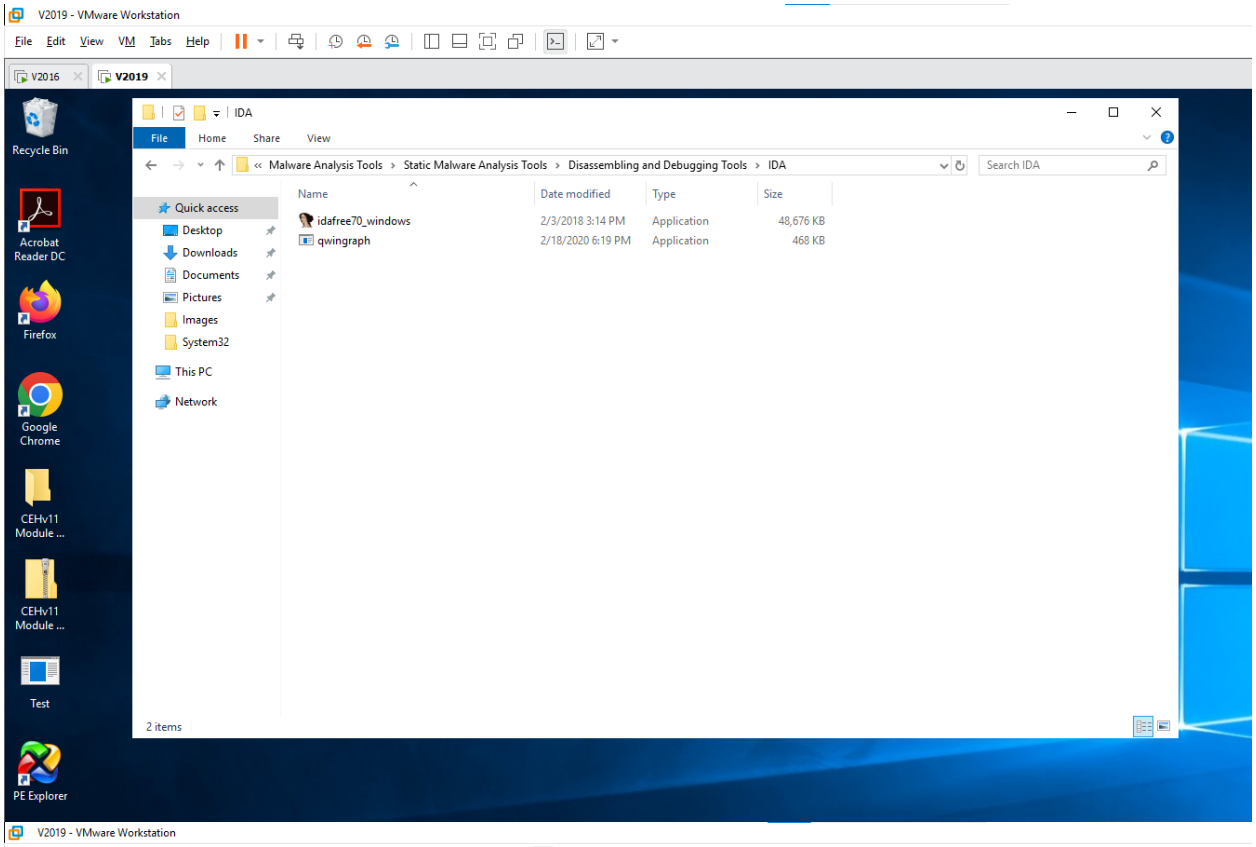

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Manage
Dependency Walker
Dependency Walker
File View Options Help
Open
Look in: Klez Virus Live!
Quick access
Desktop
Libraries
This PC
Network
Name
Date modified
Type
mortal 12/12/2019 2:31 PM
MSN 12/12/2019 2:31 PM
Nimda 12/12/2019 2:31 PM
Parparosa 12/12/2019 2:31 PM
Photo 12/12/2019 2:31 PM
s60 virus 12/12/2019 2:31 PM
Sasser.a 12/12/2019 2:31 PM
Sasser.B 12/12/2019 2:31 PM
Sasser.c 12/12/2019 2:31 PM
snoopy 12/12/2019 2:31 PM
Welchia.a 12/12/2019 2:31 PM
File name: snoopy
Files of type: All Files (*.*)
Open
Cancel
Help
For Help, press F1
Recycle
PE Explorer

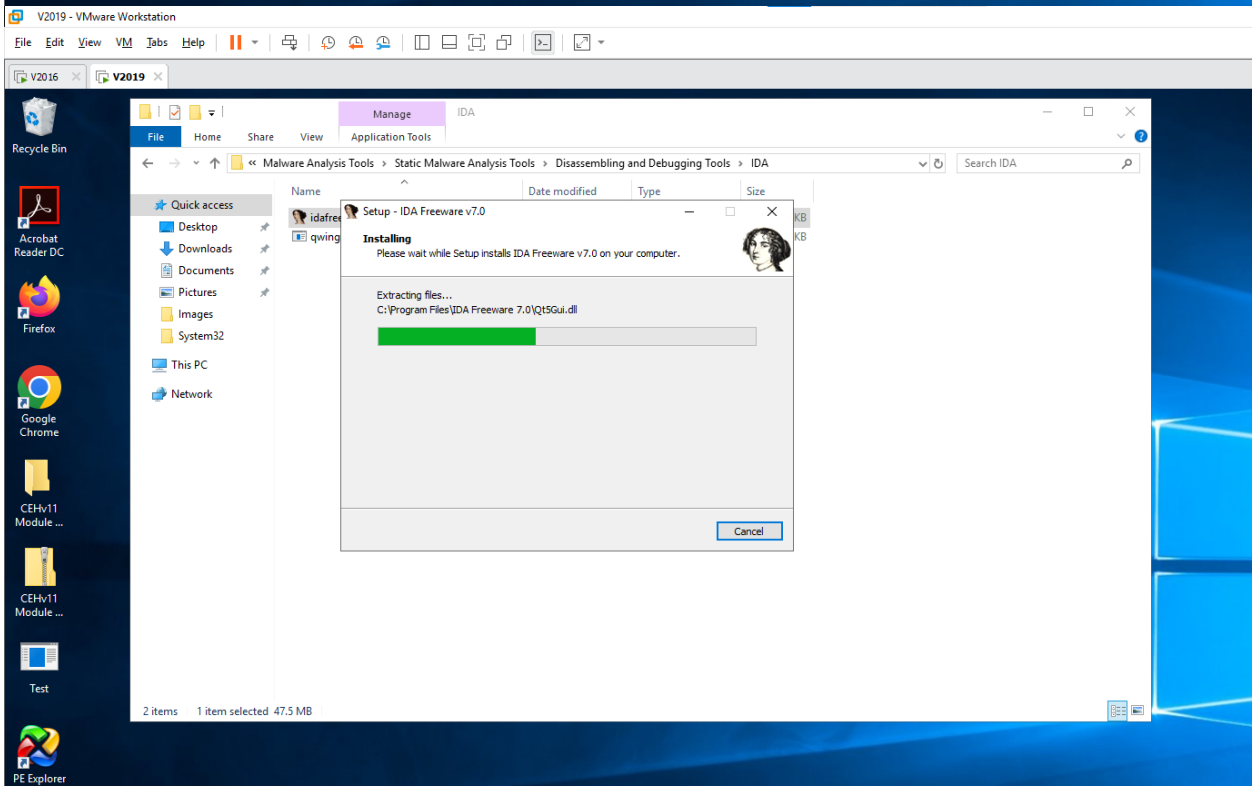

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Manage
Dependency Walker
Dependency Walker - [snoopy]
File Edit View Options Profile Window Help
SNOOPY.EXE
KERNEL32.DLL
API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
NTDLL.DLL
KERNELBASE.DLL
NTDLL.DLL
API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
PI Ordinal ^ Hint Function Entry Point
E Ordinal ^ Hint Function Entry Point
Dependency Walker
Errors were detected when processing "c:\users\administrator\desktop\cehv11 module 07 malware threats\cehv11 module 07 malware threats\viruses\klez virus live!\SNOOPY.EXE". See the log window for details.
OK
Module
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL
API-MS-WIN-CORE-COMM-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL
Error opening file. The system cannot find the file specified (2).
CPU Subsystem Symbols Preferred Base Actual Base
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.
For Help, press F1
Recycle
PE Explorer

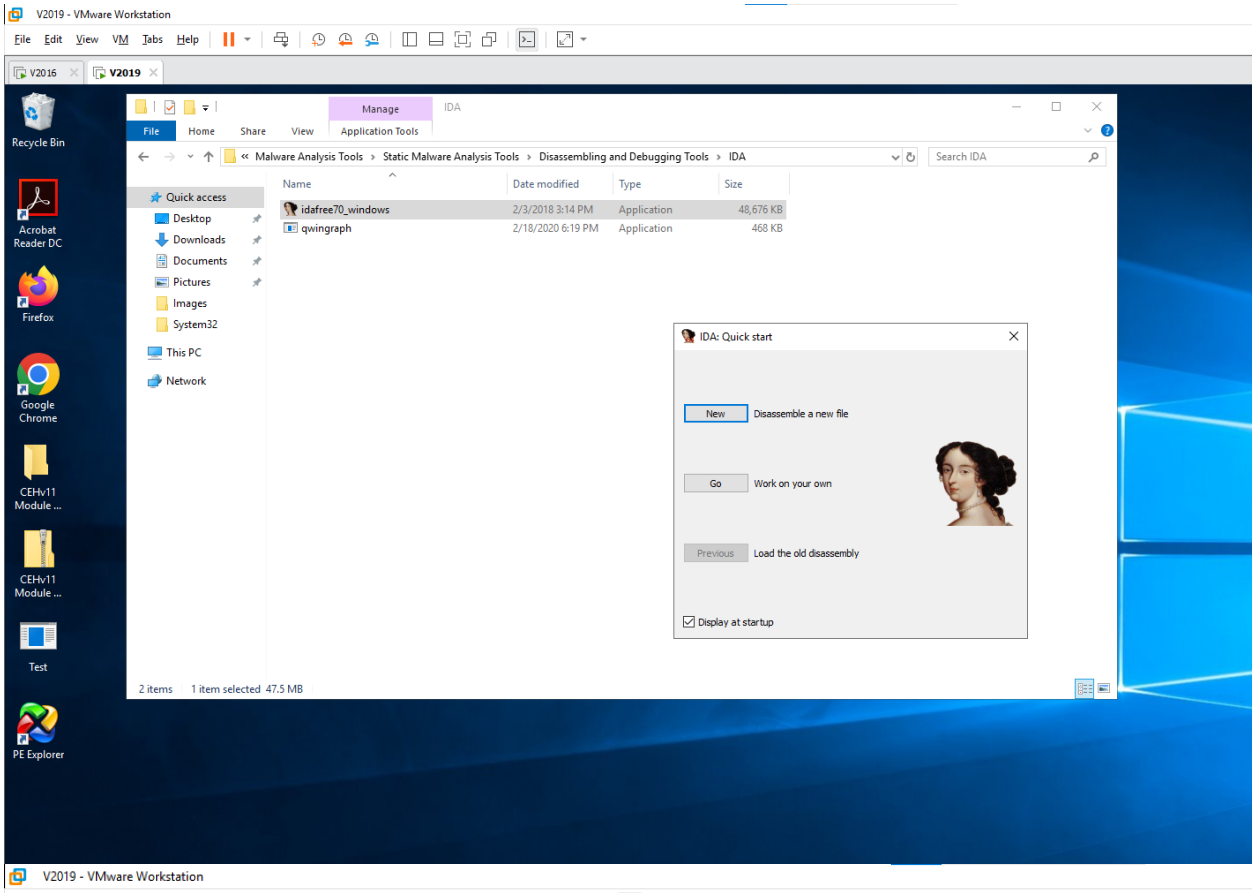

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle
Manage
Dependency Walker - [snoopy]
File Edit View Options Profile Window Help
SNOOPY.EXE
KERNEL32.DLL
ADVAPI32.DLL
WS2_32.DLL
MPR.DLL
Module
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
Error open

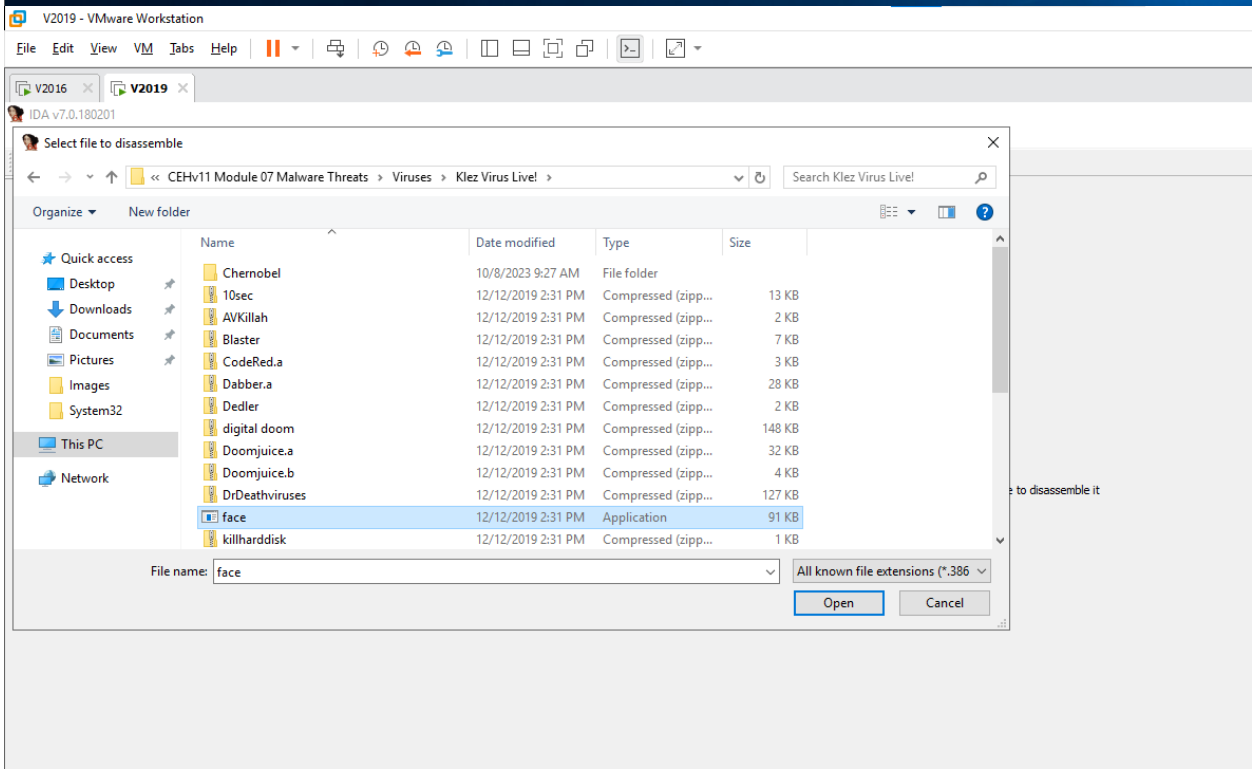


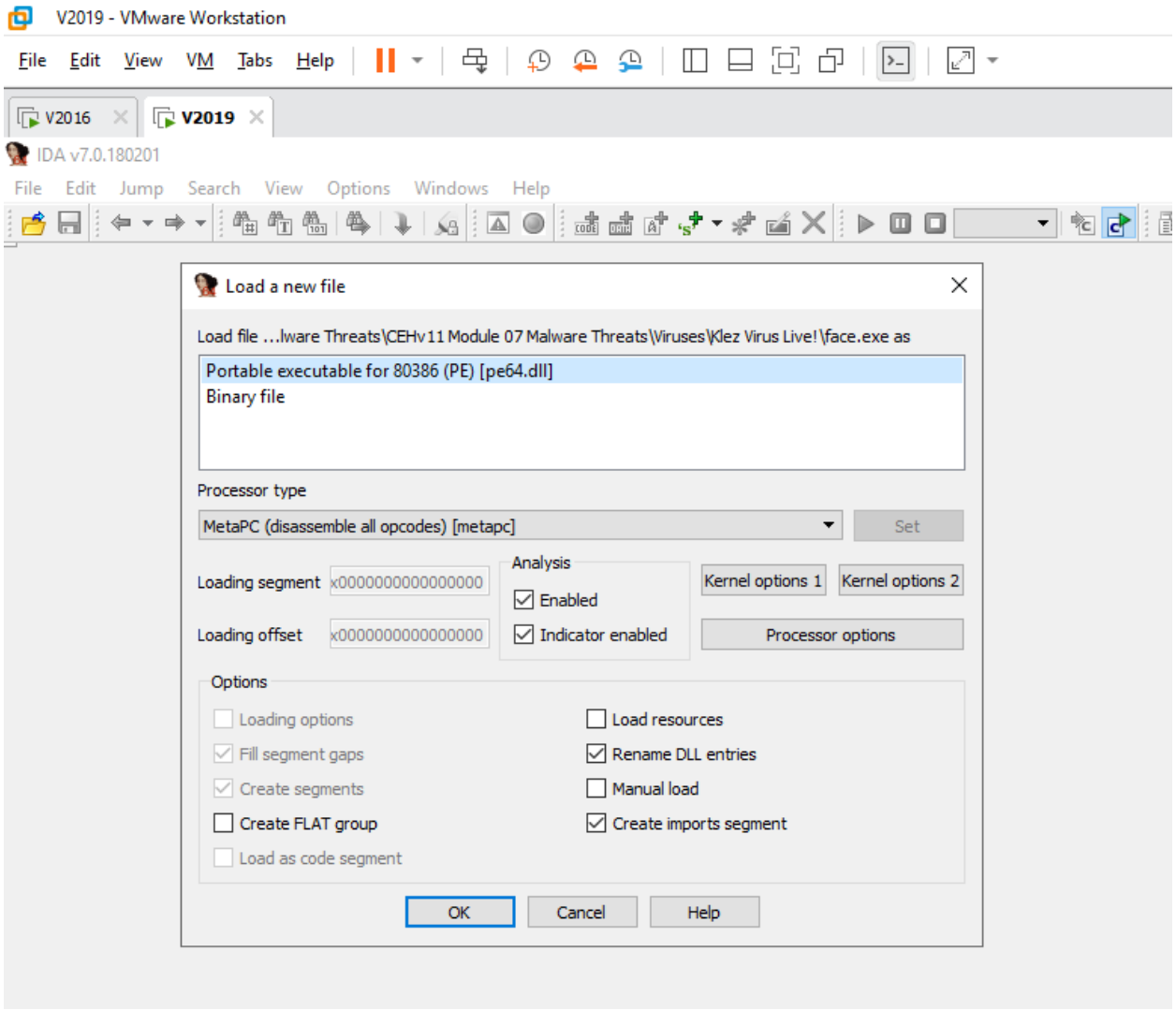
3.6 Perform Malware Disassembly using IDA and OllyDbg
- Open Windows 10

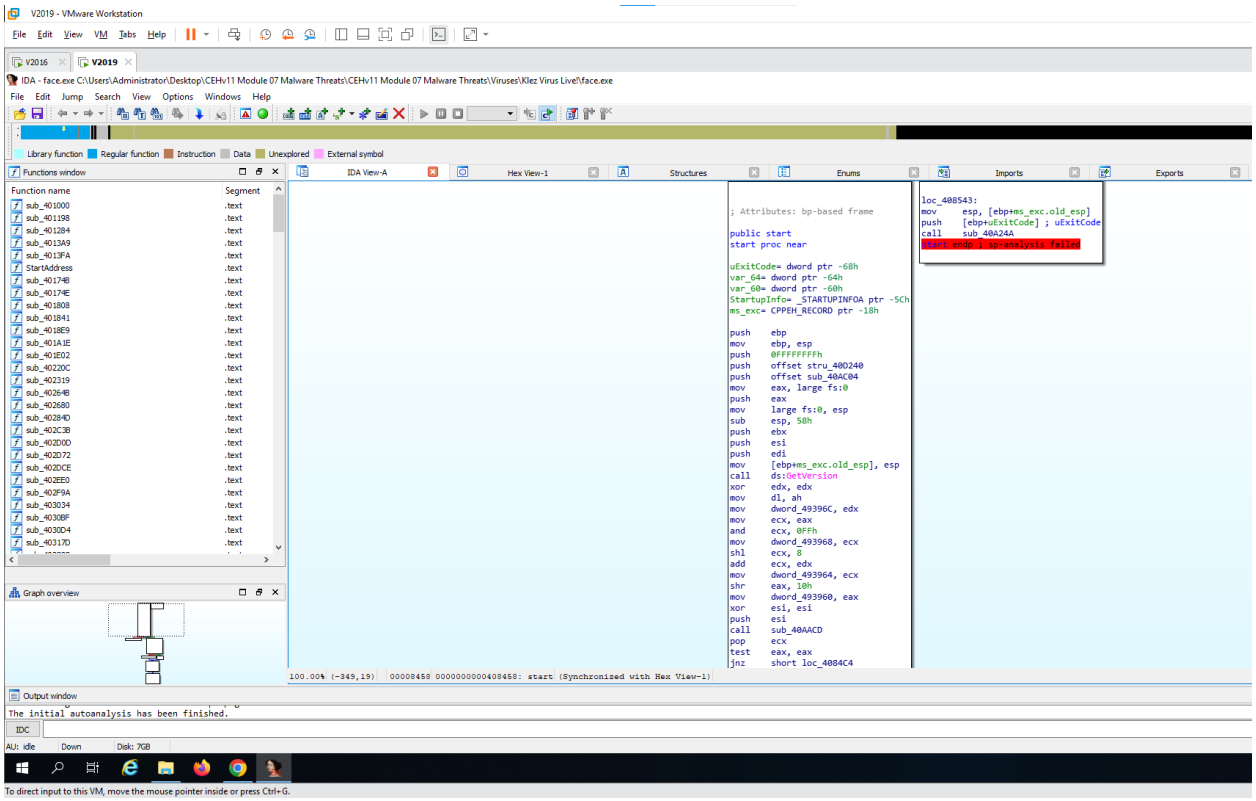

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
PE Explorer
IDA
File Home Share View
Malware Analysis Tools › Static Malware Analysis Tools › Disassembling and Debugging Tools › IDA
Search IDA
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
idafree70_windows
2/3/2018 3:14 PM
Application
48,676 KB
qwingraph
2/18/2020 6:19 PM
Application
468 KB
2 items

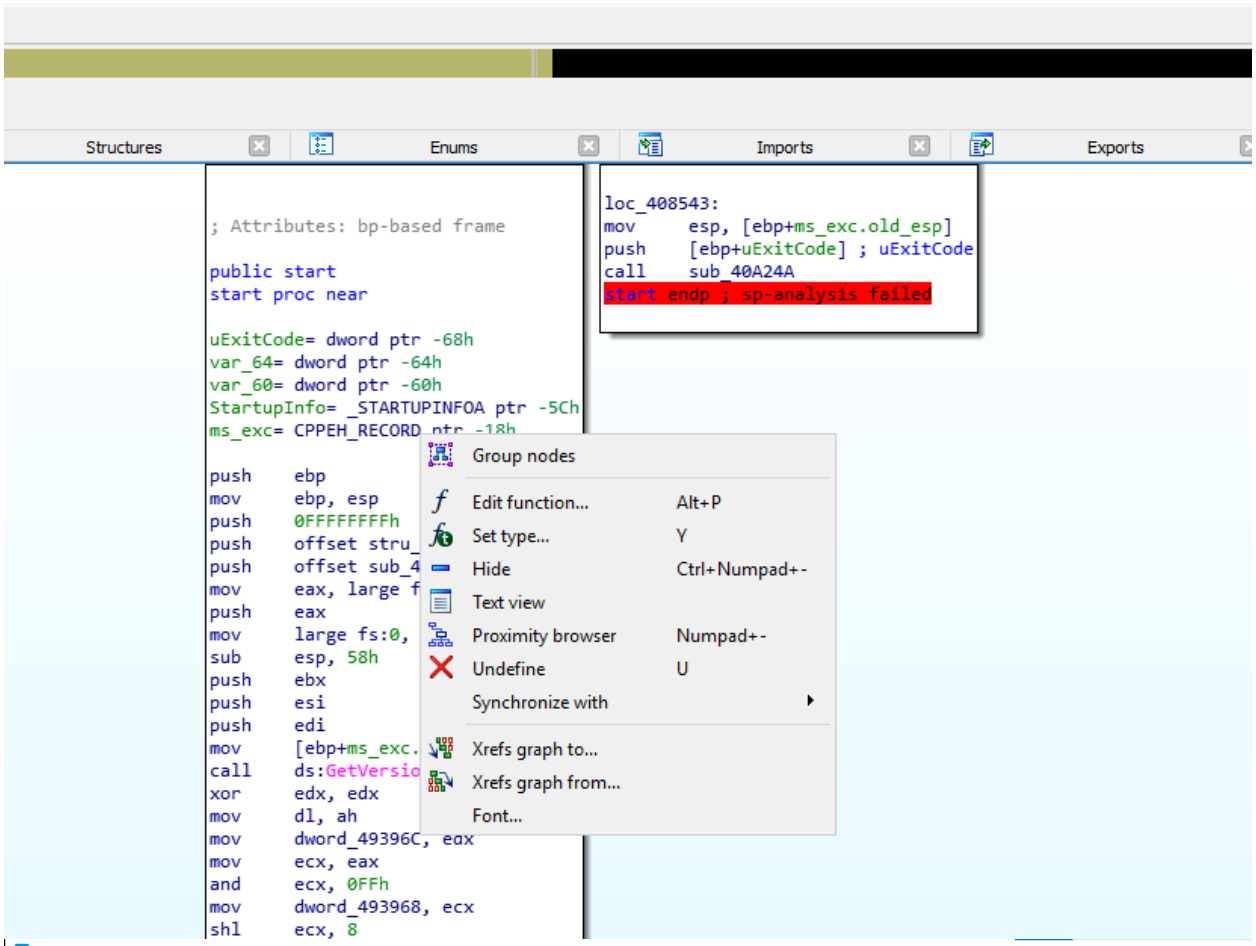

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
PE Explorer
Manage
IDA
File Home Share View Application Tools
Malware Analysis Tools › Static Malware Analysis Tools › Disassembling and Debugging Tools › IDA
Search IDA
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
Setup - IDA Freeware v7.0
Installing
Please wait while Setup installs IDA Freeware v7.0 on your computer.
Extracting files...
C:\Program Files\IDA Freeware 7.0\Qt5Gui.dll
Cancel
2 items
1 item selected 47.5 MB

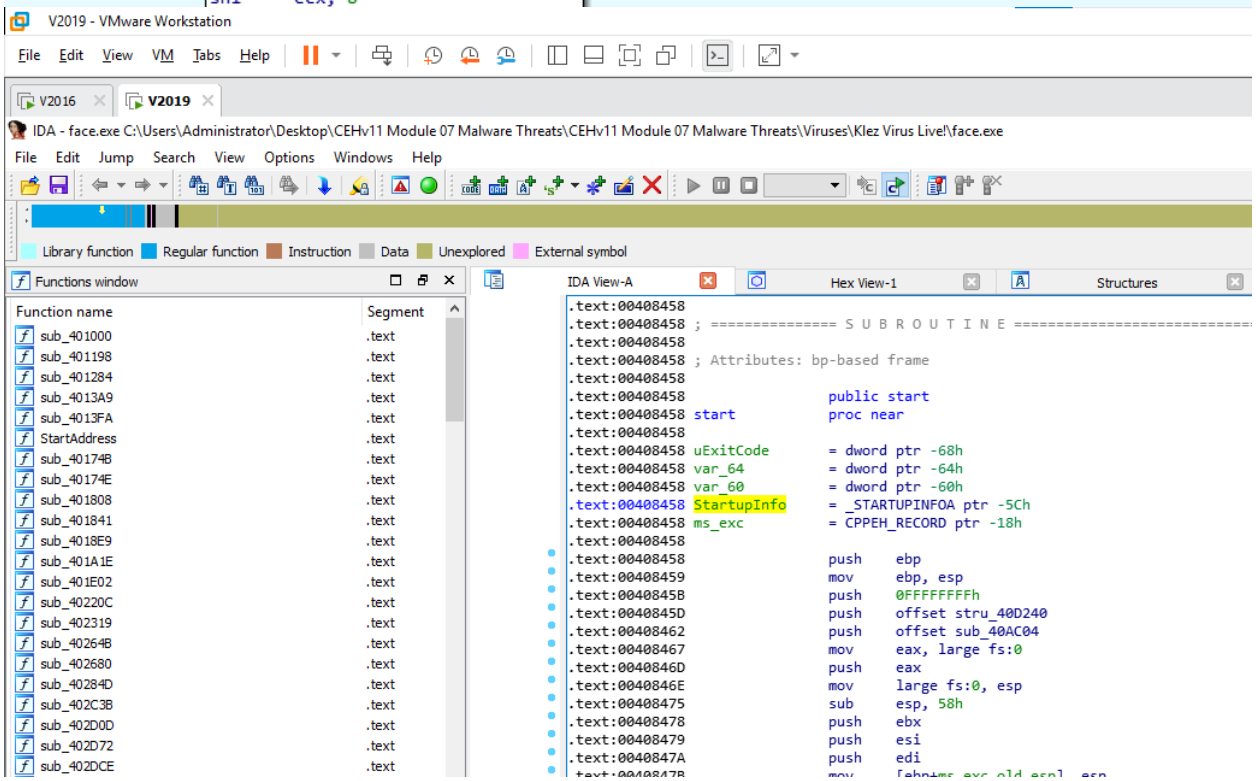

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
PE Explorer
Manage
IDA
File Home Share View Application Tools
Malware Analysis Tools › Static Malware Analysis Tools › Disassembling and Debugging Tools › IDA
Search IDA
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name Date modified Type Size
idafree70_windows 2/3/2018 3:14 PM Application 48,676 KB
qwingraph 2/18/2020 6:19 PM Application 468 KB
IDA: Quick start
New Disassemble a new file
Go Work on your own
Previous Load the old disassembly
Display at startup
2 items 1 item selected 47.5 MB

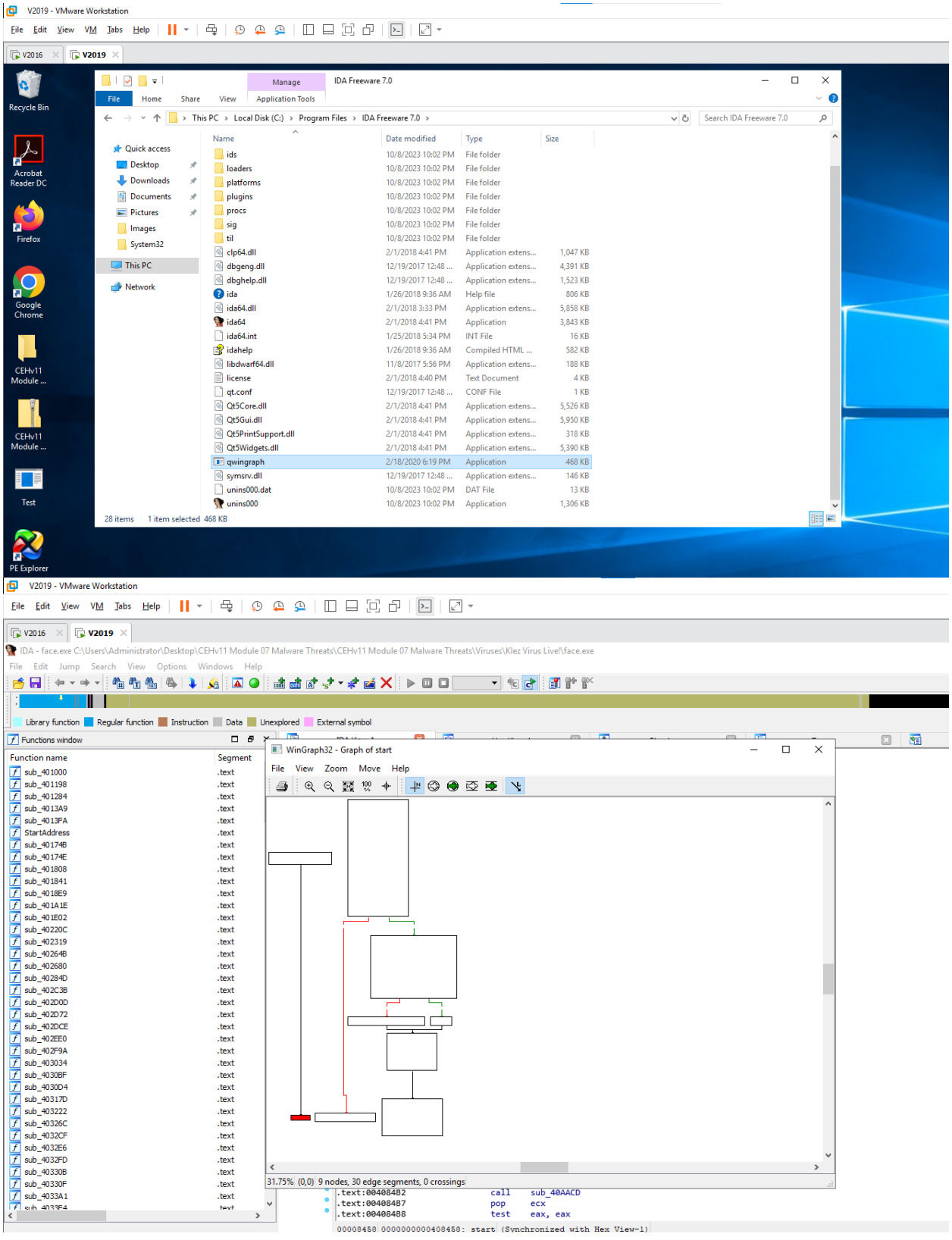

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
IDA v7.0.180201
Select file to disassemble
CEHv11 Module 07 Malware Threats › Viruses › Klez Virus Live! ›
Search Klez Virus Live!
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name Date modified Type Size
Chernobel 10/8/2023 9:27 AM File folder
10sec 12/12/2019 2:31 PM Compressed (zipp... 13 KB
AVKillah 12/12/2019 2:31 PM Compressed (zipp... 2 KB
Blaster 12/12/2019 2:31 PM Compressed (zipp... 7 KB
CodeRed.a 12/12/2019 2:31 PM Compressed (zipp... 3 KB
Dabber.a 12/12/2019 2:31 PM Compressed (zipp... 28 KB
Dedler 12/12/2019 2:31 PM Compressed (zipp... 2 KB
digital doom 12/12/2019 2:31 PM Compressed (zipp... 148 KB
Doomjuice.a 12/12/2019 2:31 PM Compressed (zipp... 32 KB
Doomjuice.b 12/12/2019 2:31 PM Compressed (zipp... 4 KB
DrDeathviruses 12/12/2019 2:31 PM Compressed (zipp... 127 KB
face 12/12/2019 2:31 PM Application 91 KB
killharddisk 12/12/2019 2:31 PM Compressed (zipp... 1 KB
File name: face
All known file extensions (*.386
Open
Cancel
to disassemble it

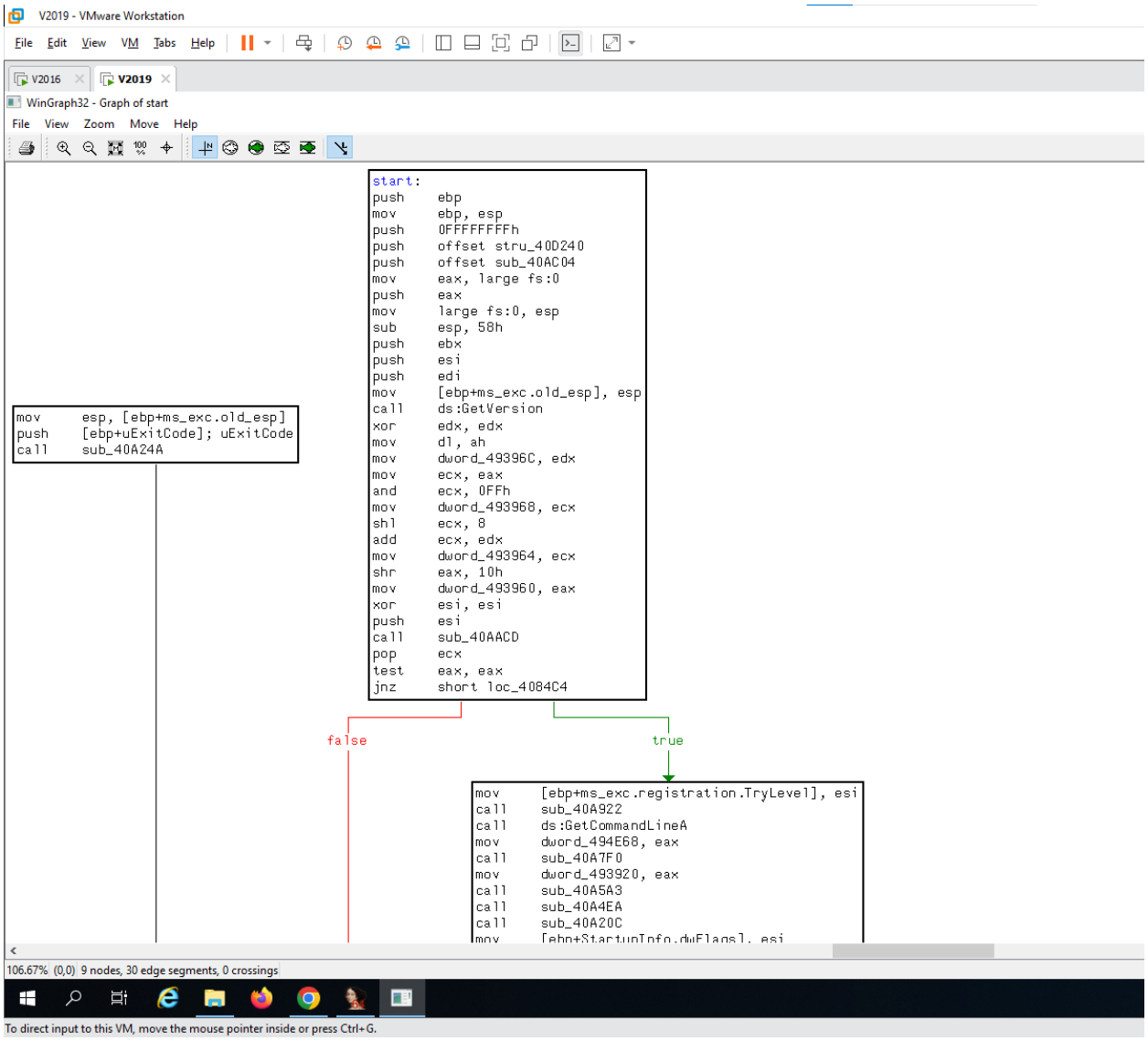

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
IDA v7.0.180201
File Edit Jump Search View Options Windows Help
Load a new file
Load file ...lware Threats\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!\face.exe as
Portable executable for 80386 (PE) [pe64.dll]
Binary file
Processor type
MetaPC (disassemble all opcodes) [metapc]
Set
Loading segment
x0000000000000000
Loading offset
x0000000000000000
Analysis
Enabled
Indicator enabled
Kernel options 1
Kernel options 2
Processor options
Options
Loading options
Fill segment gaps
Create segments
Create FLAT group
Load as code segment
Load resources
Rename DLL entries
Manual load
Create imports segment
OK
Cancel
Help

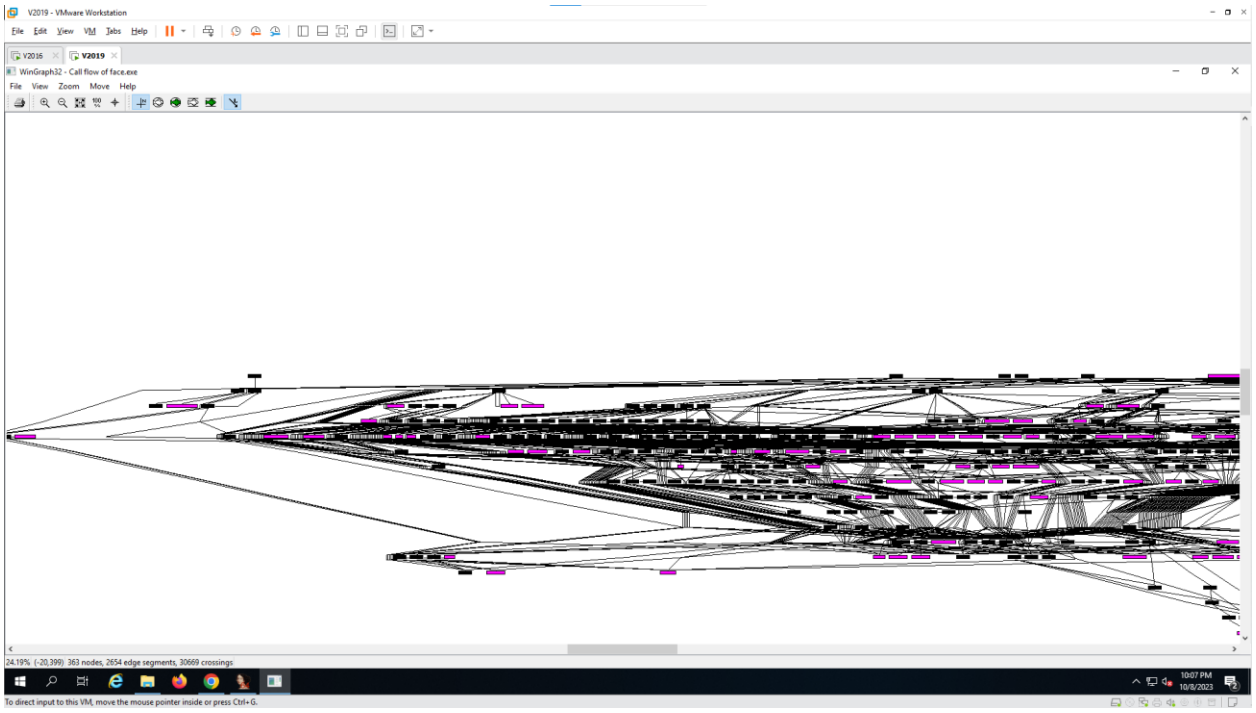

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
IDA - face.exe C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware Threats\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!\face.exe
File Edit Jump Search View Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol
Functions window
Function name
Segment
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Graph overview
Output window
The initial autoanalysis has been finished.
IDC
AU: idle
Down
Disk: 7GB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

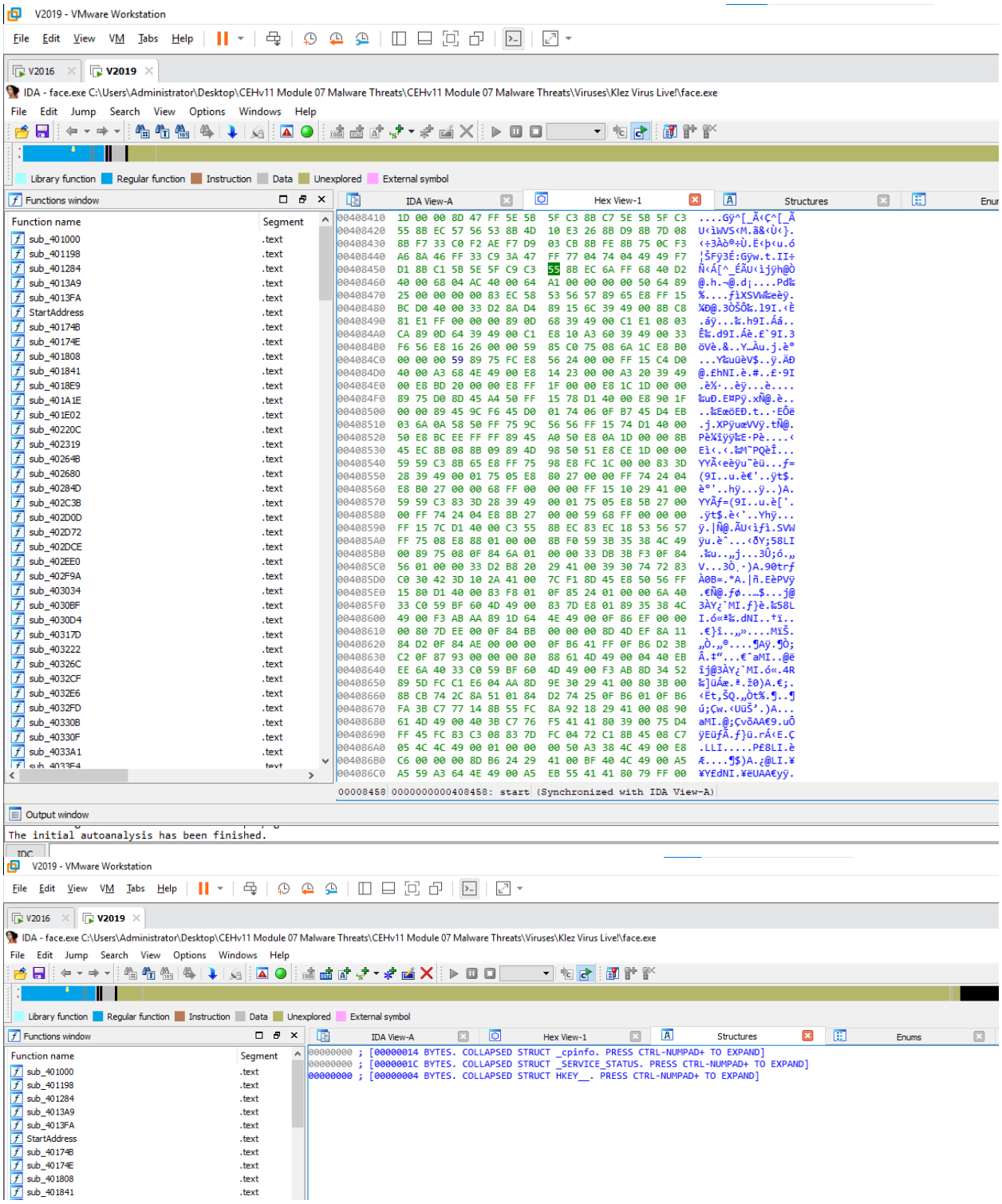

Structures
Enums
Imports
Exports
; Attributes: bp-based frame
public start
start proc near
uExitCode= dword ptr -68h
var_64= dword ptr -64h
var_60= dword ptr -60h
StartupInfo= _STARTUPINFOA ptr -5Ch
ms_exc= CPPEH_RECORD ptr -18h
push ebp
mov ebp, esp
push 0FFFFFFFFh
push offset stru_
push offset sub_4
mov eax, large f
push eax
mov large fs:0,
sub esp, 58h
push ebx
push esi
push edi
mov [ebp+ms_exc.
call ds:GetVersio
xor edx, edx
mov dl, ah
mov dword_49396C, eax
mov ecx, eax
and ecx, 0FFh
mov dword_493968, ecx
shl ecx, 8
loc_408543:
mov esp, [ebp+ms_exc.old_esp]
push [ebp+uExitCode] ; uExitCode
call sub_40A24A
start endp ; sp-analysis failed
Group nodes
Edit function... Alt+P
Set type... Y
Hide Ctrl+Numpad+-
Text view
Proximity browser Numpad+-
Undefine U
Synchronize with
Xrefs graph to...
Xrefs graph from...
Font...

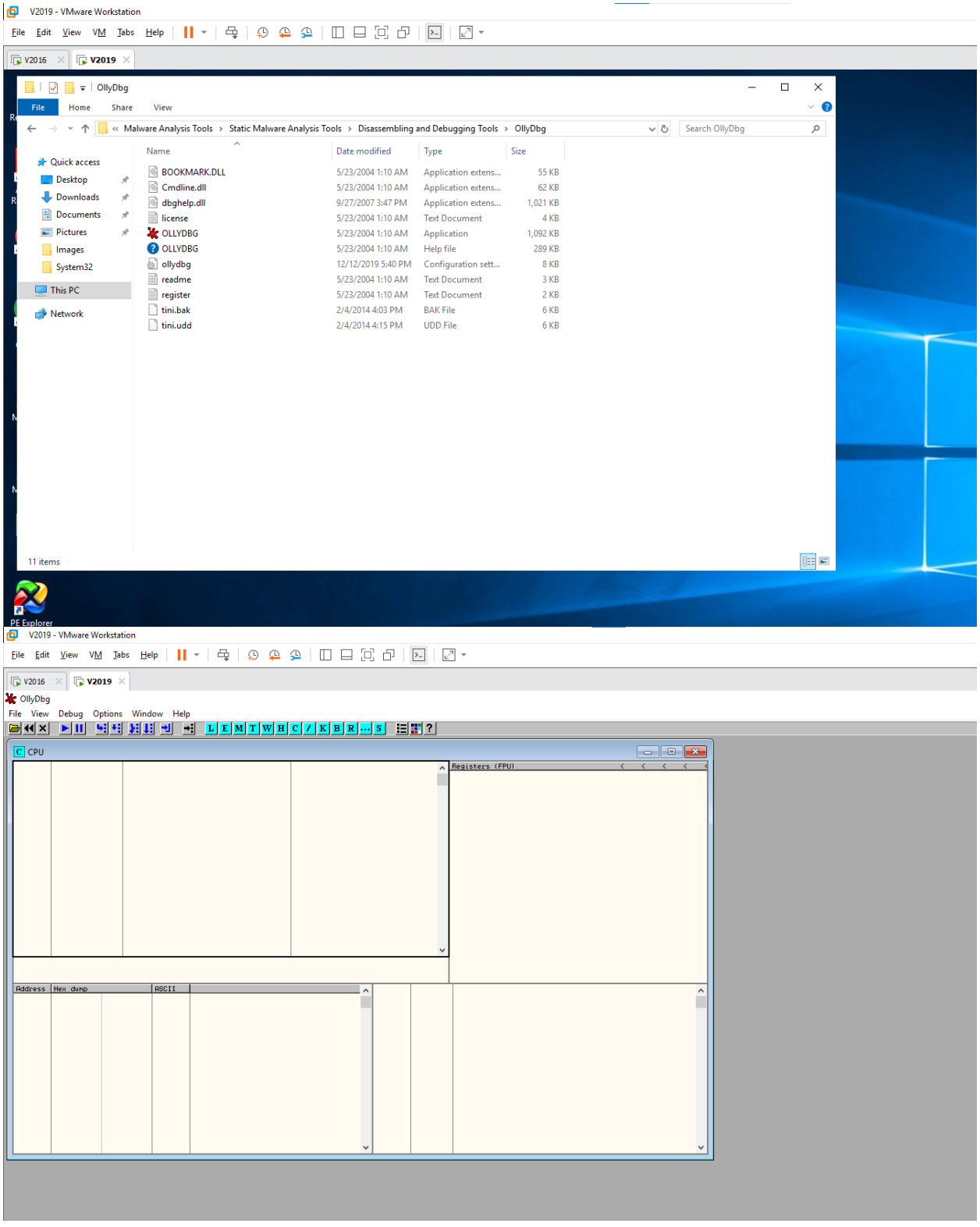

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
IDA - face.exe C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware Threats\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!\face.exe
File Edit Jump Search View Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol
Functions window
Function name
Segment
sub_401000 .text
sub_401198 .text
sub_401284 .text
sub_4013A9 .text
sub_4013FA .text
StartAddress .text
sub_40174B .text
sub_40174E .text
sub_401808 .text
sub_401841 .text
sub_4018E9 .text
sub_401A1E .text
sub_401E02 .text
sub_40220C .text
sub_402319 .text
sub_40264B .text
sub_402680 .text
sub_40284D .text
sub_402C3B .text
sub_402D0D .text
sub_402D72 .text
sub_402DCE .text
IDA View-A
Hex View-1
Structures
.text:00408458
.text:00408458 ; =============== S U B R O U T I N E ===============
.text:00408458
.text:00408458 ; Attributes: bp-based frame
.text:00408458
.text:00408458 public start
.text:00408458 start proc near
.text:00408458
.text:00408458 uExitCode = dword ptr -68h
.text:00408458 var_64 = dword ptr -64h
.text:00408458 var_60 = dword ptr -60h
.text:00408458 StartupInfo = _STARTUPINFOA ptr -5Ch
.text:00408458 ms_exc = CPPEH_RECORD ptr -18h
.text:00408458
.text:00408458 push ebp
.text:00408459 mov ebp, esp
.text:0040845B push 0FFFFFFFFh
.text:0040845D push offset stru_40D240
.text:00408462 push offset sub_40AC04
.text:00408467 mov eax, large fs:0
.text:0040846D push eax
.text:0040846E mov large fs:0, esp
.text:00408475 sub esp, 58h
.text:00408478 push ebx
.text:00408479 push esi
.text:0040847A push edi

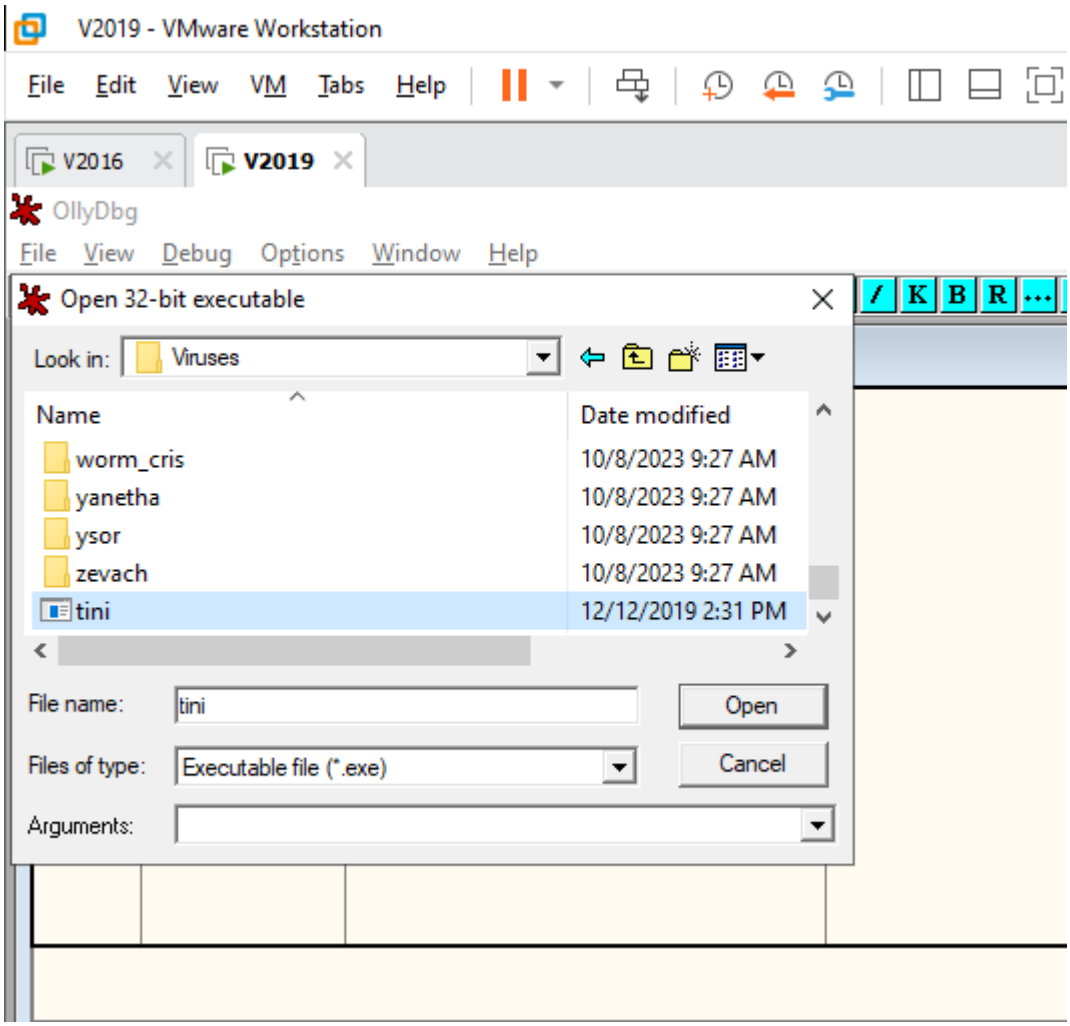

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
PE Explorer
Manage
IDA Freeware 7.0
File Home Share View Application Tools
This PC › Local Disk (C:) › Program Files › IDA Freeware 7.0 ›
Search IDA Freeware 7.0
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name Date modified Type Size
ids 10/8/2023 10:02 PM File folder
loaders 10/8/2023 10:02 PM File folder
platforms 10/8/2023 10:02 PM File folder
plugins 10/8/2023 10:02 PM File folder
procs 10/8/2023 10:02 PM File folder
sig 10/8/2023 10:02 PM File folder
til 10/8/2023 10:02 PM File folder
clp64.dll 2/1/2018 4:41 PM Application extens... 1,047 KB
dbgeng.dll 12/19/2017 12:48 ... Application extens... 4,391 KB
dbghelp.dll 12/19/2017 12:48 ... Application extens... 1,523 KB
ida 1/26/2018 9:36 AM Help file 806 KB
ida64.dll 2/1/2018 3:33 PM Application extens... 5,858 KB
ida64 2/1/2018 4:41 PM Application 3,843 KB
ida64.int 1/25/2018 5:34 PM INT File 16 KB
idahelp 1/26/2018 9:36 AM Compiled HTML ... 582 KB
libdwarf64.dll 11/8/2017 5:56 PM Application extens... 188 KB
license 2/1/2018 4:40 PM Text Document 4 KB
qt.conf 12/19/2017 12:48 ... CONF File 1 KB
Qt5Core.dll 2/1/2018 4:41 PM Application extens... 5,526 KB
Qt5Gui.dll 2/1/2018 4:41 PM Application extens... 5,950 KB
Qt5PrintSupport.dll 2/1/2018 4:41 PM Application extens... 318 KB
Qt5Widgets.dll 2/1/2018 4:41 PM Application extens... 5,390 KB
qwingraph 2/18/2020 6:19 PM Application 468 KB
symsrv.dll 12/19/2017 12:48 ... Application extens... 146 KB
unins000.dat 10/8/2023 10:02 PM DAT File 13 KB
unins000 10/8/2023 10:02 PM Application 1,306 KB
28 items 1 item selected 468 KB
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
IDA - face.exe C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware Threats\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!\face.exe
File Edit Jump Search View Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol
Functions window
Function name Segment
sub_401000 .text
sub_401198 .text
sub_401284 .text
sub_4013A9 .text
sub_4013FA .text
StartAddress .text
sub_40174B .text
sub_40174E .text
sub_401808 .text
sub_401841 .text
sub_4018E9 .text
sub_401A1E .text
sub_401E02 .text
sub_40220C .text
sub_402319 .text
sub_40264B .text
sub_402680 .text
sub_40284D .text
sub_402C3B .text
sub_402D0D .text
sub_402D72 .text
sub_402DCE .text
sub_402EE0 .text
sub_402F9A .text
sub_403034 .text
sub_4030BF .text
sub_4030D4 .text
sub_40317D .text
sub_403222 .text
sub_40326C .text
sub_4032CF .text
sub_4032E6 .text
sub_4032FD .text
sub_40330B .text
sub_40330F .text
sub_4033A1 .text
WinGraph32 - Graph of start
File View Zoom Move Help
31.75% (0,0) 9 nodes, 30 edge segments, 0 crossings
.text:004084B2 call sub_40AACD
.text:004084B7 pop ecx
.text:004084B8 test eax, eax
00008458 0000000000408458: start (Synchronized with Hex View-1)

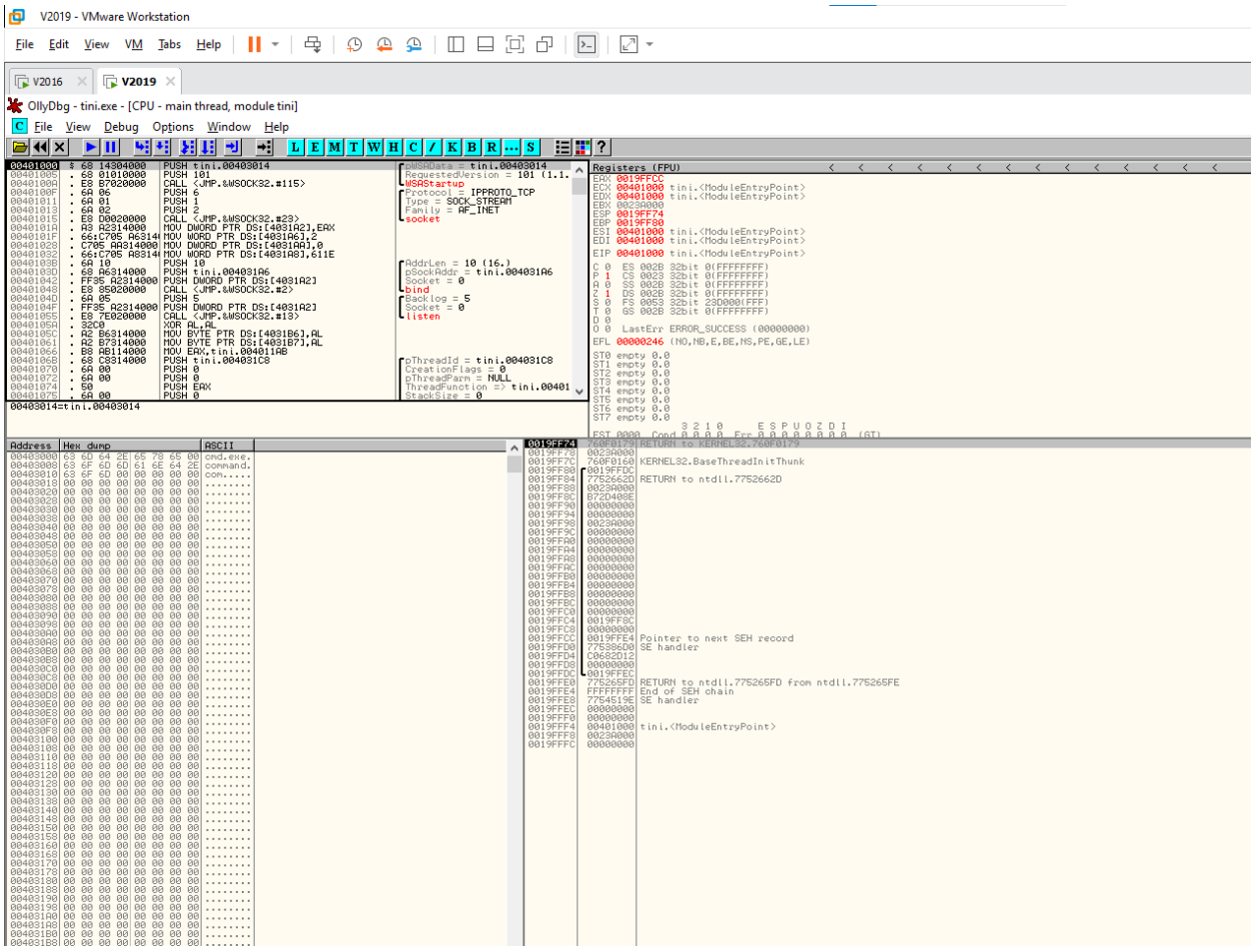

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
WinGraph32 - Graph of start
File View Zoom Move Help
start:
push ebp
mov ebp, esp
push 0FFFFFFFFh
push offset stru_40D240
push offset sub_40AC04
mov eax, large fs:0
push eax
mov large fs:0, esp
sub esp, 58h
push ebx
push esi
push edi
mov [ebp+ms_exc.old_esp], esp
call ds:GetVersion
xor edx, edx
mov dl, ah
mov dword_49396C, edx
mov ecx, eax
and ecx, 0FFh
mov dword_493968, ecx
shl ecx, 8
add ecx, edx
mov dword_493964, ecx
shr eax, 10h
mov dword_493960, eax
xor esi, esi
push esi
call sub_40AACD
pop ecx
test eax, eax
jnz short loc_4084C4
mov esp, [ebp+ms_exc.old_esp]
push [ebp+uExitCode]; uExitCode
call sub_40A24A
false
true
mov [ebp+ms_exc.registration.TryLevel], esi
call sub_40A922
call ds:GetCommandLineA
mov dword_494E68, eax
call sub_40A7F0
mov dword_493920, eax
call sub_40A5A3
call sub_40A4EA
call sub_40A20C
106.67% (0,0) 9 nodes, 30 edge segments, 0 crossings
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

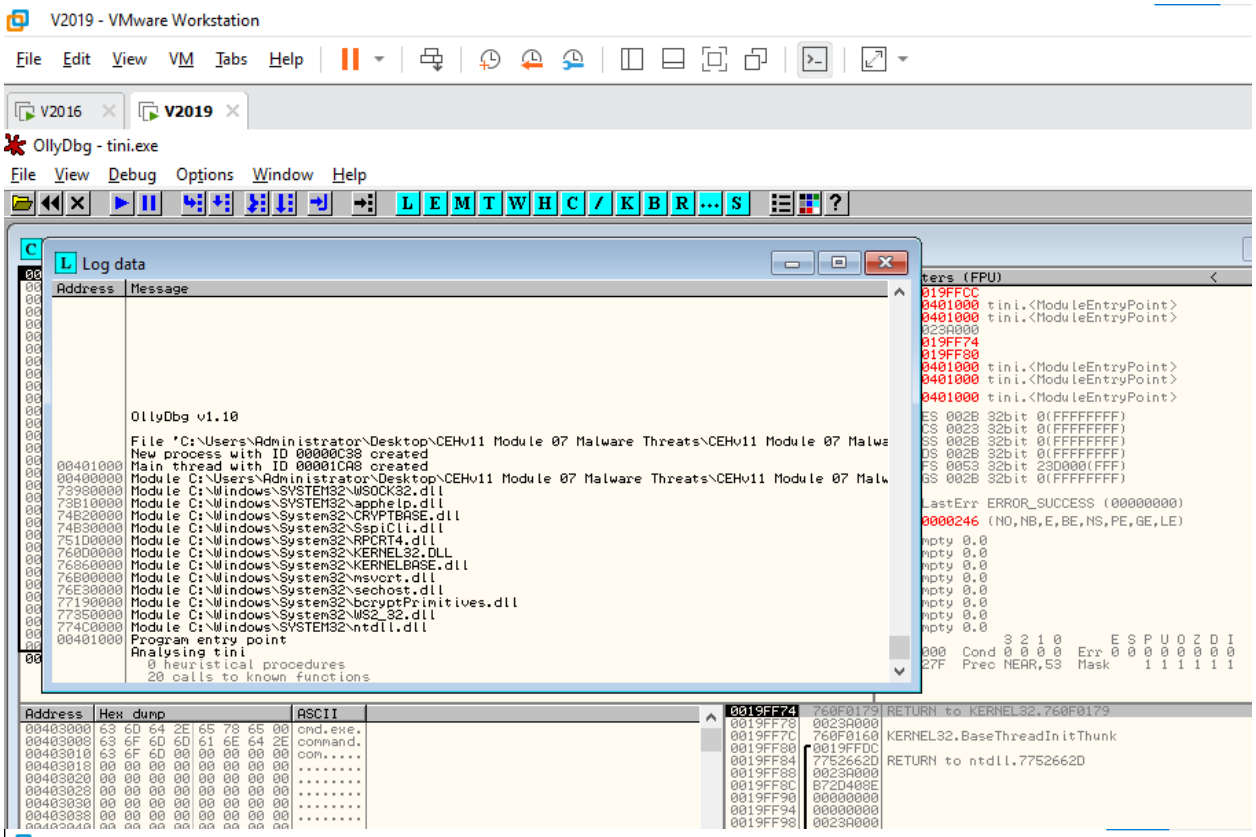

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
WinGraph32 - Call flow of face.exe
File View Zoom Move Help
24.19% (-20,399) 363 nodes, 2654 edge segments, 30669 crossings
10:07 PM
10/8/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

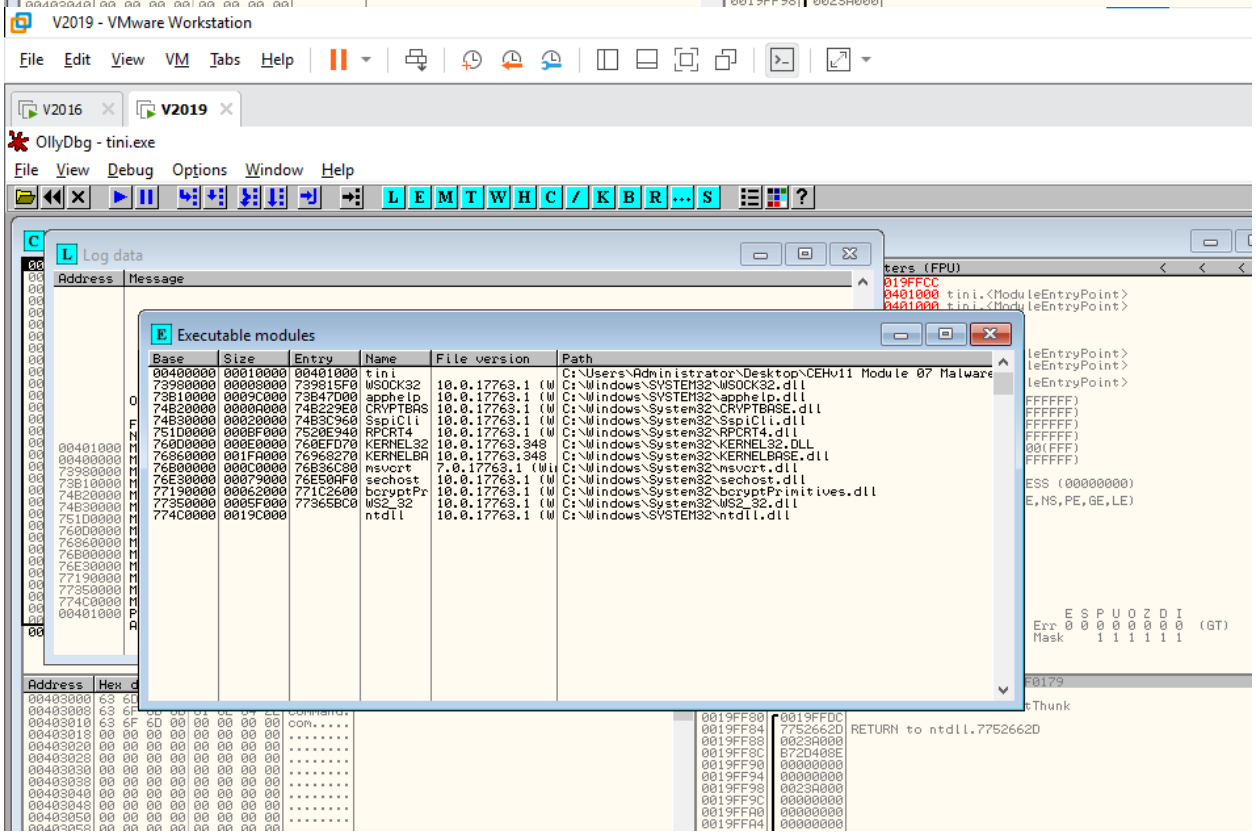

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
IDA - face.exe C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware Threats\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!\face.exe
File Edit Jump Search View Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol
Functions window
Function name
Segment
sub_401000 .text
sub_401198 .text
sub_401284 .text
sub_4013A9 .text
sub_4013FA .text
StartAddress .text
sub_40174B .text
sub_40174E .text
sub_401808 .text
sub_401841 .text
sub_4018E9 .text
sub_401A1E .text
sub_401E02 .text
sub_40220C .text
sub_402319 .text
sub_40264B .text
sub_402680 .text
sub_40284D .text
sub_402C3B .text
sub_402D0D .text
sub_402D72 .text
sub_402DCE .text
sub_402EE0 .text
sub_402F9A .text
sub_403034 .text
sub_4030BF .text
sub_4030D4 .text
sub_40317D .text
sub_403222 .text
sub_40326C .text
sub_4032CF .text
sub_4032E6 .text
sub_4032FD .text
sub_40330B .text
sub_40330F .text
sub_4033A1 .text
IDA View-A
Hex View-1
Structures
Enum
00408458 0000000000408458: start (Synchronized with IDA View-A)
Output window
The initial autoanalysis has been finished.
IDC
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
IDA - face.exe C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware Threats\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!\face.exe
File Edit Jump Search View Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol
Functions window
Function name
Segment
sub_401000 .text
sub_401198 .text
sub_401284 .text
sub_4013A9 .text
sub_4013FA .text
StartAddress .text
sub_40174B .text
sub_40174E .text
sub_401808 .text
sub_401841 .text
IDA View-A
Hex View-1
Structures
Enums
00000000 ; [00000014 BYTES. COLLAPSED STRUCT _cpinfo. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; [0000001C BYTES. COLLAPSED STRUCT _SERVICE_STATUS. PRESS CTRL-NUMPAD+ TO EXPAND]
00000000 ; [00000004 BYTES. COLLAPSED STRUCT HKEY__. PRESS CTRL-NUMPAD+ TO EXPAND]


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
OllyDbg
File Home Share View
Malware Analysis Tools › Static Malware Analysis Tools › Disassembling and Debugging Tools › OllyDbg
Search OllyDbg
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
BOOKMARK.DLL 5/23/2004 1:10 AM Application extens... 55 KB
Cmdline.dll 5/23/2004 1:10 AM Application extens... 62 KB
dbghelp.dll 9/27/2007 3:47 PM Application extens... 1,021 KB
license 5/23/2004 1:10 AM Text Document 4 KB
OLLYDBG 5/23/2004 1:10 AM Application 1,092 KB
OLLYDBG 5/23/2004 1:10 AM Help file 289 KB
ollydbg 12/12/2019 5:40 PM Configuration sett... 8 KB
readme 5/23/2004 1:10 AM Text Document 3 KB
register 5/23/2004 1:10 AM Text Document 2 KB
tini.bak 2/4/2014 4:03 PM BAK File 6 KB
tini.udd 2/4/2014 4:15 PM UDD File 6 KB
11 items
PE Explorer
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
OllyDbg
File View Debug Options Window Help
CPU
Registers (FPU)
Address
Hex dump
ASCII


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
OllyDbg
File View Debug Options Window Help
Open 32-bit executable
Look in: Viruses
Name
Date modified
worm_cris 10/8/2023 9:27 AM
yanetha 10/8/2023 9:27 AM
ysor 10/8/2023 9:27 AM
zevach 10/8/2023 9:27 AM
tini 12/12/2019 2:31 PM
File name: tini
Open
Files of type: Executable file (*.exe)
Cancel
Arguments:


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
OllyDbg - tini.exe - [CPU - main thread, module tini]
File View Debug Options Window Help
Registers (FPU)
Address Hex dump ASCII


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
OllyDbg - tini.exe
File View Debug Options Window Help
Log data
Address Message
OllyDbg v1.10
File 'C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware Threats\CEHv11 Module 07 Malwa
New process with ID 00000C38 created
Main thread with ID 00001CA8 created
Module C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware Threats\CEHv11 Module 07 Malw
Module C:\Windows\SYSTEM32\WSOCK32.dll
Module C:\Windows\SYSTEM32\apphelp.dll
Module C:\Windows\System32\CRYPTBASE.dll
Module C:\Windows\System32\SspiCli.dll
Module C:\Windows\System32\RPCRT4.dll
Module C:\Windows\System32\KERNEL32.DLL
Module C:\Windows\System32\KERNELBASE.dll
Module C:\Windows\System32\msvcrt.dll
Module C:\Windows\System32\sechost.dll
Module C:\Windows\System32\bcryptPrimitives.dll
Module C:\Windows\System32\WS2_32.dll
Module C:\Windows\SYSTEM32\ntdll.dll
Program entry point
Analysing tini
0 heuristical procedures
20 calls to known functions
Address Hex dump ASCII
RETURN to KERNEL32.760F0179
KERNEL32.BaseThreadInitThunk
RETURN to ntdll.7752662D


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
OllyDbg - tini.exe
File View Debug Options Window Help
Log data
Address Message
Executable modules
Base Size Entry Name File version Path
00400000 00010000 00401000 tini C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware
73980000 00008000 739815F0 WSOCK32 10.0.17763.1 (W C:\Windows\SYSTEM32\WSOCK32.dll
73B10000 0009C000 73B47D00 apphelp 10.0.17763.1 (W C:\Windows\SYSTEM32\apphelp.dll
74B20000 0000A000 74B229E0 CRYPTBAS 10.0.17763.1 (W C:\Windows\System32\CRYPTBASE.dll
74B30000 00020000 74B3C960 SspiCli 10.0.17763.1 (W C:\Windows\System32\SspiCli.dll
751D0000 000BF000 7520E940 RPCRT4 10.0.17763.1 (W C:\Windows\System32\RPCRT4.dll
760D0000 000E0000 760EFD70 KERNEL32 10.0.17763.348 C:\Windows\System32\KERNEL32.DLL
76860000 001FA000 76968270 KERNELBA 10.0.17763.348 C:\Windows\System32\KERNELBASE.dll
76B00000 000C0000 76B36C80 msvcrt 7.0.17763.1 (Wi C:\Windows\System32\msvcrt.dll
76E30000 00079000 76E50AF0 sechost 10.0.17763.1 (W C:\Windows\System32\sechost.dll
77190000 00062000 771C2600 bcryptPr 10.0.17763.1 (W C:\Windows\System32\bcryptPrimitives.dll
77350000 0005F000 77365BC0 WS2_32 10.0.17763.1 (W C:\Windows\System32\WS2_32.dll
774C0000 0019C000 ntdll 10.0.17763.1 (W C:\Windows\SYSTEM32\ntdll.dll
RETURN to ntdll.7752662D