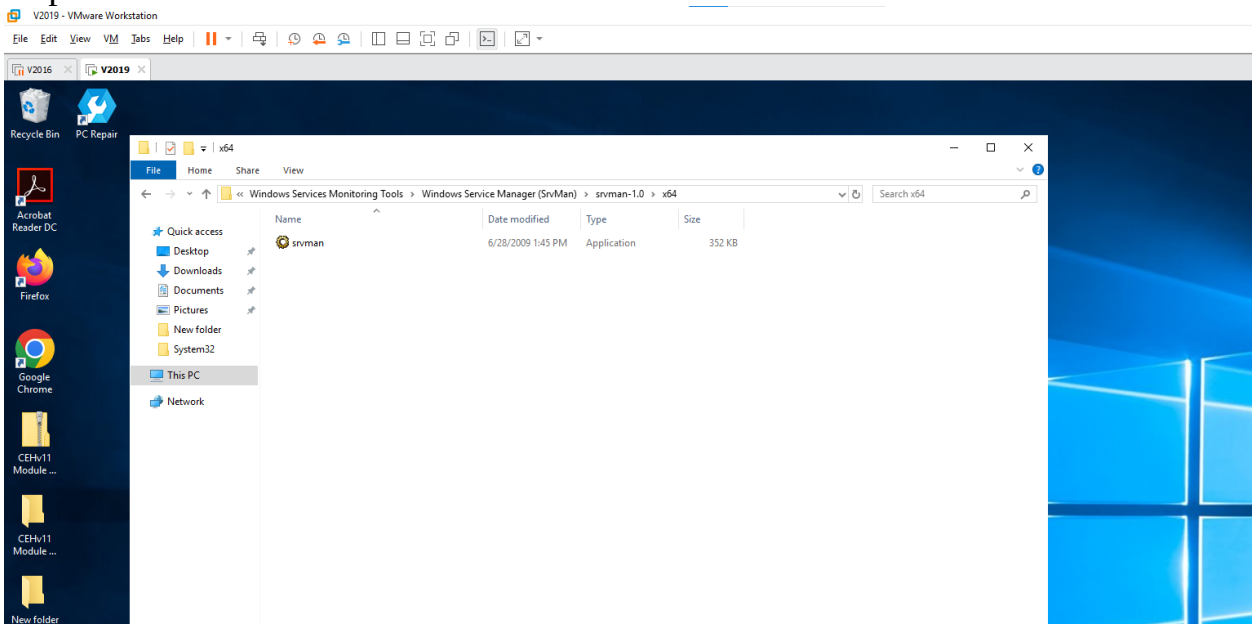
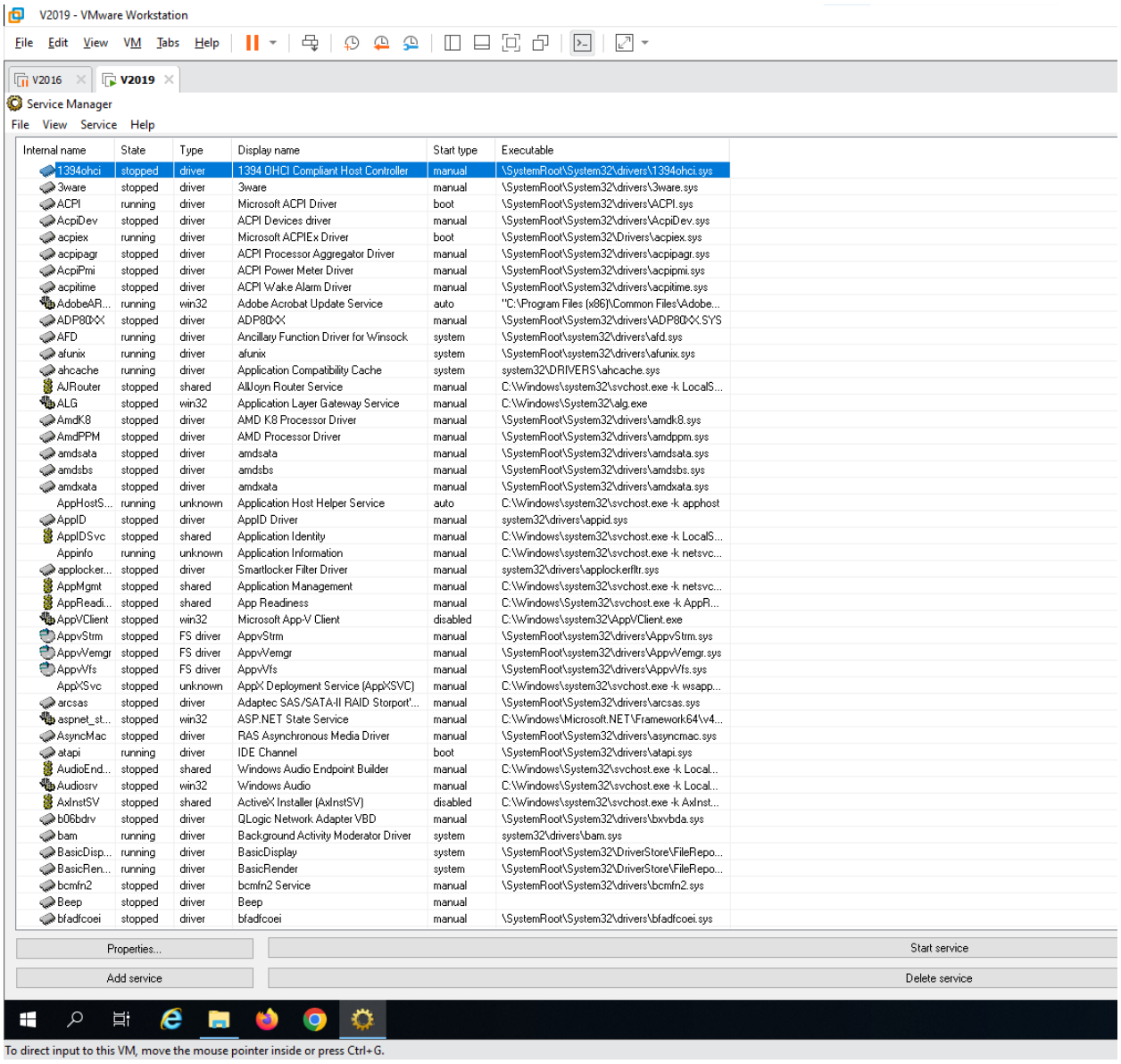
Lab 9: Malware Threats

Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 11/10/2023

4.4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)

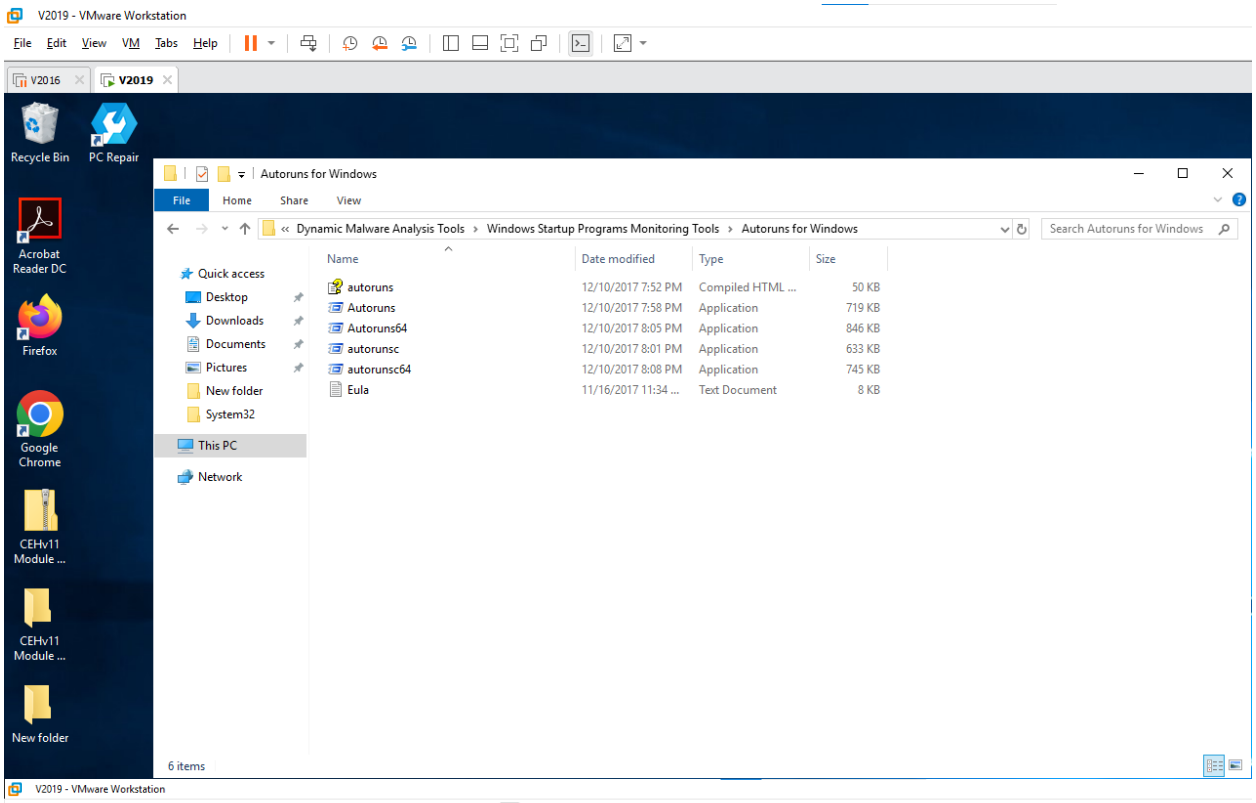
- Open Windows 10

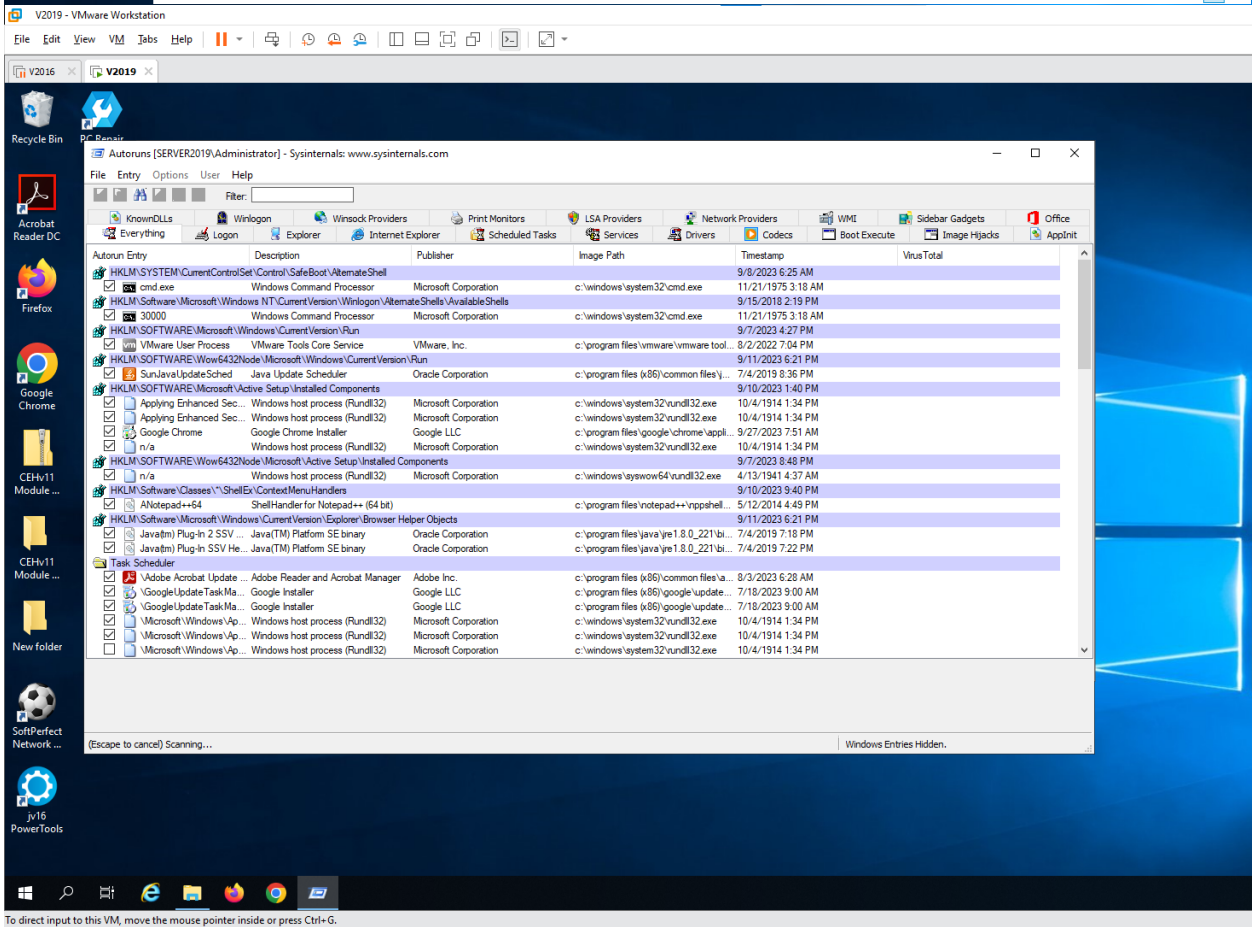


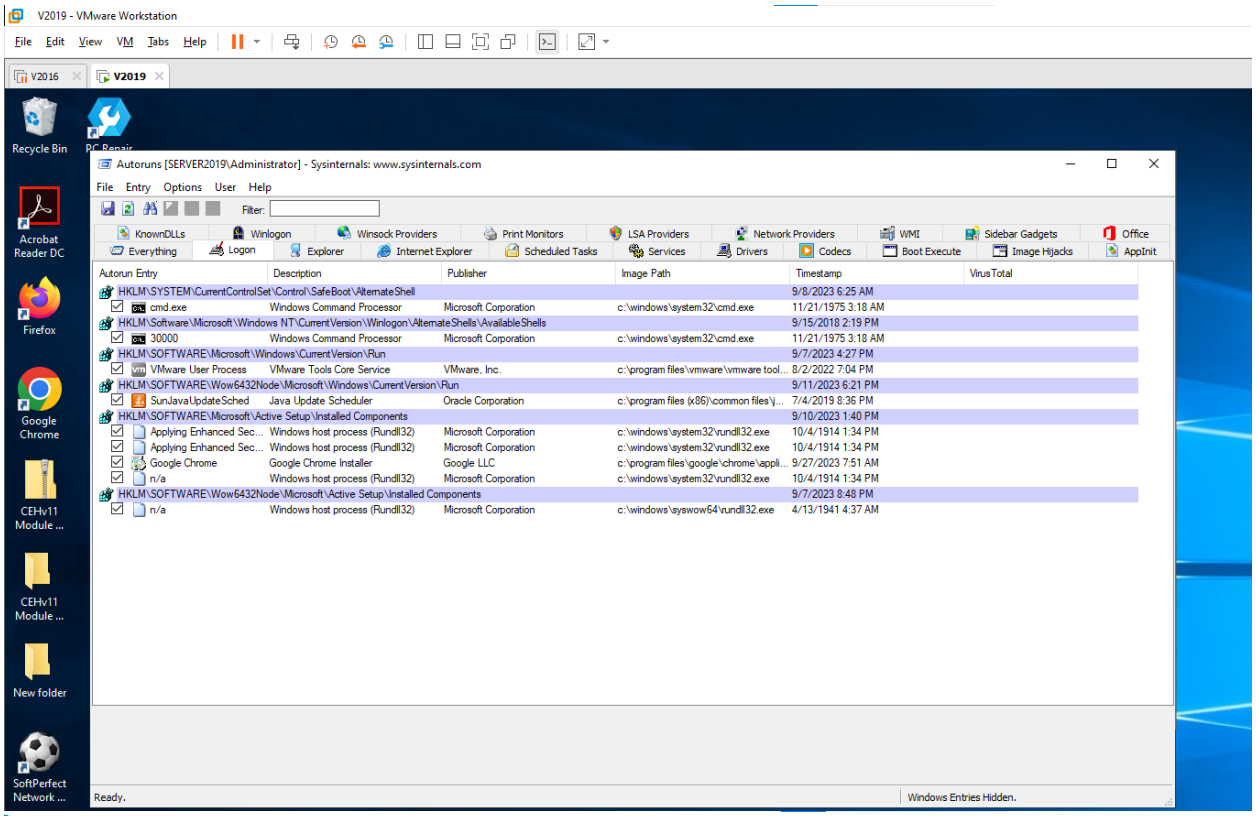


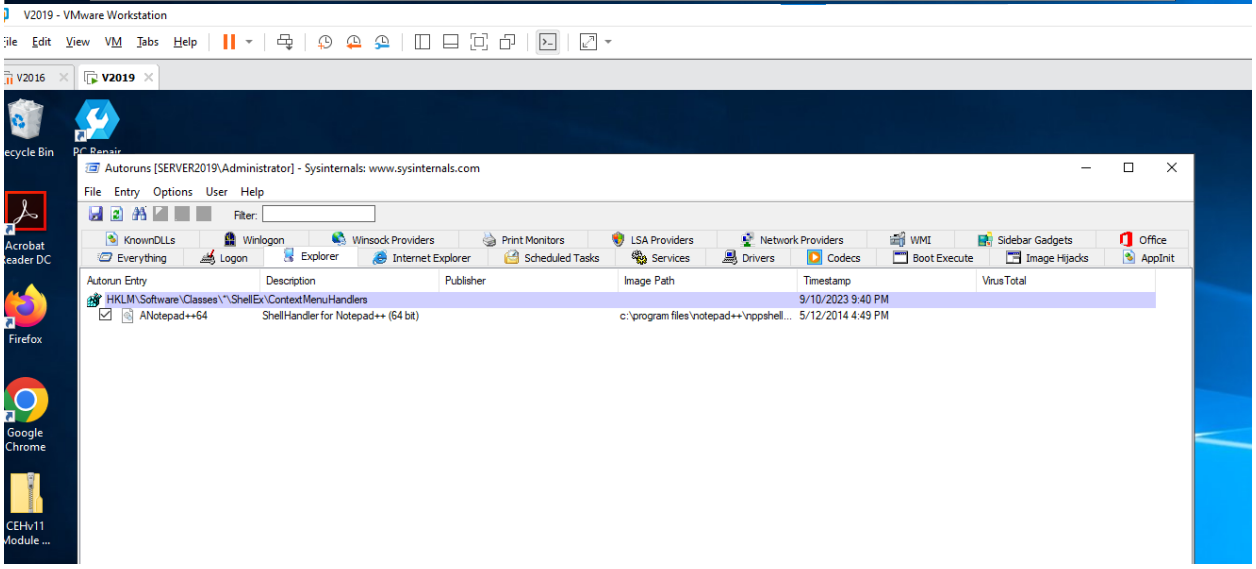
4.5 Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol

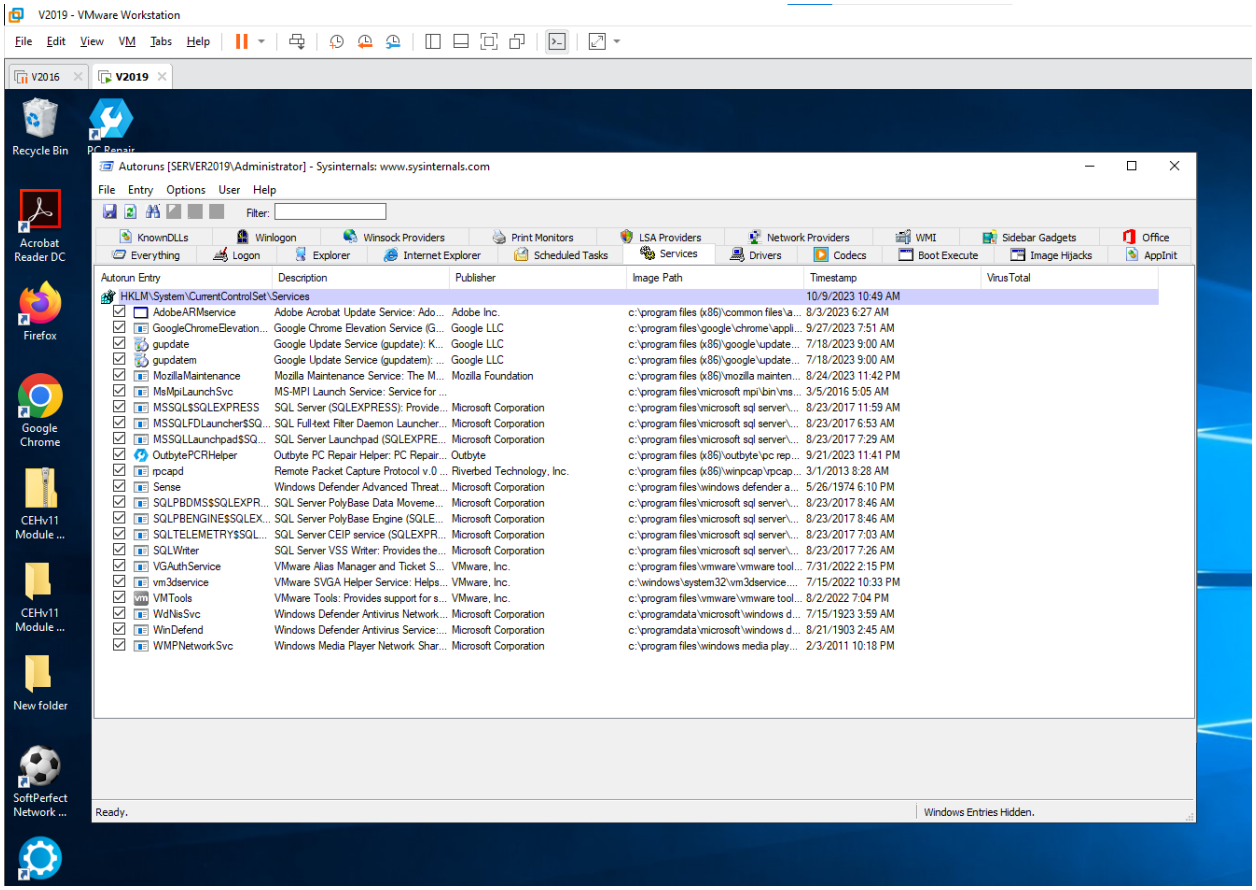
- Open Windows 10

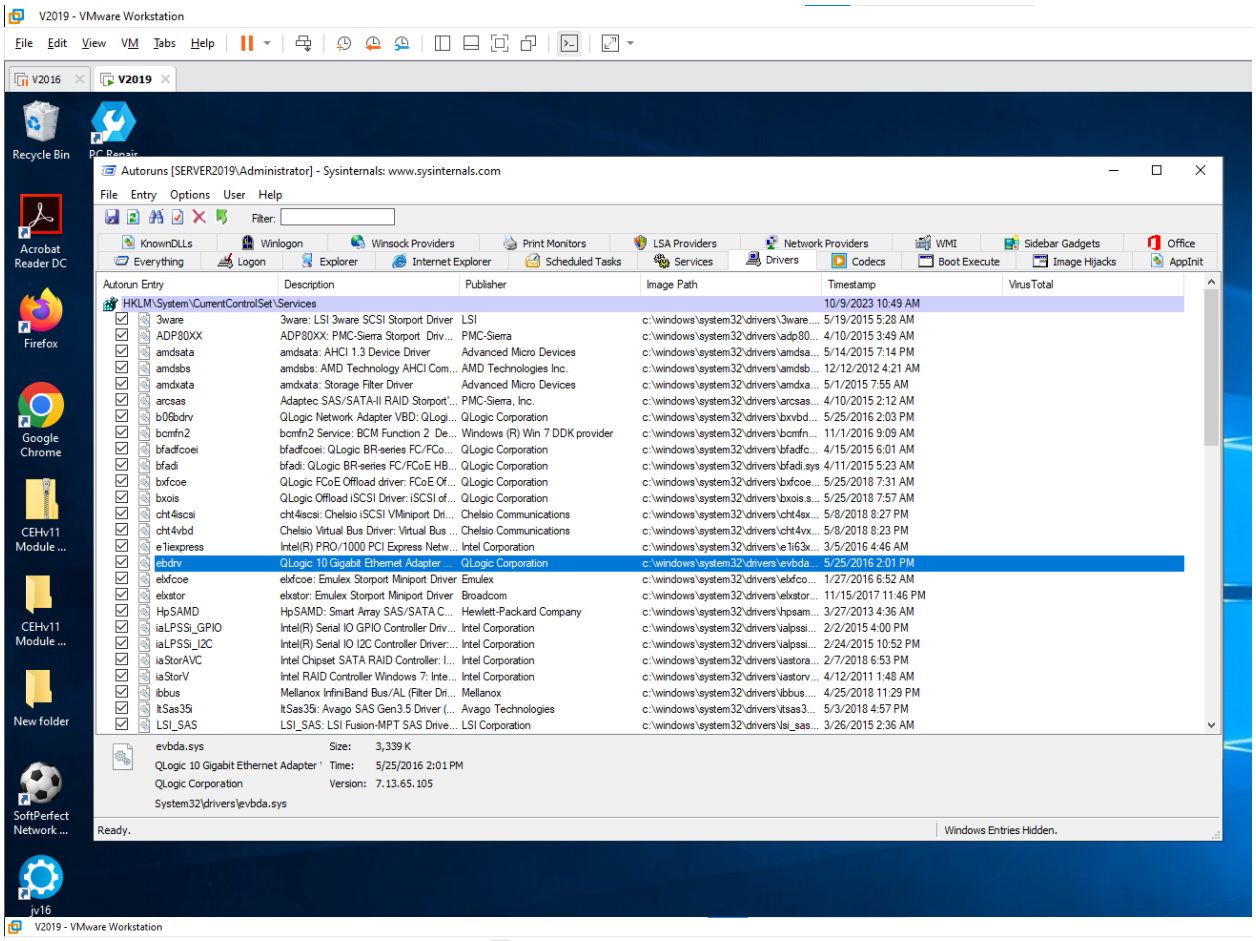

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
Autoruns for Windows
File Home Share View
« Dynamic Malware Analysis Tools › Windows Startup Programs Monitoring Tools › Autoruns for Windows
Search Autoruns for Windows
Quick access
Desktop
Downloads
Documents
Pictures
New folder
System32
This PC
Network
Name
Date modified
Type
Size
autoruns 12/10/2017 7:52 PM Compiled HTML ... 50 KB
Autoruns 12/10/2017 7:58 PM Application 719 KB
Autoruns64 12/10/2017 8:05 PM Application 846 KB
autorunsc 12/10/2017 8:01 PM Application 633 KB
autorunsc64 12/10/2017 8:08 PM Application 745 KB
Eula 11/16/2017 11:34 ... Text Document 8 KB
6 items

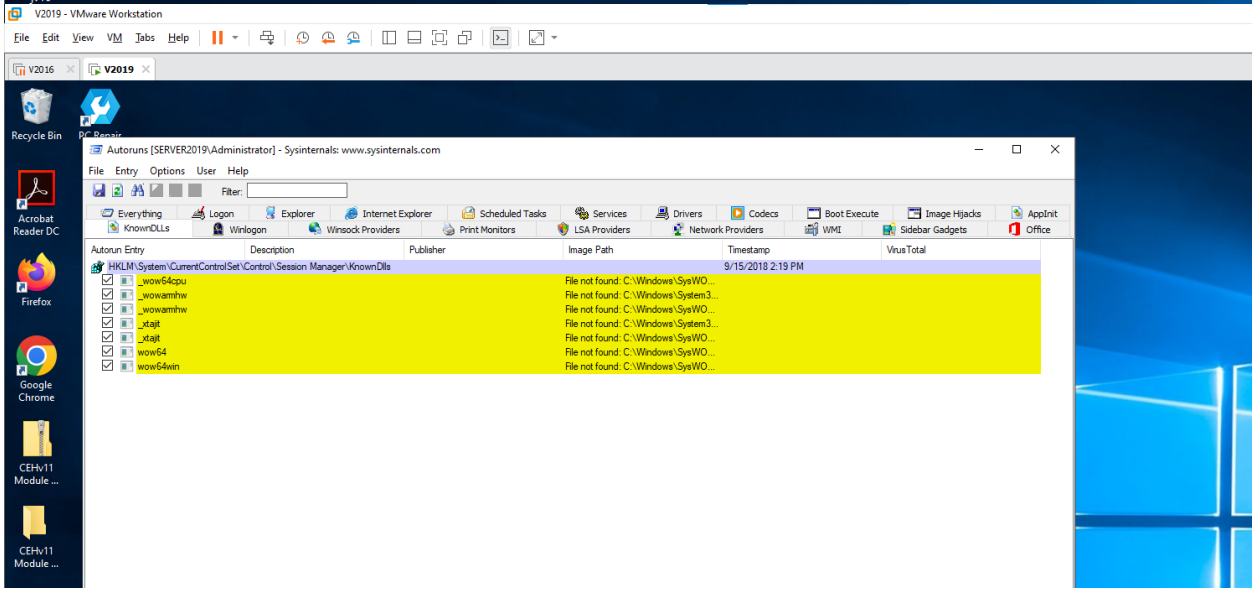

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
jv16 PowerTools
Autoruns [SERVER2019\Administrator] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell 9/8/2023 6:25 AM
cmd.exe Windows Command Processor Microsoft Corporation c:\windows\system32\cmd.exe 11/21/1975 3:18 AM
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells 9/15/2018 2:19 PM
30000 Windows Command Processor Microsoft Corporation c:\windows\system32\cmd.exe 11/21/1975 3:18 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 9/7/2023 4:27 PM
VMware User Process VMware Tools Core Service VMware, Inc. c:\program files\vmware\vmware tool... 8/2/2022 7:04 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run 9/11/2023 6:21 PM
SunJavaUpdateSched Java Update Scheduler Oracle Corporation c:\program files (x86)\common files\j... 7/4/2019 8:36 PM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components 9/10/2023 1:40 PM
Applying Enhanced Sec... Windows host process (Rundll32) Microsoft Corporation c:\windows\system32\rundll32.exe 10/4/1914 1:34 PM
Applying Enhanced Sec... Windows host process (Rundll32) Microsoft Corporation c:\windows\system32\rundll32.exe 10/4/1914 1:34 PM
Google Chrome Google Chrome Installer Google LLC c:\program files\google\chrome\appli... 9/27/2023 7:51 AM
n/a Windows host process (Rundll32) Microsoft Corporation c:\windows\system32\rundll32.exe 10/4/1914 1:34 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components 9/7/2023 8:48 PM
n/a Windows host process (Rundll32) Microsoft Corporation c:\windows\syswow64\rundll32.exe 4/13/1941 4:37 AM
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers 9/10/2023 9:40 PM
ANotepad++64 ShellHandler for Notepad++ (64 bit) c:\program files\notepad++\nppshell... 5/12/2014 4:49 PM
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects 9/11/2023 6:21 PM
Java(tm) Plug-In 2 SSV ... Java(TM) Platform SE binary Oracle Corporation c:\program files\java\jre1.8.0_221\bi... 7/4/2019 7:18 PM
Java(tm) Plug-In SSV He... Java(TM) Platform SE binary Oracle Corporation c:\program files\java\jre1.8.0_221\bi... 7/4/2019 7:22 PM
Task Scheduler
\Adobe Acrobat Update ... Adobe Reader and Acrobat Manager Adobe Inc. c:\program files (x86)\common files\a... 8/3/2023 6:28 AM
\GoogleUpdateTaskMa... Google Installer Google LLC c:\program files (x86)\google\update... 7/18/2023 9:00 AM
\GoogleUpdateTaskMa... Google Installer Google LLC c:\program files (x86)\google\update... 7/18/2023 9:00 AM
\Microsoft\Windows\Ap... Windows host process (Rundll32) Microsoft Corporation c:\windows\system32\rundll32.exe 10/4/1914 1:34 PM
\Microsoft\Windows\Ap... Windows host process (Rundll32) Microsoft Corporation c:\windows\system32\rundll32.exe 10/4/1914 1:34 PM
\Microsoft\Windows\Ap... Windows host process (Rundll32) Microsoft Corporation c:\windows\system32\rundll32.exe 10/4/1914 1:34 PM
(Escape to cancel) Scanning...
Windows Entries Hidden.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

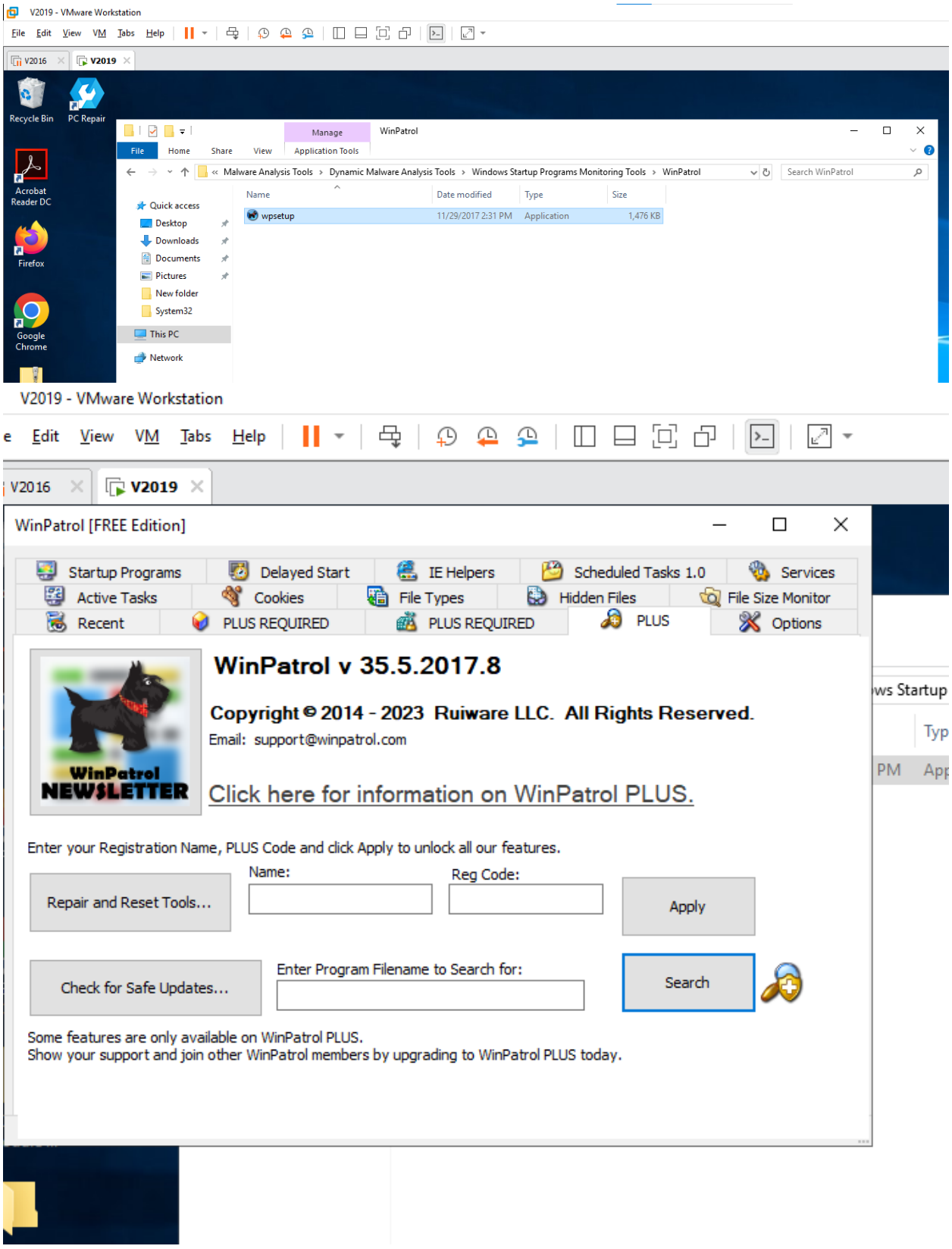

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
Autoruns [SERVER2019\Administrator] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell 9/8/2023 6:25 AM
cmd.exe Windows Command Processor Microsoft Corporation c:\windows\system32\cmd.exe 11/21/1975 3:18 AM
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells 9/15/2018 2:19 PM
30000 Windows Command Processor Microsoft Corporation c:\windows\system32\cmd.exe 11/21/1975 3:18 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 9/7/2023 4:27 PM
VMware User Process VMware Tools Core Service VMware, Inc. c:\program files\vmware\vmware tool... 8/2/2022 7:04 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run 9/11/2023 6:21 PM
SunJavaUpdateSched Java Update Scheduler Oracle Corporation c:\program files (x86)\common files\j... 7/4/2019 8:36 PM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components 9/10/2023 1:40 PM
Applying Enhanced Sec... Windows host process (Rundll32) Microsoft Corporation c:\windows\system32\rundll32.exe 10/4/1914 1:34 PM
Applying Enhanced Sec... Windows host process (Rundll32) Microsoft Corporation c:\windows\system32\rundll32.exe 10/4/1914 1:34 PM
Google Chrome Google Chrome Installer Google LLC c:\program files\google\chrome\appli... 9/27/2023 7:51 AM
n/a Windows host process (Rundll32) Microsoft Corporation c:\windows\system32\rundll32.exe 10/4/1914 1:34 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components 9/7/2023 8:48 PM
n/a Windows host process (Rundll32) Microsoft Corporation c:\windows\syswow64\rundll32.exe 4/13/1941 4:37 AM
Ready.
Windows Entries Hidden.

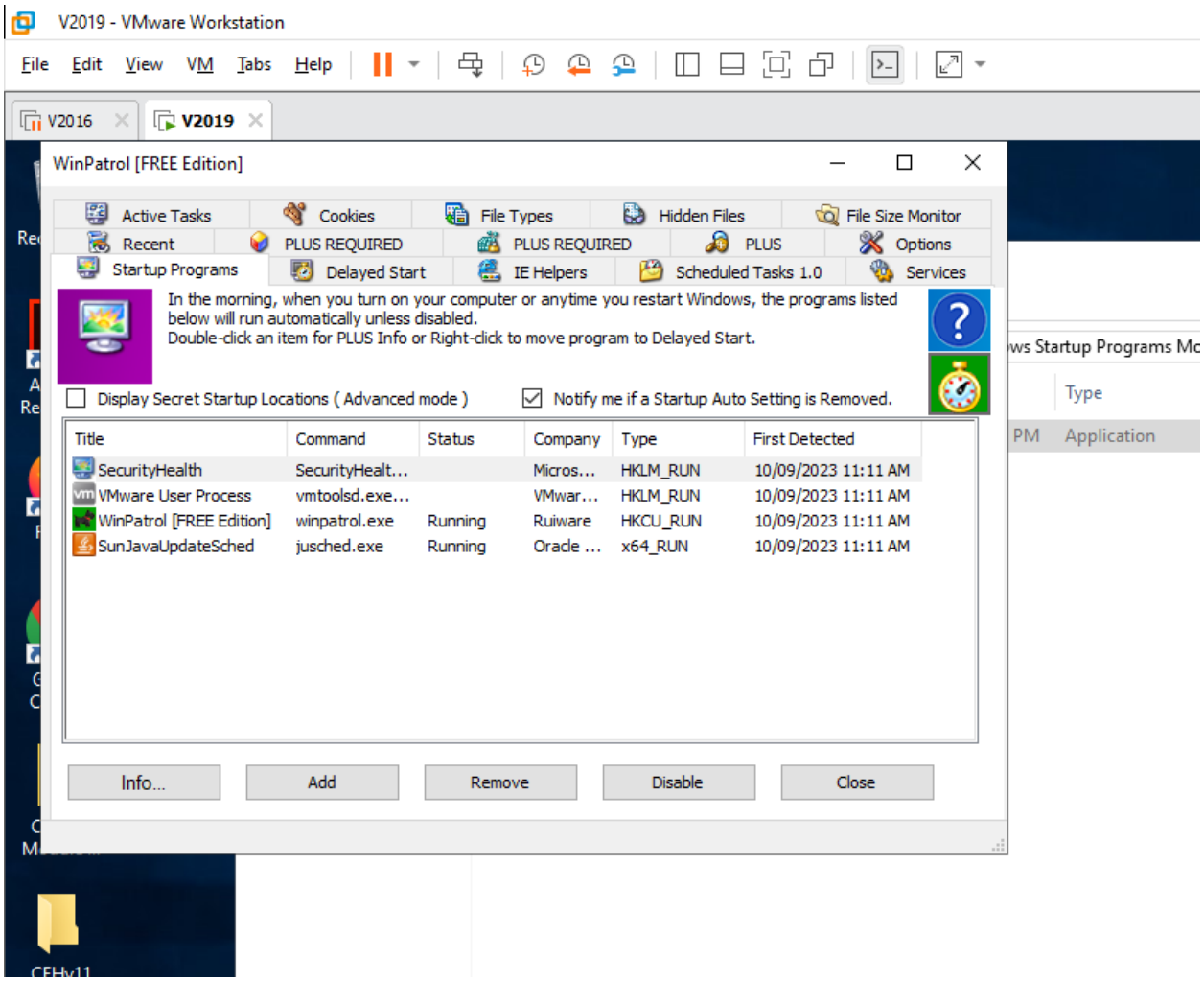

V2019 - VMware Workstation
V2016
V2019
Autoruns [SERVER2019\Administrator] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers 9/10/2023 9:40 PM
ANotepad++64 ShellHandler for Notepad++ (64 bit) c:\program files\notepad++\nppshell... 5/12/2014 4:49 PM

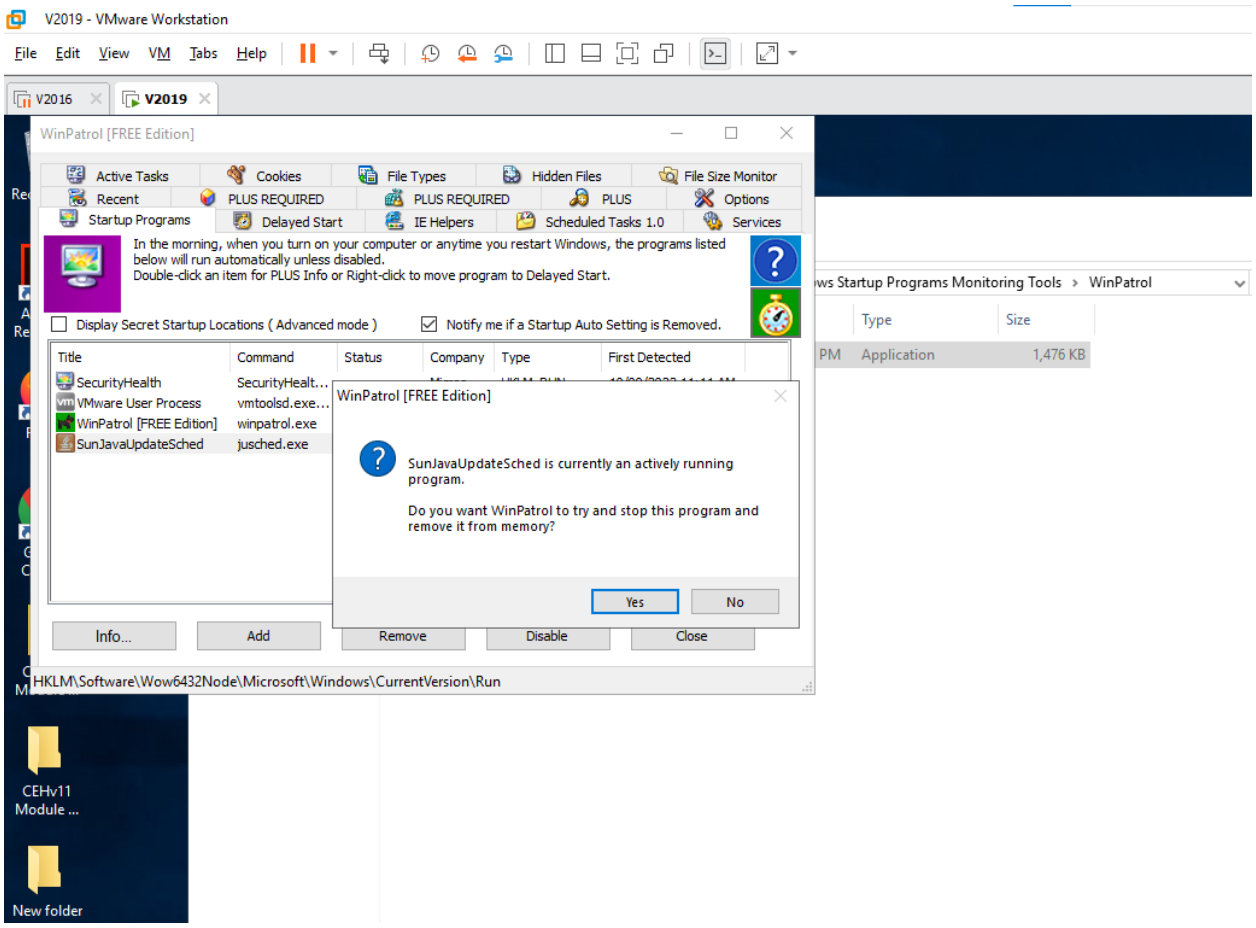

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
Autoruns [SERVER2019\Administrator] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
HKLM\System\CurrentControlSet\Services 10/9/2023 10:49 AM
AdobeARMservice Adobe Acrobat Update Service: Ado... Adobe Inc. c:\program files (x86)\common files\a... 8/3/2023 6:27 AM
GoogleChromeElevation... Google Chrome Elevation Service (G... Google LLC c:\program files\google\chrome\appli... 9/27/2023 7:51 AM
gupdate Google Update Service (gupdate): K... Google LLC c:\program files (x86)\google\update... 7/18/2023 9:00 AM
gupdatem Google Update Service (gupdatem): ... Google LLC c:\program files (x86)\google\update... 7/18/2023 9:00 AM
MozillaMaintenance Mozilla Maintenance Service: The M... Mozilla Foundation c:\program files (x86)\mozilla mainten... 8/24/2023 11:42 PM
MsMpiLaunchSvc MS-MPI Launch Service: Service for ... c:\program files\microsoft mpi\bin\ms... 3/5/2016 5:05 AM
MSSQL$SQLEXPRESS SQL Server (SQLEXPRESS): Provide... Microsoft Corporation c:\program files\microsoft sql server\... 8/23/2017 11:59 AM
MSSQLFDLauncher$SQ... SQL Full-text Filter Daemon Launcher... Microsoft Corporation c:\program files\microsoft sql server\... 8/23/2017 6:53 AM
MSSQLLaunchpad$SQ... SQL Server Launchpad (SQLEXPRE... Microsoft Corporation c:\program files\microsoft sql server\... 8/23/2017 7:29 AM
OutbytePCRHelper Outbyte PC Repair Helper: PC Repair... Outbyte c:\program files (x86)\outbyte\pc rep... 9/21/2023 11:41 PM
rpcapd Remote Packet Capture Protocol v.0 ... Riverbed Technology, Inc. c:\program files (x86)\winpcap\rpcap... 3/1/2013 8:28 AM
Sense Windows Defender Advanced Threat... Microsoft Corporation c:\program files\windows defender a... 5/26/1974 6:10 PM
SQLPBDMS$SQLEXPR... SQL Server PolyBase Data Moveme... Microsoft Corporation c:\program files\microsoft sql server\... 8/23/2017 8:46 AM
SQLPBENGINE$SQLEX... SQL Server PolyBase Engine (SQLE... Microsoft Corporation c:\program files\microsoft sql server\... 8/23/2017 8:46 AM
SQLTELEMETRY$SQL... SQL Server CEIP service (SQLEXPR... Microsoft Corporation c:\program files\microsoft sql server\... 8/23/2017 7:03 AM
SQLWriter SQL Server VSS Writer: Provides the... Microsoft Corporation c:\program files\microsoft sql server\... 8/23/2017 7:26 AM
VGAuthService VMware Alias Manager and Ticket S... VMware, Inc. c:\program files\vmware\vmware tool... 7/31/2022 2:15 PM
vm3dservice VMware SVGA Helper Service: Helps... VMware, Inc. c:\windows\system32\vm3dservice.... 7/15/2022 10:33 PM
VMTools VMware Tools: Provides support for s... VMware, Inc. c:\program files\vmware\vmware tool... 8/2/2022 7:04 PM
WdNisSvc Windows Defender Antivirus Network... Microsoft Corporation c:\programdata\microsoft\windows d... 7/15/1923 3:59 AM
WinDefend Windows Defender Antivirus Service:... Microsoft Corporation c:\programdata\microsoft\windows d... 8/21/1903 2:45 AM
WMPNetworkSvc Windows Media Player Network Shar... Microsoft Corporation c:\program files\windows media play... 2/3/2011 10:18 PM
Ready.
Windows Entries Hidden.

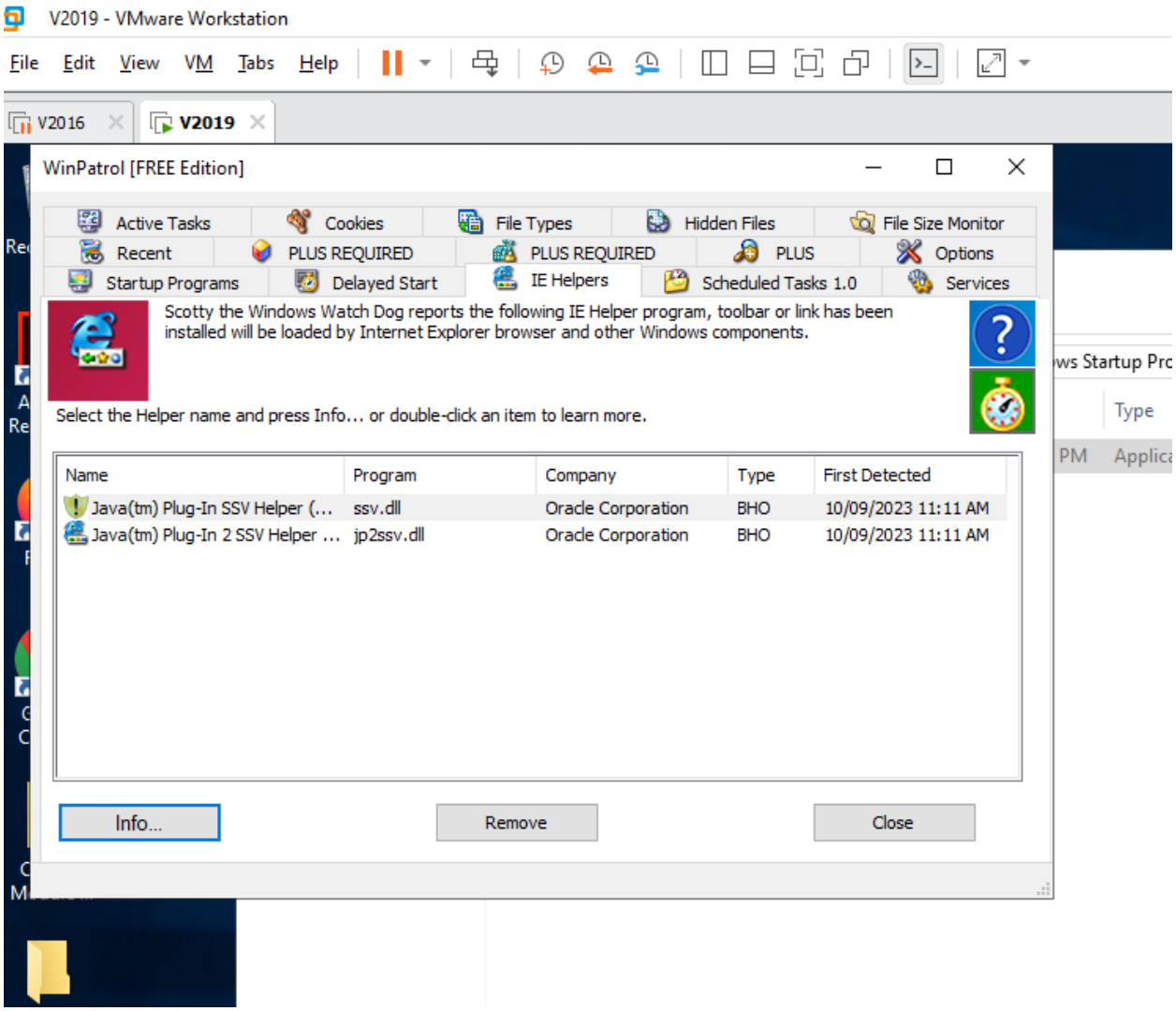

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
jv16
Autoruns [SERVER2019\Administrator] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
HKLM\System\CurrentControlSet\Services 10/9/2023 10:49 AM
3ware 3ware: LSI 3ware SCSI Storport Driver LSI c:\windows\system32\drivers\3ware.... 5/19/2015 5:28 AM
ADP80XX ADP80XX: PMC-Sierra Storport Driv... PMC-Sierra c:\windows\system32\drivers\adp80... 4/10/2015 3:49 AM
amdsata amdsata: AHCI 1.3 Device Driver Advanced Micro Devices c:\windows\system32\drivers\amdsa... 5/14/2015 7:14 PM
amdsbs amdsbs: AMD Technology AHCI Com... AMD Technologies Inc. c:\windows\system32\drivers\amdsb... 12/12/2012 4:21 AM
amdxata amdxata: Storage Filter Driver Advanced Micro Devices c:\windows\system32\drivers\amdxa... 5/1/2015 7:55 AM
arcsas Adaptec SAS/SATA-II RAID Storport'... PMC-Sierra, Inc. c:\windows\system32\drivers\arcsas... 4/10/2015 2:12 AM
b06bdrv QLogic Network Adapter VBD: QLogi... QLogic Corporation c:\windows\system32\drivers\bxvbd... 5/25/2016 2:03 PM
bcmfn2 bcmfn2 Service: BCM Function 2 De... Windows (R) Win 7 DDK provider c:\windows\system32\drivers\bcmfn... 11/1/2016 9:09 AM
bfadfcoei bfadfcoei: QLogic BR-series FC/FCo... QLogic Corporation c:\windows\system32\drivers\bfadfc... 4/15/2015 6:01 AM
bfadi bfadi: QLogic BR-series FC/FCoE HB... QLogic Corporation c:\windows\system32\drivers\bfadi.sys 4/11/2015 5:23 AM
bxfcoe QLogic FCoE Offload driver: FCoE Of... QLogic Corporation c:\windows\system32\drivers\bxfcoe... 5/25/2018 7:31 AM
bxois QLogic Offload iSCSI Driver: iSCSI of... QLogic Corporation c:\windows\system32\drivers\bxois.s... 5/25/2018 7:57 AM
cht4iscsi cht4iscsi: Chelsio iSCSI VMiniport Dri... Chelsio Communications c:\windows\system32\drivers\cht4sx... 5/8/2018 8:27 PM
cht4vbd Chelsio Virtual Bus Driver: Virtual Bus ... Chelsio Communications c:\windows\system32\drivers\cht4vx... 5/8/2018 8:23 PM
e1iexpress Intel(R) PRO/1000 PCI Express Netw... Intel Corporation c:\windows\system32\drivers\e1i63x... 3/5/2016 4:46 AM
ebdrv QLogic 10 Gigabit Ethernet Adapter ... QLogic Corporation c:\windows\system32\drivers\evbda... 5/25/2016 2:01 PM
elxfcoe elxfcoe: Emulex Storport Miniport Driver Emulex c:\windows\system32\drivers\elxfco... 1/27/2016 6:52 AM
elxstor elxstor: Emulex Storport Miniport Driver Broadcom c:\windows\system32\drivers\elxstor... 11/15/2017 11:46 PM
HpSAMD HpSAMD: Smart Array SAS/SATA C... Hewlett-Packard Company c:\windows\system32\drivers\hpsam... 3/27/2013 4:36 AM
iaLPSSi_GPIO Intel(R) Serial IO GPIO Controller Driv... Intel Corporation c:\windows\system32\drivers\ialpssi... 2/2/2015 4:00 PM
iaLPSSi_I2C Intel(R) Serial IO I2C Controller Driver:... Intel Corporation c:\windows\system32\drivers\ialpssi... 2/24/2015 10:52 PM
iaStorAVC Intel Chipset SATA RAID Controller: I... Intel Corporation c:\windows\system32\drivers\iastora... 2/7/2018 6:53 PM
iaStorV Intel RAID Controller Windows 7: Inte... Intel Corporation c:\windows\system32\drivers\iastorv... 4/12/2011 1:48 AM
ibbus Mellanox InfiniBand Bus/AL (Filter Dri... Mellanox c:\windows\system32\drivers\ibbus.... 4/25/2018 11:29 PM
ltSas35i ltSas35i: Avago SAS Gen3.5 Driver (... Avago Technologies c:\windows\system32\drivers\ltsas3... 5/3/2018 4:57 PM
LSI_SAS LSI_SAS: LSI Fusion-MPT SAS Drive... LSI Corporation c:\windows\system32\drivers\lsi_sas... 3/26/2015 2:36 AM
evbda.sys
QLogic 10 Gigabit Ethernet Adapter '
QLogic Corporation
System32\drivers\evbda.sys
Size: 3,339 K
Time: 5/25/2016 2:01 PM
Version: 7.13.65.105
Ready.
Windows Entries Hidden.

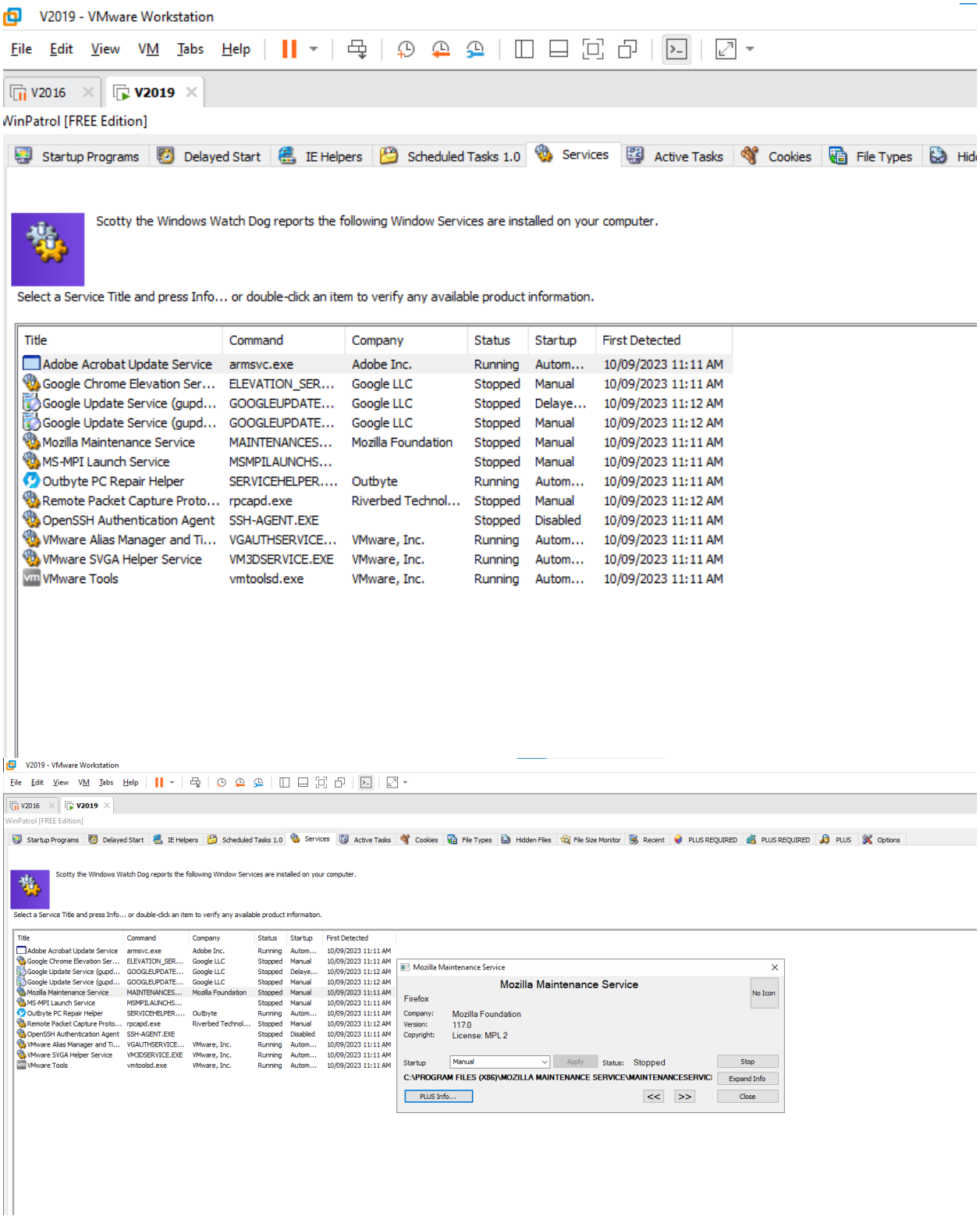

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Autoruns [SERVER2019\Administrator] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit
KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls 9/15/2018 2:19 PM
_wow64cpu File not found: C:\Windows\SysWO...
_wowarmhw File not found: C:\Windows\System3...
_wowarmhw File not found: C:\Windows\SysWO...
_xtajit File not found: C:\Windows\System3...
_xtajit File not found: C:\Windows\SysWO...
wow64 File not found: C:\Windows\SysWO...
wow64win File not found: C:\Windows\SysWO...

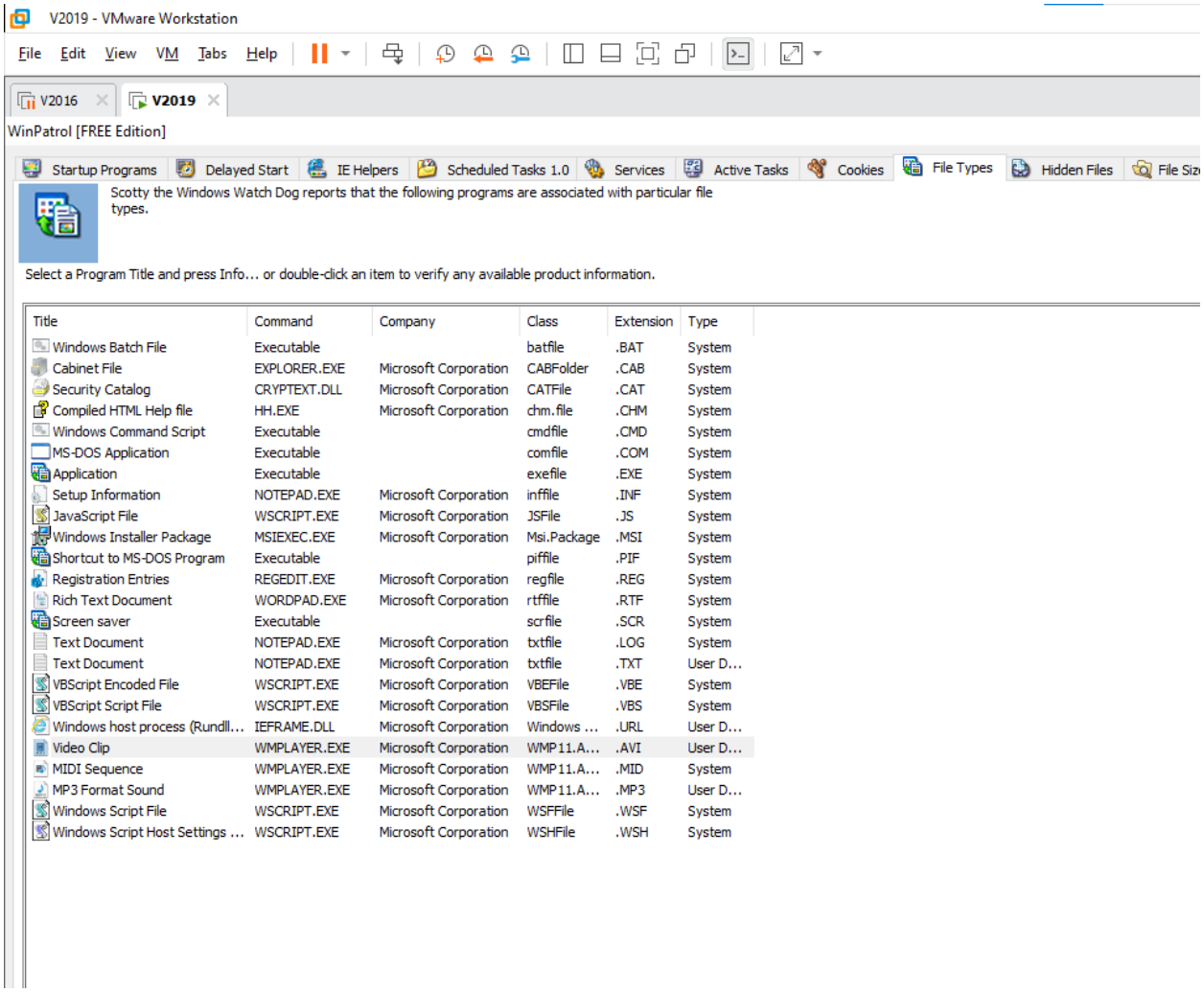

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Firefox
Google Chrome
Manage
WinPatrol
File Home Share View Application Tools
Malware Analysis Tools › Dynamic Malware Analysis Tools › Windows Startup Programs Monitoring Tools › WinPatrol
Search WinPatrol
Quick access
Desktop
Downloads
Documents
Pictures
New folder
System32
This PC
Network
Name
Date modified
Type
Size
wpsetup
11/29/2017 2:31 PM
Application
1,476 KB
V2019 - VMware Workstation
e Edit View VM Tabs Help
V2016
V2019
WinPatrol [FREE Edition]
Startup Programs
Delayed Start
IE Helpers
Scheduled Tasks 1.0
Services
Active Tasks
Cookies
File Types
Hidden Files
File Size Monitor
Recent
PLUS REQUIRED
PLUS REQUIRED
PLUS
Options
WinPatrol v 35.5.2017.8
Copyright © 2014 - 2023 Ruiware LLC. All Rights Reserved.
Email: support@winpatrol.com
WinPatrol NEWSLETTER
Click here for information on WinPatrol PLUS.
Enter your Registration Name, PLUS Code and click Apply to unlock all our features.
Repair and Reset Tools...
Name:
Reg Code:
Apply
Check for Safe Updates...
Enter Program Filename to Search for:
Search
Some features are only available on WinPatrol PLUS.
Show your support and join other WinPatrol members by upgrading to WinPatrol PLUS today.


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
WinPatrol [FREE Edition]
Active Tasks
Cookies
File Types
Hidden Files
File Size Monitor
Recent
PLUS REQUIRED
PLUS REQUIRED
PLUS
Options
Startup Programs
Delayed Start
IE Helpers
Scheduled Tasks 1.0
Services
In the morning, when you turn on your computer or anytime you restart Windows, the programs listed below will run automatically unless disabled.
Double-click an item for PLUS Info or Right-click to move program to Delayed Start.
Display Secret Startup Locations (Advanced mode)
Notify me if a Startup Auto Setting is Removed.
Title
Command
Status
Company
Type
First Detected
SecurityHealth
SecurityHealt...
Micros...
HKLM_RUN
10/09/2023 11:11 AM
VMware User Process
vmtoolsd.exe...
VMwar...
HKLM_RUN
10/09/2023 11:11 AM
WinPatrol [FREE Edition]
winpatrol.exe
Running
Ruiware
HKCU_RUN
10/09/2023 11:11 AM
SunJavaUpdateSched
jusched.exe
Running
Oracle ...
x64_RUN
10/09/2023 11:11 AM
Info...
Add
Remove
Disable
Close
Type
PM
Application


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
WinPatrol [FREE Edition]
Active Tasks
Cookies
File Types
Hidden Files
File Size Monitor
Recent
PLUS REQUIRED
PLUS REQUIRED
PLUS
Options
Startup Programs
Delayed Start
IE Helpers
Scheduled Tasks 1.0
Services
In the morning, when you turn on your computer or anytime you restart Windows, the programs listed below will run automatically unless disabled.
Double-click an item for PLUS Info or Right-click to move program to Delayed Start.
Display Secret Startup Locations (Advanced mode)
Notify me if a Startup Auto Setting is Removed.
Title
Command
Status
Company
Type
First Detected
SecurityHealth
SecurityHealt...
VMware User Process
vmtoolsd.exe...
WinPatrol [FREE Edition]
winpatrol.exe
SunJavaUpdateSched
jusched.exe
WinPatrol [FREE Edition]
SunJavaUpdateSched is currently an actively running program.
Do you want WinPatrol to try and stop this program and remove it from memory?
Yes
No
Info...
Add
Remove
Disable
Close
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
ws Startup Programs Monitoring Tools › WinPatrol
Type
Size
PM
Application
1,476 KB
CEHv11 Module ...
New folder


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
WinPatrol [FREE Edition]
Active Tasks
Cookies
File Types
Hidden Files
File Size Monitor
Recent
PLUS REQUIRED
PLUS REQUIRED
PLUS
Options
Startup Programs
Delayed Start
IE Helpers
Scheduled Tasks 1.0
Services
Scotty the Windows Watch Dog reports the following IE Helper program, toolbar or link has been installed will be loaded by Internet Explorer browser and other Windows components.
Select the Helper name and press Info... or double-click an item to learn more.
Name
Program
Company
Type
First Detected
Java(tm) Plug-In SSV Helper (...
ssv.dll
Oracle Corporation
BHO
10/09/2023 11:11 AM
Java(tm) Plug-In 2 SSV Helper ...
jp2ssv.dll
Oracle Corporation
BHO
10/09/2023 11:11 AM
Info...
Remove
Close

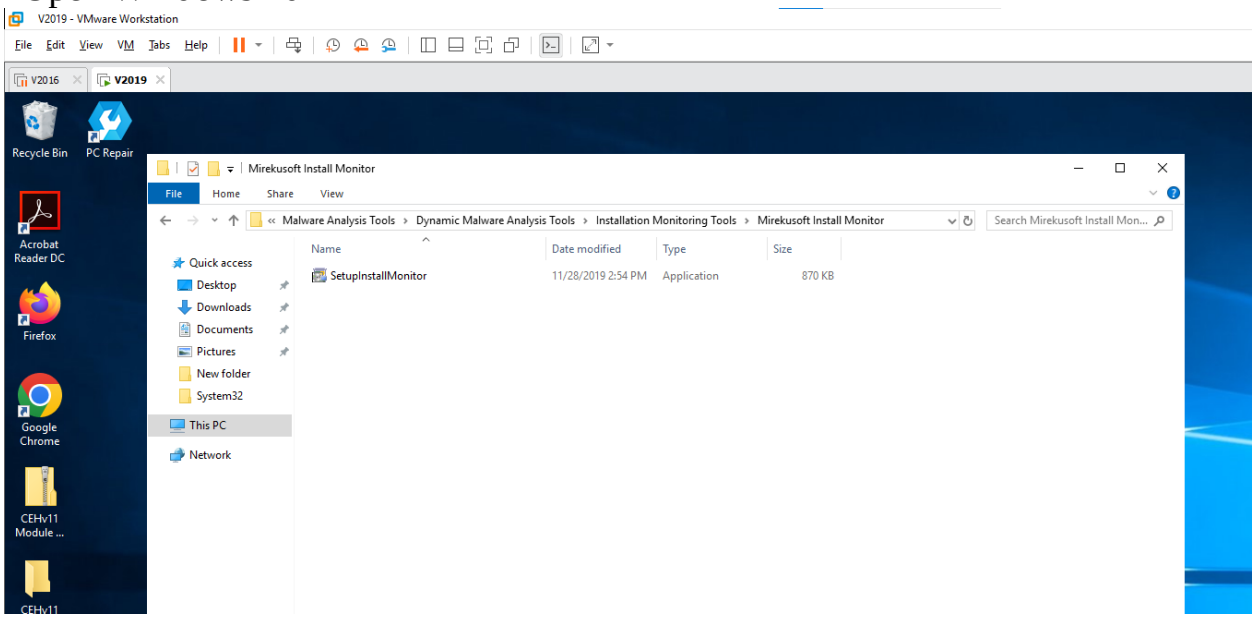

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
WinPatrol [FREE Edition]
Startup Programs
Delayed Start
IE Helpers
Scheduled Tasks 1.0
Services
Active Tasks
Cookies
File Types
Scotty the Windows Watch Dog reports the following Window Services are installed on your computer.
Select a Service Title and press Info... or double-click an item to verify any available product information.
Title
Command
Company
Status
Startup
First Detected
Adobe Acrobat Update Service
armsvc.exe
Adobe Inc.
Running
Autom...
10/09/2023 11:11 AM
Google Chrome Elevation Ser...
ELEVATION_SER...
Google LLC
Stopped
Manual
10/09/2023 11:11 AM
Google Update Service (gupd...
GOOGLEUPDATE...
Google LLC
Stopped
Delaye...
10/09/2023 11:12 AM
Google Update Service (gupd...
GOOGLEUPDATE...
Google LLC
Stopped
Manual
10/09/2023 11:12 AM
Mozilla Maintenance Service
MAINTENANCES...
Mozilla Foundation
Stopped
Manual
10/09/2023 11:11 AM
MS-MPI Launch Service
MSMPILAUNCHS...
Stopped
Manual
10/09/2023 11:11 AM
Outbyte PC Repair Helper
SERVICEHELPER....
Outbyte
Running
Autom...
10/09/2023 11:11 AM
Remote Packet Capture Proto...
rpcapd.exe
Riverbed Technol...
Stopped
Manual
10/09/2023 11:12 AM
OpenSSH Authentication Agent
SSH-AGENT.EXE
Stopped
Disabled
10/09/2023 11:11 AM
VMware Alias Manager and Ti...
VGAUTHSERVICE...
VMware, Inc.
Running
Autom...
10/09/2023 11:11 AM
VMware SVGA Helper Service
VM3DSERVICE.EXE
VMware, Inc.
Running
Autom...
10/09/2023 11:11 AM
VMware Tools
vmtoolsd.exe
VMware, Inc.
Running
Autom...
10/09/2023 11:11 AM
Mozilla Maintenance Service
Firefox
Company: Mozilla Foundation
Version: 117.0
Copyright: License: MPL 2
Startup
Manual
Apply
Status: Stopped
Stop
C:\PROGRAM FILES (X86)\MOZILLA MAINTENANCE SERVICE\MAINTENANCESERVICE
Expand Info
PLUS Info...
<<
>>
Close
No Icon

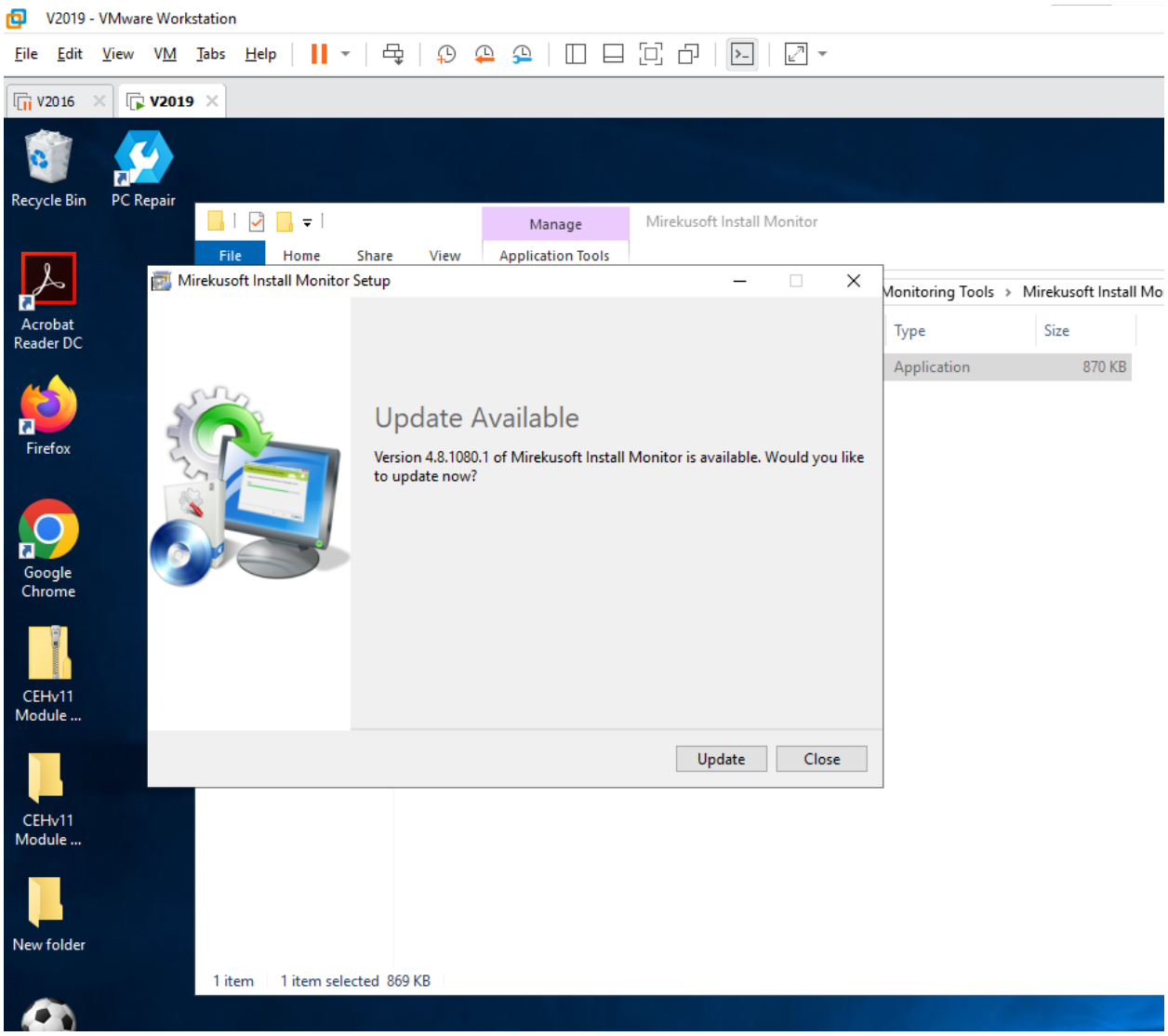


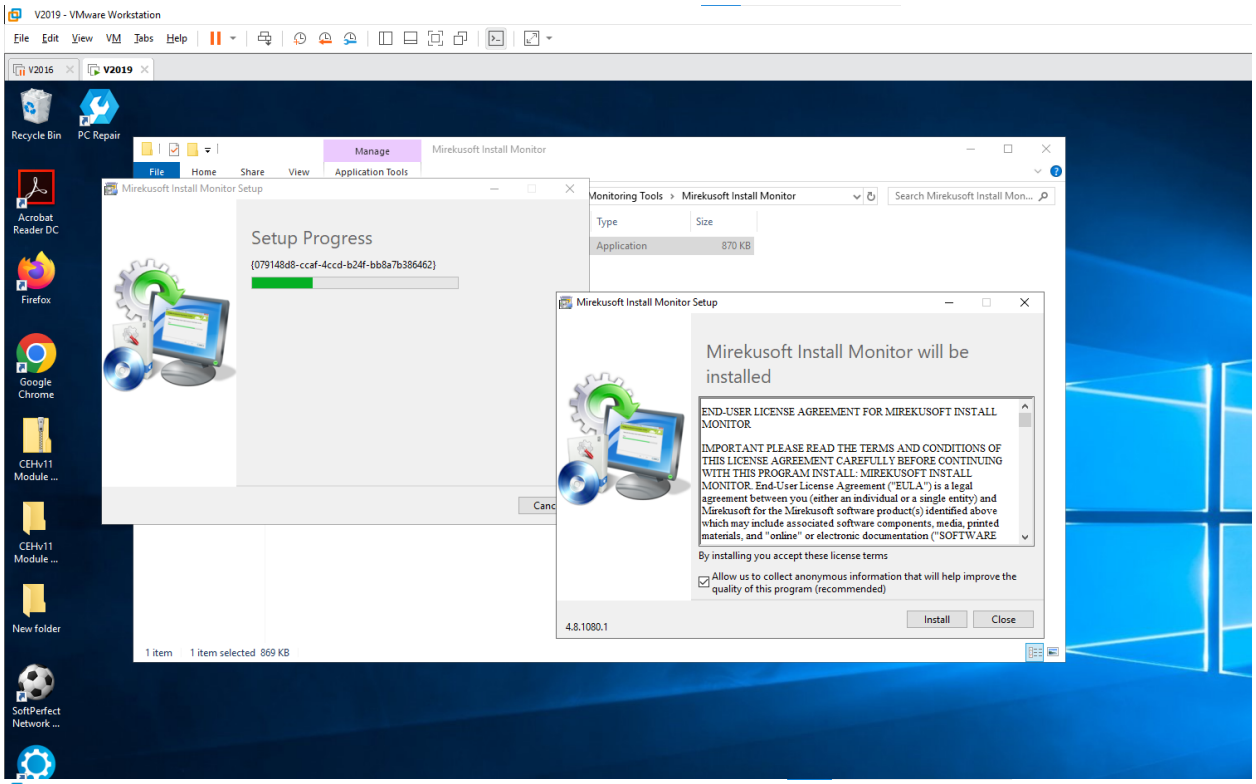
Title	Command	Company	Class	Extension	Type
Windows Batch File	Executable		batfile	.BAT	System
Cabinet File	EXPLORER.EXE	Microsoft Corporation	CABFolder	.CAB	System
Security Catalog	CRYPTEXT.DLL	Microsoft Corporation	CATFile	.CAT	System
Compiled HTML Help file	HH.EXE	Microsoft Corporation	chm.file	.CHM	System
Windows Command Script	Executable		cmdfile	.CMD	System
MS-DOS Application	Executable		comfile	.COM	System
Application	Executable		exefile	.EXE	System
Setup Information	NOTEPAD.EXE	Microsoft Corporation	inffile	.INF	System
JavaScript File	WSCRIPT.EXE	Microsoft Corporation	JSFile	.JS	System
Windows Installer Package	MSIEXEC.EXE	Microsoft Corporation	Msi.Package	.MSI	System
Shortcut to MS-DOS Program	Executable		piffile	.PIF	System
Registration Entries	REGEDIT.EXE	Microsoft Corporation	regfile	.REG	System
Rich Text Document	WORDPAD.EXE	Microsoft Corporation	rtffile	.RTF	System
Screen saver	Executable		scrfile	.SCR	System
Text Document	NOTEPAD.EXE	Microsoft Corporation	txtfile	.LOG	System
Text Document	NOTEPAD.EXE	Microsoft Corporation	txtfile	.TXT	User D...
VBScript Encoded File	WSCRIPT.EXE	Microsoft Corporation	VBEFile	.VBE	System
VBScript Script File	WSCRIPT.EXE	Microsoft Corporation	VBSFile	.VBS	System
Windows host process (Rundll...	IEFRAME.DLL	Microsoft Corporation	Windows ...	.URL	User D...
Video Clip	WMPLAYER.EXE	Microsoft Corporation	WMP11.A...	.AVI	User D...
MIDI Sequence	WMPLAYER.EXE	Microsoft Corporation	WMP11.A...	.MID	System
MP3 Format Sound	WMPLAYER.EXE	Microsoft Corporation	WMP11.A...	.MP3	User D...
Windows Script File	WSCRIPT.EXE	Microsoft Corporation	WSFFile	.WSF	System
Windows Script Host Settings ...	WSCRIPT.EXE	Microsoft Corporation	WSHFile	.WSH	System

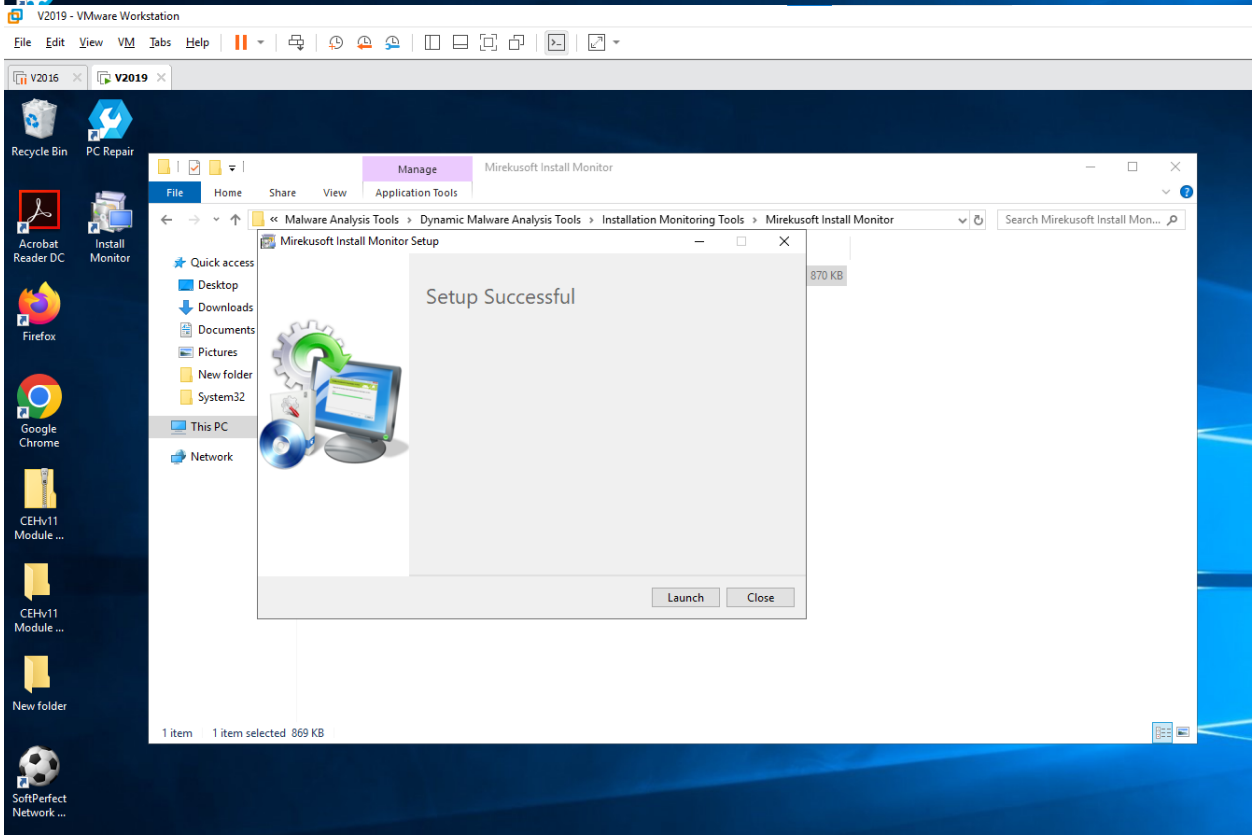
4.6 Perform Installation Monitoring using Mirekusoft Install Monitor

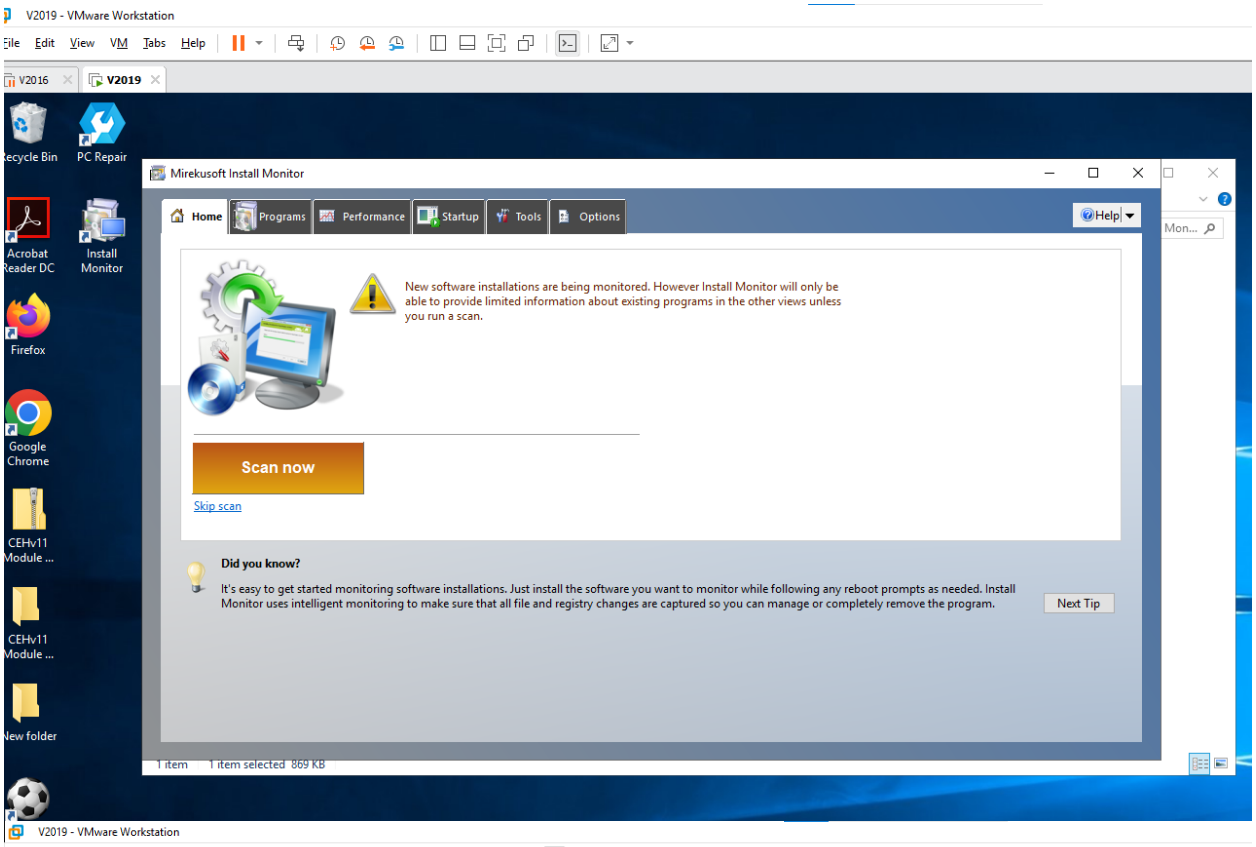
- Open Windows 10

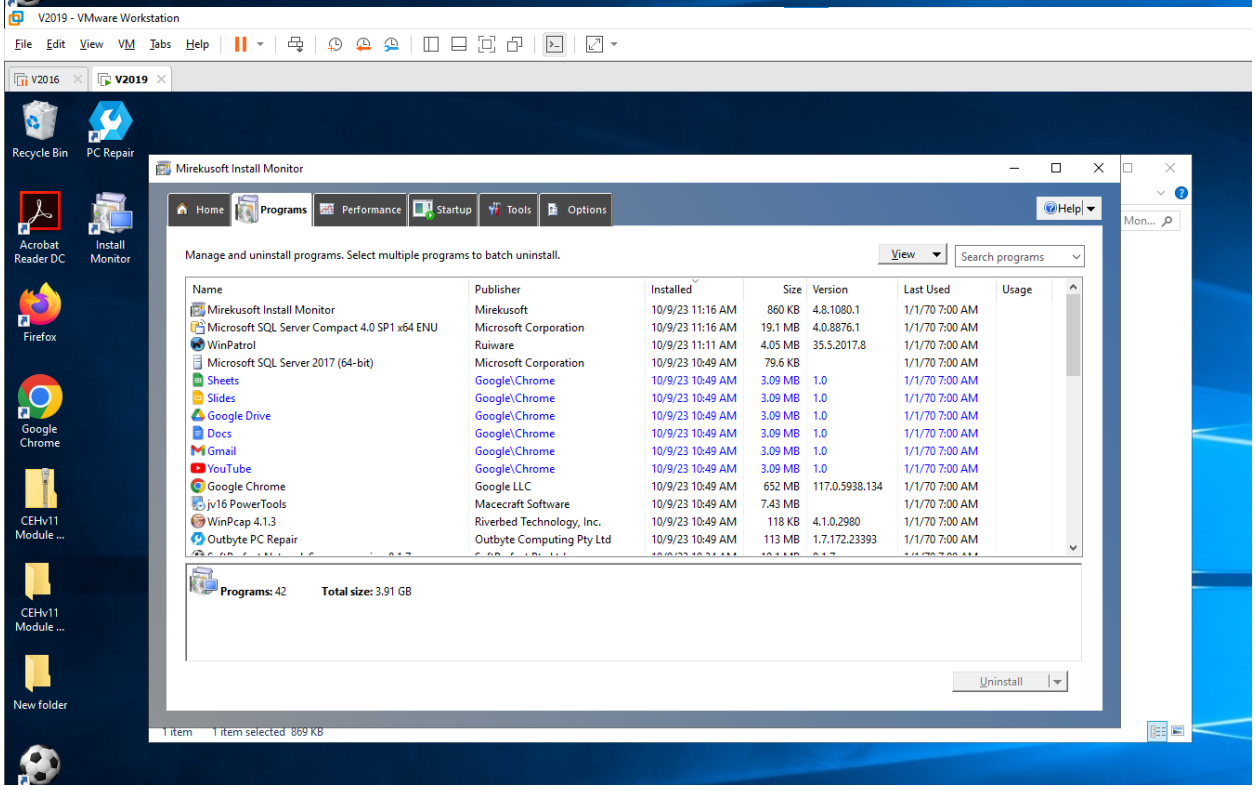


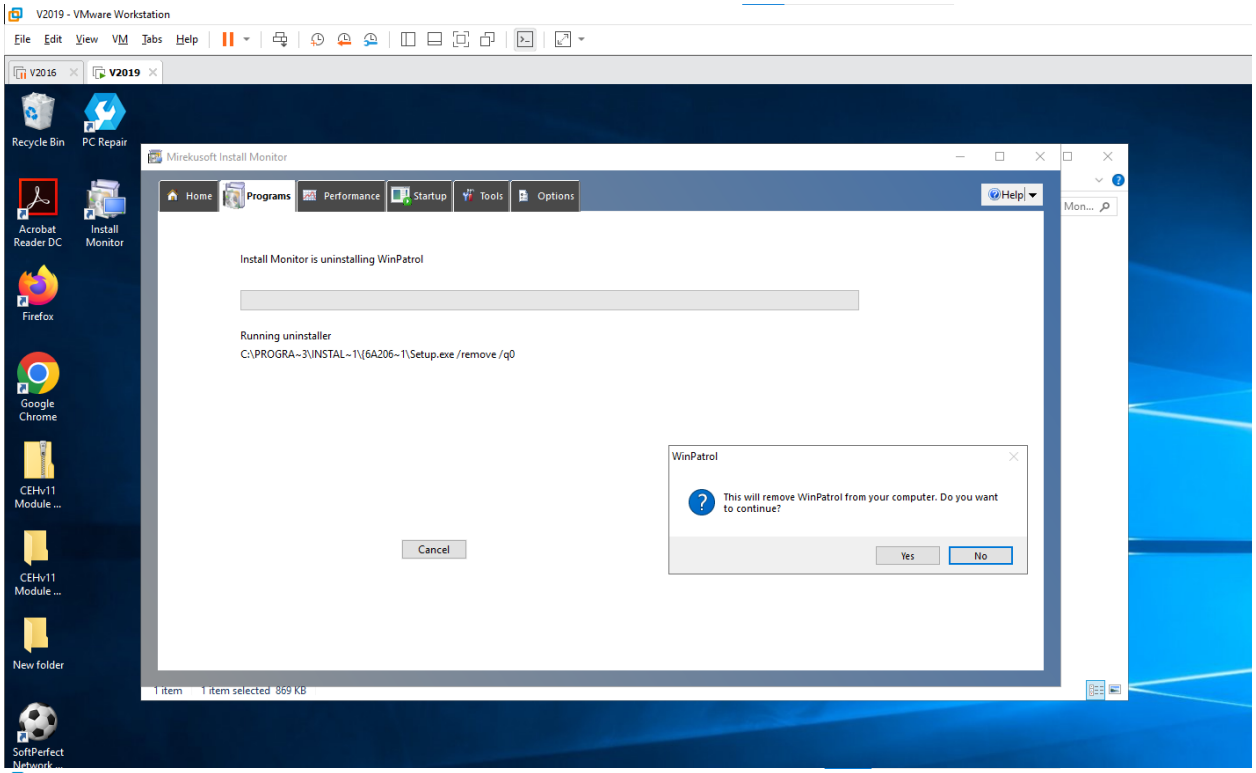

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
Manage
Mirekusoft Install Monitor
File Home Share View Application Tools
Mirekusoft Install Monitor Setup
Update Available
Version 4.8.1080.1 of Mirekusoft Install Monitor is available. Would you like to update now?
Update
Close
Monitoring Tools › Mirekusoft Install Mo
Type Size
Application 870 KB
1 item 1 item selected 869 KB

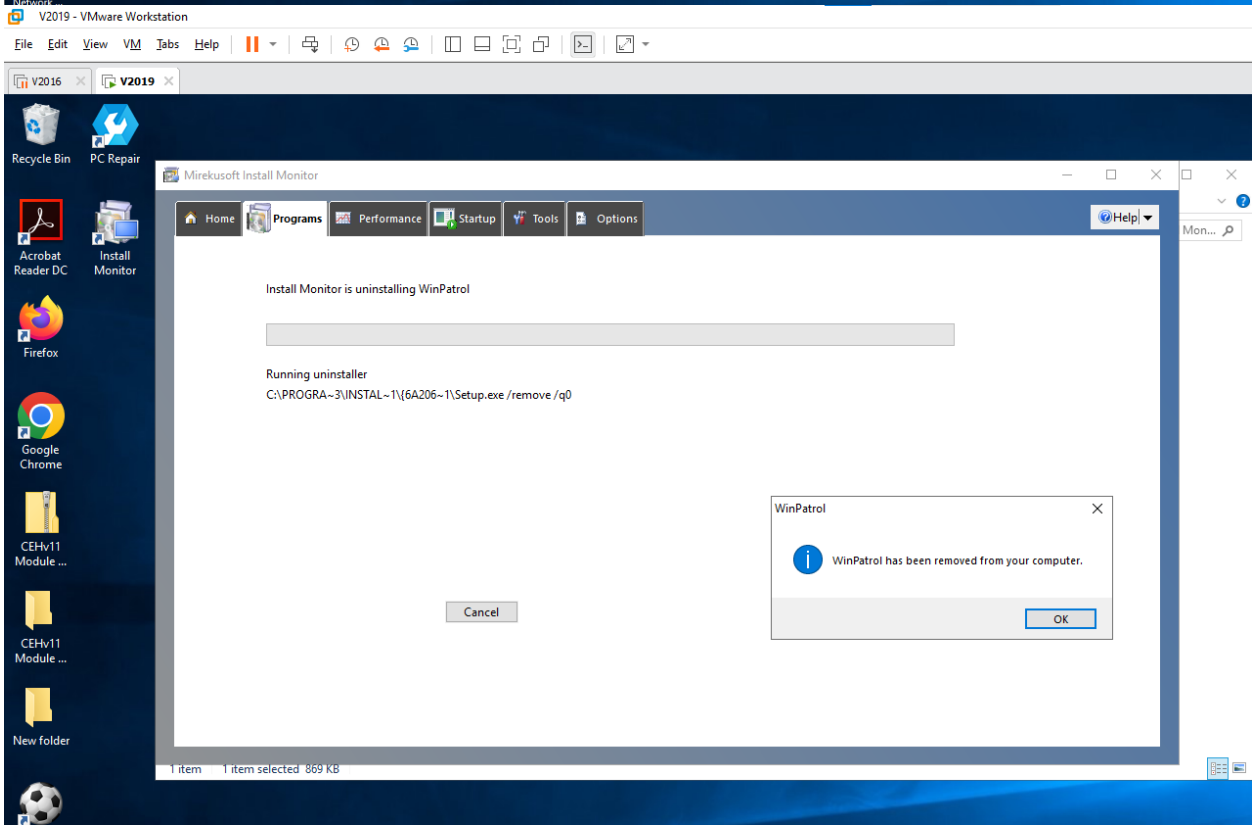

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
Manage
Mirekusoft Install Monitor
File Home Share View Application Tools
Mirekusoft Install Monitor Setup
Setup Progress
{079148d8-ccaf-4ccd-b24f-bb8a7b386462}
Monitoring Tools › Mirekusoft Install Monitor
Search Mirekusoft Install Mon...
Type
Size
Application
870 KB
Mirekusoft Install Monitor Setup
Mirekusoft Install Monitor will be installed
END-USER LICENSE AGREEMENT FOR MIREKUSOFT INSTALL MONITOR
IMPORTANT PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL: MIREKUSOFT INSTALL MONITOR. End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Mirekusoft for the Mirekusoft software product(s) identified above which may include associated software components, media, printed materials, and "online" or electronic documentation ("SOFTWARE
By installing you accept these license terms
Allow us to collect anonymous information that will help improve the quality of this program (recommended)
4.8.1080.1
Install
Close
1 item
1 item selected 869 KB

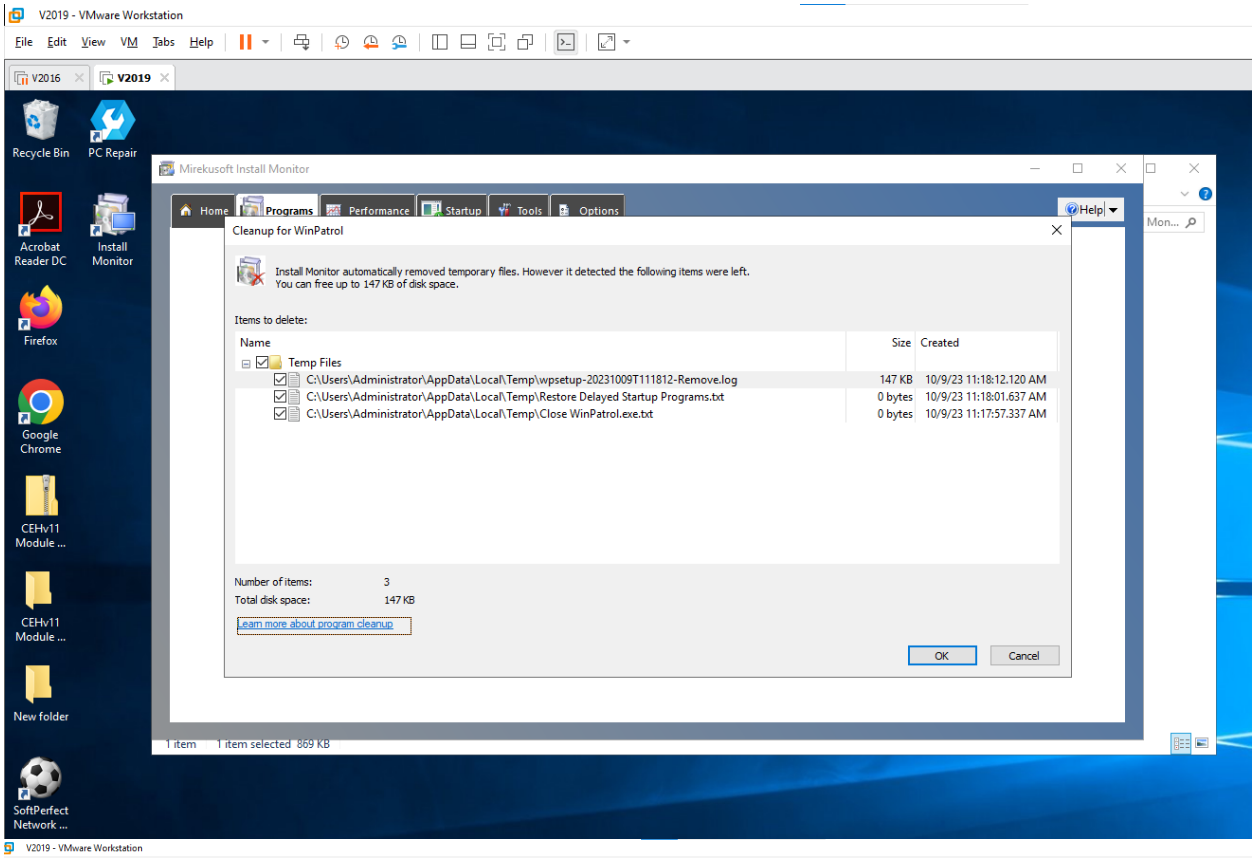

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
Manage
Mirekusoft Install Monitor
File Home Share View Application Tools
Malware Analysis Tools › Dynamic Malware Analysis Tools › Installation Monitoring Tools › Mirekusoft Install Monitor
Search Mirekusoft Install Mon...
Mirekusoft Install Monitor Setup
Quick access
Desktop
Downloads
Documents
Pictures
New folder
System32
This PC
Network
Setup Successful
870 KB
Launch
Close
1 item
1 item selected 869 KB

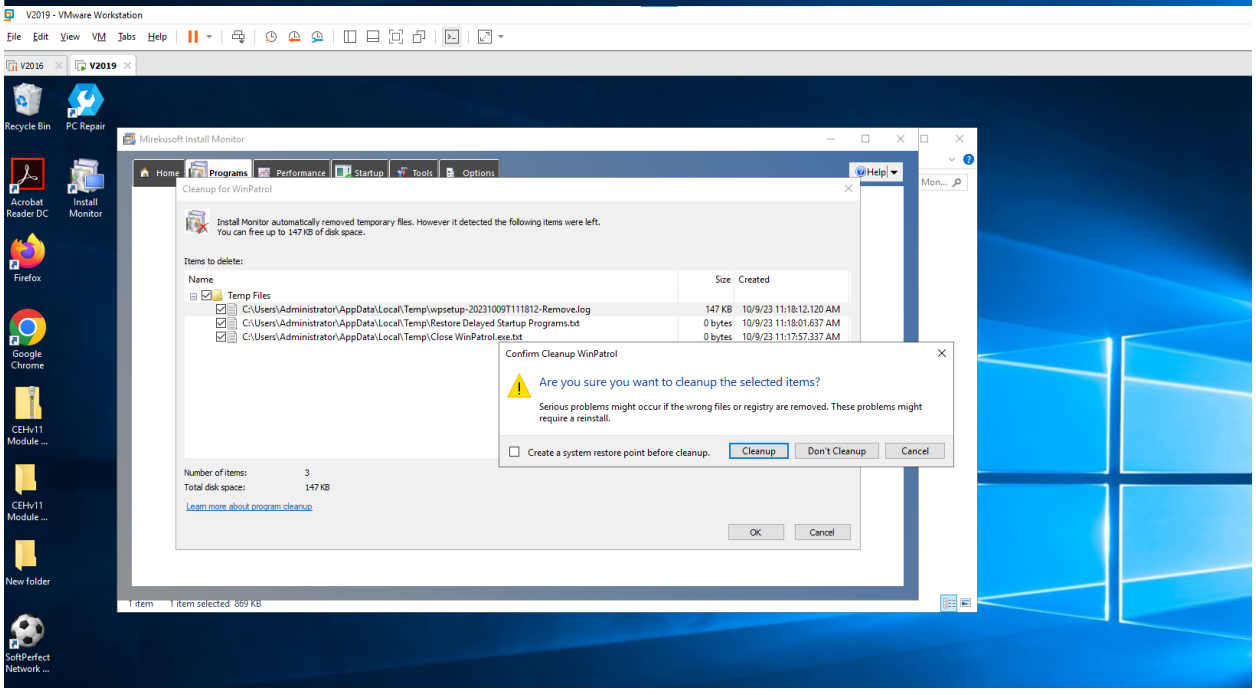

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
Mirekusoft Install Monitor
Home
Programs
Performance
Startup
Tools
Options
Help
New software installations are being monitored. However Install Monitor will only be able to provide limited information about existing programs in the other views unless you run a scan.
Scan now
Skip scan
Did you know?
It's easy to get started monitoring software installations. Just install the software you want to monitor while following any reboot prompts as needed. Install Monitor uses intelligent monitoring to make sure that all file and registry changes are captured so you can manage or completely remove the program.
Next Tip
1 item
1 item selected 869 KB

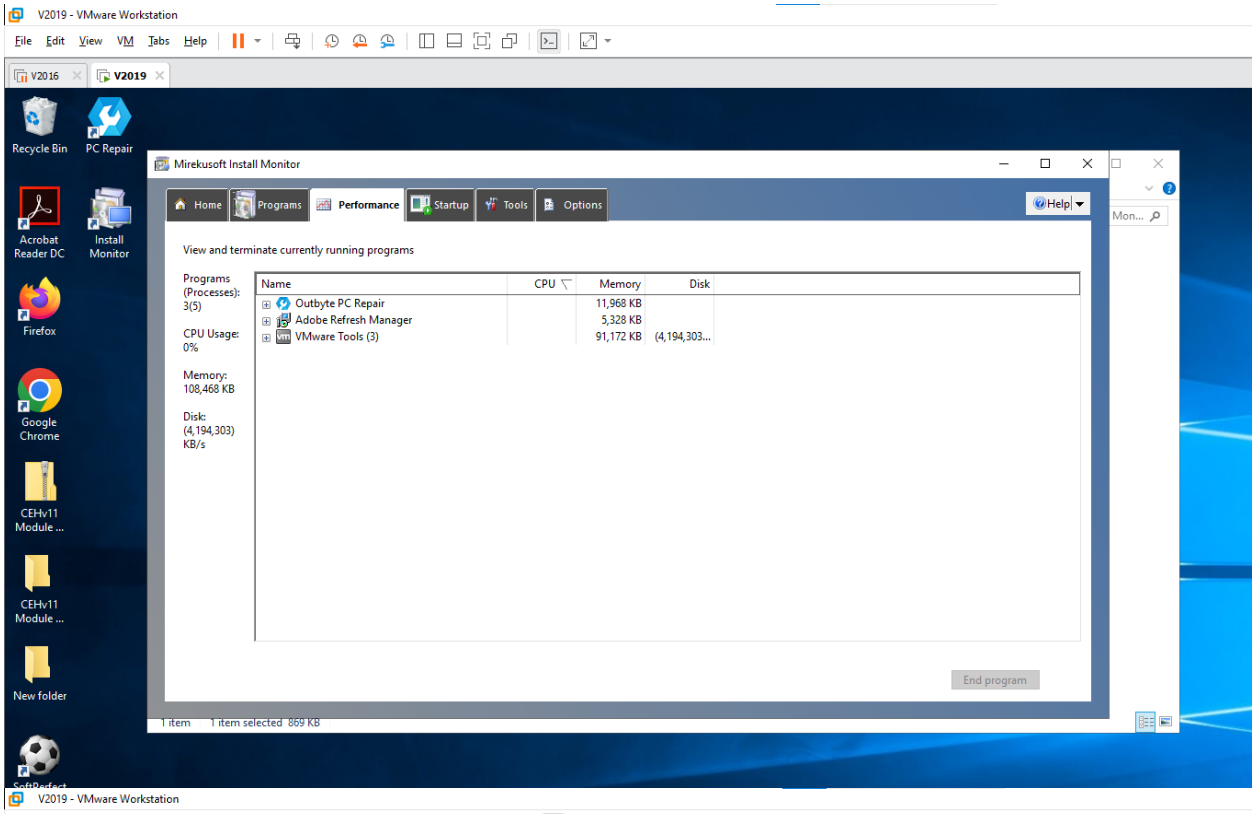

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
Mirekusoft Install Monitor
Home
Programs
Performance
Startup
Tools
Options
Help
Manage and uninstall programs. Select multiple programs to batch uninstall.
View
Search programs
Name
Publisher
Installed
Size
Version
Last Used
Usage
Mirekusoft Install Monitor Mirekusoft 10/9/23 11:16 AM 860 KB 4.8.1080.1 1/1/70 7:00 AM
Microsoft SQL Server Compact 4.0 SP1 x64 ENU Microsoft Corporation 10/9/23 11:16 AM 19.1 MB 4.0.8876.1 1/1/70 7:00 AM
WinPatrol Ruiware 10/9/23 11:11 AM 4.05 MB 35.5.2017.8 1/1/70 7:00 AM
Microsoft SQL Server 2017 (64-bit) Microsoft Corporation 10/9/23 10:49 AM 79.6 KB 1/1/70 7:00 AM
Sheets Google\Chrome 10/9/23 10:49 AM 3.09 MB 1.0 1/1/70 7:00 AM
Slides Google\Chrome 10/9/23 10:49 AM 3.09 MB 1.0 1/1/70 7:00 AM
Google Drive Google\Chrome 10/9/23 10:49 AM 3.09 MB 1.0 1/1/70 7:00 AM
Docs Google\Chrome 10/9/23 10:49 AM 3.09 MB 1.0 1/1/70 7:00 AM
Gmail Google\Chrome 10/9/23 10:49 AM 3.09 MB 1.0 1/1/70 7:00 AM
YouTube Google\Chrome 10/9/23 10:49 AM 3.09 MB 1.0 1/1/70 7:00 AM
Google Chrome Google LLC 10/9/23 10:49 AM 652 MB 117.0.5938.134 1/1/70 7:00 AM
jv16 PowerTools Macecraft Software 10/9/23 10:49 AM 7.43 MB 1/1/70 7:00 AM
WinPcap 4.1.3 Riverbed Technology, Inc. 10/9/23 10:49 AM 118 KB 4.1.0.2980 1/1/70 7:00 AM
Outbyte PC Repair Outbyte Computing Pty Ltd 10/9/23 10:49 AM 113 MB 1.7.172.23393 1/1/70 7:00 AM
Programs: 42
Total size: 3.91 GB
Uninstall
1 item
1 item selected 869 KB

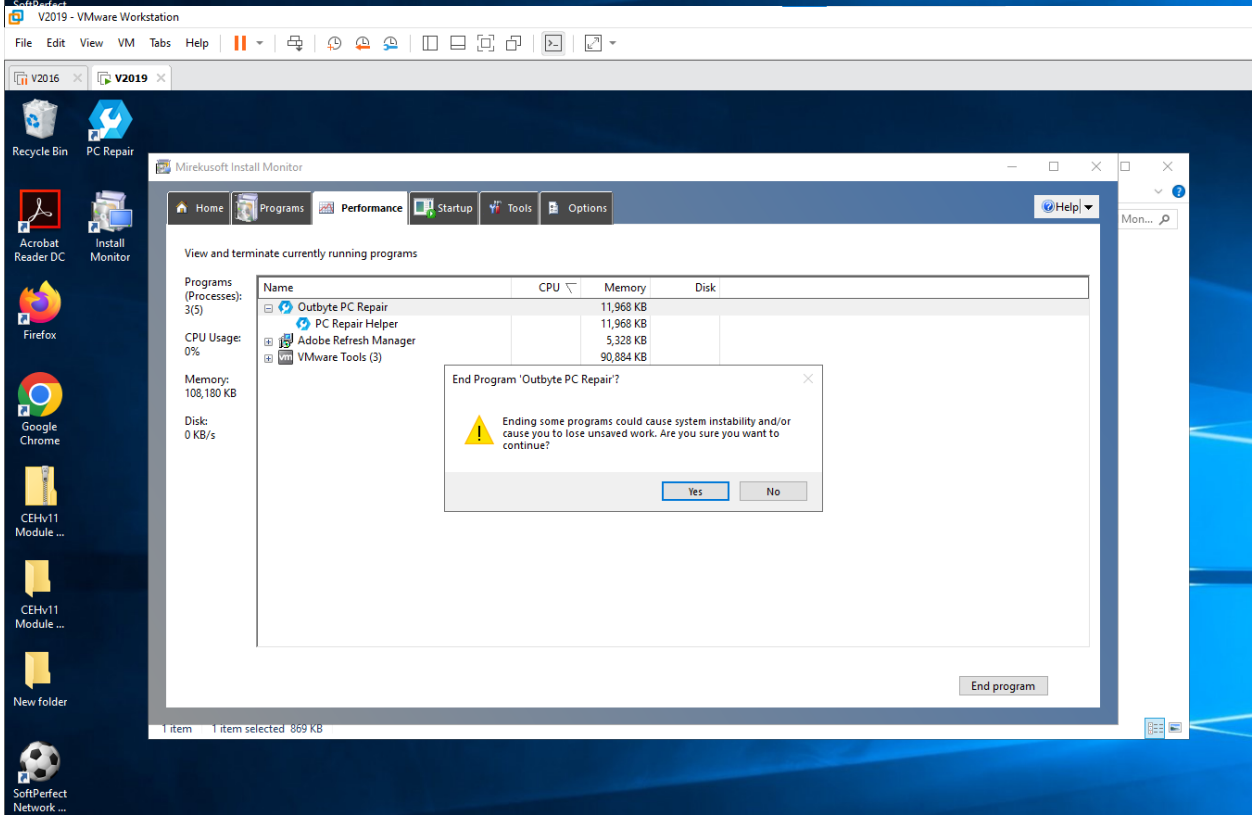

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network
Mirekusoft Install Monitor
Home
Programs
Performance
Startup
Tools
Options
Help
Install Monitor is uninstalling WinPatrol
Running uninstaller
C:\PROGRA~3\INSTAL~1\{6A206~1\Setup.exe /remove /q0
Cancel
WinPatrol
This will remove WinPatrol from your computer. Do you want to continue?
Yes
No
1 item
1 item selected 869 KB


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
Mirekusoft Install Monitor
Home
Programs
Performance
Startup
Tools
Options
Help
Install Monitor is uninstalling WinPatrol
Running uninstaller
C:\PROGRA~3\INSTAL~1\{6A206~1\Setup.exe /remove /q0
Cancel
WinPatrol
WinPatrol has been removed from your computer.
OK
1 item
1 item selected 869 KB


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
Mirekusoft Install Monitor
Home
Programs
Performance
Startup
Tools
Options
Help
Cleanup for WinPatrol
Install Monitor automatically removed temporary files. However it detected the following items were left.
You can free up to 147 KB of disk space.
Items to delete:
Name
Size
Created
Temp Files
C:\Users\Administrator\AppData\Local\Temp\wpsetup-20231009T111812-Remove.log
147 KB
10/9/23 11:18:12.120 AM
C:\Users\Administrator\AppData\Local\Temp\Restore Delayed Startup Programs.txt
0 bytes
10/9/23 11:18:01.637 AM
C:\Users\Administrator\AppData\Local\Temp\Close WinPatrol.exe.txt
0 bytes
10/9/23 11:17:57.337 AM
Number of items: 3
Total disk space: 147 KB
Learn more about program cleanup
OK
Cancel
1 item
1 item selected 869 KB

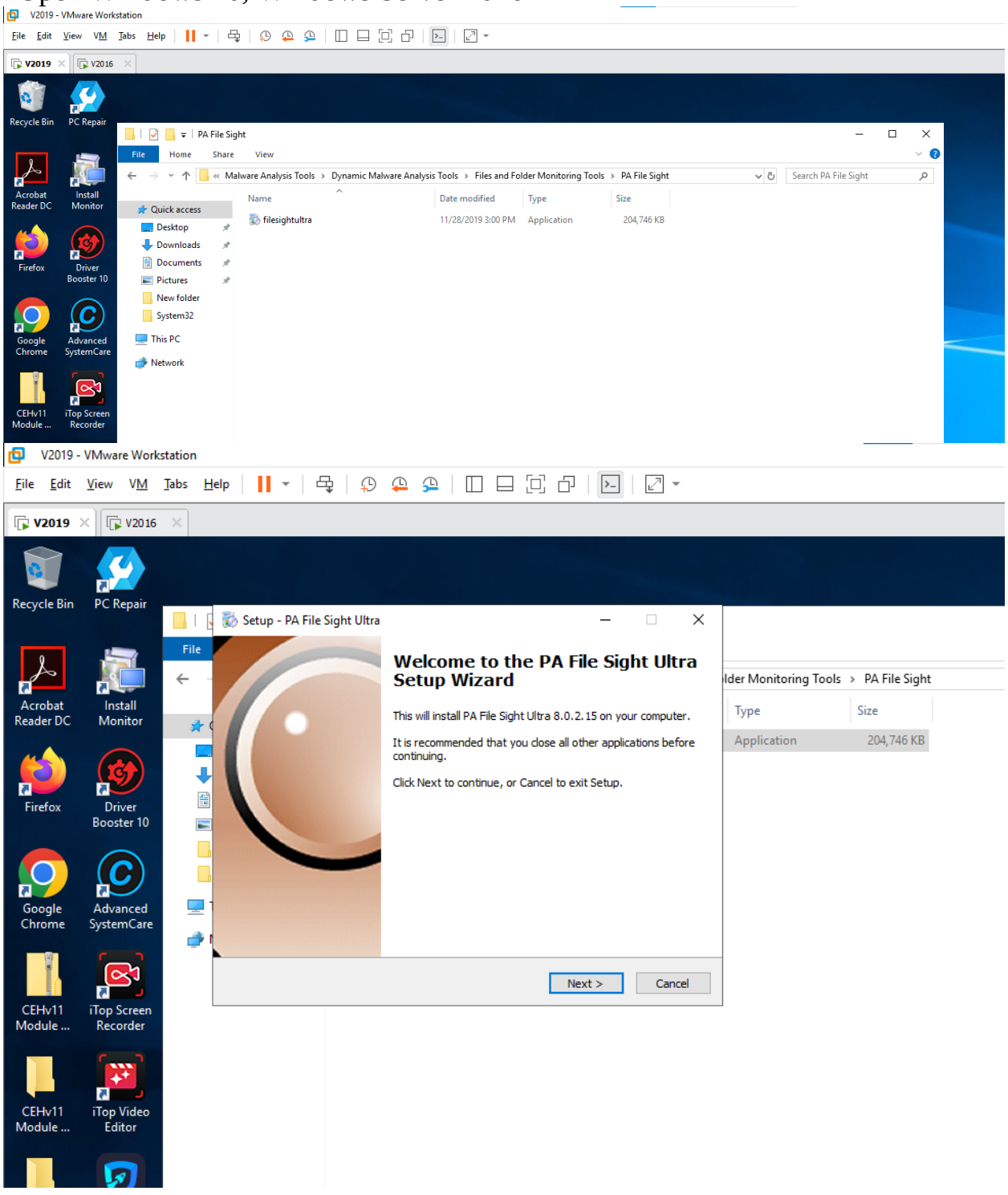

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
Mirekusoft Install Monitor
Home
Programs
Performance
Startup
Tools
Options
Help
Cleanup for WinPatrol
Install Monitor automatically removed temporary files. However it detected the following items were left.
You can free up to 147 KB of disk space.
Items to delete:
Name
Size
Created
Temp Files
C:\Users\Administrator\AppData\Local\Temp\wpsetup-20231009T111812-Remove.log
147 KB
10/9/23 11:18:12.120 AM
C:\Users\Administrator\AppData\Local\Temp\Restore Delayed Startup Programs.txt
0 bytes
10/9/23 11:18:01.637 AM
C:\Users\Administrator\AppData\Local\Temp\Close WinPatrol.exe.txt
0 bytes
10/9/23 11:17:57.337 AM
Confirm Cleanup WinPatrol
Are you sure you want to cleanup the selected items?
Serious problems might occur if the wrong files or registry are removed. These problems might require a reinstall.
Create a system restore point before cleanup.
Cleanup
Don't Cleanup
Cancel
Number of items: 3
Total disk space: 147 KB
Learn more about program cleanup
OK
Cancel
1 item
1 item selected 869 KB

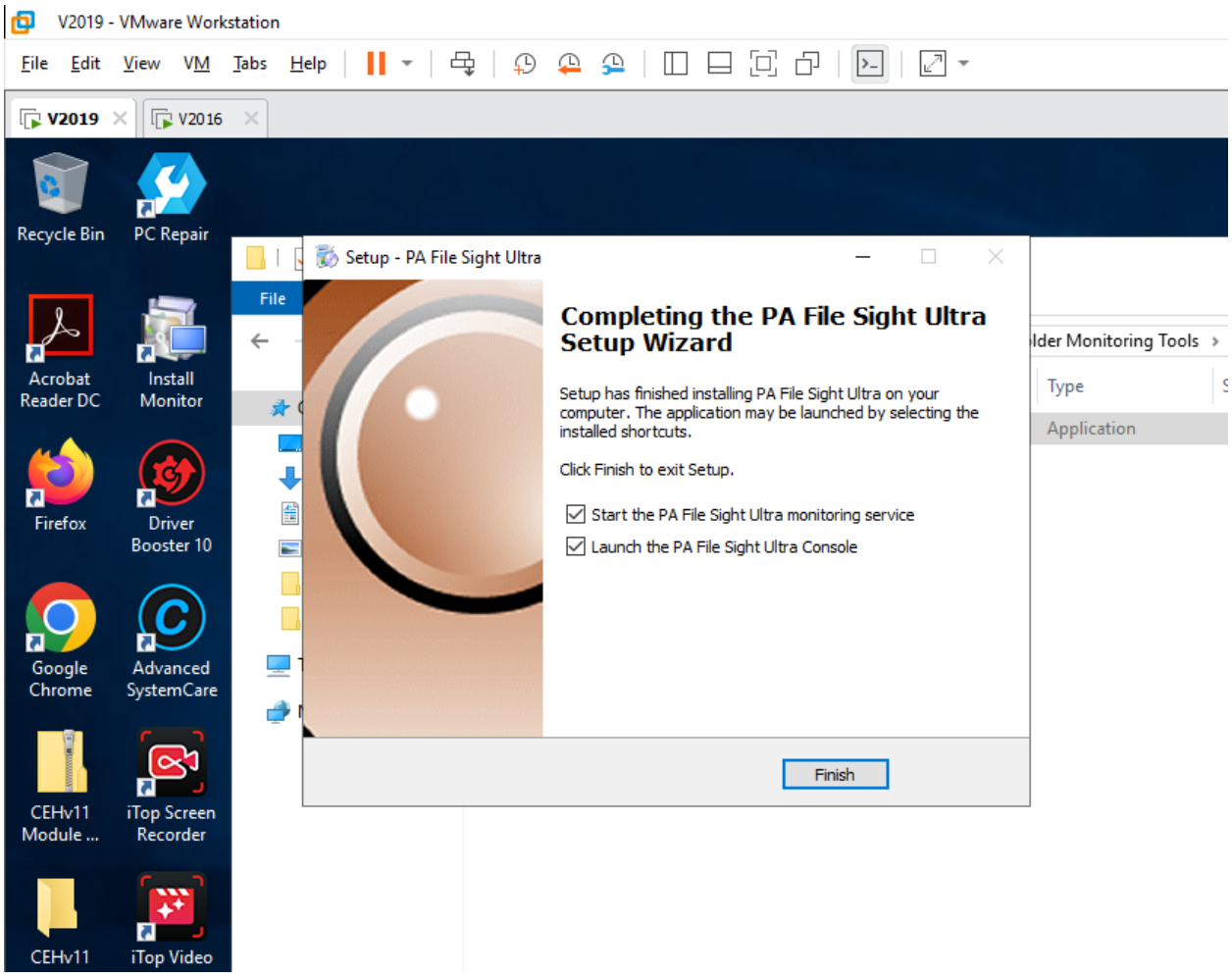


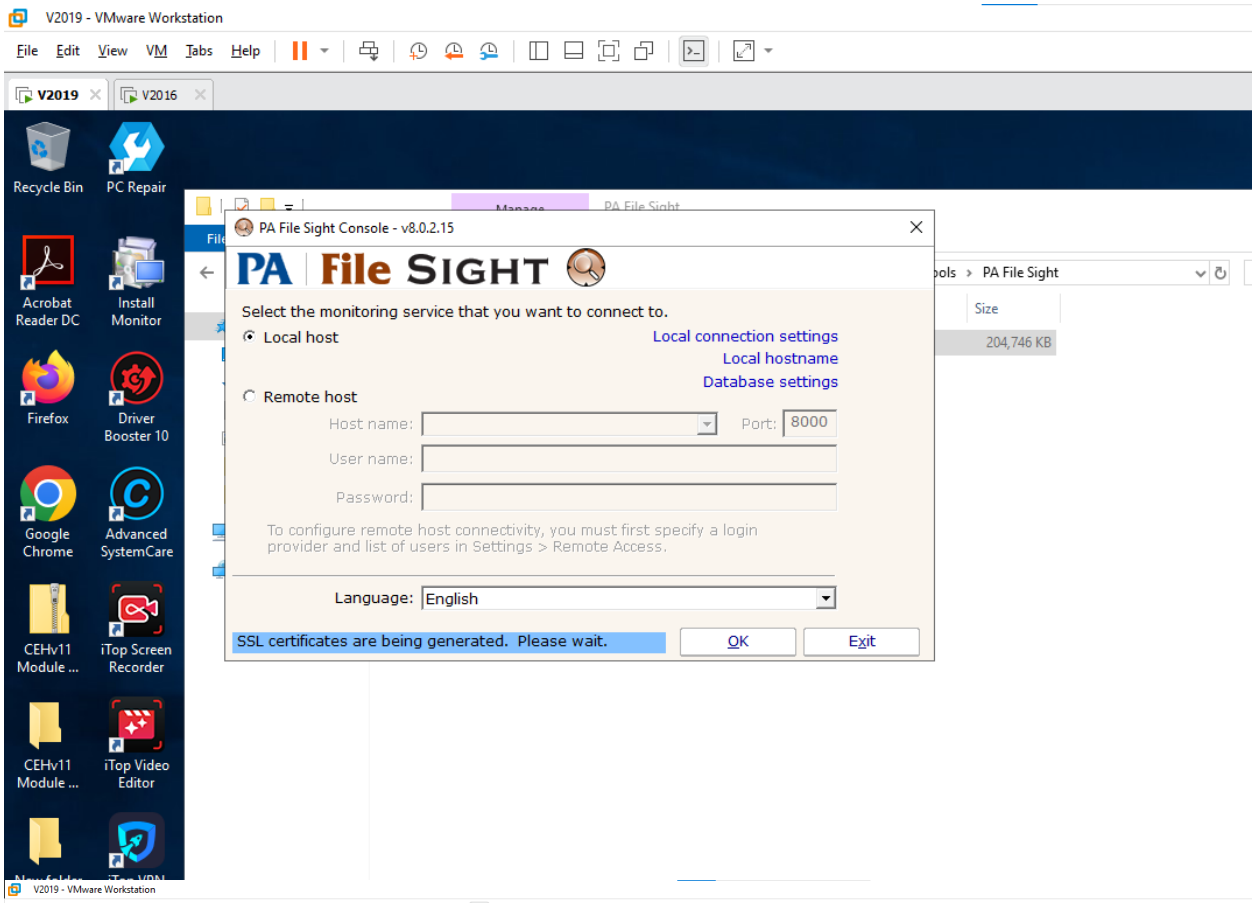


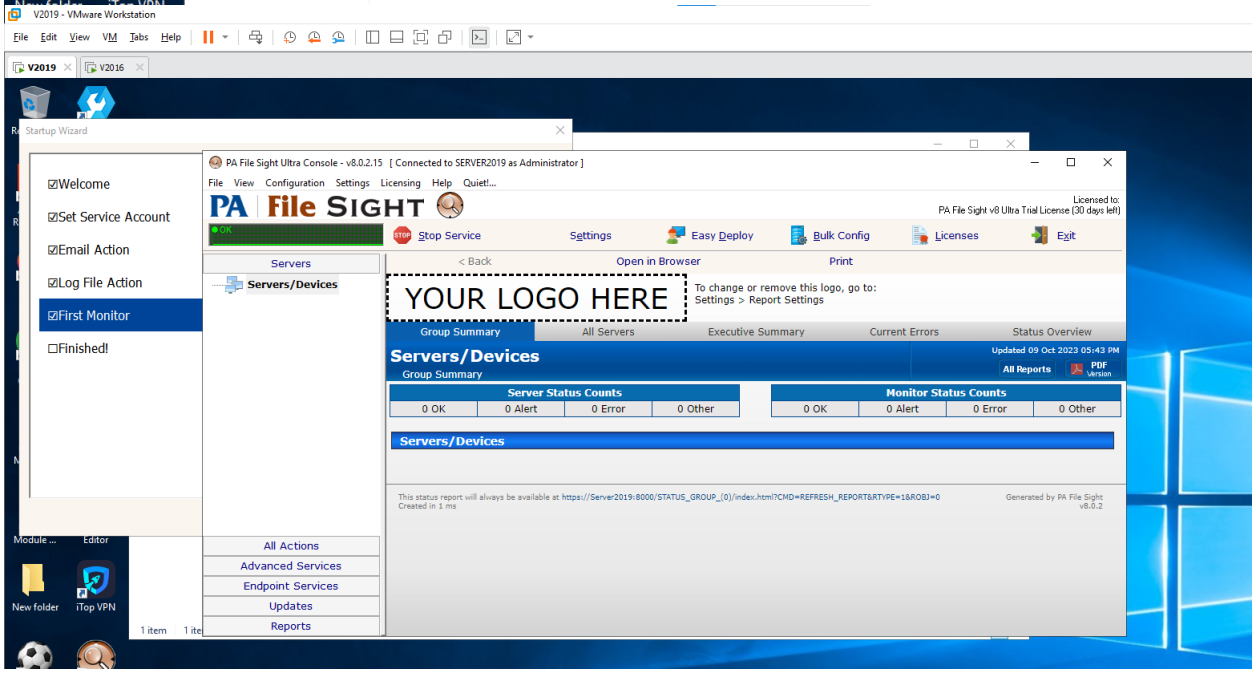
4.7 Perform Files and Folder Monitoring using PA File Sight

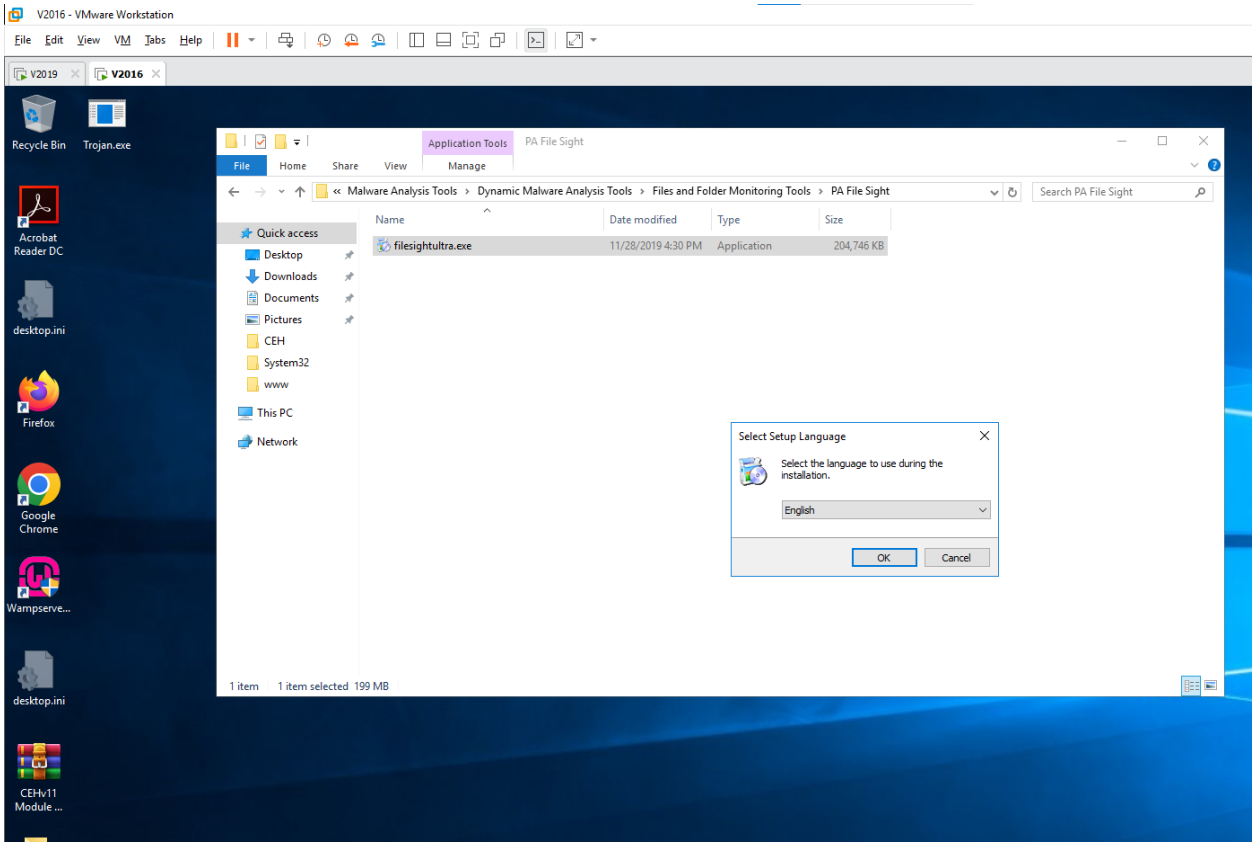
- Open Windows 10, Windows Server 2016

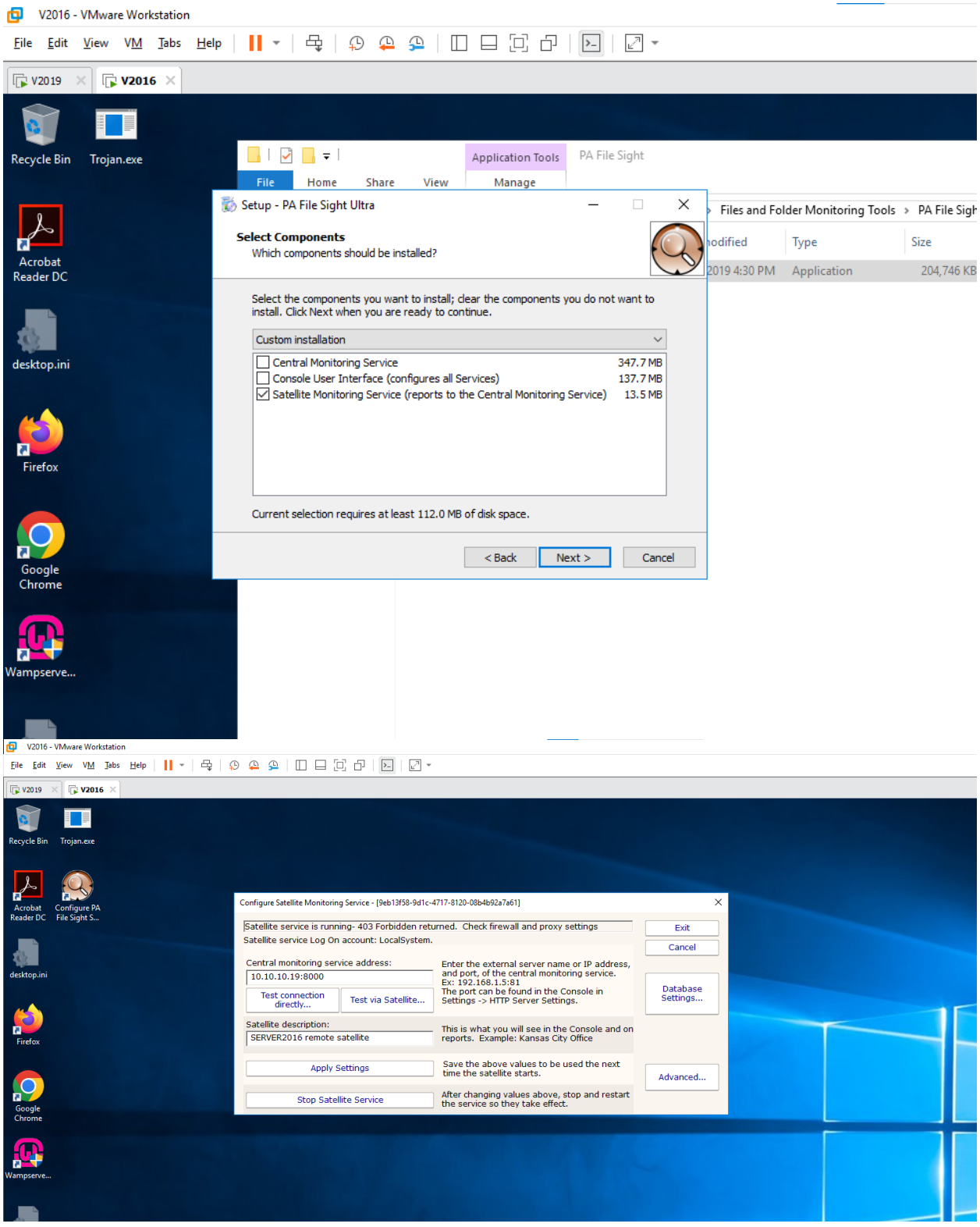


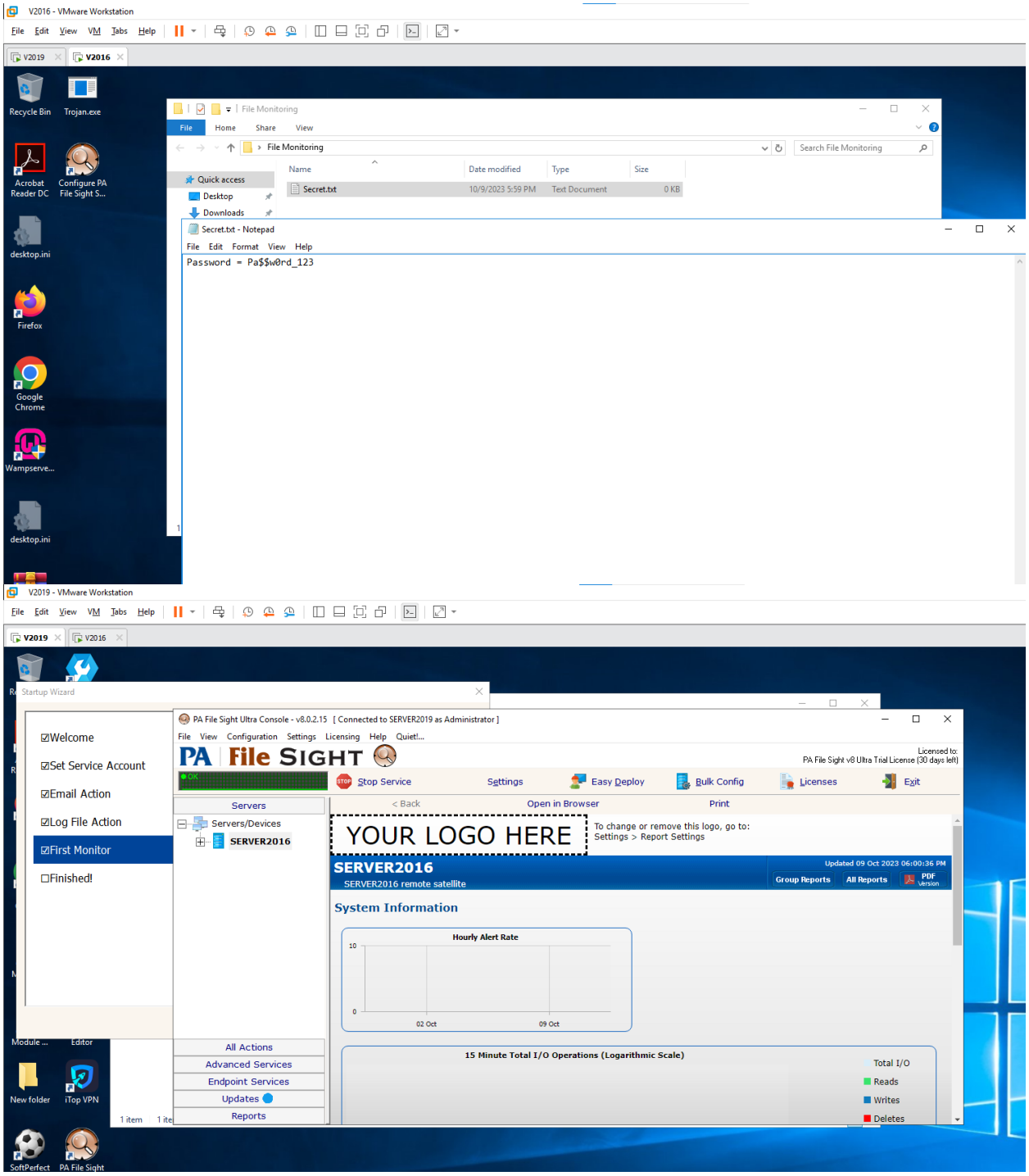

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
Advanced SystemCare
CEHv11 Module ...
iTop Screen Recorder
CEHv11
iTop Video
Setup - PA File Sight Ultra
Completing the PA File Sight Ultra Setup Wizard
Setup has finished installing PA File Sight Ultra on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Start the PA File Sight Ultra monitoring service
Launch the PA File Sight Ultra Console
Finish
File
Type
Application

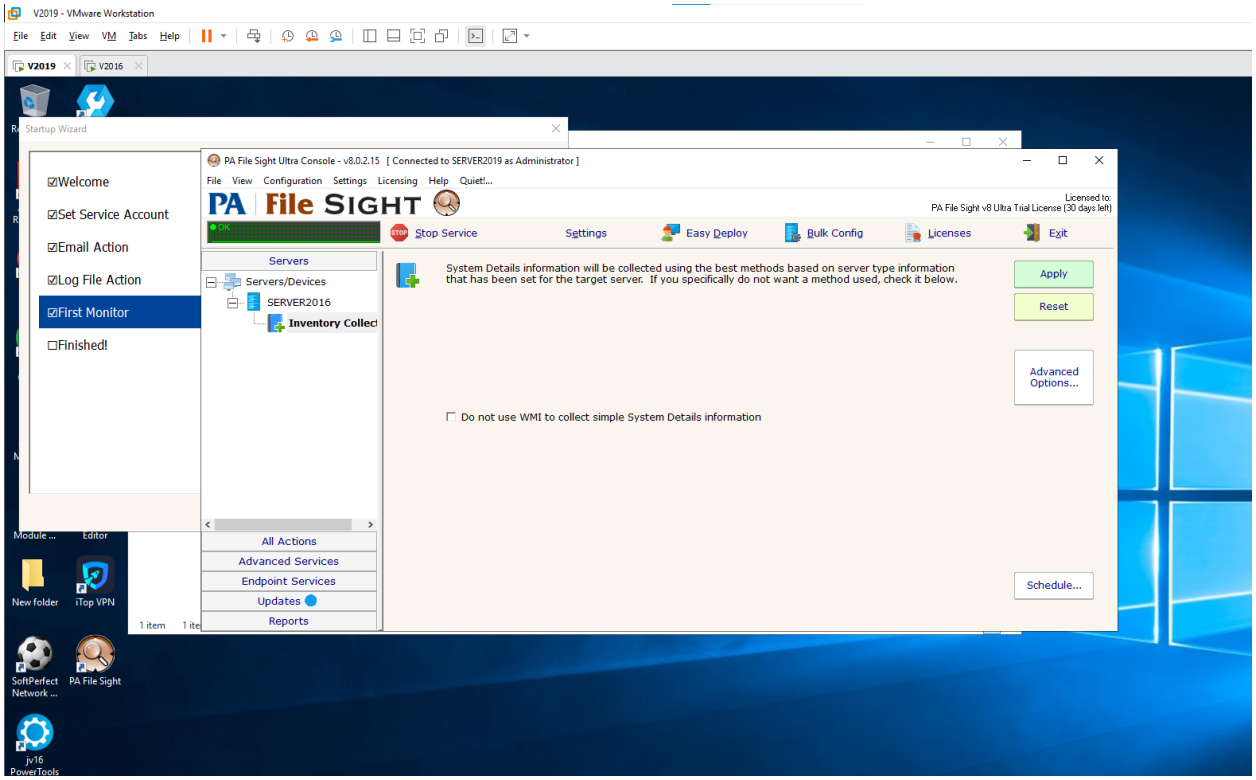

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
Advanced SystemCare
CEHv11 Module ...
iTop Screen Recorder
CEHv11 Module ...
iTop Video Editor
PA File Sight Console - v8.0.2.15
PA File SIGHT
Select the monitoring service that you want to connect to.
Local host
Local connection settings
Local hostname
Database settings
Remote host
Host name:
Port: 8000
User name:
Password:
To configure remote host connectivity, you must first specify a login provider and list of users in Settings > Remote Access.
Language: English
SSL certificates are being generated. Please wait.
OK
Exit
PA File Sight
Size
204,746 KB

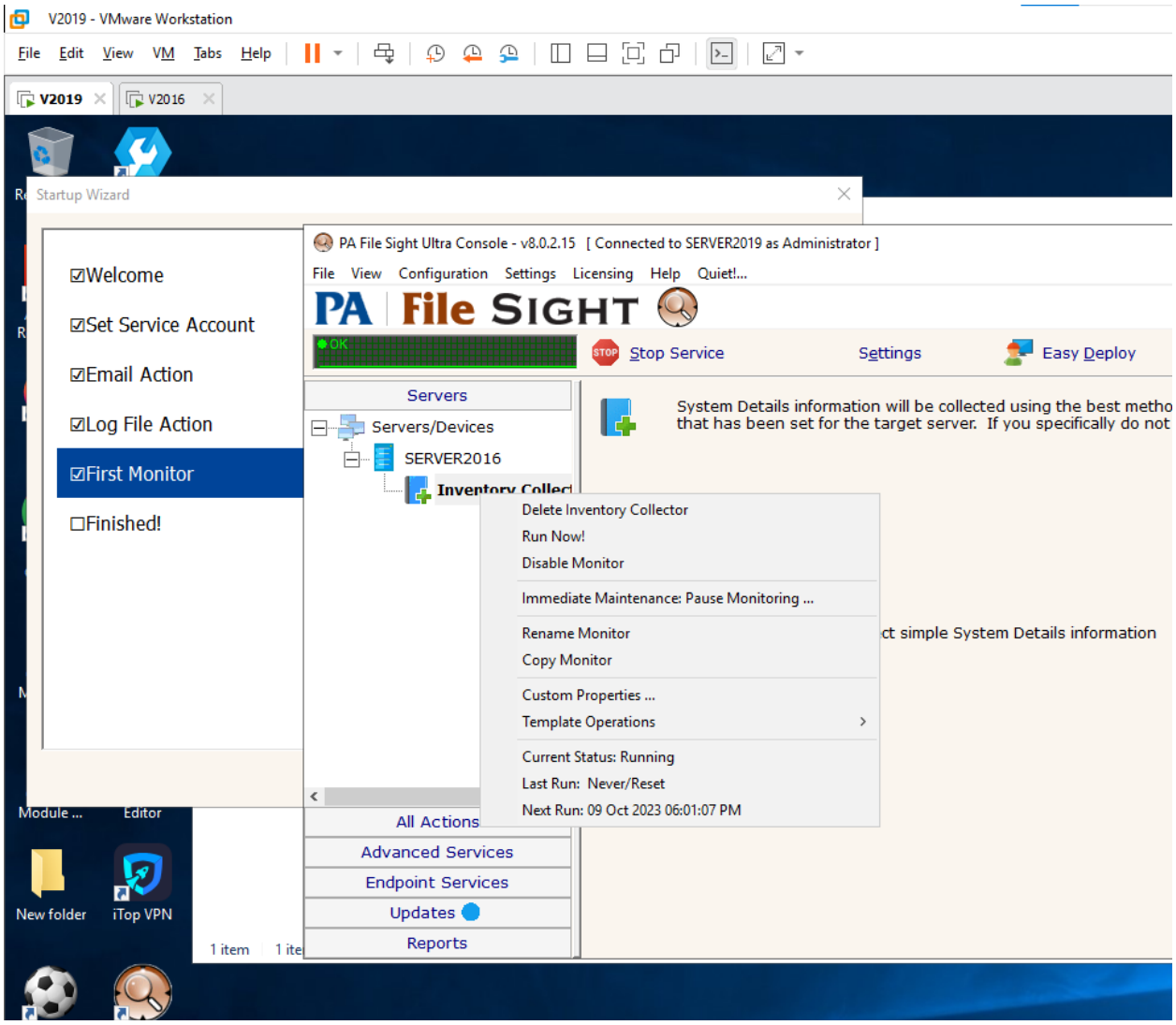

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Startup Wizard
☑Welcome
☑Set Service Account
☑Email Action
☑Log File Action
☑First Monitor
☐Finished!
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
Licensed to:
PA File Sight v8 Ultra Trial License (30 days left)
Stop Service
Settings
Easy Deploy
Bulk Config
Licenses
Exit
Servers
Servers/Devices
< Back
Open in Browser
Print
YOUR LOGO HERE
To change or remove this logo, go to:
Settings > Report Settings
Group Summary
All Servers
Executive Summary
Current Errors
Status Overview
Servers/Devices
Group Summary
Updated 09 Oct 2023 05:43 PM
All Reports
PDF Version
Server Status Counts
0 OK
0 Alert
0 Error
0 Other
Monitor Status Counts
0 OK
0 Alert
0 Error
0 Other
Servers/Devices
All Actions
Advanced Services
Endpoint Services
Updates
Reports
New folder
iTop VPN

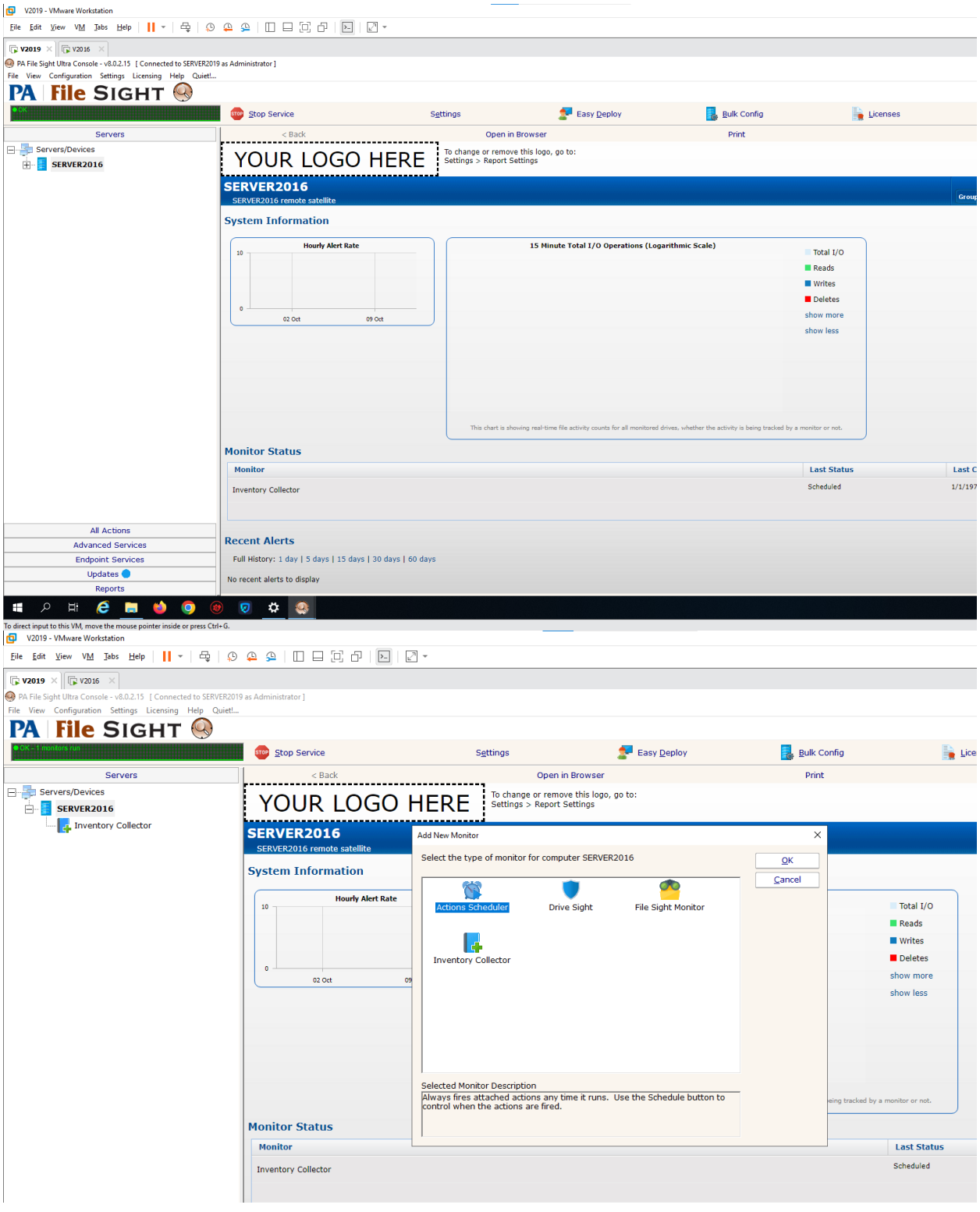

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Recycle Bin
Trojan.exe
Acrobat Reader DC
desktop.ini
Firefox
Google Chrome
Wampserve...
desktop.ini
CEHv11 Module ...
Application Tools
PA File Sight
File Home Share View Manage
Malware Analysis Tools › Dynamic Malware Analysis Tools › Files and Folder Monitoring Tools › PA File Sight
Search PA File Sight
Quick access
Desktop
Downloads
Documents
Pictures
CEH
System32
www
This PC
Network
Name
Date modified
Type
Size
filesightultra.exe
11/28/2019 4:30 PM
Application
204,746 KB
Select Setup Language
Select the language to use during the installation.
English
OK
Cancel
1 item
1 item selected 199 MB

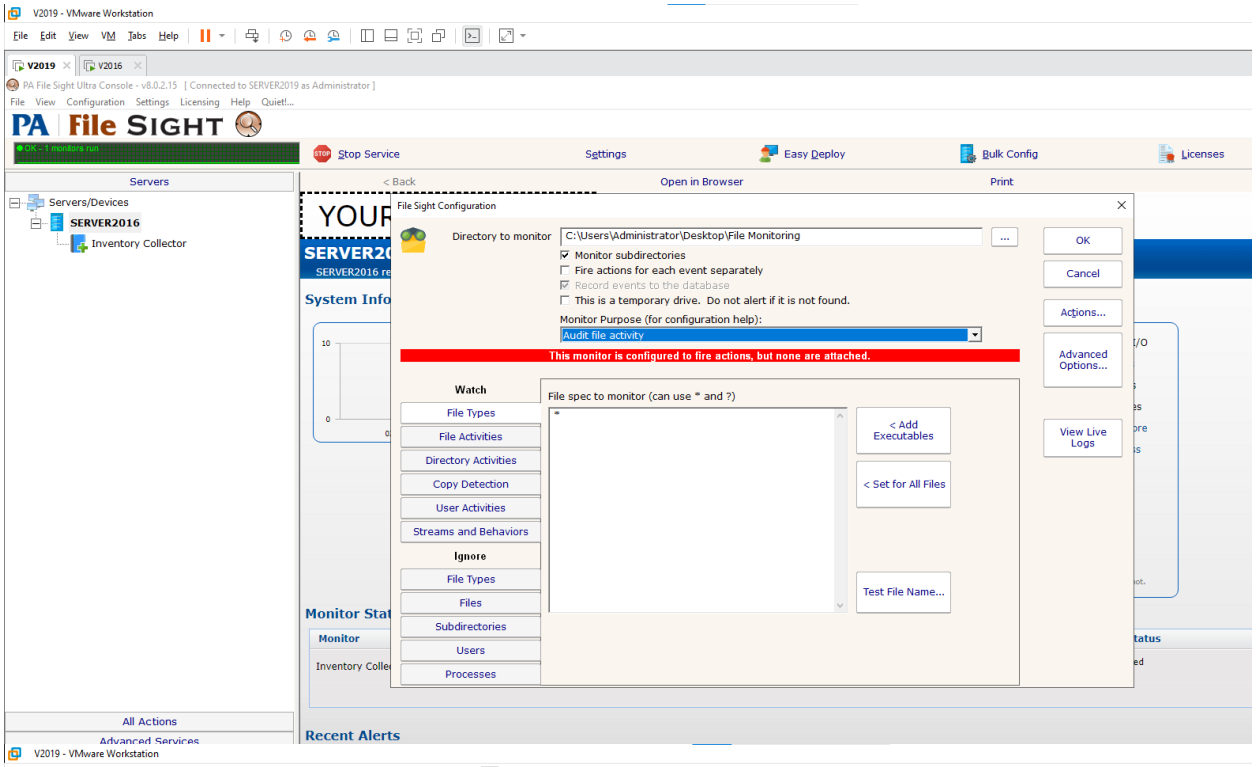

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Recycle Bin
Trojan.exe
Acrobat Reader DC
desktop.ini
Firefox
Google Chrome
Wampserve...
Application Tools
PA File Sight
File Home Share View Manage
Setup - PA File Sight Ultra
Select Components
Which components should be installed?
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.
Custom installation
Central Monitoring Service 347.7 MB
Console User Interface (configures all Services) 137.7 MB
Satellite Monitoring Service (reports to the Central Monitoring Service) 13.5 MB
Current selection requires at least 112.0 MB of disk space.
< Back
Next >
Cancel
Files and Folder Monitoring Tools
PA File Sigh
Type
Size
Application
204,746 KB
Configure PA File Sight S...
Configure Satellite Monitoring Service - [9eb13f58-9d1c-4717-8120-08b4b92a7a61]
Satellite service is running- 403 Forbidden returned. Check firewall and proxy settings
Satellite service Log On account: LocalSystem.
Exit
Cancel
Central monitoring service address:
10.10.10.19:8000
Enter the external server name or IP address, and port, of the central monitoring service.
Ex: 192.168.1.5:81
The port can be found in the Console in Settings -> HTTP Server Settings.
Test connection directly...
Test via Satellite...
Database Settings...
Satellite description:
SERVER2016 remote satellite
This is what you will see in the Console and on reports. Example: Kansas City Office
Apply Settings
Save the above values to be used the next time the satellite starts.
Advanced...
Stop Satellite Service
After changing values above, stop and restart the service so they take effect.

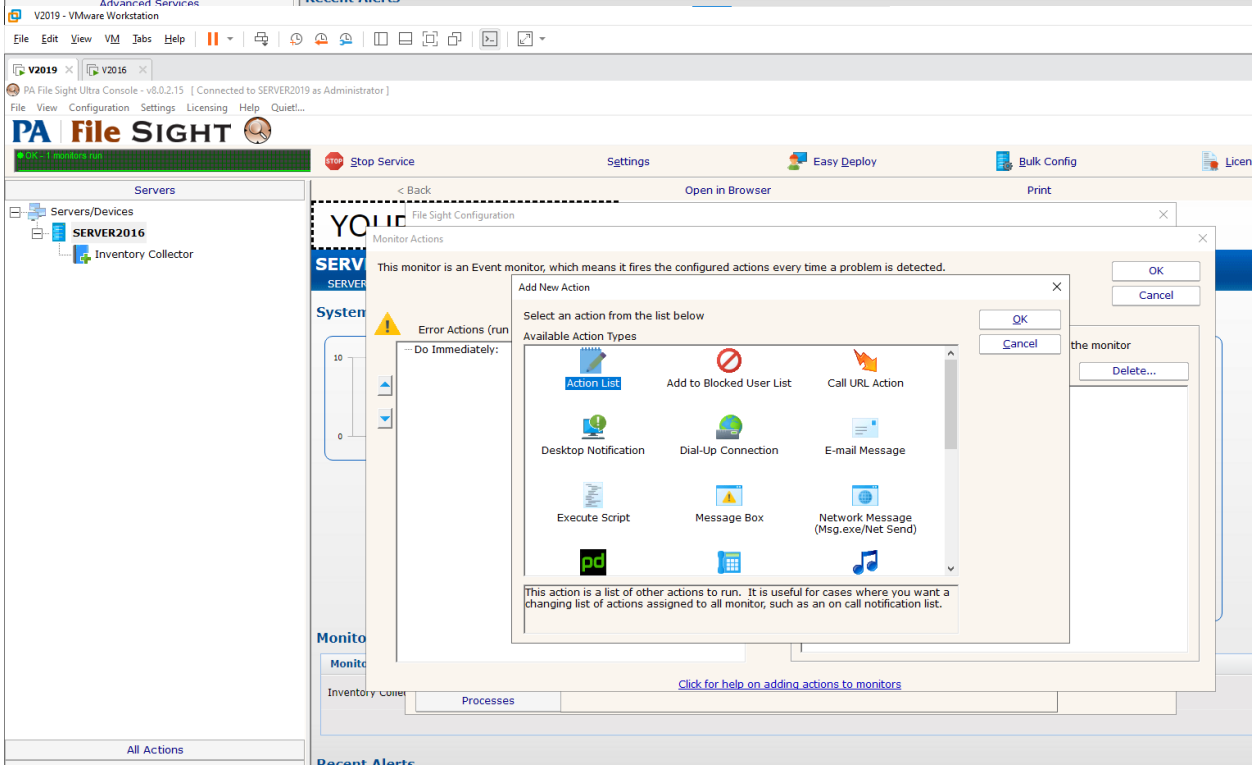

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Recycle Bin
Trojan.exe
Acrobat Reader DC
Configure PA File Sight S...
desktop.ini
Firefox
Google Chrome
Wampserve...
desktop.ini
File Monitoring
File Home Share View
File Monitoring
Search File Monitoring
Quick access
Desktop
Downloads
Name
Date modified
Type
Size
Secret.txt
10/9/2023 5:59 PM
Text Document
0 KB
Secret.txt - Notepad
File Edit Format View Help
Password = Pa$$w0rd_123
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Startup Wizard
Welcome
Set Service Account
Email Action
Log File Action
First Monitor
Finished!
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
Licensed to:
PA File Sight v8 Ultra Trial License (30 days left)
Stop Service
Settings
Easy Deploy
Bulk Config
Licenses
Exit
Servers
Servers/Devices
SERVER2016
< Back
Open in Browser
Print
YOUR LOGO HERE
To change or remove this logo, go to:
Settings > Report Settings
SERVER2016
SERVER2016 remote satellite
Updated 09 Oct 2023 06:00:36 PM
Group Reports
All Reports
PDF Version
System Information
Hourly Alert Rate
10
0
02 Oct
09 Oct
15 Minute Total I/O Operations (Logarithmic Scale)
Total I/O
Reads
Writes
Deletes
All Actions
Advanced Services
Endpoint Services
Updates
Reports
New folder
iTop VPN
SoftPerfect
PA File Sight

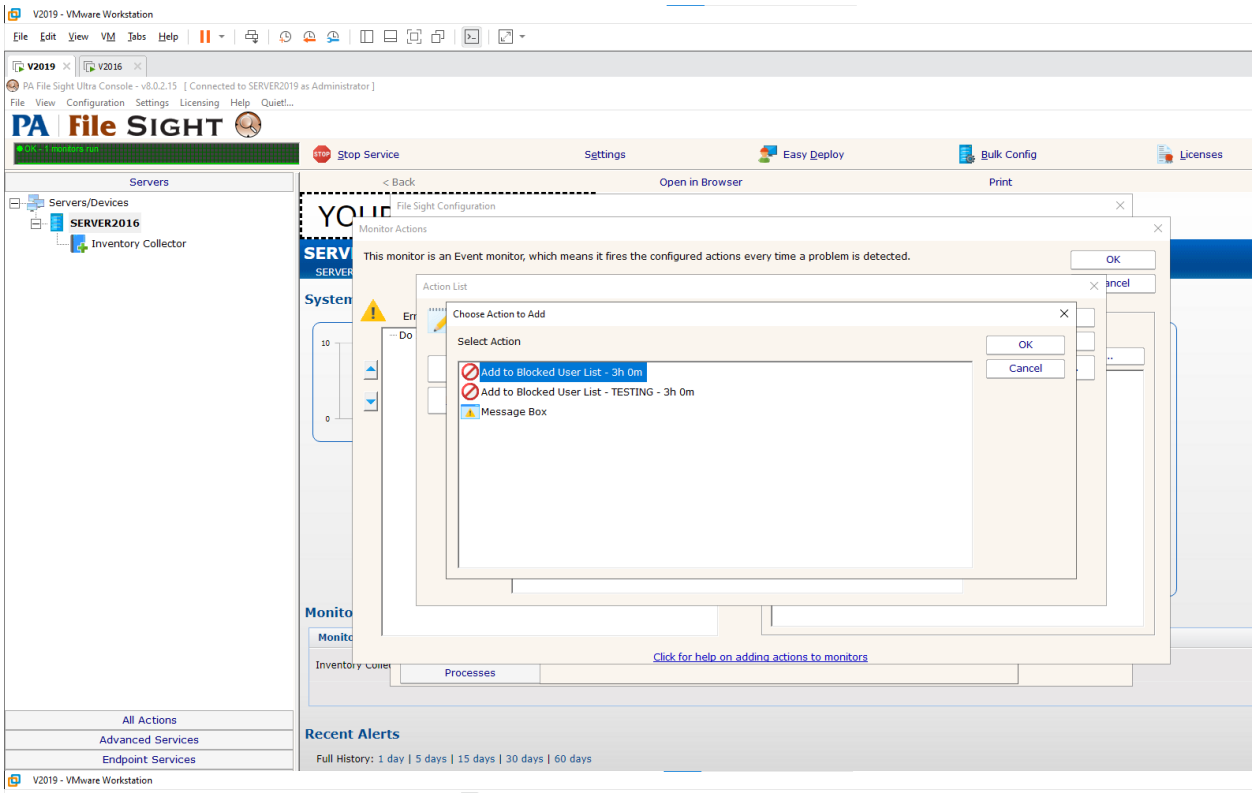

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Startup Wizard
☑Welcome
☑Set Service Account
☑Email Action
☑Log File Action
☑First Monitor
☐Finished!
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
Licensed to:
PA File Sight v8 Ultra Trial License (30 days left)
Stop Service
Settings
Easy Deploy
Bulk Config
Licenses
Exit
Servers
Servers/Devices
SERVER2016
Inventory Collect
System Details information will be collected using the best methods based on server type information that has been set for the target server. If you specifically do not want a method used, check it below.
Apply
Reset
Advanced Options...
Do not use WMI to collect simple System Details information
Schedule...
All Actions
Advanced Services
Endpoint Services
Updates
Reports
New folder
iTop VPN
SoftPerfect Network ...
PA File Sight
jv16 PowerTools

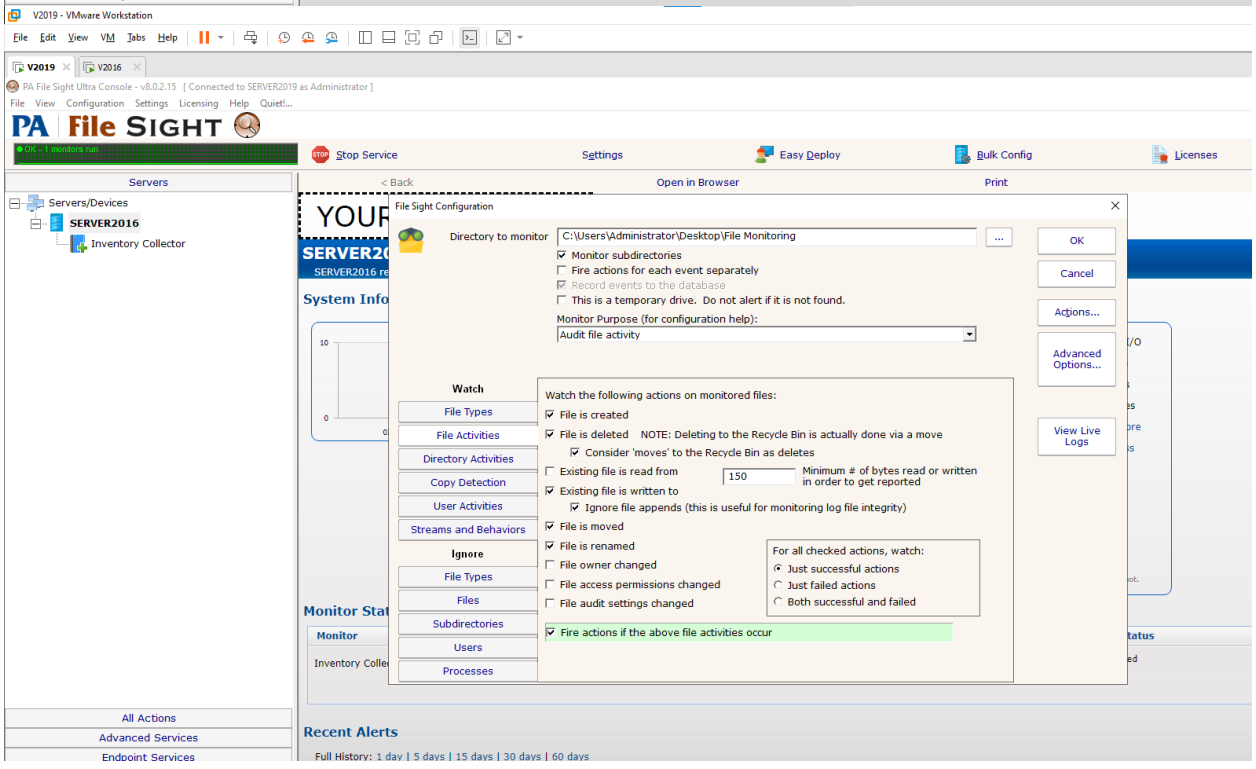

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Startup Wizard
☑Welcome
☑Set Service Account
☑Email Action
☑Log File Action
☑First Monitor
☐Finished!
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
OK
Stop Service
Settings
Easy Deploy
Servers
Servers/Devices
SERVER2016
Inventory Collec
Delete Inventory Collector
Run Now!
Disable Monitor
Immediate Maintenance: Pause Monitoring ...
Rename Monitor
Copy Monitor
Custom Properties ...
Template Operations
Current Status: Running
Last Run: Never/Reset
Next Run: 09 Oct 2023 06:01:07 PM
System Details information will be collected using the best metho
that has been set for the target server. If you specifically do not
ct simple System Details information
All Actions
Advanced Services
Endpoint Services
Updates
Reports
Module ...
Editor
New folder
iTop VPN
1 item
1 ite

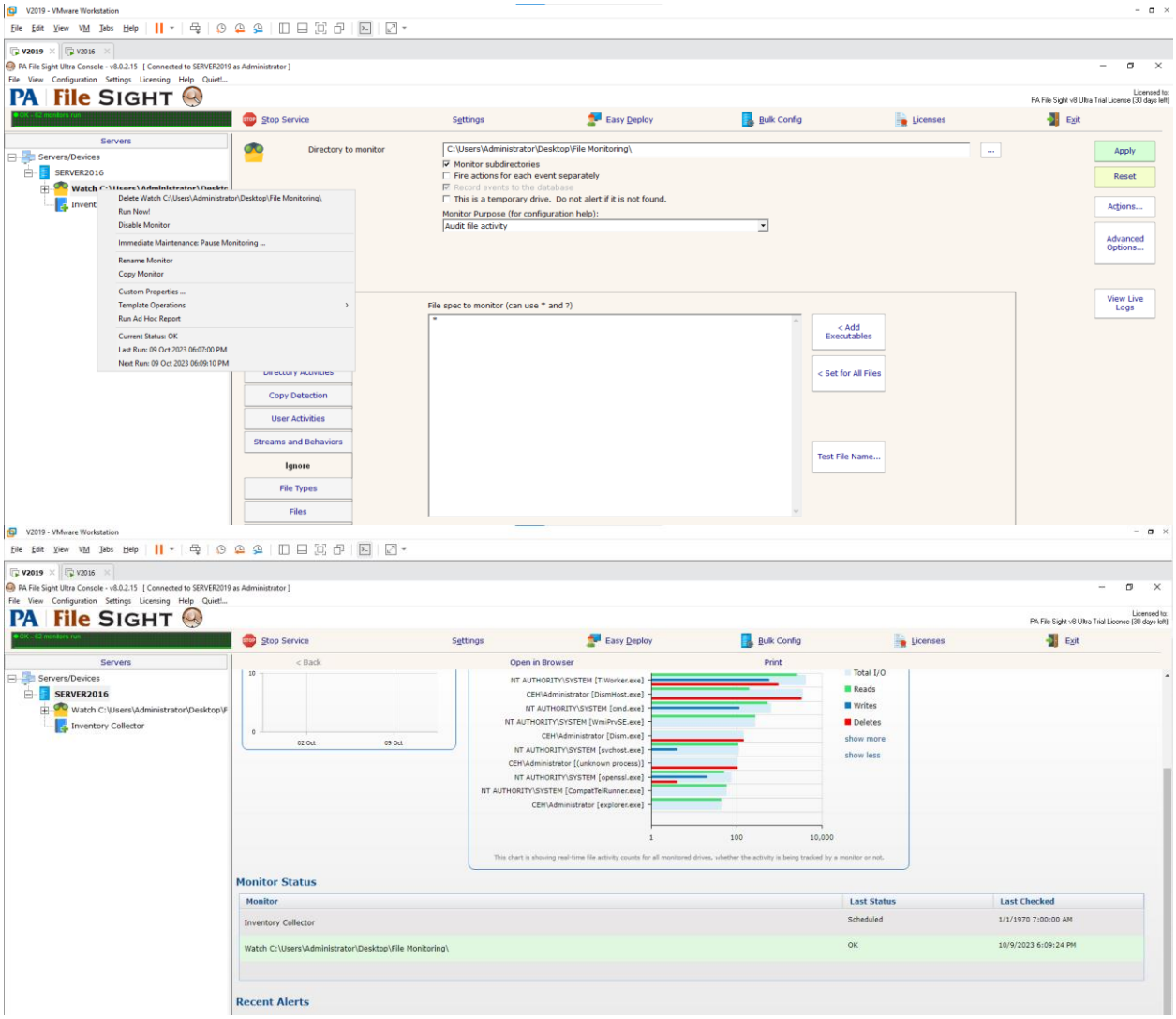

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
Stop Service
Settings
Easy Deploy
Bulk Config
Licenses
Servers
Servers/Devices
SERVER2016
< Back
Open in Browser
Print
YOUR LOGO HERE
To change or remove this logo, go to:
Settings > Report Settings
SERVER2016
SERVER2016 remote satellite
System Information
Hourly Alert Rate
10
0
02 Oct
09 Oct
15 Minute Total I/O Operations (Logarithmic Scale)
Total I/O
Reads
Writes
Deletes
show more
show less
This chart is showing real-time file activity counts for all monitored drives, whether the activity is being tracked by a monitor or not.
Monitor Status
Monitor
Last Status
Inventory Collector
Scheduled
All Actions
Advanced Services
Endpoint Services
Updates
Reports
Recent Alerts
Full History: 1 day | 5 days | 15 days | 30 days | 60 days
No recent alerts to display
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
Stop Service
Settings
Easy Deploy
Bulk Config
Servers
Servers/Devices
SERVER2016
Inventory Collector
< Back
Open in Browser
Print
YOUR LOGO HERE
To change or remove this logo, go to:
Settings > Report Settings
SERVER2016
SERVER2016 remote satellite
Add New Monitor
Select the type of monitor for computer SERVER2016
OK
Cancel
Actions Scheduler
Drive Sight
File Sight Monitor
Inventory Collector
Selected Monitor Description
Always fires attached actions any time it runs. Use the Schedule button to control when the actions are fired.
System Information
Hourly Alert Rate
10
0
02 Oct
Total I/O
Reads
Writes
Deletes
show more
show less
Monitor Status
Monitor
Last Status
Inventory Collector
Scheduled


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
Stop Service
Settings
Easy Deploy
Bulk Config
Licenses
Servers
Servers/Devices
SERVER2016
Inventory Collector
< Back
Open in Browser
Print
File Sight Configuration
Directory to monitor
C:\Users\Administrator\Desktop\File Monitoring
Monitor subdirectories
Fire actions for each event separately
Record events to the database
This is a temporary drive. Do not alert if it is not found.
Monitor Purpose (for configuration help):
Audit file activity
This monitor is configured to fire actions, but none are attached.
OK
Cancel
Actions...
Advanced Options...
View Live Logs
Watch
File Types
File Activities
Directory Activities
Copy Detection
User Activities
Streams and Behaviors
Ignore
File Types
Files
Subdirectories
Users
Processes
File spec to monitor (can use * and ?)
< Add Executables
< Set for All Files
Test File Name...
Monitor Stat
Monitor
Inventory Colle
All Actions
Recent Alerts

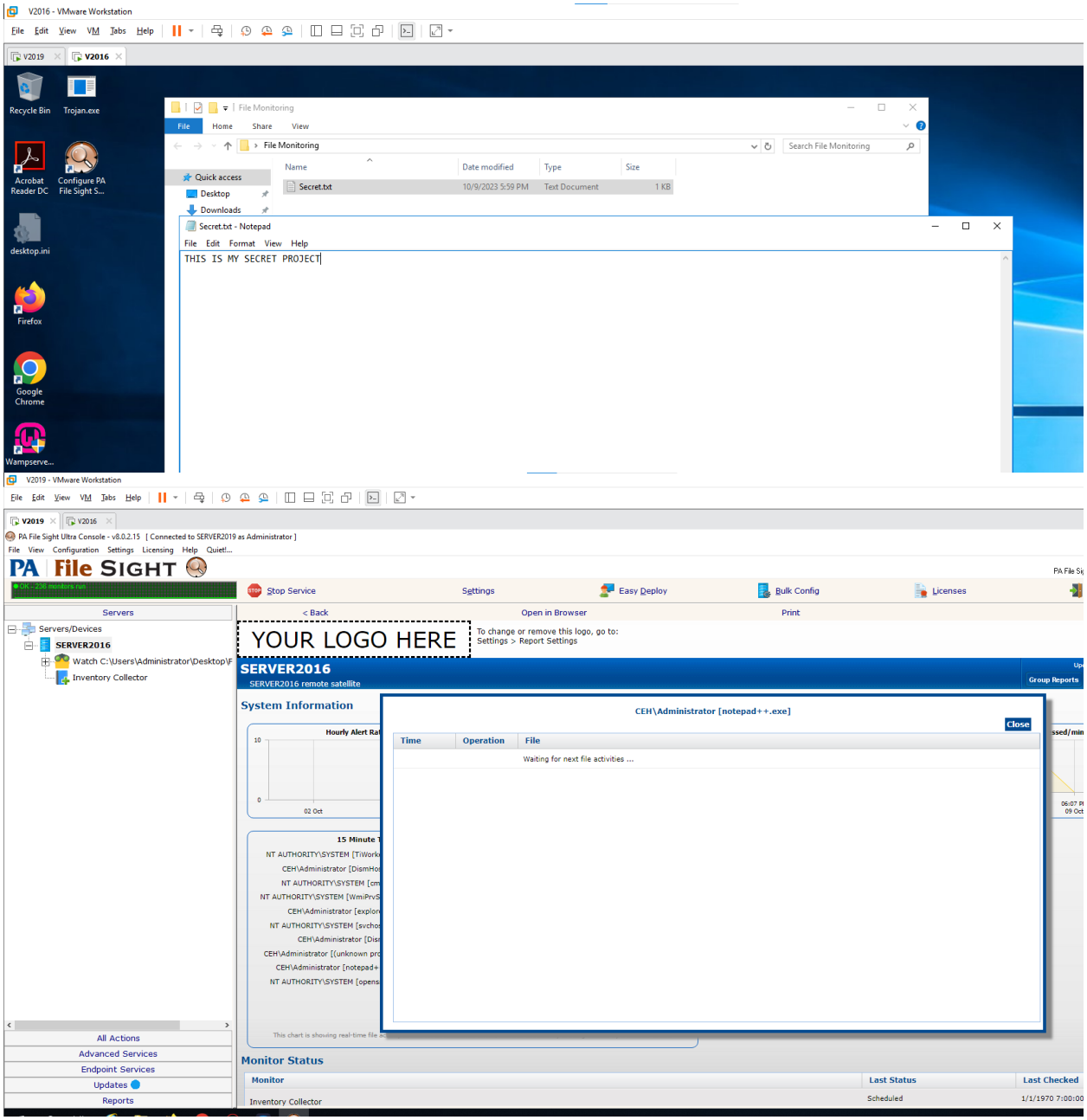

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
Stop Service
Settings
Easy Deploy
Bulk Config
Servers
Servers/Devices
SERVER2016
Inventory Collector
< Back
Open in Browser
Print
File Sight Configuration
Monitor Actions
This monitor is an Event monitor, which means it fires the configured actions every time a problem is detected.
OK
Cancel
Add New Action
Select an action from the list below
Available Action Types
OK
Cancel
Error Actions (run
Do Immediately:
Action List
Add to Blocked User List
Call URL Action
Desktop Notification
Dial-Up Connection
E-mail Message
Execute Script
Message Box
Network Message (Msg.exe/Net Send)
This action is a list of other actions to run. It is useful for cases where you want a changing list of actions assigned to all monitor, such as an on call notification list.
the monitor
Delete...
Click for help on adding actions to monitors
Processes
All Actions


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
Stop Service
Settings
Easy Deploy
Bulk Config
Licenses
Servers
Servers/Devices
SERVER2016
Inventory Collector
< Back
Open in Browser
Print
File Sight Configuration
Monitor Actions
This monitor is an Event monitor, which means it fires the configured actions every time a problem is detected.
OK
Action List
Choose Action to Add
Select Action
OK
Cancel
Add to Blocked User List - 3h 0m
Add to Blocked User List - TESTING - 3h 0m
Message Box
Click for help on adding actions to monitors
Processes
All Actions
Advanced Services
Endpoint Services
Recent Alerts
Full History: 1 day | 5 days | 15 days | 30 days | 60 days

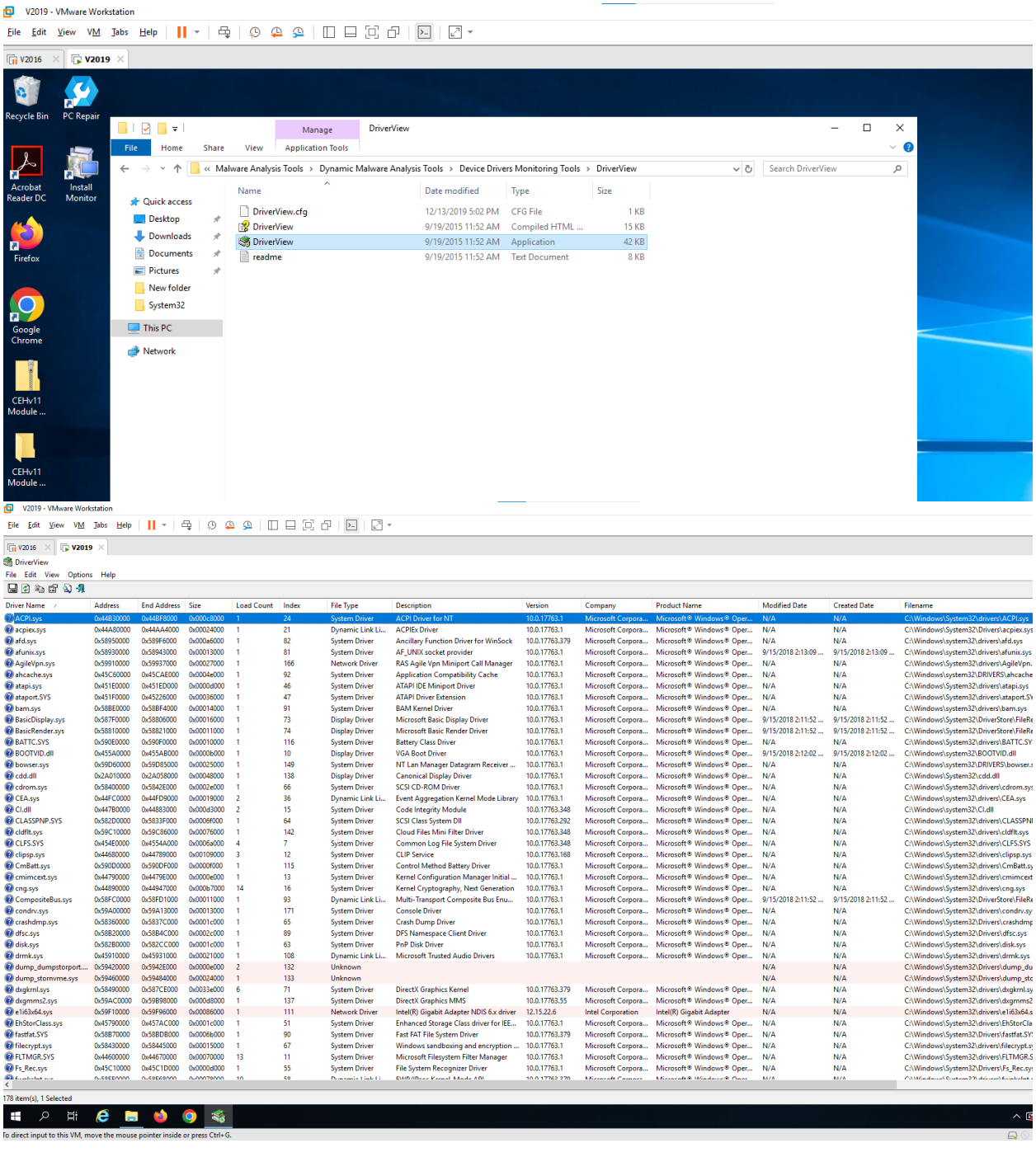

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
Stop Service
Settings
Easy Deploy
Bulk Config
Licenses
Servers
Servers/Devices
SERVER2016
Inventory Collector
< Back
Open in Browser
Print
File Sight Configuration
Directory to monitor
C:\Users\Administrator\Desktop\File Monitoring
Monitor subdirectories
Fire actions for each event separately
Record events to the database
This is a temporary drive. Do not alert if it is not found.
Monitor Purpose (for configuration help):
Audit file activity
OK
Cancel
Actions...
Advanced Options...
View Live Logs
Watch
File Types
File Activities
Directory Activities
Copy Detection
User Activities
Streams and Behaviors
Ignore
File Types
Files
Subdirectories
Users
Processes
Watch the following actions on monitored files:
File is created
File is deleted NOTE: Deleting to the Recycle Bin is actually done via a move
Consider 'moves' to the Recycle Bin as deletes
Existing file is read from
150
Minimum # of bytes read or written in order to get reported
Existing file is written to
Ignore file appends (this is useful for monitoring log file integrity)
File is moved
File is renamed
File owner changed
File access permissions changed
File audit settings changed
For all checked actions, watch:
Just successful actions
Just failed actions
Both successful and failed
Fire actions if the above file activities occur
All Actions
Advanced Services
Endpoint Services
Recent Alerts
Full History: 1 day | 5 days | 15 days | 30 days | 60 days


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
File View Configuration Settings Licensing Help Quiet!...
PA File SIGHT
Licensed to:
PA File Sight v8 Ultra Trial License [30 days left]
Stop Service
Settings
Easy Deploy
Bulk Config
Licenses
Exit
Servers
Servers/Devices
SERVER2016
Inventory Collector
Directory to monitor
C:\Users\Administrator\Desktop\File Monitoring\
Monitor subdirectories
Fire actions for each event separately
Record events to the database
This is a temporary drive. Do not alert if it is not found.
Monitor Purpose (for configuration help):
Audit file activity
Apply
Reset
Actions...
Advanced Options...
View Live Logs
Delete Watch C:\Users\Administrator\Desktop\File Monitoring\
Run Now!
Disable Monitor
Immediate Maintenance: Pause Monitoring ...
Rename Monitor
Copy Monitor
Custom Properties ...
Template Operations
Run Ad Hoc Report
Current Status: OK
Last Run: 09 Oct 2023 06:07:00 PM
Next Run: 09 Oct 2023 06:09:10 PM
File spec to monitor (can use * and ?)
< Add Executables
< Set for All Files
Test File Name...
Copy Detection
User Activities
Streams and Behaviors
Ignore
File Types
Files

V2019 - VMware Workstation
PA File Sight Ultra Console - v8.0.2.15 [Connected to SERVER2019 as Administrator]
PA File SIGHT
Stop Service
Settings
Easy Deploy
Bulk Config
Licenses
Exit
Servers
Servers/Devices
SERVER2016
Inventory Collector
< Back
Open in Browser
Print
Total I/O
Reads
Writes
Deletes
show more
show less
Monitor Status
Monitor
Last Status
Last Checked
Inventory Collector
Scheduled
1/1/1970 7:00:00 AM
Watch C:\Users\Administrator\Desktop\File Monitoring\
OK
10/9/2023 6:09:24 PM
Recent Alerts



4.8 Perform Device Driver Monitoring using DriverView and Driver Booster - Open Windows 10

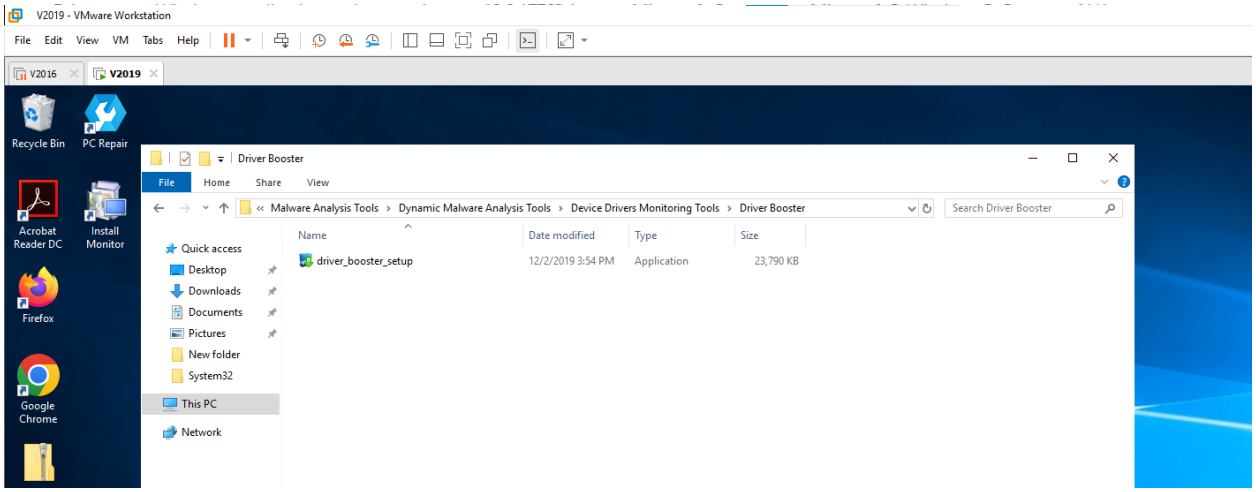

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Manage
DriverView
File Home Share View Application Tools
Malware Analysis Tools › Dynamic Malware Analysis Tools › Device Drivers Monitoring Tools › DriverView
Search DriverView
Quick access
Desktop
Downloads
Documents
Pictures
New folder
System32
This PC
Network
Name
Date modified
Type
Size
DriverView.cfg 12/13/2019 5:02 PM CFG File 1 KB
DriverView 9/19/2015 11:52 AM Compiled HTML ... 15 KB
DriverView 9/19/2015 11:52 AM Application 42 KB
readme 9/19/2015 11:52 AM Text Document 8 KB
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
DriverView
File Edit View Options Help
Driver Name
Address
End Address
Size
Load Count
Index
File Type
Description
Version
Company
Product Name
Modified Date
Created Date
Filename
ACPI.sys 0x44B30000 0x44BF8000 0x000c8000 1 24 System Driver ACPI Driver for NT 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\ACPI.sys
acpiex.sys 0x44A80000 0x44AA4000 0x00024000 1 21 Dynamic Link Li... ACPIEx Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\Drivers\acpiex.sys
afd.sys 0x58950000 0x589F6000 0x000a6000 1 82 System Driver Ancillary Function Driver for WinSock 10.0.17763.379 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\system32\drivers\afd.sys
afunix.sys 0x58930000 0x58943000 0x00013000 1 81 System Driver AF_UNIX socket provider 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... 9/15/2018 2:13:09 ... 9/15/2018 2:13:09 ... C:\Windows\system32\drivers\afunix.sys
AgileVpn.sys 0x59910000 0x59937000 0x00027000 1 166 Network Driver RAS Agile Vpn Miniport Call Manager 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\AgileVpn.
ahcache.sys 0x45C60000 0x45CAE000 0x0004e000 1 92 System Driver Application Compatibility Cache 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\system32\DRIVERS\ahcache
atapi.sys 0x451E0000 0x451ED000 0x0000d000 1 46 System Driver ATAPI IDE Miniport Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\atapi.sys
ataport.SYS 0x451F0000 0x45226000 0x00036000 1 47 System Driver ATAPI Driver Extension 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\ataport.SY
bam.sys 0x58BE0000 0x58BF4000 0x00014000 1 91 System Driver BAM Kernel Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\system32\drivers\bam.sys
BasicDisplay.sys 0x587F0000 0x58806000 0x00016000 1 73 Display Driver Microsoft Basic Display Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... 9/15/2018 2:11:52 ... 9/15/2018 2:11:52 ... C:\Windows\System32\DriverStore\FileRe
BasicRender.sys 0x58810000 0x58821000 0x00011000 1 74 Display Driver Microsoft Basic Render Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... 9/15/2018 2:11:52 ... 9/15/2018 2:11:52 ... C:\Windows\System32\DriverStore\FileRe
BATTC.SYS 0x590E0000 0x590F0000 0x00010000 1 116 System Driver Battery Class Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\BATTC.SY
BOOTVID.dll 0x455A0000 0x455AB000 0x0000b000 1 10 Display Driver VGA Boot Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... 9/15/2018 2:12:02 ... 9/15/2018 2:12:02 ... C:\Windows\system32\BOOTVID.dll
bowser.sys 0x59D60000 0x59D85000 0x00025000 1 149 System Driver NT Lan Manager Datagram Receiver ... 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\system32\DRIVERS\bowser.
cdd.dll 0x2A010000 0x2A058000 0x00048000 1 138 Display Driver Canonical Display Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\cdd.dll
cdrom.sys 0x58400000 0x5842E000 0x0002e000 1 66 System Driver SCSI CD-ROM Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\cdrom.sys
CEA.sys 0x44FC0000 0x44FD9000 0x00019000 2 36 Dynamic Link Li... Event Aggregation Kernel Mode Library 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\CEA.sys
CI.dll 0x447B0000 0x44883000 0x000d3000 2 15 System Driver Code Integrity Module 10.0.17763.348 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\system32\CI.dll
CLASSPNP.SYS 0x582D0000 0x5833F000 0x0006f000 1 64 System Driver SCSI Class System Dll 10.0.17763.292 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\CLASSPNI
cldflt.sys 0x59C10000 0x59C86000 0x00076000 1 142 System Driver Cloud Files Mini Filter Driver 10.0.17763.348 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\cldflt.sys
CLFS.SYS 0x454E0000 0x4554A000 0x0006a000 4 7 System Driver Common Log File System Driver 10.0.17763.348 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\CLFS.SYS
clipsp.sys 0x44680000 0x44789000 0x00109000 3 12 System Driver CLIP Service 10.0.17763.168 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\clipsp.sys
CmBatt.sys 0x590D0000 0x590DF000 0x0000f000 1 115 System Driver Control Method Battery Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\CmBatt.sy
cmimcext.sys 0x44790000 0x4479E000 0x0000e000 1 13 System Driver Kernel Configuration Manager Initial ... 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\cmimcext
cng.sys 0x44890000 0x44947000 0x000b7000 14 16 System Driver Kernel Cryptography, Next Generation 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\cng.sys
CompositeBus.sys 0x58FC0000 0x58FD1000 0x00011000 1 93 Dynamic Link Li... Multi-Transport Composite Bus Enu... 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... 9/15/2018 2:11:52 ... 9/15/2018 2:11:52 ... C:\Windows\System32\DriverStore\FileRe
condrv.sys 0x59A00000 0x59A13000 0x00013000 1 171 System Driver Console Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\condrv.sy
crashdmp.sys 0x58360000 0x5837C000 0x0001c000 1 65 System Driver Crash Dump Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\Drivers\crashdmp
dfsc.sys 0x58B20000 0x58B4C000 0x0002c000 1 89 System Driver DFS Namespace Client Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\dfsc.sys
disk.sys 0x582B0000 0x582CC000 0x0001c000 1 63 System Driver PnP Disk Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\disk.sys
drmk.sys 0x45910000 0x45931000 0x00021000 1 108 Dynamic Link Li... Microsoft Trusted Audio Drivers 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\drmk.sys
dump_dumpstorport.... 0x59420000 0x5942E000 0x0000e000 2 132 Unknown N/A N/A C:\Windows\System32\Drivers\dump_du
dump_stornvme.sys 0x59460000 0x59484000 0x00024000 1 133 Unknown N/A N/A C:\Windows\System32\Drivers\dump_stc
dxgkrnl.sys 0x58490000 0x587CE000 0x0033e000 6 71 System Driver DirectX Graphics Kernel 10.0.17763.379 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\dxgkrnl.sy
dxgmms2.sys 0x59AC0000 0x59B98000 0x000d8000 1 137 System Driver DirectX Graphics MMS 10.0.17763.55 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\dxgmms2
e1i63x64.sys 0x59F10000 0x59F96000 0x00086000 1 111 Network Driver Intel(R) Gigabit Adapter NDIS 6.x driver 12.15.22.6 Intel Corporation Intel(R) Gigabit Adapter N/A N/A C:\Windows\System32\drivers\e1i63x64.s
EhStorClass.sys 0x45790000 0x457AC000 0x0001c000 1 51 System Driver Enhanced Storage Class driver for IEE... 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\EhStorCla
fastfat.SYS 0x58B70000 0x58BDB000 0x0006b000 1 90 System Driver Fast FAT File System Driver 10.0.17763.379 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\Drivers\fastfat.SY
filecrypt.sys 0x58430000 0x58445000 0x00015000 1 67 System Driver Windows sandboxing and encryption ... 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\system32\drivers\filecrypt.s
FLTMGR.SYS 0x44600000 0x44670000 0x00070000 13 11 System Driver Microsoft Filesystem Filter Manager 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\drivers\FLTMGR.S
Fs_Rec.sys 0x45C10000 0x45C1D000 0x0000d000 1 55 System Driver File System Recognizer Driver 10.0.17763.1 Microsoft Corpora... Microsoft® Windows® Oper... N/A N/A C:\Windows\System32\Drivers\Fs_Rec.sy
178 item(s), 1 Selected
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

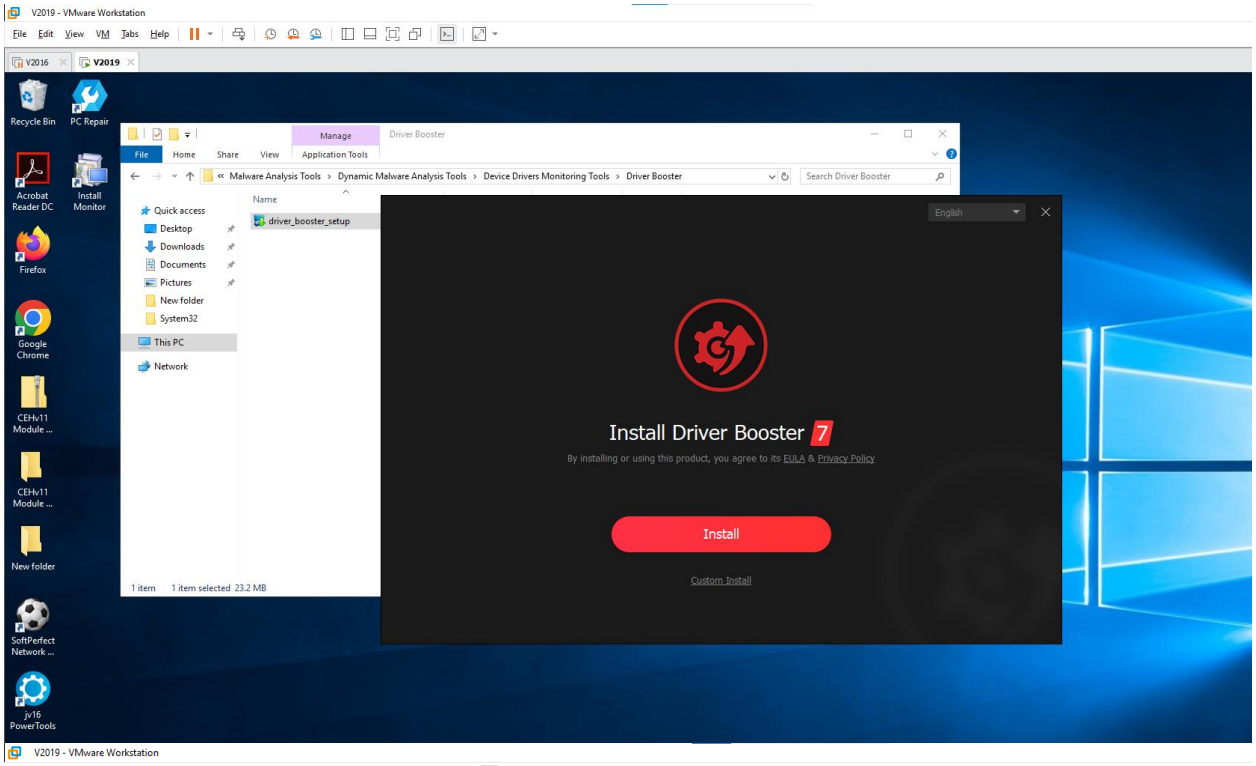
ystem Driver	Ancillary Function Driver for WinSock	10.0.17763.379	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A
ystem Driver	AF_UNIX socket provider	10.0.17763.1	Microsoft Corpora...	Microsoft® Windows® Oper...	9/15/2018 2:13:09 ...
etwork Driver	RAS Agile Vpn Miniport Call Manager	10.0.17763.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A
ystem Driver	Application Compatibility Cache	10.0.17763.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A
ystem Driver	ATAPI IDE Miniport Driver	10.0.17763.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A
ystem Driver	ATAPI Dr			ows® Oper...	N/A
ystem Driver	BAM Ker			ows® Oper...	N/A
isplay Driver	Microsof			ows® Oper...	9/15/2018 2:11:52 ...
isplay Driver	Microsof			ows® Oper...	9/15/2018 2:11:52 ...
ystem Driver	Battery C			ows® Oper...	N/A
isplay Driver	VGA Boo			ows® Oper...	9/15/2018 2:12:02 ...
ystem Driver	NT Lan M			ows® Oper...	N/A
isplay Driver	Canonic			ows® Oper...	N/A
ystem Driver	SCSI CD-			ows® Oper...	N/A
ynamic Link Li...	Event Ag			ows® Oper...	N/A
ystem Driver	Code Int			ows® Oper...	N/A
ystem Driver	SCSI Clas			ows® Oper...	N/A
ystem Driver	Cloud Fil			ows® Oper...	N/A
ystem Driver	Commo			ows® Oper...	N/A
ystem Driver	CLIP Serv			ows® Oper...	N/A
ystem Driver	Control M			ows® Oper...	N/A
ystem Driver	Kernel C			ows® Oper...	N/A
ystem Driver	Kernel C			ows® Oper...	N/A
ynamic Link Li...	Multi-Tra			ows® Oper...	9/15/2018 2:11:52 ...
ystem Driver	Console			ows® Oper...	N/A
ystem Driver	Crash Du			ows® Oper...	N/A
ystem Driver	DFS Nam			ows® Oper...	N/A
ystem Driver	PnP Disk			ows® Oper...	N/A
ynamic Link Li...	Microsof			ows® Oper...	N/A
nknown					N/A
nknown					N/A
ystem Driver	DirectX Graphics Kernel			ows® Oper...	N/A
ystem Driver	DirectX Graphics MMS	10.0.17763.55	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A
etwork Driver	Intel(R) Gigabit Adapter NDIS 6.x driver	12.15.22.6	Intel Corporation	Intel(R) Gigabit Adapter	N/A
ystem Driver	Enhanced Storage Class driver for IEE...	10.0.17763.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A
ystem Driver	Fast FAT File System Driver	10.0.17763.379	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A

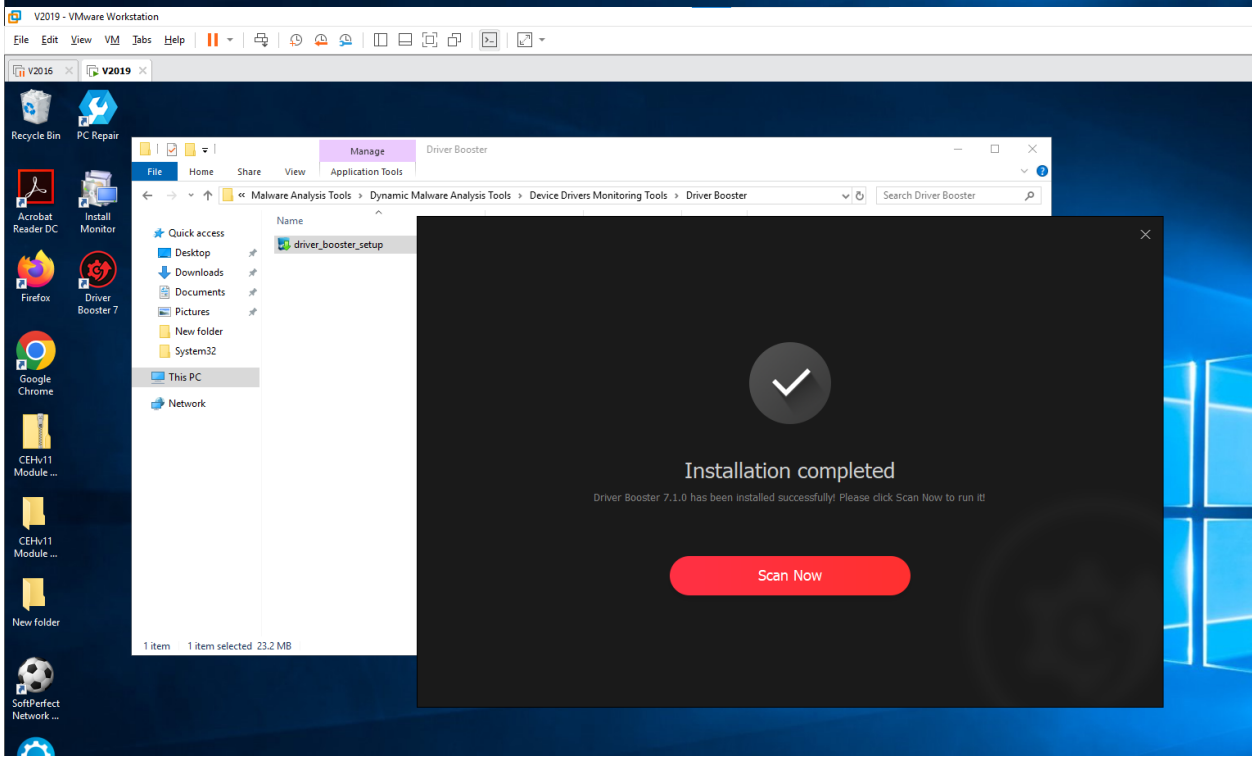
Properties

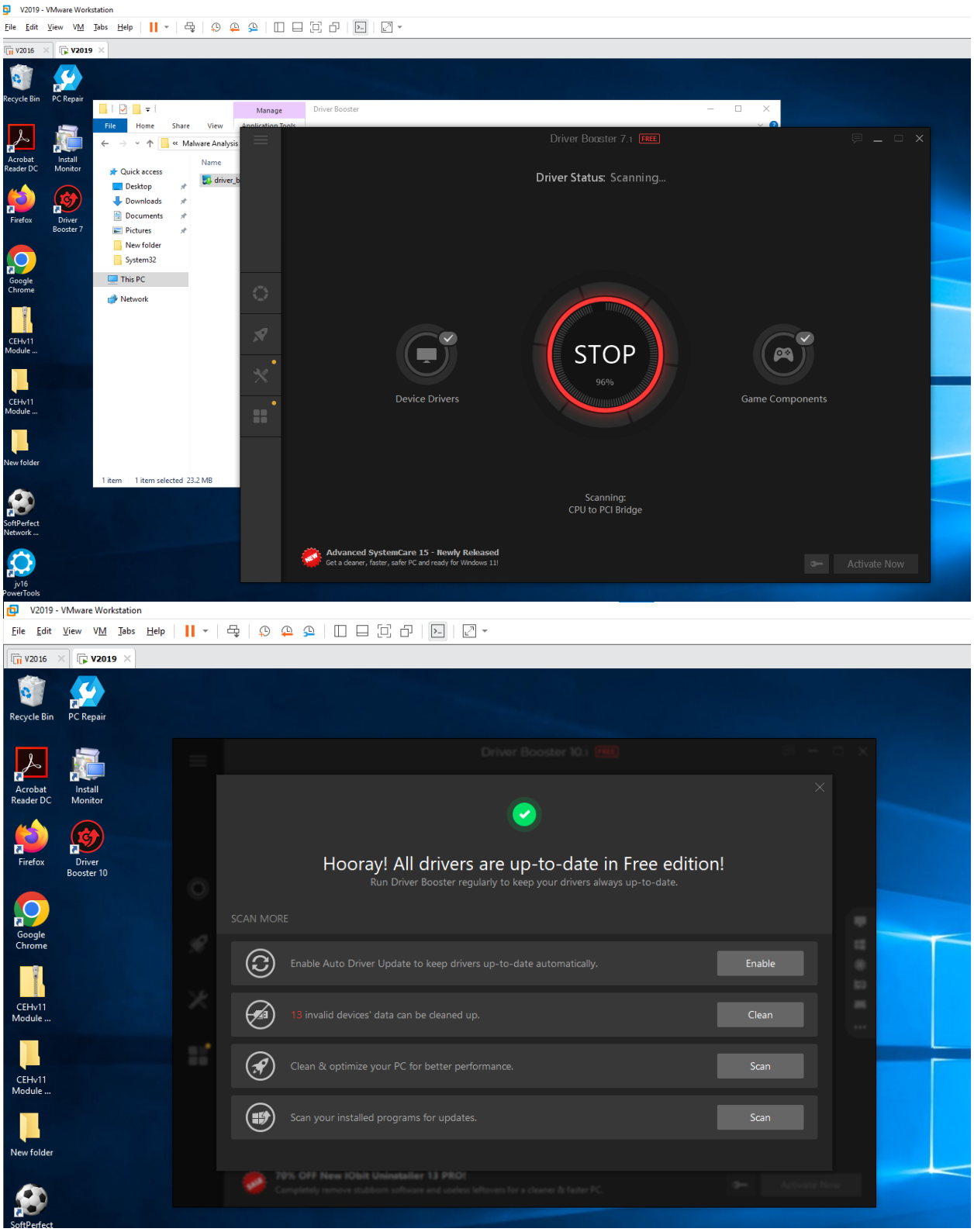
Driver Name:	afunix.sys
Address:	0x58930000
End Address:	0x58943000
Size:	0x00013000
Load Count:	1
Index:	81
File Type:	System Driver
Description:	AF_UNIX socket provider
Version:	10.0.17763.1
Company:	Microsoft Corporation
Product Name:	Microsoft® Windows® Operating System
Modified Date:	9/15/2018 2:13:09 PM
Created Date:	9/15/2018 2:13:09 PM
Filename:	C:\Windows\system32\drivers\afunix.sys
File Attributes:	A
Service Name:	afunix
Service Display Name:	afunix
Digital Signature:	

OK

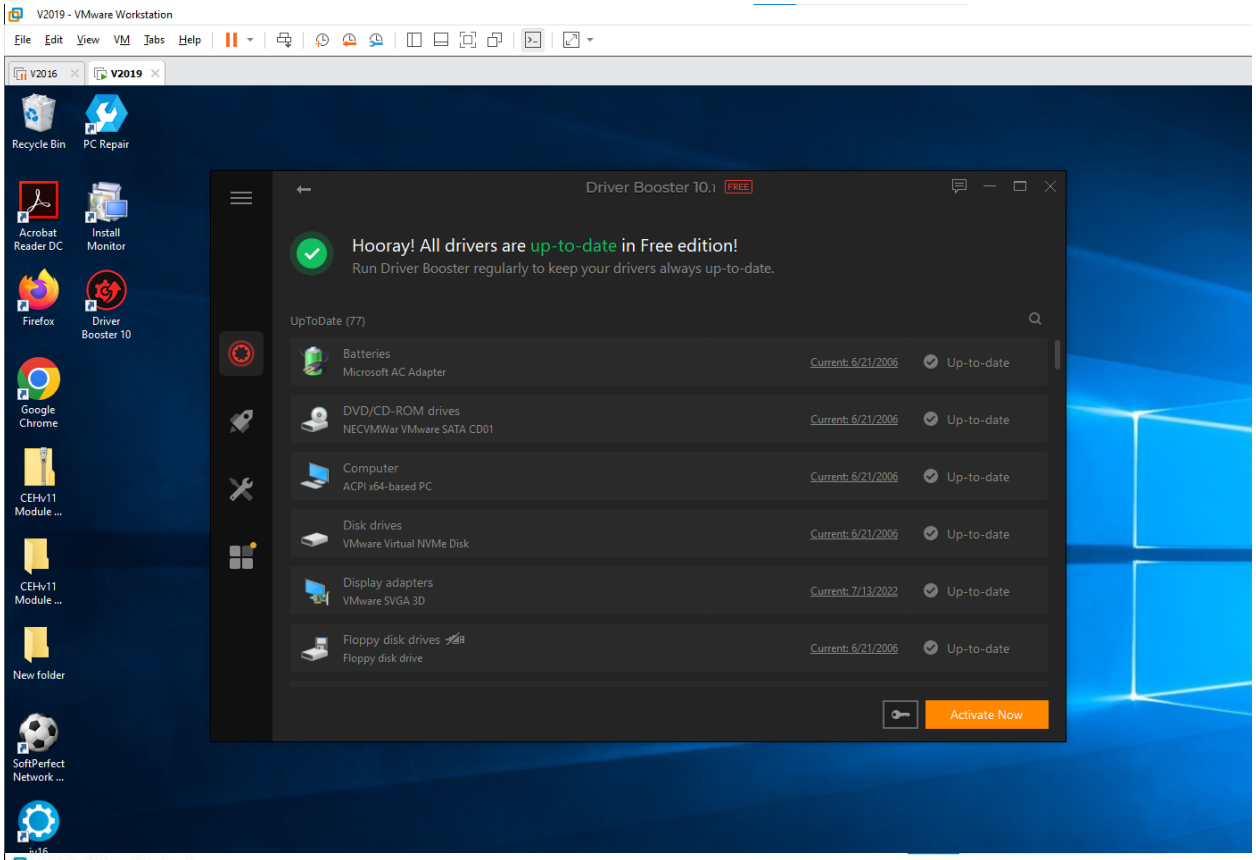


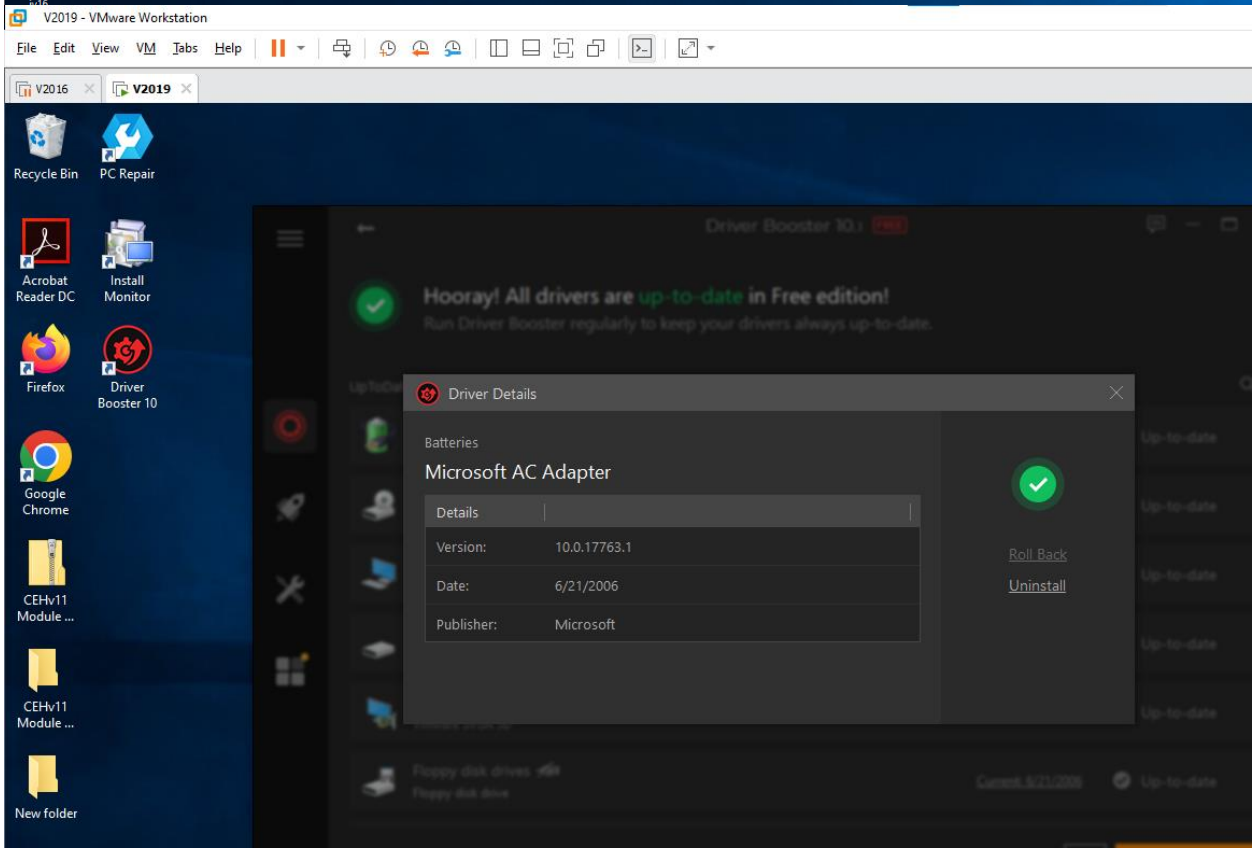

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
jv16 PowerTools
Manage
Driver Booster
File Home Share View Application Tools
Malware Analysis Tools › Dynamic Malware Analysis Tools › Device Drivers Monitoring Tools › Driver Booster
Search Driver Booster
Quick access
Desktop
Downloads
Documents
Pictures
New folder
System32
This PC
Network
Name
driver_booster_setup
1 item 1 item selected 23.2 MB
English
Install Driver Booster 7
By installing or using this product, you agree to its EULA & Privacy Policy
Install
Custom Install

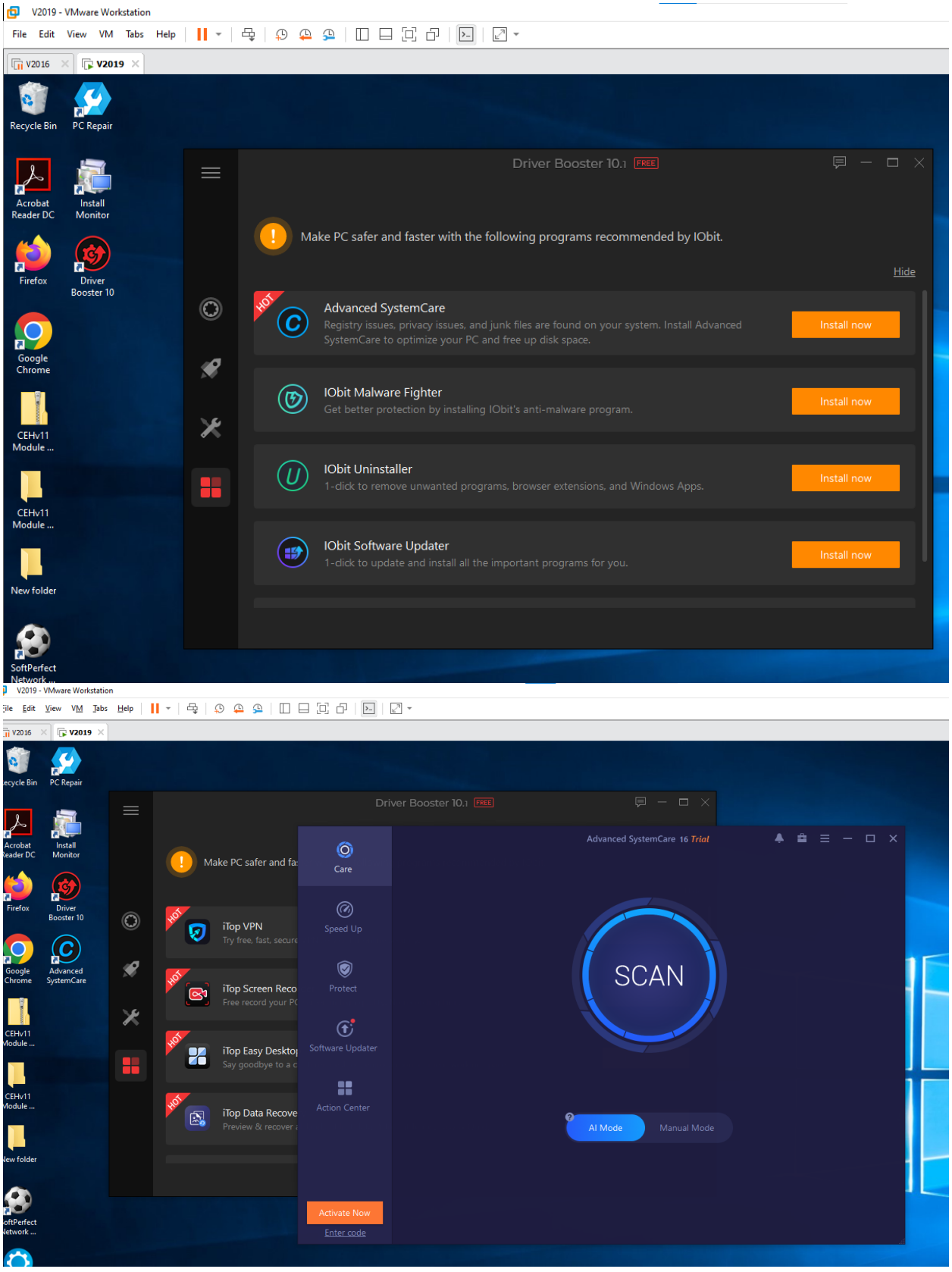

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 7
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
Manage
Driver Booster
File Home Share View Application Tools
Malware Analysis Tools › Dynamic Malware Analysis Tools › Device Drivers Monitoring Tools › Driver Booster
Search Driver Booster
Quick access
Desktop
Downloads
Documents
Pictures
New folder
System32
This PC
Network
Name
driver_booster_setup
1 item 1 item selected 23.2 MB
Installation completed
Driver Booster 7.1.0 has been installed successfully! Please click Scan Now to run it!
Scan Now


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 7
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
jv16 PowerTools
Manage
Driver Booster
File Home Share View
Application Tools
Malware Analysis
Quick access
Desktop
Downloads
Documents
Pictures
New folder
System32
This PC
Network
Name
driver_b
1 item
1 item selected 23.2 MB
Driver Booster 7.1 FREE
Driver Status: Scanning...
Device Drivers
STOP
96%
Game Components
Scanning:
CPU to PCI Bridge
Advanced SystemCare 15 - Newly Released
Get a cleaner, faster, safer PC and ready for Windows 11!
Activate Now

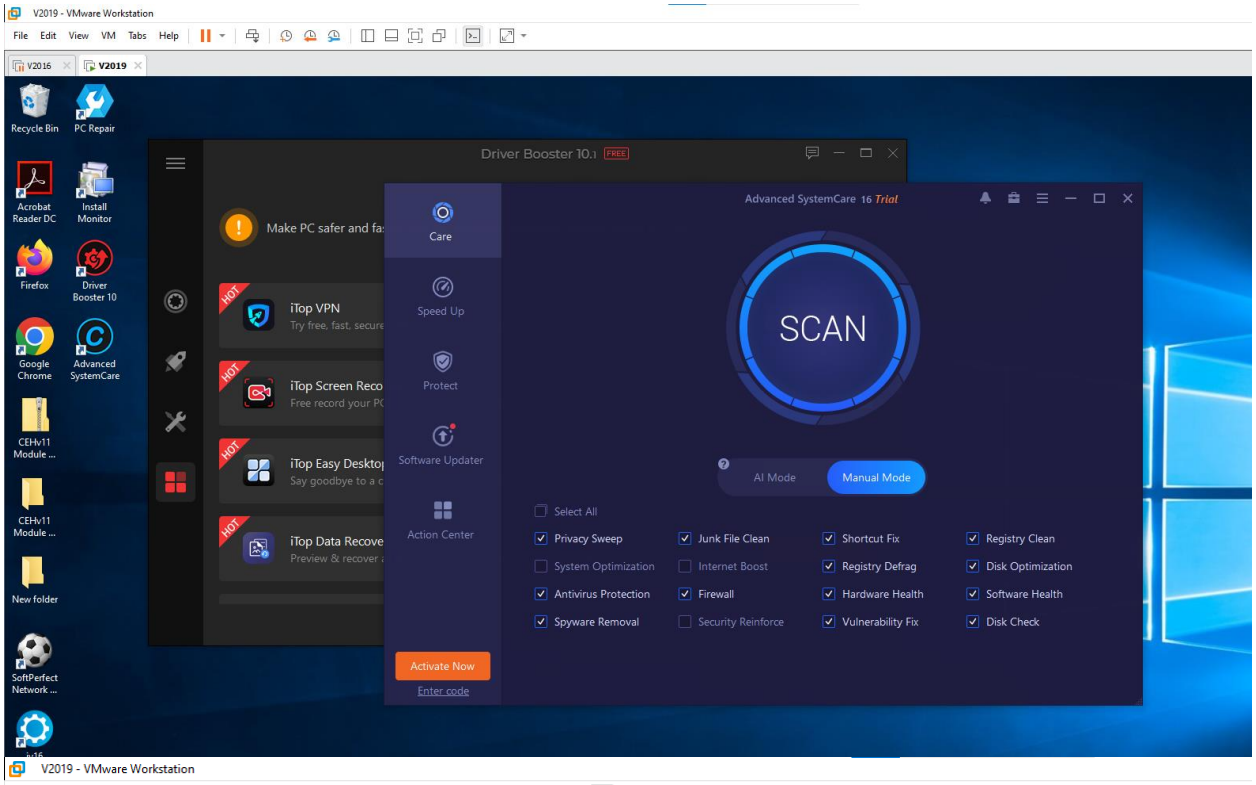
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect
Driver Booster 10.1 FREE
Hooray! All drivers are up-to-date in Free edition!
Run Driver Booster regularly to keep your drivers always up-to-date.
SCAN MORE
Enable Auto Driver Update to keep drivers up-to-date automatically.
Enable
13 invalid devices' data can be cleaned up.
Clean
Clean & optimize your PC for better performance.
Scan
Scan your installed programs for updates.
Scan

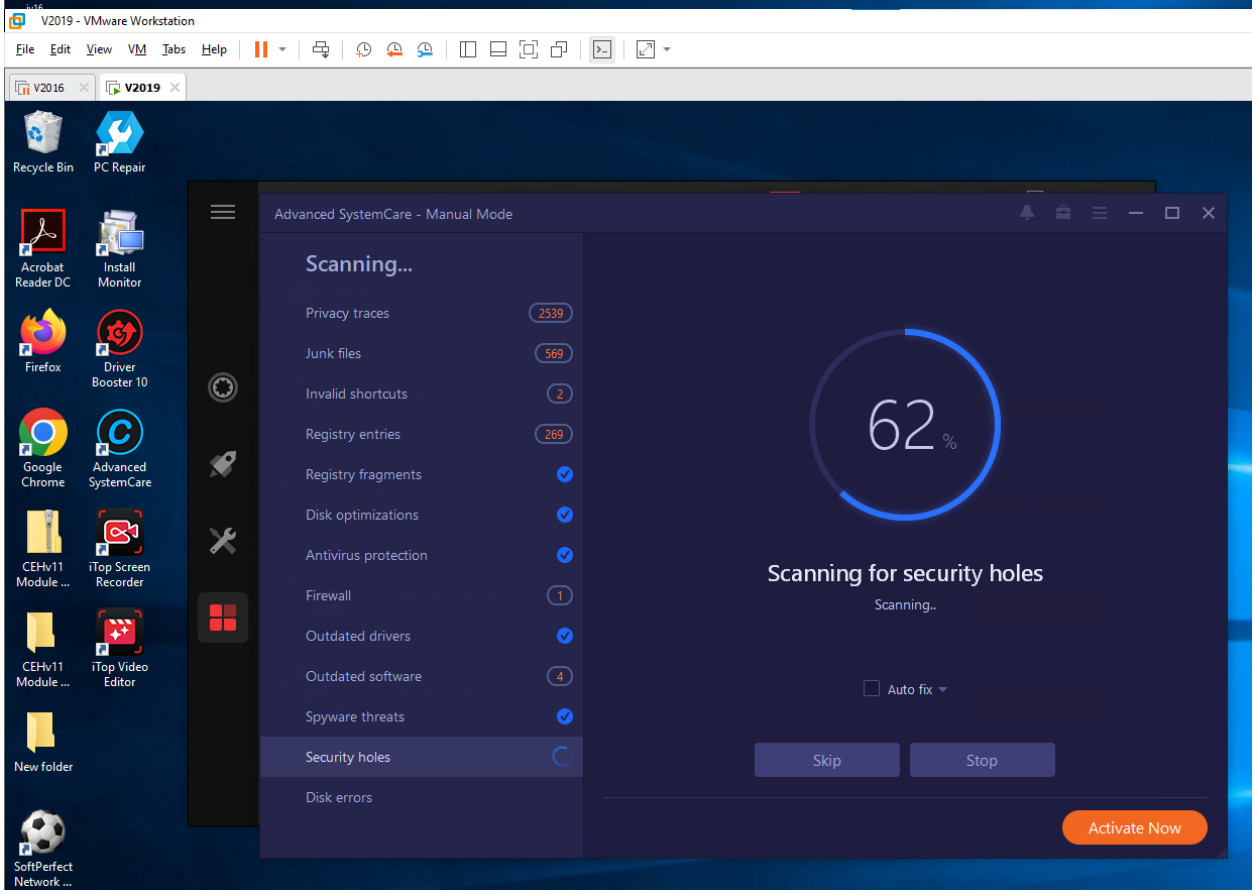

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
Driver Booster 10.1 FREE
Hooray! All drivers are up-to-date in Free edition!
Run Driver Booster regularly to keep your drivers always up-to-date.
UpToDate (77)
Batteries
Microsoft AC Adapter
Current: 6/21/2006
Up-to-date
DVD/CD-ROM drives
NECVMWar VMware SATA CD01
Current: 6/21/2006
Up-to-date
Computer
ACPI x64-based PC
Current: 6/21/2006
Up-to-date
Disk drives
VMware Virtual NVMe Disk
Current: 6/21/2006
Up-to-date
Display adapters
VMware SVGA 3D
Current: 7/13/2022
Up-to-date
Floppy disk drives
Floppy disk drive
Current: 6/21/2006
Up-to-date
Activate Now

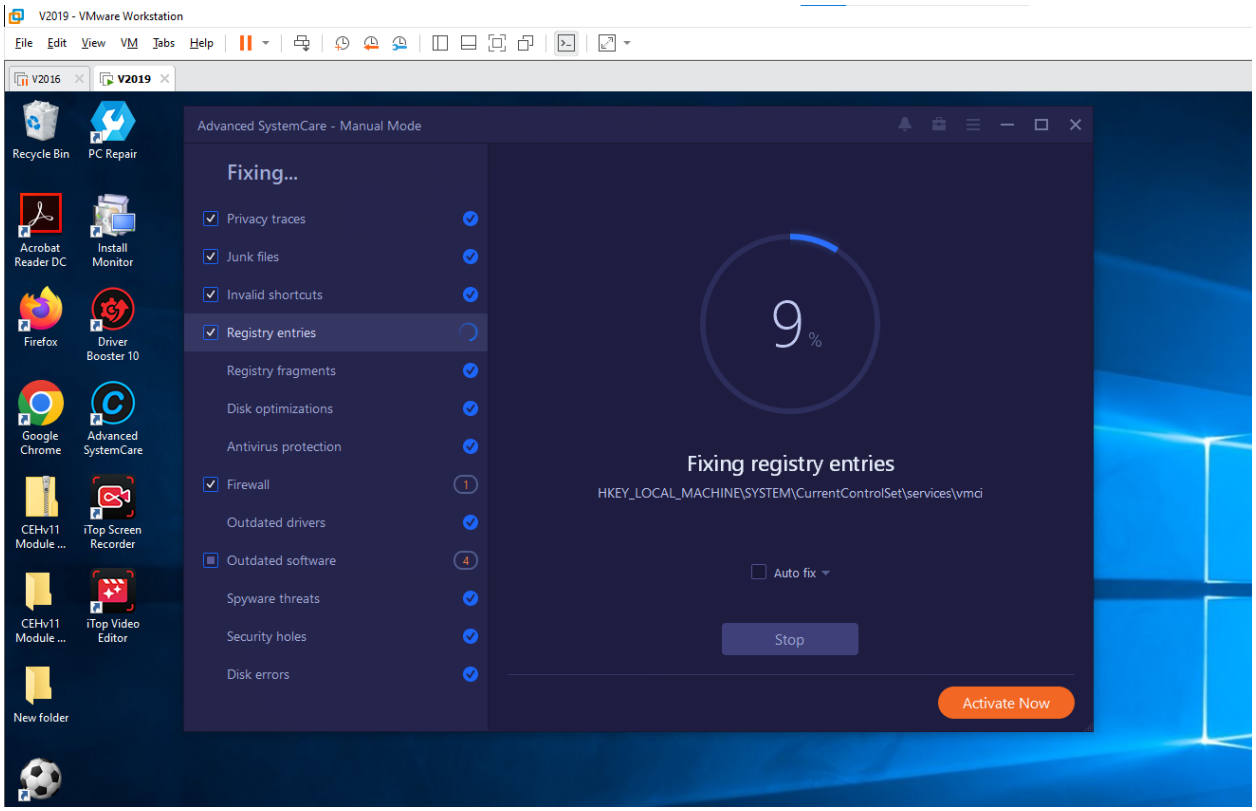

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
Driver Details
Batteries
Microsoft AC Adapter
Details
Version: 10.0.17763.1
Date: 6/21/2006
Publisher: Microsoft
Roll Back
Uninstall


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
Driver Booster 10.1 FREE
Make PC safer and faster with the following programs recommended by IObit.
Hide
HOT
Advanced SystemCare
Registry issues, privacy issues, and junk files are found on your system. Install Advanced SystemCare to optimize your PC and free up disk space.
Install now
IObit Malware Fighter
Get better protection by installing IObit's anti-malware program.
Install now
IObit Uninstaller
1-click to remove unwanted programs, browser extensions, and Windows Apps.
Install now
IObit Software Updater
1-click to update and install all the important programs for you.
Install now

V2019 - VMware Workstation
V2016
V2019
Driver Booster 10.1 FREE
Make PC safer and fa
HOT
iTop VPN
Try free, fast, secure
iTop Screen Reco
Free record your PC
iTop Easy Desktop
Say goodbye to a c
iTop Data Recove
Preview & recover
Advanced SystemCare 16 Trial
Care
Speed Up
Protect
Software Updater
Action Center
SCAN
AI Mode
Manual Mode
Activate Now
Enter code

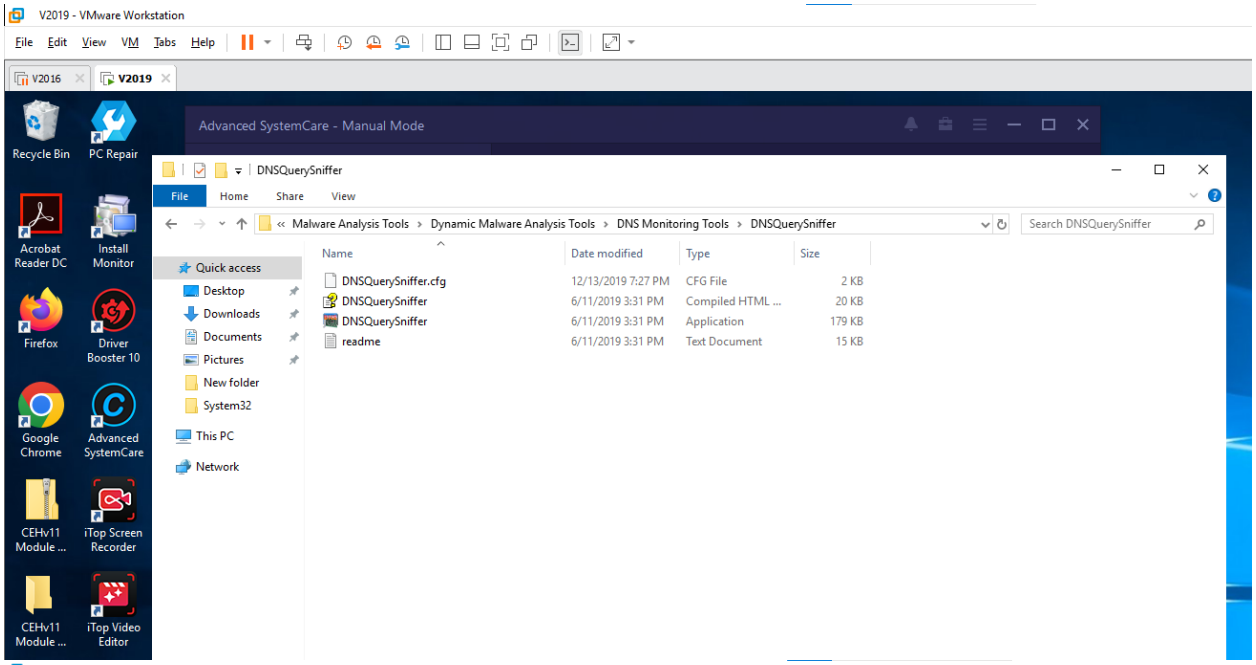

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
Advanced SystemCare
CEHv11 Module ...
CEHv11 Module ...
New folder
SoftPerfect Network ...
Driver Booster 10.1 FREE
Make PC safer and fa
iTop VPN
Try free, fast, secure
iTop Screen Reco
Free record your PC
iTop Easy Desktop
Say goodbye to a c
iTop Data Recove
Preview & recover
Care
Speed Up
Protect
Software Updater
Action Center
Activate Now
Enter code
Advanced SystemCare 16 Trial
SCAN
AI Mode
Manual Mode
Select All
Privacy Sweep
Junk File Clean
Shortcut Fix
Registry Clean
System Optimization
Internet Boost
Registry Defrag
Disk Optimization
Antivirus Protection
Firewall
Hardware Health
Software Health
Spyware Removal
Security Reinforce
Vulnerability Fix
Disk Check

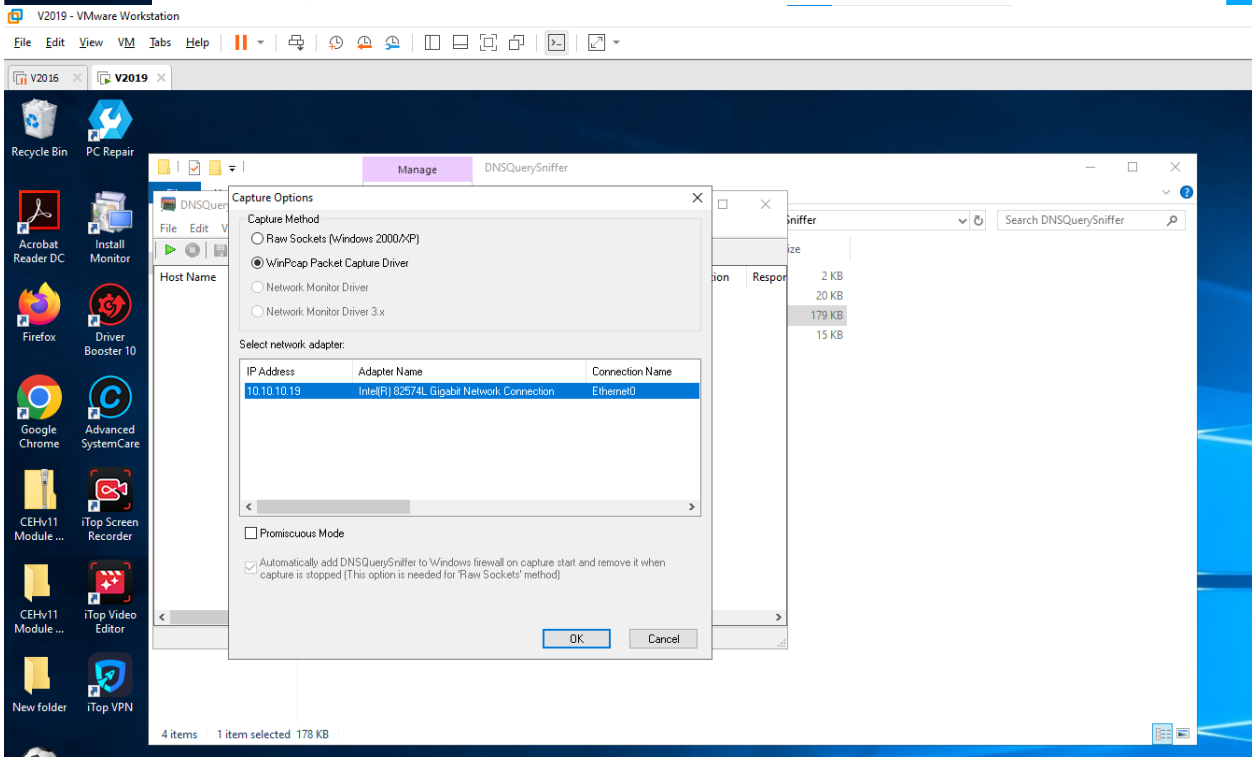

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
Advanced SystemCare
CEHv11 Module ...
iTop Screen Recorder
CEHv11 Module ...
iTop Video Editor
New folder
SoftPerfect Network ...
Advanced SystemCare - Manual Mode
Scanning...
Privacy traces 2539
Junk files 569
Invalid shortcuts 2
Registry entries 269
Registry fragments
Disk optimizations
Antivirus protection
Firewall 1
Outdated drivers
Outdated software 4
Spyware threats
Security holes
Disk errors
62 %
Scanning for security holes
Scanning..
Auto fix
Skip
Stop
Activate Now

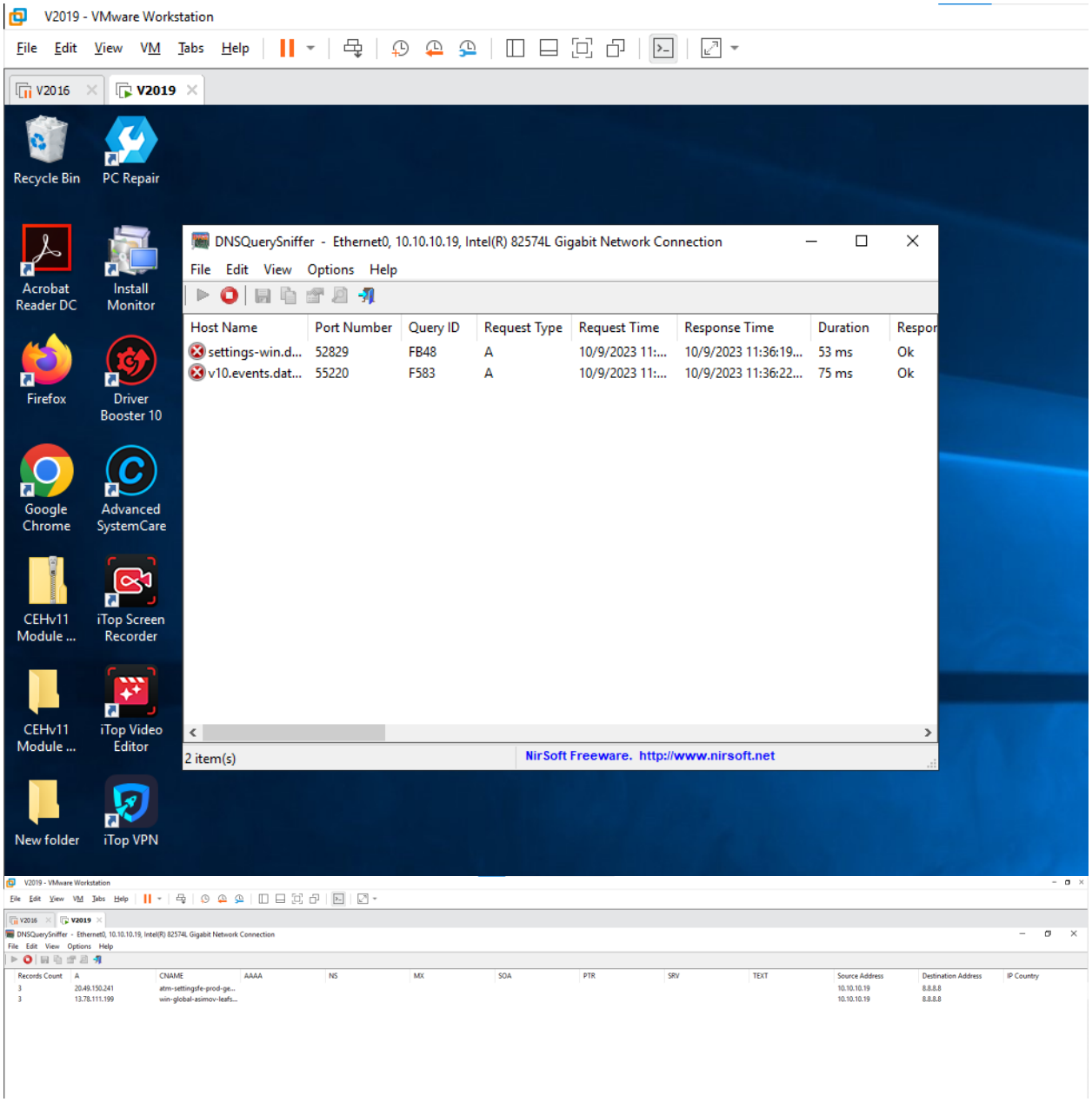


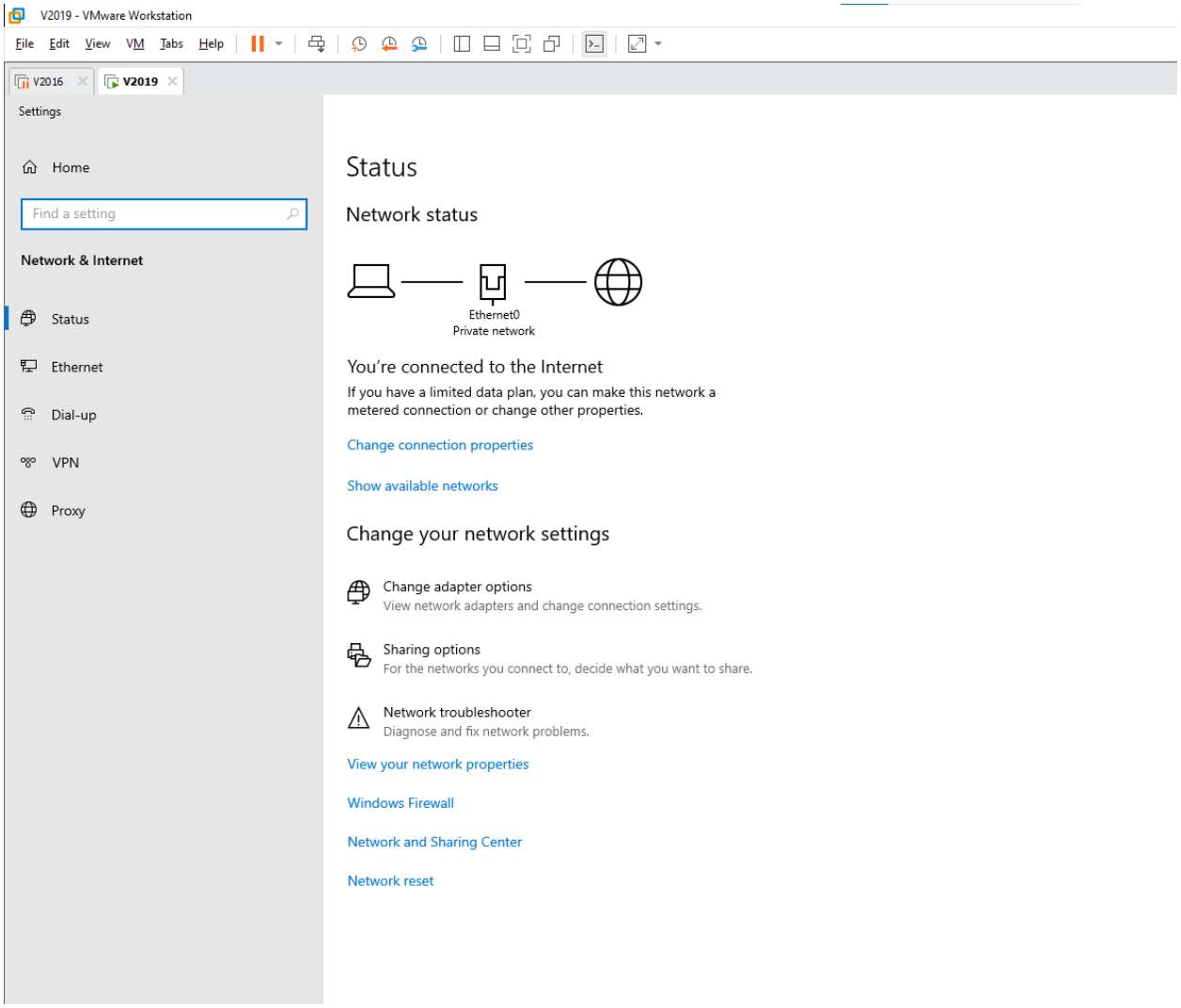
4.9 Perform DNS Monitoring using DNSQuerySniffer

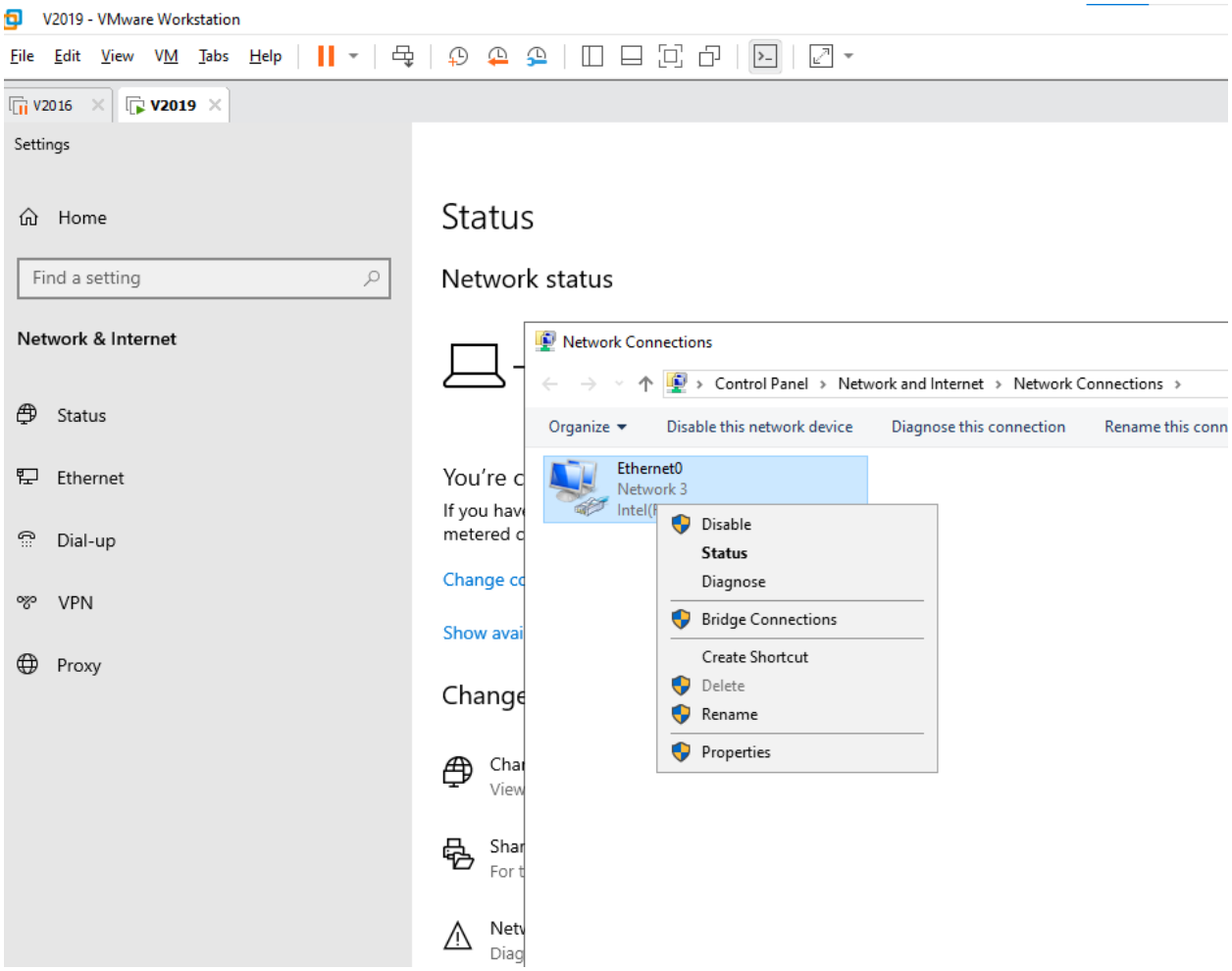
- Open Windows 10

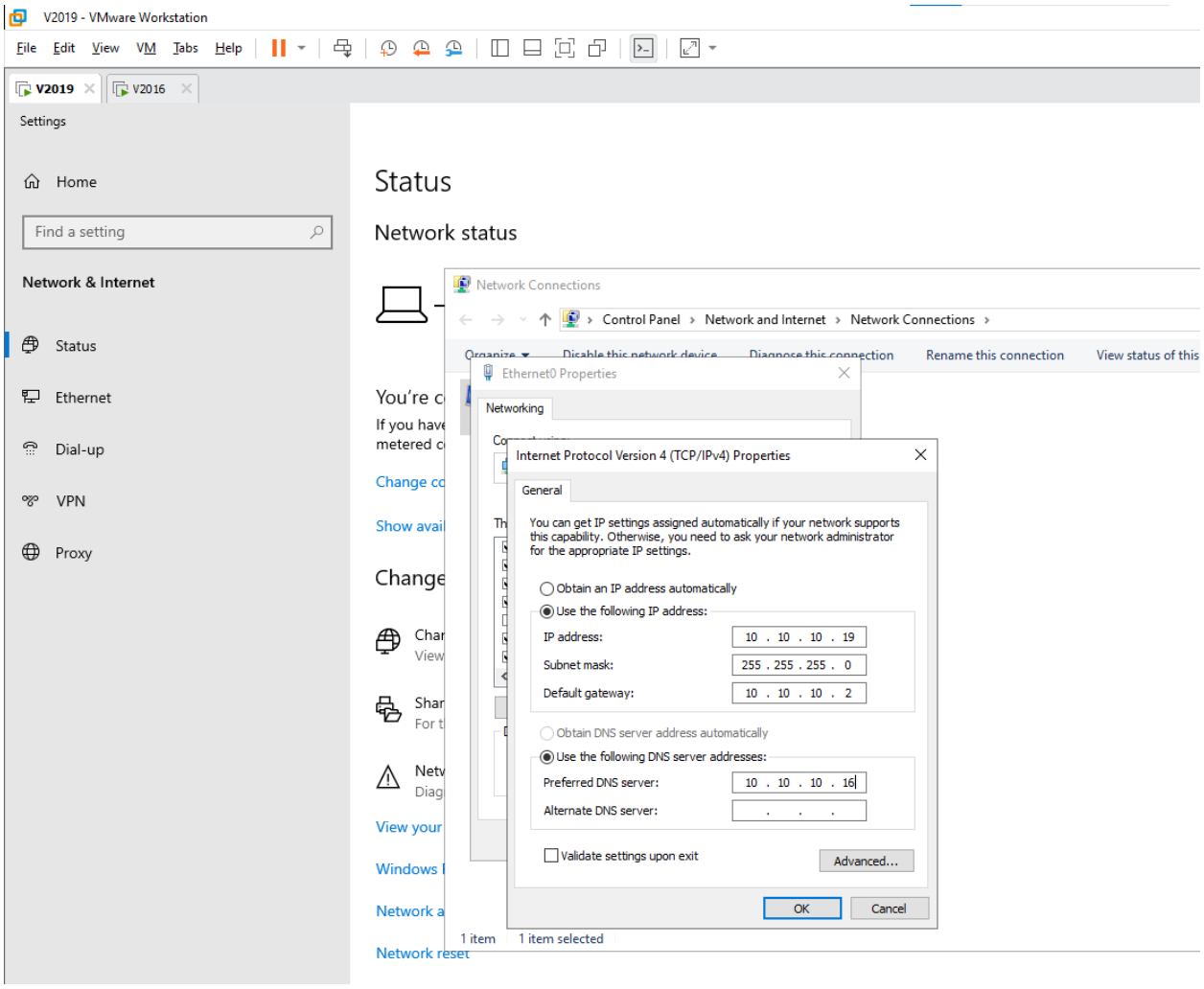

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Advanced SystemCare - Manual Mode
DNSQuerySniffer
File Home Share View
Malware Analysis Tools › Dynamic Malware Analysis Tools › DNS Monitoring Tools › DNSQuerySniffer
Search DNSQuerySniffer
Quick access
Desktop
Downloads
Documents
Pictures
New folder
System32
This PC
Network
Name
Date modified
Type
Size
DNSQuerySniffer.cfg 12/13/2019 7:27 PM CFG File 2 KB
DNSQuerySniffer 6/11/2019 3:31 PM Compiled HTML ... 20 KB
DNSQuerySniffer 6/11/2019 3:31 PM Application 179 KB
readme 6/11/2019 3:31 PM Text Document 15 KB
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
Advanced SystemCare
CEHv11 Module ...
iTop Screen Recorder
CEHv11 Module ...
iTop Video Editor

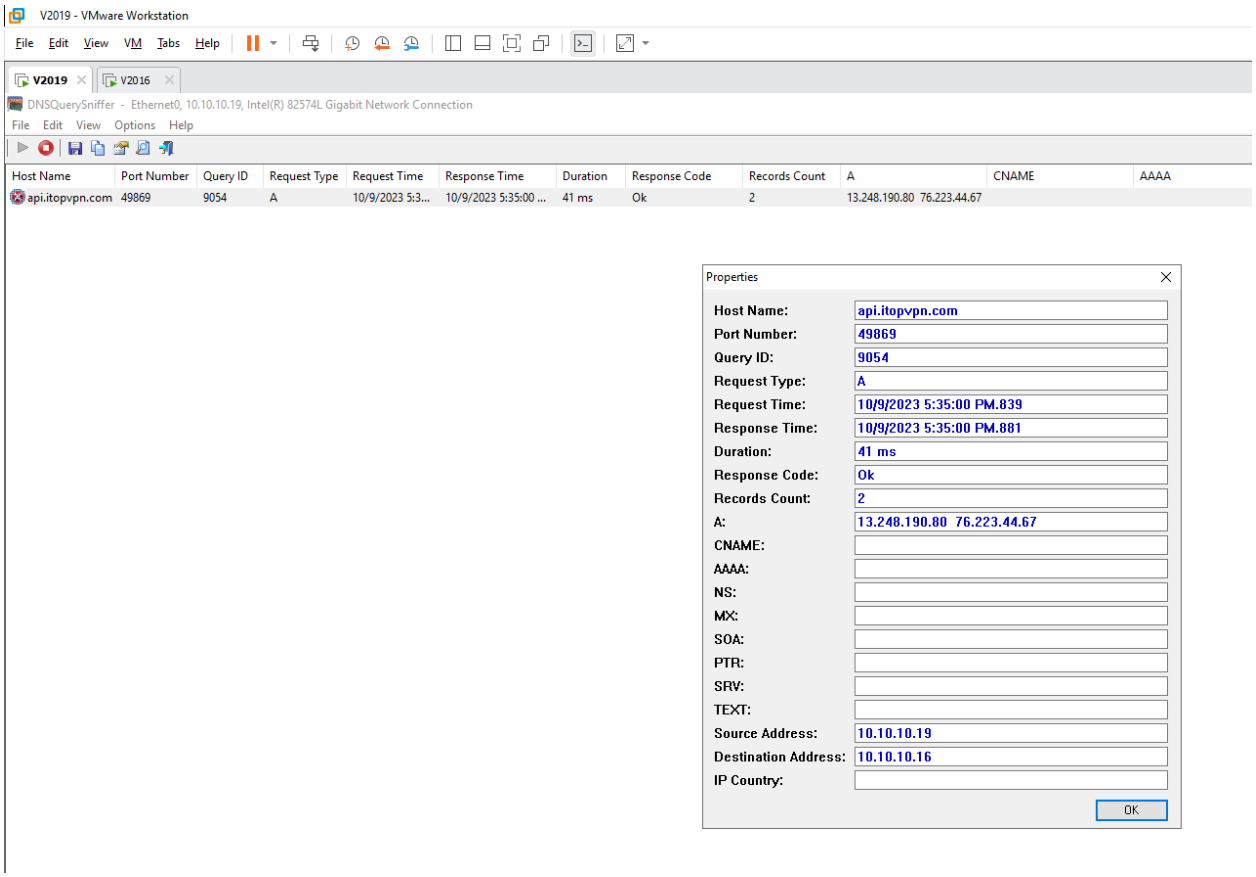

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Manage
DNSQuerySniffer
Capture Options
Capture Method
Raw Sockets (Windows 2000/XP)
WinPcap Packet Capture Driver
Network Monitor Driver
Network Monitor Driver 3.x
Select network adapter:
IP Address
Adapter Name
Connection Name
10.10.10.19
Intel(R) 82574L Gigabit Network Connection
Ethernet0
Promiscuous Mode
Automatically add DNSQuerySniffer to Windows firewall on capture start and remove it when capture is stopped (This option is needed for 'Raw Sockets' method)
OK
Cancel
Host Name
Search DNSQuerySniffer
4 items
1 item selected 178 KB
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
Advanced SystemCare
CEHv11 Module ...
iTop Screen Recorder
CEHv11 Module ...
iTop Video Editor
New folder
iTop VPN


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
PC Repair
Acrobat Reader DC
Install Monitor
Firefox
Driver Booster 10
Google Chrome
Advanced SystemCare
CEHv11 Module ...
iTop Screen Recorder
CEHv11 Module ...
iTop Video Editor
New folder
iTop VPN
DNSQuerySniffer - Ethernet0, 10.10.10.19, Intel(R) 82574L Gigabit Network Connection
File Edit View Options Help
Host Name | Port Number | Query ID | Request Type | Request Time | Response Time | Duration | Respor
settings-win.d... | 52829 | FB48 | A | 10/9/2023 11:... | 10/9/2023 11:36:19... | 53 ms | Ok
v10.events.dat... | 55220 | F583 | A | 10/9/2023 11:... | 10/9/2023 11:36:22... | 75 ms | Ok
2 item(s)
NirSoft Freeware. http://www.nirsoft.net


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
Status
Network status
Ethernet0
Private network
You're connected to the Internet
If you have a limited data plan, you can make this network a metered connection or change other properties.
Change connection properties
Show available networks
Change your network settings
Change adapter options
View network adapters and change connection settings.
Sharing options
For the networks you connect to, decide what you want to share.
Network troubleshooter
Diagnose and fix network problems.
View your network properties
Windows Firewall
Network and Sharing Center
Network reset


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
Status
Network status
Network Connections
Control Panel › Network and Internet › Network Connections ›
Organize
Disable this network device
Diagnose this connection
Rename this conn
Ethernet0
Network 3
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
Status
Network status
Network Connections
Control Panel › Network and Internet › Network Connections ›
Rename this connection
View status of this
Ethernet0 Properties
Networking
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 10 . 10 . 19
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 10 . 2
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 10 . 16
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
1 item
1 item selected
Network reset


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
DNSQuerySniffer - Ethernet0, 10.10.10.19, Intel(R) 82574L Gigabit Network Connection
File Edit View Options Help
Host Name Port Number Query ID Request Type Request Time Response Time Duration Response Code Records Count A CNAME AAAA
api.itopvpn.com 49869 9054 A 10/9/2023 5:3... 10/9/2023 5:35:00 ... 41 ms Ok 2 13.248.190.80 76.223.44.67
Properties
Host Name: api.itopvpn.com
Port Number: 49869
Query ID: 9054
Request Type: A
Request Time: 10/9/2023 5:35:00 PM.839
Response Time: 10/9/2023 5:35:00 PM.881
Duration: 41 ms
Response Code: Ok
Records Count: 2
A: 13.248.190.80 76.223.44.67
CNAME:
AAAA:
NS:
MX:
SOA:
PTR:
SRV:
TEXT:
Source Address: 10.10.10.19
Destination Address: 10.10.10.16
IP Country:
OK