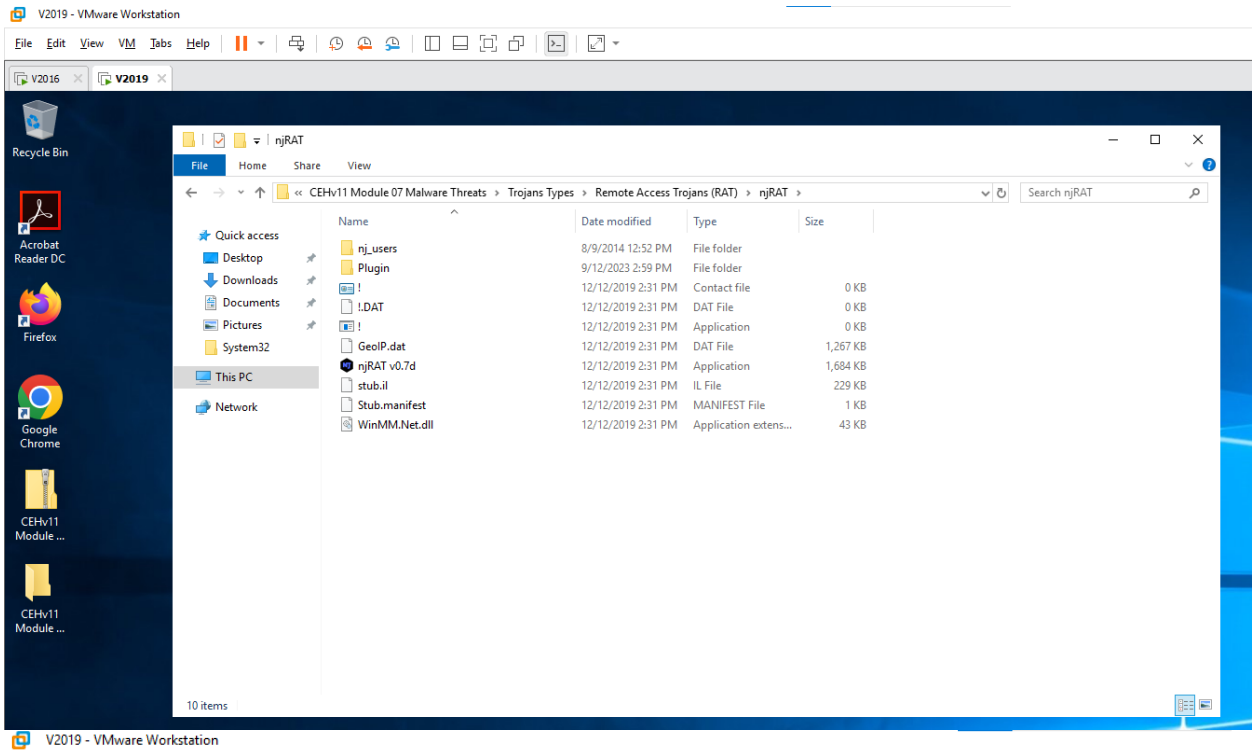
# Lab 9: Malware Threats

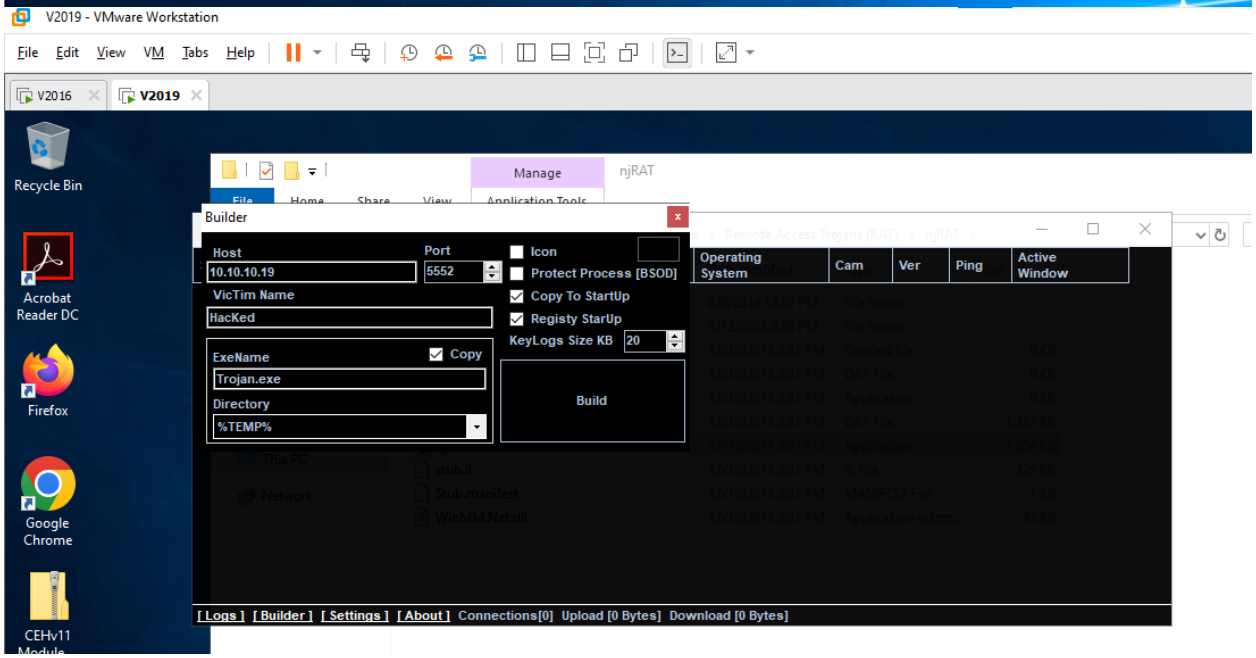
**Course Name**: Ethical Hacking and Offensive Security(HOD401)
**Student Name**: Nguyễn Trần Vinh – SE160258
**Instructor Name**: Mai Hoàng Đỉnh
**Lab Due Date**: 07/10/2023

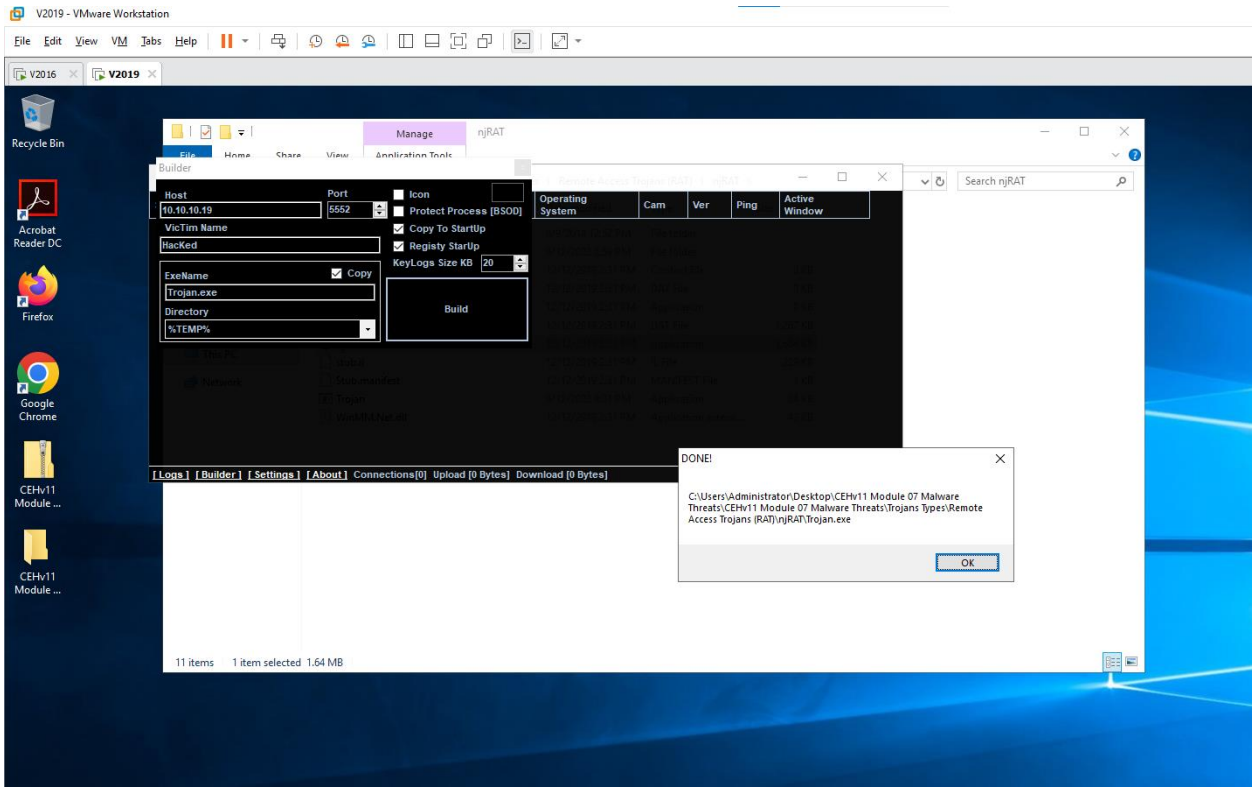
## 4. Perform Dynamic Malware Analysis

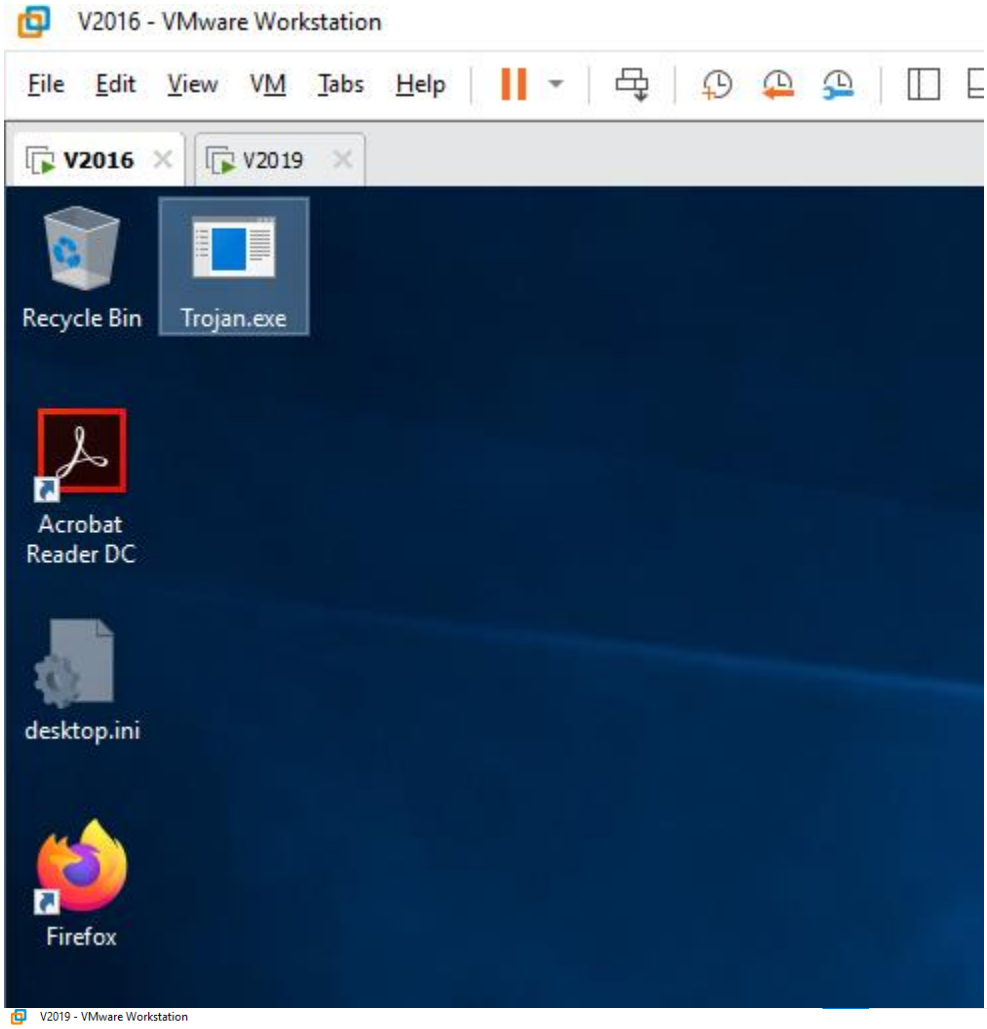
4.1 Perform Port Monitoring using TCPView and CurrPorts

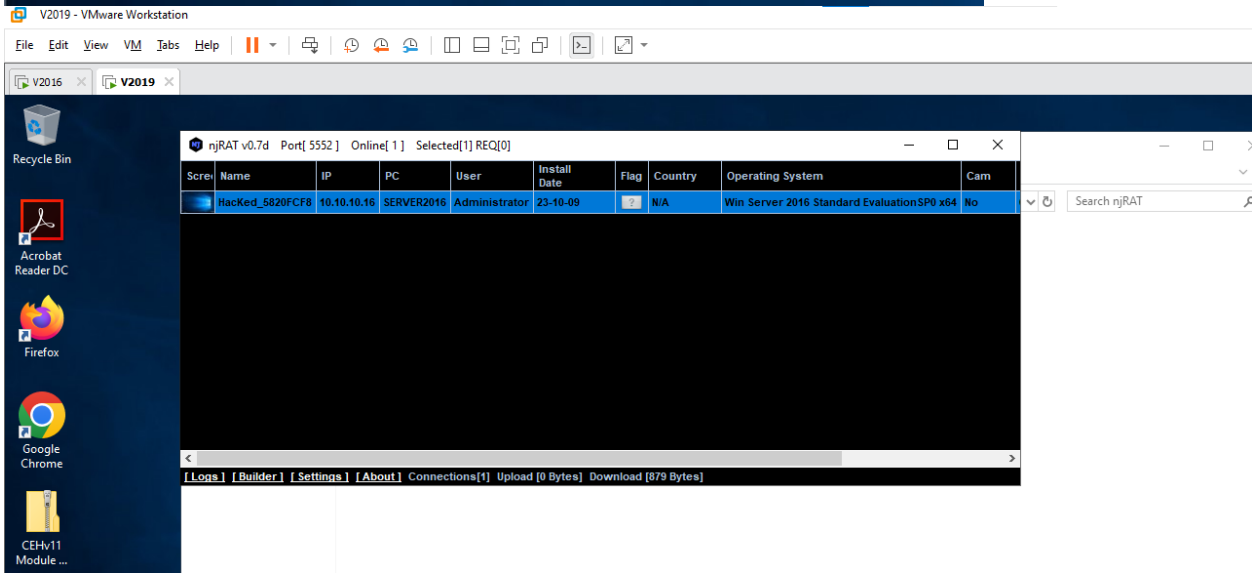
- Open Windows 10, Windows Server 2016

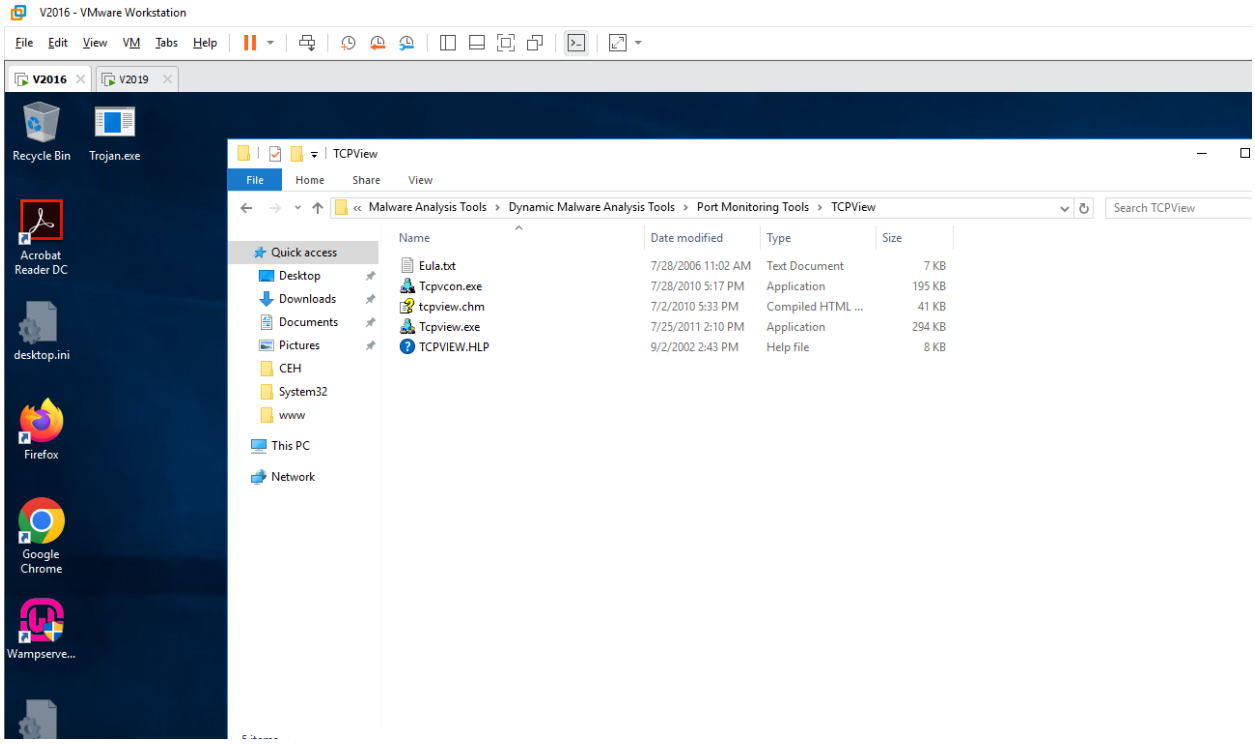

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
njRAT
File Home Share View
« CEHv11 Module 07 Malware Threats › Trojans Types › Remote Access Trojans (RAT) › njRAT ›
Search njRAT
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name Date modified Type Size
nj_users 8/9/2014 12:52 PM File folder
Plugin 9/12/2023 2:59 PM File folder
! 12/12/2019 2:31 PM Contact file 0 KB
!.DAT 12/12/2019 2:31 PM DAT File 0 KB
! 12/12/2019 2:31 PM Application 0 KB
GeoIP.dat 12/12/2019 2:31 PM DAT File 1,267 KB
njRAT v0.7d 12/12/2019 2:31 PM Application 1,684 KB
stub.il 12/12/2019 2:31 PM IL File 229 KB
Stub.manifest 12/12/2019 2:31 PM MANIFEST File 1 KB
WinMM.Net.dll 12/12/2019 2:31 PM Application extens... 43 KB
10 items

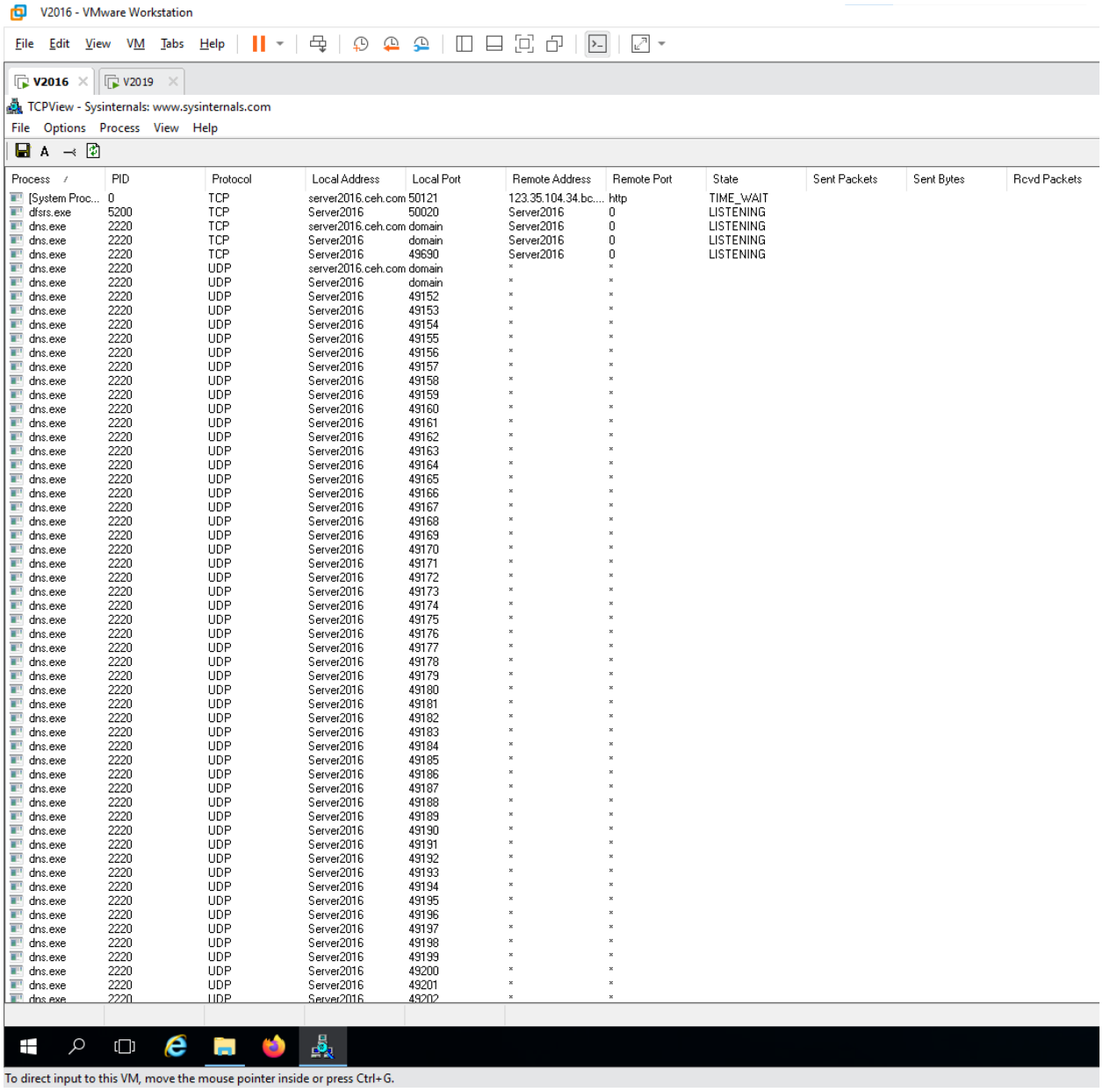

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module
Manage
njRAT
Builder
Host
10.10.10.19
Port
5552
Icon
Protect Process [BSOD]
Copy To StartUp
Regisity StarUp
KeyLogs Size KB
20
VicTim Name
HacKed
ExeName
Copy
Trojan.exe
Directory
%TEMP%
Build
Operating System
Cam
Ver
Ping
Active Window
[ Logs ] [ Builder ] [ Settings ] [ About ] Connections[0] Upload [0 Bytes] Download [0 Bytes]


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Manage
njRAT
Builder
Host
10.10.10.19
Port
5552
Icon
Protect Process [BSOD]
VicTim Name
HacKed
Copy To StartUp
Registy StartUp
KeyLogs Size KB
20
ExeName
Copy
Trojan.exe
Directory
%TEMP%
Build
Operating System
Cam
Ver
Ping
Active Window
Search njRAT
[Logs] [Builder] [Settings] [About] Connections[0] Upload [0 Bytes] Download [0 Bytes]
DONE!
C:\Users\Administrator\Desktop\CEHv11 Module 07 Malware Threats\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT\Trojan.exe
OK
11 items
1 item selected 1.64 MB

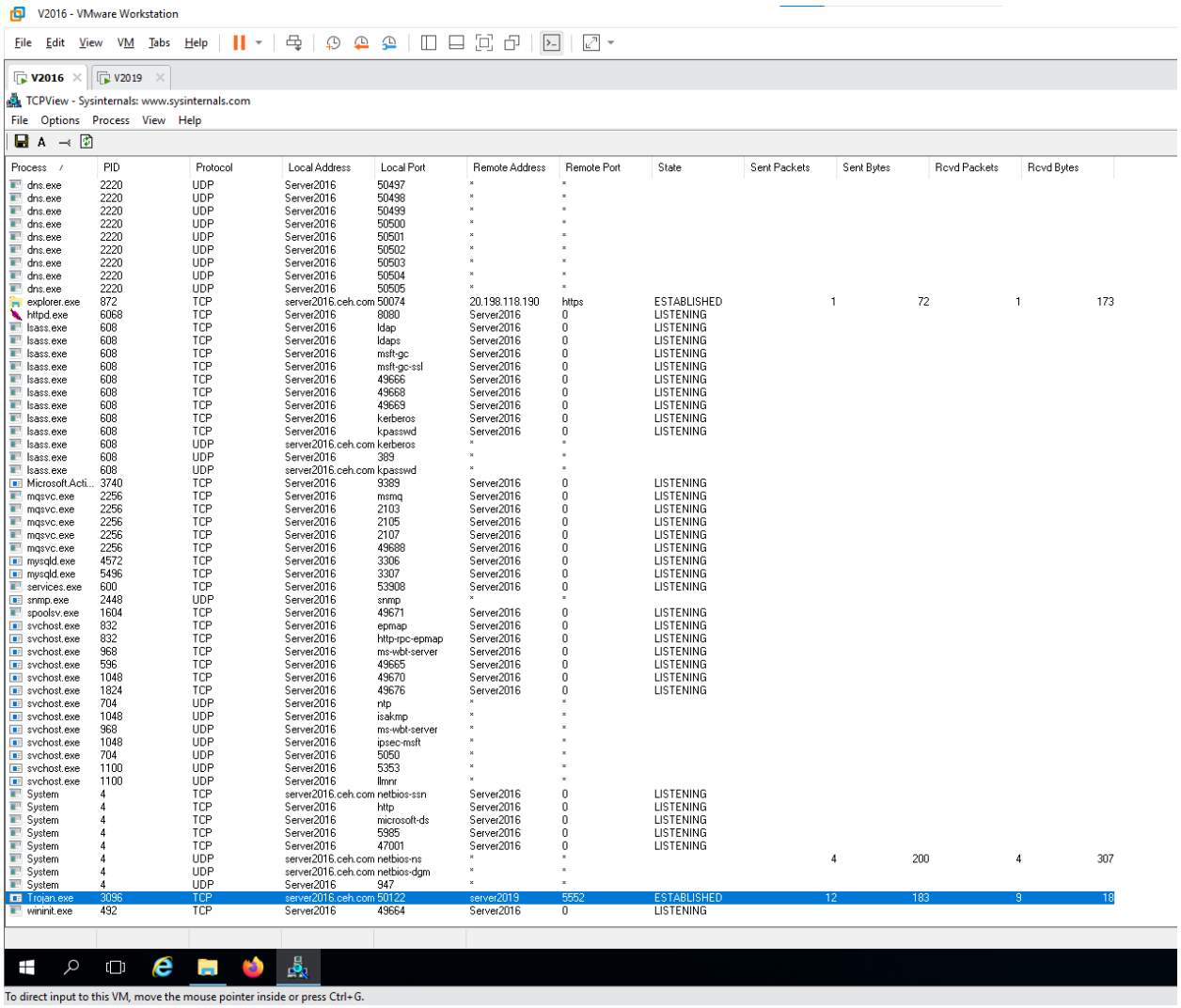

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Trojan.exe
Acrobat Reader DC
desktop.ini
Firefox


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
njRAT v0.7d Port[ 5552 ] Online[ 1 ] Selected[1] REQ[0]
Scre
Name
IP
PC
User
Install Date
Flag
Country
Operating System
Cam
HacKed_5820FCF8
10.10.10.16
SERVER2016
Administrator
23-10-09
N/A
Win Server 2016 Standard Evaluation SP0 x64
No
Search njRAT
[ Logs ] [ Builder ] [ Settings ] [ About ] Connections[1] Upload [0 Bytes] Download [879 Bytes]

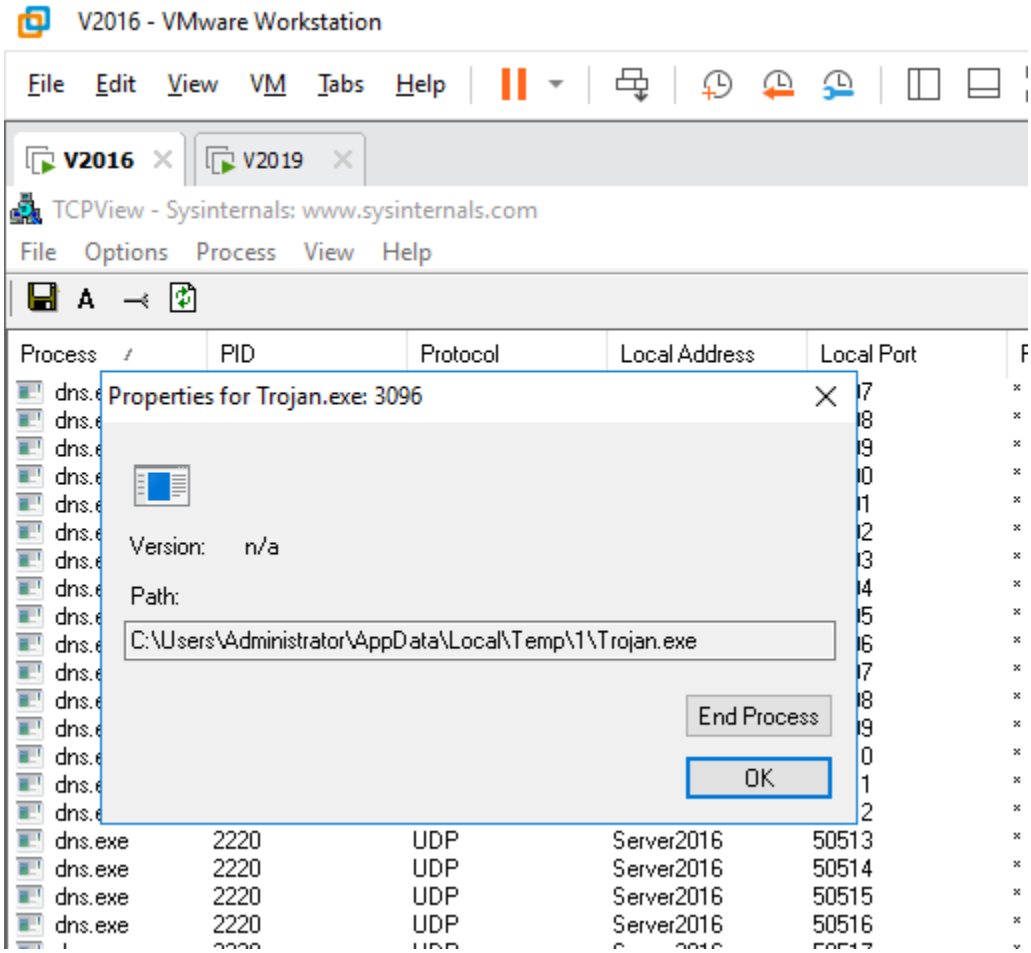

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Trojan.exe
Acrobat Reader DC
desktop.ini
Firefox
Google Chrome
Wampserve...
TCPView
File Home Share View
Malware Analysis Tools › Dynamic Malware Analysis Tools › Port Monitoring Tools › TCPView
Search TCPView
Quick access
Desktop
Downloads
Documents
Pictures
CEH
System32
www
This PC
Network
Name
Date modified
Type
Size
Eula.txt 7/28/2006 11:02 AM Text Document 7 KB
Tcpvcon.exe 7/28/2010 5:17 PM Application 195 KB
tcpview.chm 7/2/2010 5:33 PM Compiled HTML ... 41 KB
Tcpview.exe 7/25/2011 2:10 PM Application 294 KB
TCPVIEW.HLP 9/2/2002 2:43 PM Help file 8 KB

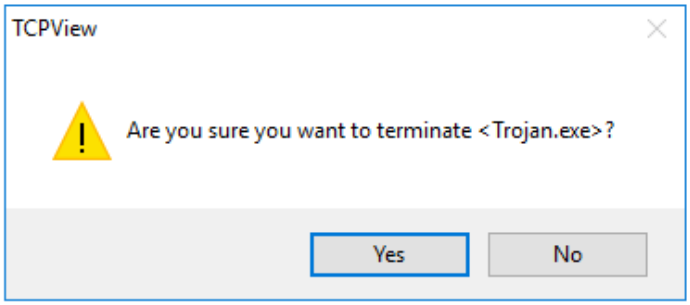


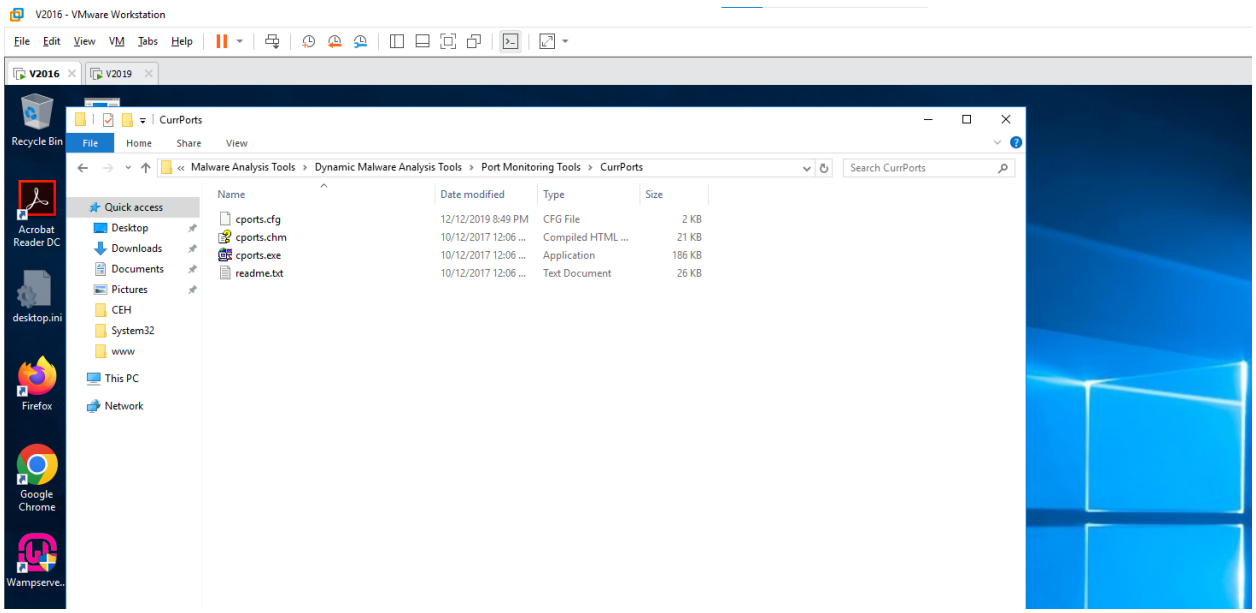

| Process | PID | Protocol | Local Address | Local Port | Remote Address | Remote Port | State | Sent Packets | Sent Bytes | Rcvd Packets |
|---|---|---|---|---|---|---|---|---|---|---|
| [System Proc... | 0 | TCP | server2016.ceh.com | 50121 | 123.35.104.34.bc.... | http | TIME_WAIT | | | |
| dfsrs.exe | 5200 | TCP | Server2016 | 50020 | Server2016 | 0 | LISTENING | | | |
| dns.exe | 2220 | TCP | server2016.ceh.com | domain | Server2016 | 0 | LISTENING | | | |
| dns.exe | 2220 | TCP | Server2016 | domain | Server2016 | 0 | LISTENING | | | |
| dns.exe | 2220 | TCP | Server2016 | 49690 | Server2016 | 0 | LISTENING | | | |
| dns.exe | 2220 | UDP | server2016.ceh.com | domain | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | domain | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49152 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49153 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49154 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49155 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49156 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49157 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49158 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49159 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49160 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49161 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49162 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49163 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49164 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49165 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49166 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49167 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49168 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49169 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49170 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49171 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49172 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49173 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49174 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49175 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49176 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49177 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49178 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49179 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49180 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49181 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49182 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49183 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49184 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49185 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49186 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49187 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49188 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49189 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49190 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49191 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49192 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49193 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49194 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49195 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49196 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49197 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49198 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49199 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49200 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49201 | * | * | | | | |
| dns.exe | 2220 | UDP | Server2016 | 49202 | * | * | | | | |

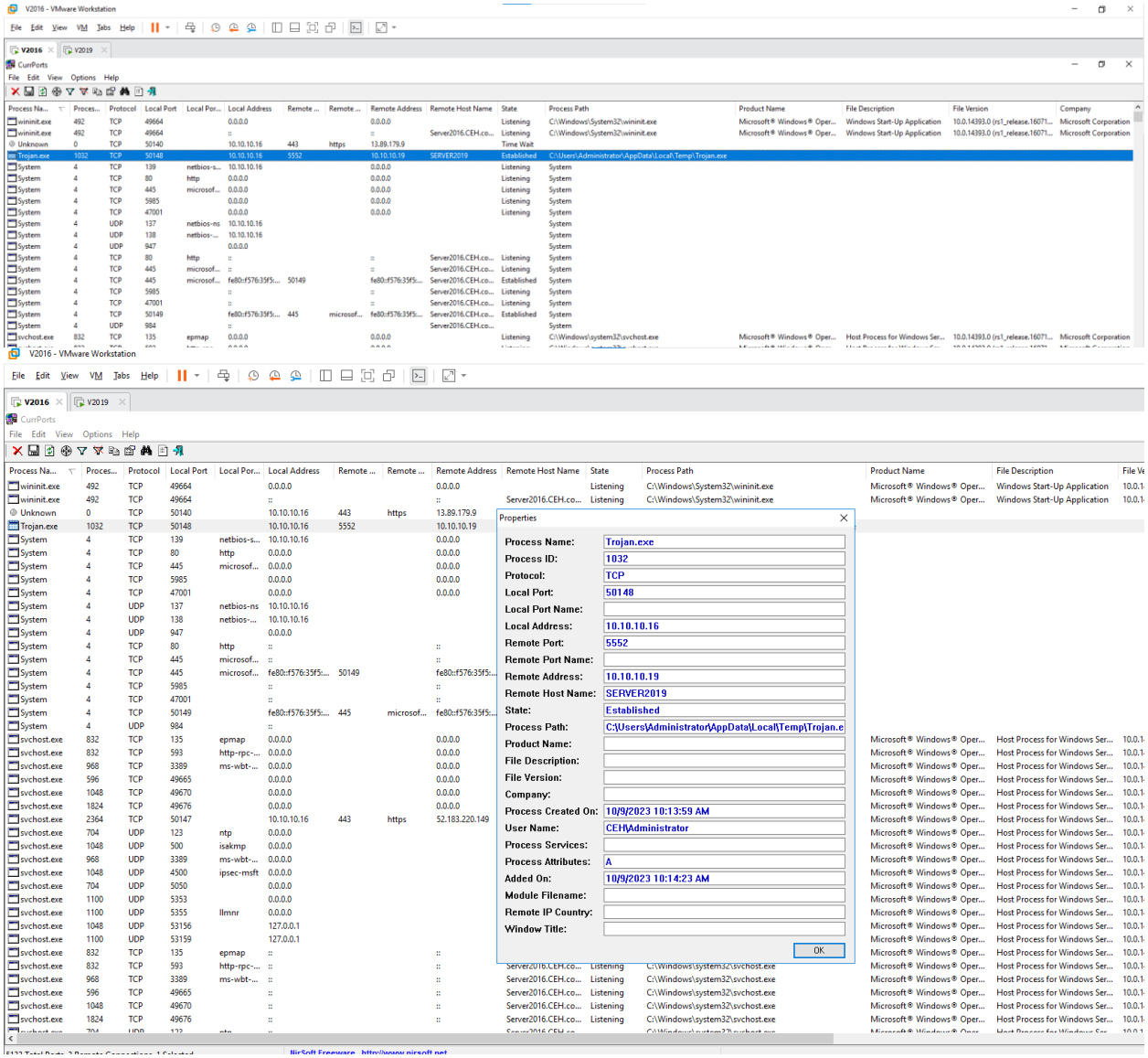



| Process | PID | Protocol | Local Address | Local Port | Remote Address | Remote Port | State | Sent Packets | Sent Bytes | Rcvd Packets | Rcvd Bytes |
|---|---|---|---|---|---|---|---|---|---|---|---|
| dns.exe | 2220 | UDP | Server2016 | 50497 | * | * | | | | | |
| dns.exe | 2220 | UDP | Server2016 | 50498 | * | * | | | | | |
| dns.exe | 2220 | UDP | Server2016 | 50499 | * | * | | | | | |
| dns.exe | 2220 | UDP | Server2016 | 50500 | * | * | | | | | |
| dns.exe | 2220 | UDP | Server2016 | 50501 | * | * | | | | | |
| dns.exe | 2220 | UDP | Server2016 | 50502 | * | * | | | | | |
| dns.exe | 2220 | UDP | Server2016 | 50503 | * | * | | | | | |
| dns.exe | 2220 | UDP | Server2016 | 50504 | * | * | | | | | |
| dns.exe | 2220 | UDP | Server2016 | 50505 | * | * | | | | | |
| explorer.exe | 872 | TCP | server2016.ceh.com | 50074 | 20.198.118.190 | https | ESTABLISHED | 1 | 72 | 1 | 173 |
| httpd.exe | 6068 | TCP | Server2016 | 8080 | Server2016 | 0 | LISTENING | | | | |
| lsass.exe | 608 | TCP | Server2016 | ldap | Server2016 | 0 | LISTENING | | | | |
| lsass.exe | 608 | TCP | Server2016 | ldaps | Server2016 | 0 | LISTENING | | | | |
| lsass.exe | 608 | TCP | Server2016 | msft-gc | Server2016 | 0 | LISTENING | | | | |
| lsass.exe | 608 | TCP | Server2016 | msft-gc-ssl | Server2016 | 0 | LISTENING | | | | |
| lsass.exe | 608 | TCP | Server2016 | 49666 | Server2016 | 0 | LISTENING | | | | |
| lsass.exe | 608 | TCP | Server2016 | 49668 | Server2016 | 0 | LISTENING | | | | |
| lsass.exe | 608 | TCP | Server2016 | 49669 | Server2016 | 0 | LISTENING | | | | |
| lsass.exe | 608 | TCP | Server2016 | kerberos | Server2016 | 0 | LISTENING | | | | |
| lsass.exe | 608 | TCP | Server2016 | kpasswd | Server2016 | 0 | LISTENING | | | | |
| lsass.exe | 608 | UDP | server2016.ceh.com | kerberos | * | * | | | | | |
| lsass.exe | 608 | UDP | Server2016 | 389 | * | * | | | | | |
| lsass.exe | 608 | UDP | server2016.ceh.com | kpasswd | * | * | | | | | |
| Microsoft.Acti... | 3740 | TCP | Server2016 | 9389 | Server2016 | 0 | LISTENING | | | | |
| mqsvc.exe | 2256 | TCP | Server2016 | msmq | Server2016 | 0 | LISTENING | | | | |
| mqsvc.exe | 2256 | TCP | Server2016 | 2103 | Server2016 | 0 | LISTENING | | | | |
| mqsvc.exe | 2256 | TCP | Server2016 | 2105 | Server2016 | 0 | LISTENING | | | | |
| mqsvc.exe | 2256 | TCP | Server2016 | 2107 | Server2016 | 0 | LISTENING | | | | |
| mqsvc.exe | 2256 | TCP | Server2016 | 49688 | Server2016 | 0 | LISTENING | | | | |
| mysqld.exe | 4572 | TCP | Server2016 | 3306 | Server2016 | 0 | LISTENING | | | | |
| mysqld.exe | 5496 | TCP | Server2016 | 3307 | Server2016 | 0 | LISTENING | | | | |
| services.exe | 600 | TCP | Server2016 | 53908 | Server2016 | 0 | LISTENING | | | | |
| snmp.exe | 2448 | UDP | Server2016 | snmp | * | * | | | | | |
| spoolsv.exe | 1604 | TCP | Server2016 | 49671 | Server2016 | 0 | LISTENING | | | | |
| svchost.exe | 832 | TCP | Server2016 | epmap | Server2016 | 0 | LISTENING | | | | |
| svchost.exe | 832 | TCP | Server2016 | http-rpc-epmap | Server2016 | 0 | LISTENING | | | | |
| svchost.exe | 968 | TCP | Server2016 | ms-wbt-server | Server2016 | 0 | LISTENING | | | | |
| svchost.exe | 596 | TCP | Server2016 | 49665 | Server2016 | 0 | LISTENING | | | | |
| svchost.exe | 1048 | TCP | Server2016 | 49670 | Server2016 | 0 | LISTENING | | | | |
| svchost.exe | 1824 | TCP | Server2016 | 49676 | Server2016 | 0 | LISTENING | | | | |
| svchost.exe | 704 | UDP | Server2016 | ntp | * | * | | | | | |
| svchost.exe | 1048 | UDP | Server2016 | isakmp | * | * | | | | | |
| svchost.exe | 968 | UDP | Server2016 | ms-wbt-server | * | * | | | | | |
| svchost.exe | 1048 | UDP | Server2016 | ipsec-msft | * | * | | | | | |
| svchost.exe | 704 | UDP | Server2016 | 5050 | * | * | | | | | |
| svchost.exe | 1100 | UDP | Server2016 | 5353 | * | * | | | | | |
| svchost.exe | 1100 | UDP | Server2016 | llmnr | * | * | | | | | |
| System | 4 | TCP | server2016.ceh.com | netbios-ssn | Server2016 | 0 | LISTENING | | | | |
| System | 4 | TCP | Server2016 | http | Server2016 | 0 | LISTENING | | | | |
| System | 4 | TCP | Server2016 | microsoft-ds | Server2016 | 0 | LISTENING | | | | |
| System | 4 | TCP | Server2016 | 5985 | Server2016 | 0 | LISTENING | | | | |
| System | 4 | TCP | Server2016 | 47001 | Server2016 | 0 | LISTENING | | | | |
| System | 4 | UDP | server2016.ceh.com | netbios-ns | * | * | | 4 | 200 | 4 | 307 |
| System | 4 | UDP | server2016.ceh.com | netbios-dgm | * | * | | | | | |
| System | 4 | UDP | Server2016 | 947 | * | * | | | | | |
| Trojan.exe | 3096 | TCP | server2016.ceh.com | 50122 | server2019 | 5552 | ESTABLISHED | 12 | 183 | 9 | 18 |
| wininit.exe | 492 | TCP | Server2016 | 49664 | Server2016 | 0 | LISTENING | | | | |

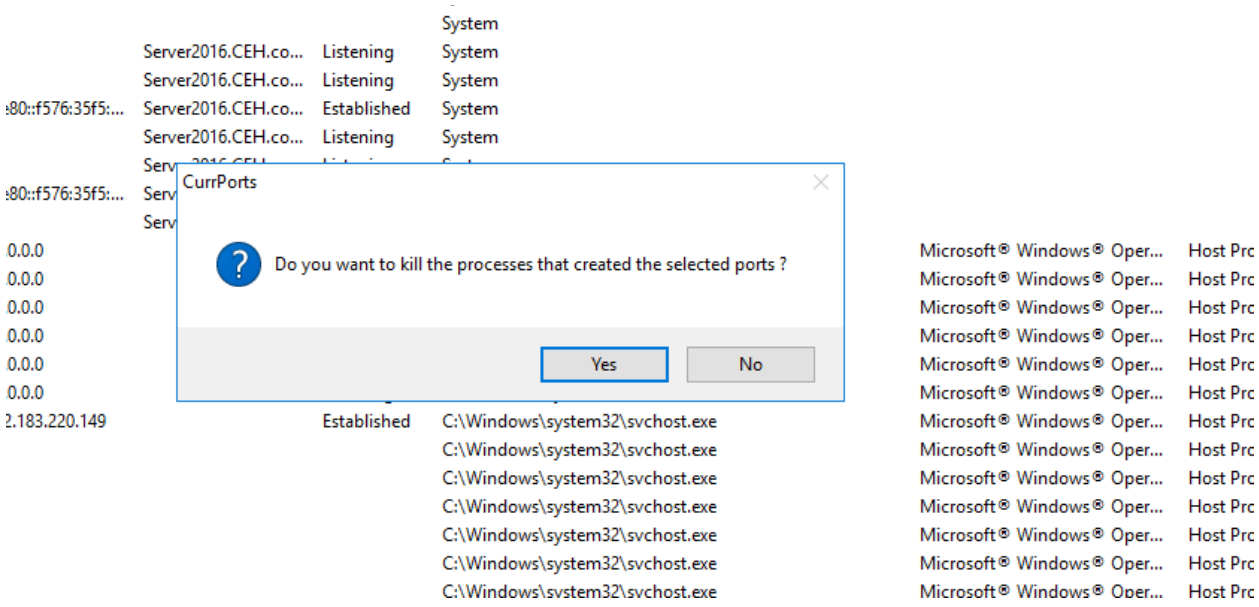

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process PID Protocol Local Address Local Port
Properties for Trojan.exe: 3096
Version: n/a
Path:
C:\Users\Administrator\AppData\Local\Temp\1\Trojan.exe
End Process
OK
dns.exe 2220 UDP Server2016 50513
dns.exe 2220 UDP Server2016 50514
dns.exe 2220 UDP Server2016 50515
dns.exe 2220 UDP Server2016 50516


TCPView
Are you sure you want to terminate <Trojan.exe>?
Yes
No

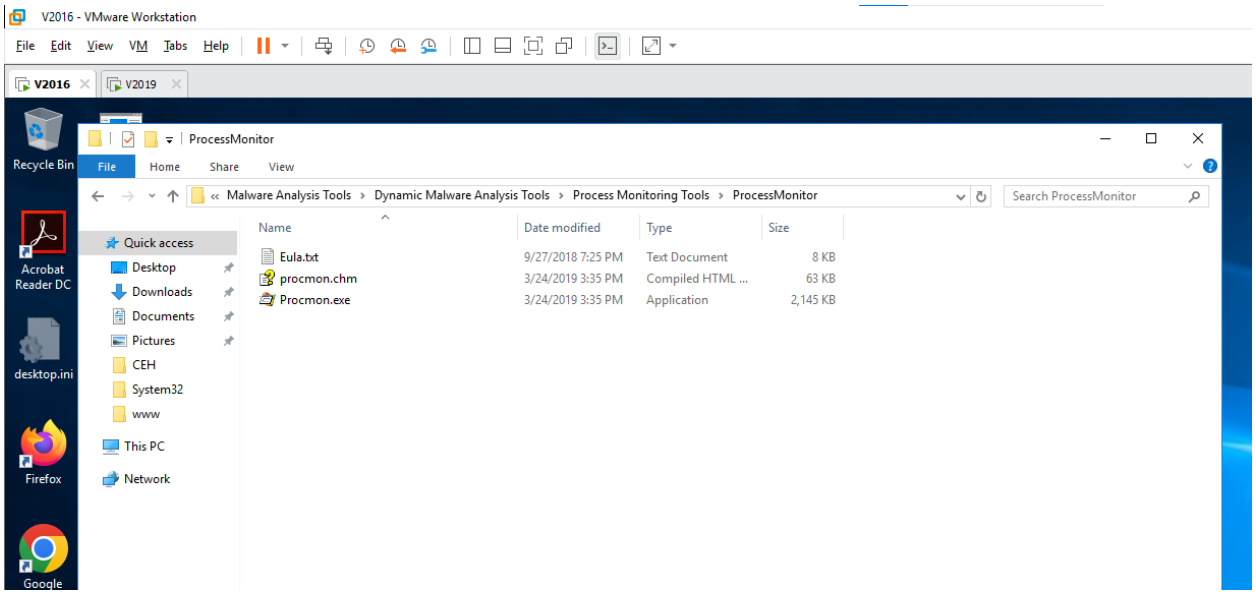

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
desktop.ini
Firefox
Google Chrome
Wampserve...
CurrPorts
File Home Share View
Malware Analysis Tools › Dynamic Malware Analysis Tools › Port Monitoring Tools › CurrPorts
Search CurrPorts
Quick access
Desktop
Downloads
Documents
Pictures
CEH
System32
www
This PC
Network
Name
Date modified
Type
Size
cports.cfg 12/12/2019 8:49 PM CFG File 2 KB
cports.chm 10/12/2017 12:06 ... Compiled HTML ... 21 KB
cports.exe 10/12/2017 12:06 ... Application 186 KB
readme.txt 10/12/2017 12:06 ... Text Document 26 KB

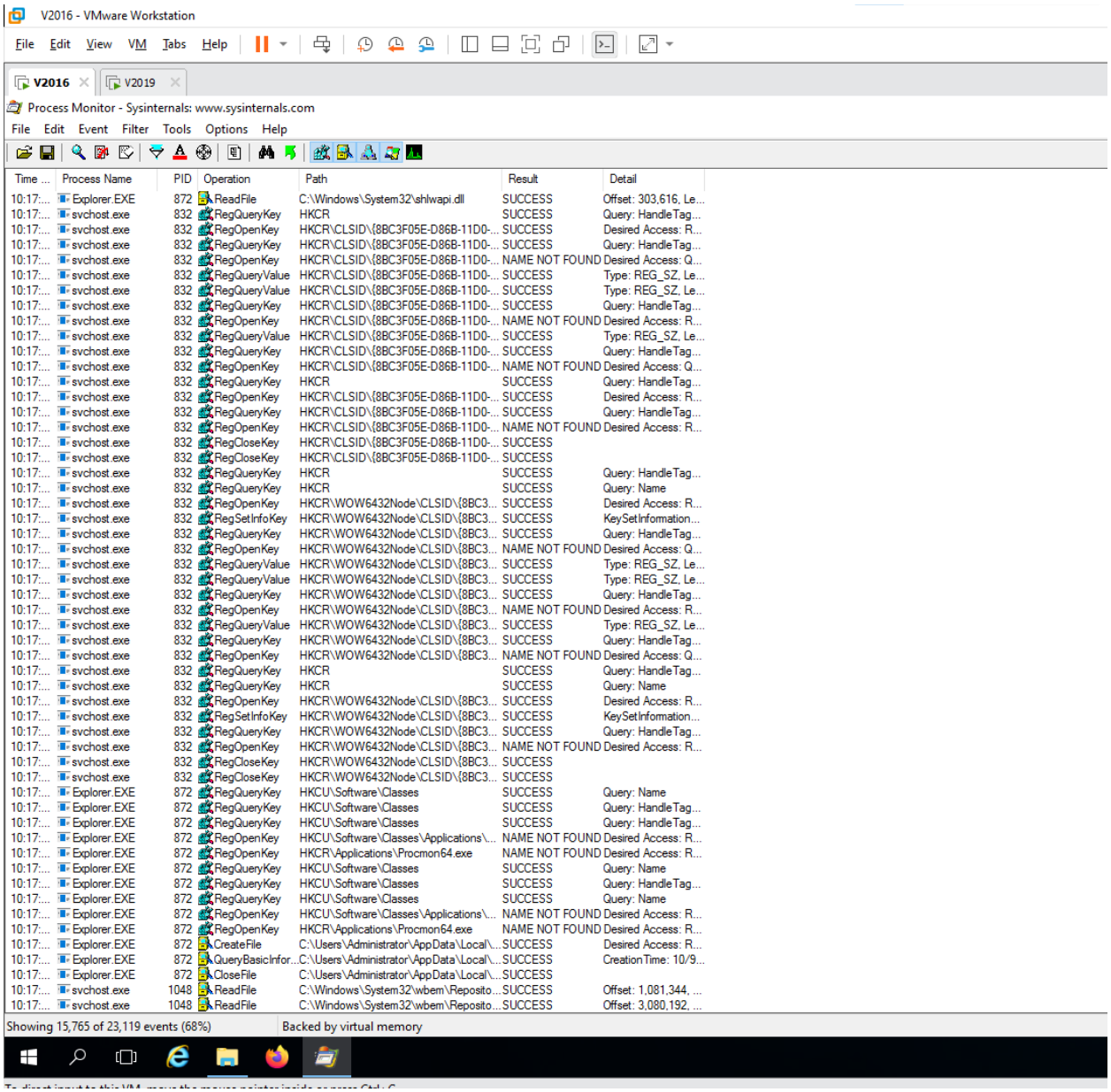

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
CurrPorts
File Edit View Options Help
Process Na... Proces... Protocol Local Port Local Por... Local Address Remote ... Remote ... Remote Address Remote Host Name State Process Path Product Name File Description File Version Company
wininit.exe 492 TCP 49664 0.0.0.0 0.0.0.0 Listening C:\Windows\System32\wininit.exe Microsoft® Windows® Oper... Windows Start-Up Application 10.0.14393.0 (rs1_release.16071... Microsoft Corporation
wininit.exe 492 TCP 49664 :: :: Server2016.CEH.co... Listening C:\Windows\System32\wininit.exe Microsoft® Windows® Oper... Windows Start-Up Application 10.0.14393.0 (rs1_release.16071... Microsoft Corporation
Unknown 0 TCP 50140 10.10.10.16 443 https 13.89.179.9 Time Wait
Trojan.exe 1032 TCP 50148 10.10.10.16 5552 10.10.10.19 SERVER2019 Established C:\Users\Administrator\AppData\Local\Temp\Trojan.exe
System 4 TCP 139 netbios-s... 10.10.10.16 0.0.0.0 Listening System
System 4 TCP 80 http 0.0.0.0 0.0.0.0 Listening System
System 4 TCP 445 microsof... 0.0.0.0 0.0.0.0 Listening System
System 4 TCP 5985 0.0.0.0 0.0.0.0 Listening System
System 4 TCP 47001 0.0.0.0 0.0.0.0 Listening System
System 4 UDP 137 netbios-ns 10.10.10.16 System
System 4 UDP 138 netbios-... 10.10.10.16 System
System 4 UDP 947 0.0.0.0 System
System 4 TCP 80 http :: :: Server2016.CEH.co... Listening System
System 4 TCP 445 microsof... :: :: Server2016.CEH.co... Listening System
System 4 TCP 445 microsof... fe80::f576:35f5:... 50149 fe80::f576:35f5:... Server2016.CEH.co... Established System
System 4 TCP 5985 :: :: Server2016.CEH.co... Listening System
System 4 TCP 47001 :: :: Server2016.CEH.co... Listening System
System 4 TCP 50149 fe80::f576:35f5:... 445 microsof... fe80::f576:35f5:... Server2016.CEH.co... Established System
System 4 UDP 984 :: Server2016.CEH.co... System
svchost.exe 832 TCP 135 epmap 0.0.0.0 0.0.0.0 Listening C:\Windows\system32\svchost.exe Microsoft® Windows® Oper... Host Process for Windows Ser... 10.0.14393.0 (rs1_release.16071... Microsoft Corporation

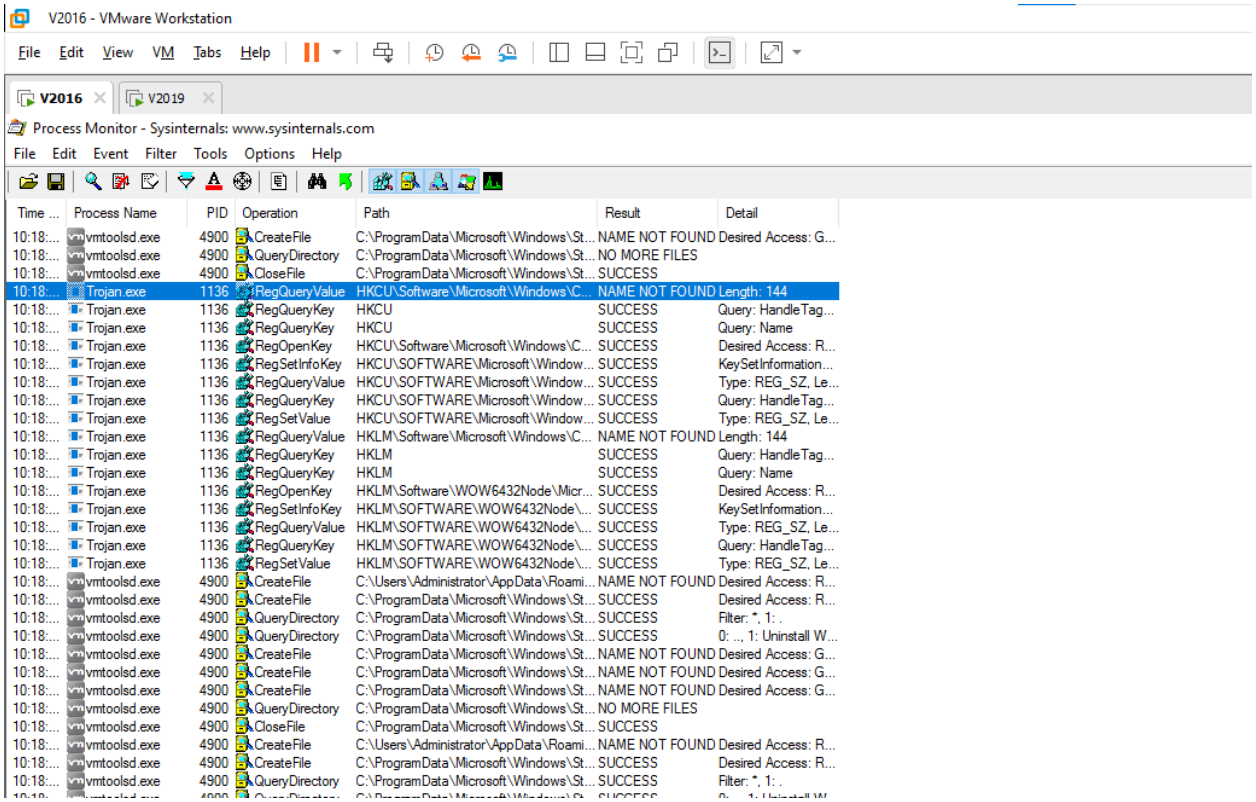

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
CurrPorts
File Edit View Options Help
Properties
Process Name: Trojan.exe
Process ID: 1032
Protocol: TCP
Local Port: 50148
Local Port Name:
Local Address: 10.10.10.16
Remote Port: 5552
Remote Port Name:
Remote Address: 10.10.10.19
Remote Host Name: SERVER2019
State: Established
Process Path: C:\Users\Administrator\AppData\Local\Temp\Trojan.e
Product Name:
File Description:
File Version:
Company:
Process Created On: 10/9/2023 10:13:59 AM
User Name: CEH\Administrator
Process Services:
Process Attributes: A
Added On: 10/9/2023 10:14:23 AM
Module Filename:
Remote IP Country:
Window Title:
OK

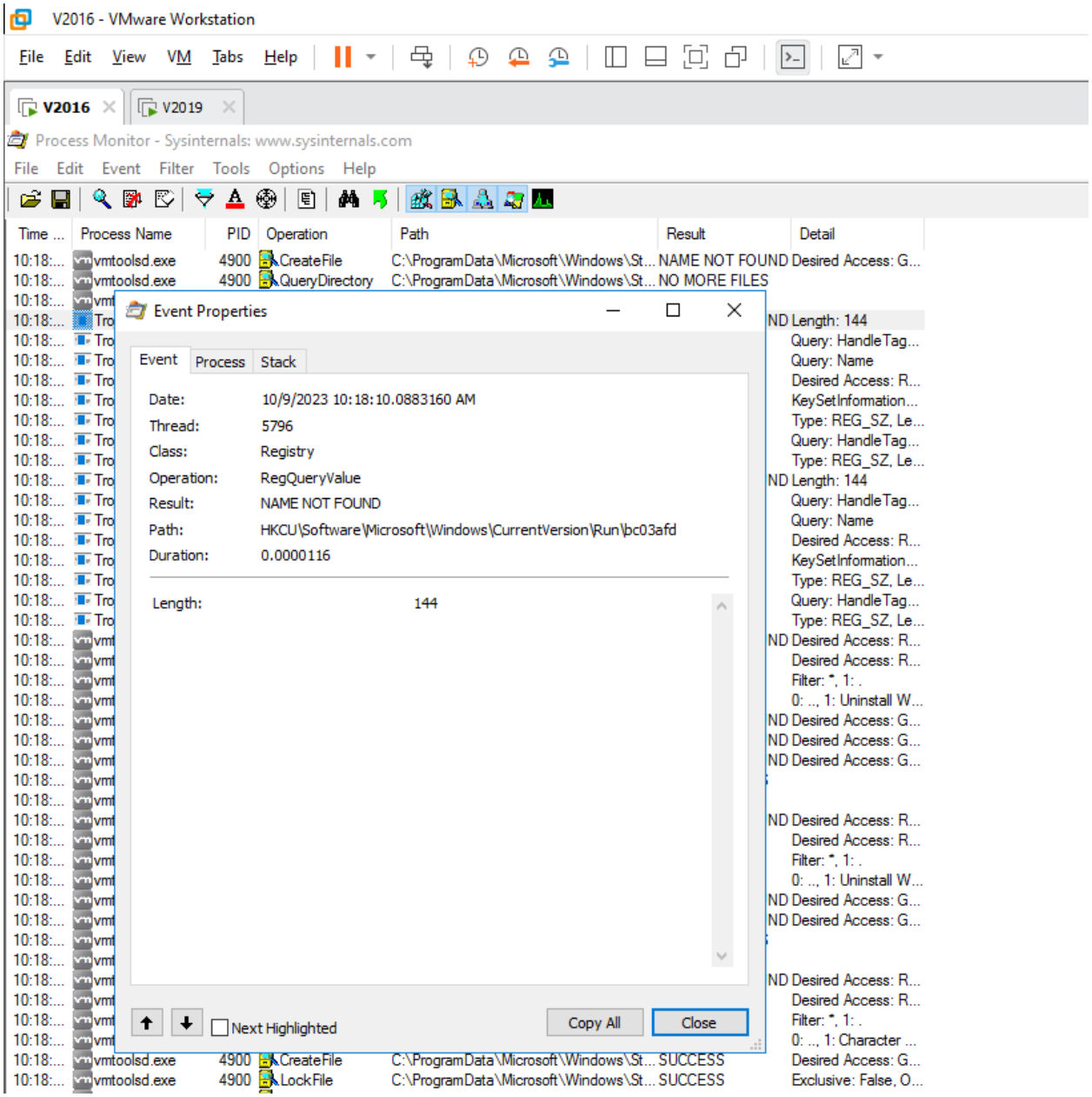


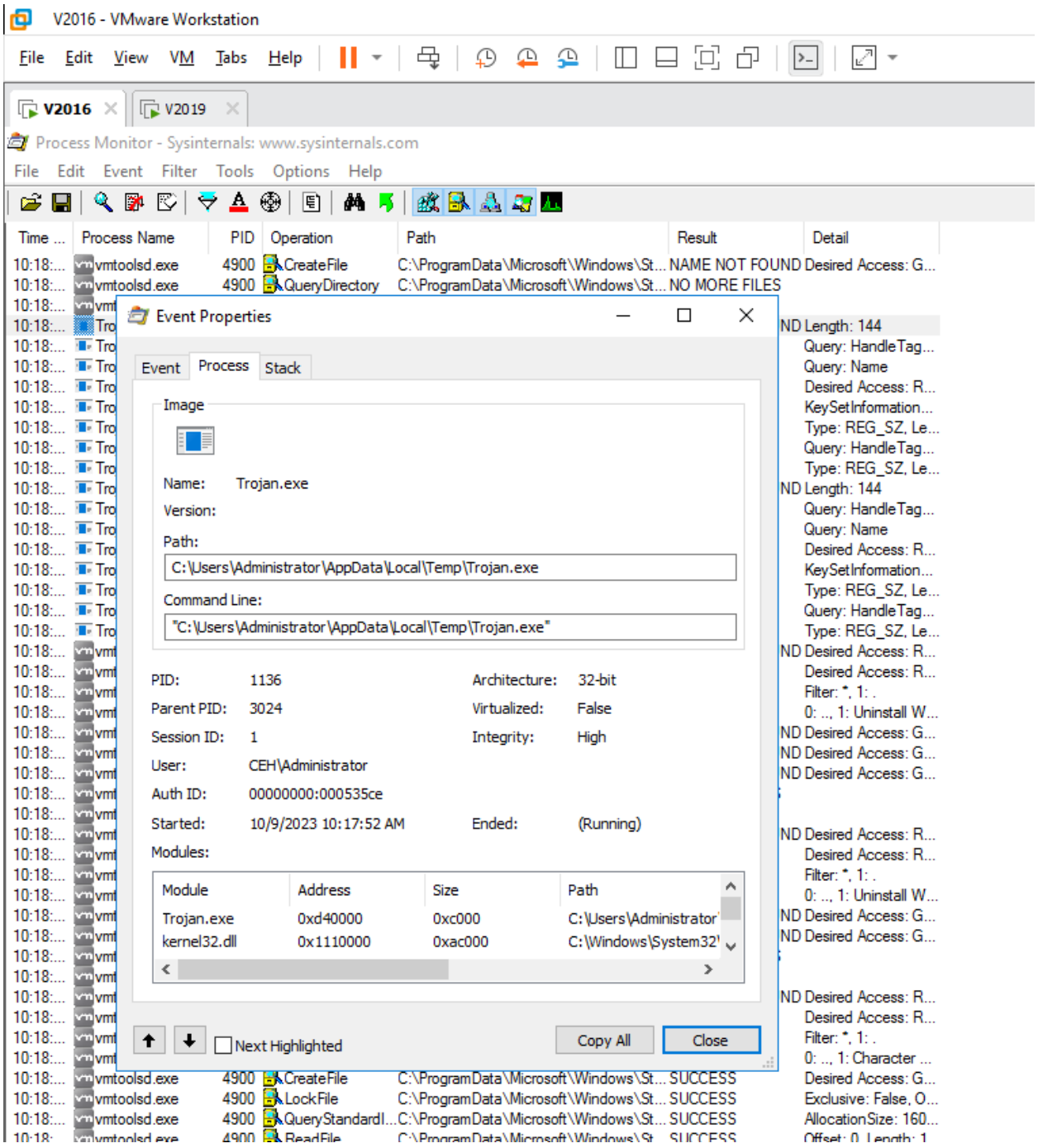

## 4.2 Perform Process Monitoring using Process Monitor - Open Windows 10, Windows Server 2016

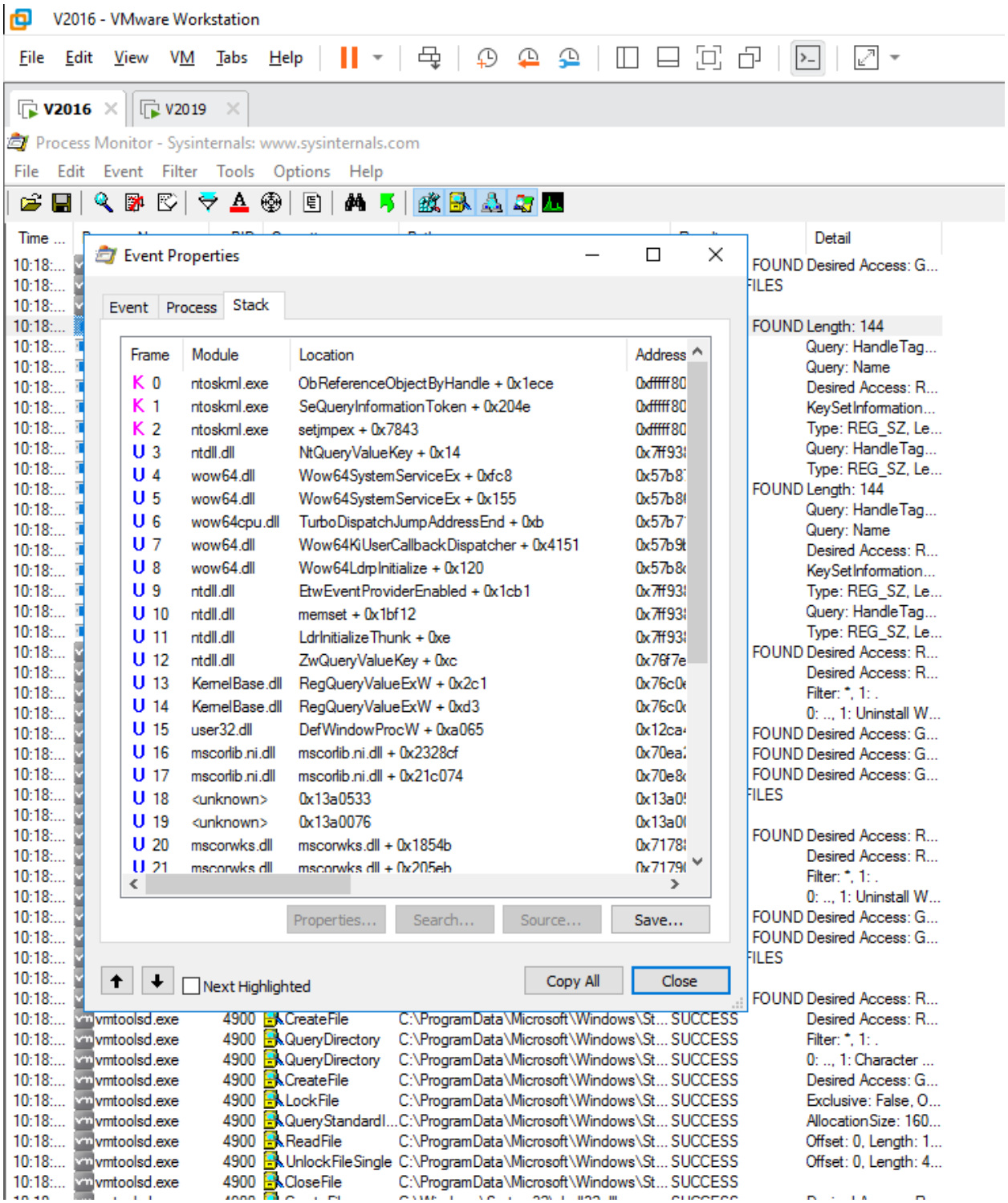

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
desktop.ini
Firefox
Google
ProcessMonitor
File Home Share View
Malware Analysis Tools › Dynamic Malware Analysis Tools › Process Monitoring Tools › ProcessMonitor
Search ProcessMonitor
Quick access
Desktop
Downloads
Documents
Pictures
CEH
System32
www
This PC
Network
Name
Date modified
Type
Size
Eula.txt 9/27/2018 7:25 PM Text Document 8 KB
procmon.chm 3/24/2019 3:35 PM Compiled HTML ... 63 KB
Procmon.exe 3/24/2019 3:35 PM Application 2,145 KB


V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
10:17:... Explorer.EXE 872 ReadFile C:\Windows\System32\shlwapi.dll SUCCESS Offset: 303,616, Le...
10:17:... svchost.exe 832 RegQueryKey HKCR SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegOpenKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS Desired Access: R...
10:17:... svchost.exe 832 RegQueryKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegOpenKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... NAME NOT FOUND Desired Access: Q...
10:17:... svchost.exe 832 RegQueryValue HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS Type: REG_SZ, Le...
10:17:... svchost.exe 832 RegQueryValue HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS Type: REG_SZ, Le...
10:17:... svchost.exe 832 RegQueryKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegOpenKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... NAME NOT FOUND Desired Access: R...
10:17:... svchost.exe 832 RegQueryValue HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS Type: REG_SZ, Le...
10:17:... svchost.exe 832 RegQueryKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegOpenKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... NAME NOT FOUND Desired Access: Q...
10:17:... svchost.exe 832 RegQueryKey HKCR SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegOpenKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS Desired Access: R...
10:17:... svchost.exe 832 RegQueryKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegOpenKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... NAME NOT FOUND Desired Access: R...
10:17:... svchost.exe 832 RegCloseKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS
10:17:... svchost.exe 832 RegCloseKey HKCR\CLSID\{8BC3F05E-D86B-11D0-... SUCCESS
10:17:... svchost.exe 832 RegQueryKey HKCR SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegQueryKey HKCR SUCCESS Query: Name
10:17:... svchost.exe 832 RegOpenKey HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS Desired Access: R...
10:17:... svchost.exe 832 RegSetInfoKey HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS KeySetInformation...
10:17:... svchost.exe 832 RegQueryKey HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegOpenKey HKCR\WOW6432Node\CLSID\{8BC3... NAME NOT FOUND Desired Access: Q...
10:17:... svchost.exe 832 RegQueryValue HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS Type: REG_SZ, Le...
10:17:... svchost.exe 832 RegQueryValue HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS Type: REG_SZ, Le...
10:17:... svchost.exe 832 RegQueryKey HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegOpenKey HKCR\WOW6432Node\CLSID\{8BC3... NAME NOT FOUND Desired Access: R...
10:17:... svchost.exe 832 RegQueryValue HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS Type: REG_SZ, Le...
10:17:... svchost.exe 832 RegQueryKey HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegOpenKey HKCR\WOW6432Node\CLSID\{8BC3... NAME NOT FOUND Desired Access: Q...
10:17:... svchost.exe 832 RegQueryKey HKCR SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegQueryKey HKCR SUCCESS Query: Name
10:17:... svchost.exe 832 RegOpenKey HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS Desired Access: R...
10:17:... svchost.exe 832 RegSetInfoKey HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS KeySetInformation...
10:17:... svchost.exe 832 RegQueryKey HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS Query: HandleTag...
10:17:... svchost.exe 832 RegOpenKey HKCR\WOW6432Node\CLSID\{8BC3... NAME NOT FOUND Desired Access: R...
10:17:... svchost.exe 832 RegCloseKey HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS
10:17:... svchost.exe 832 RegCloseKey HKCR\WOW6432Node\CLSID\{8BC3... SUCCESS
10:17:... Explorer.EXE 872 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
10:17:... Explorer.EXE 872 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
10:17:... Explorer.EXE 872 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
10:17:... Explorer.EXE 872 RegOpenKey HKCU\Software\Classes\Applications\... NAME NOT FOUND Desired Access: R...
10:17:... Explorer.EXE 872 RegOpenKey HKCR\Applications\Procmon64.exe NAME NOT FOUND Desired Access: R...
10:17:... Explorer.EXE 872 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
10:17:... Explorer.EXE 872 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
10:17:... Explorer.EXE 872 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
10:17:... Explorer.EXE 872 RegOpenKey HKCU\Software\Classes\Applications\... NAME NOT FOUND Desired Access: R...
10:17:... Explorer.EXE 872 RegOpenKey HKCR\Applications\Procmon64.exe NAME NOT FOUND Desired Access: R...
10:17:... Explorer.EXE 872 CreateFile C:\Users\Administrator\AppData\Local\... SUCCESS Desired Access: R...
10:17:... Explorer.EXE 872 QueryBasicInfor... C:\Users\Administrator\AppData\Local\... SUCCESS CreationTime: 10/9...
10:17:... Explorer.EXE 872 CloseFile C:\Users\Administrator\AppData\Local\... SUCCESS
10:17:... svchost.exe 1048 ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 1,081,344, ...
10:17:... svchost.exe 1048 ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 3,080,192, ...
Showing 15,765 of 23,119 events (68%)
Backed by virtual memory

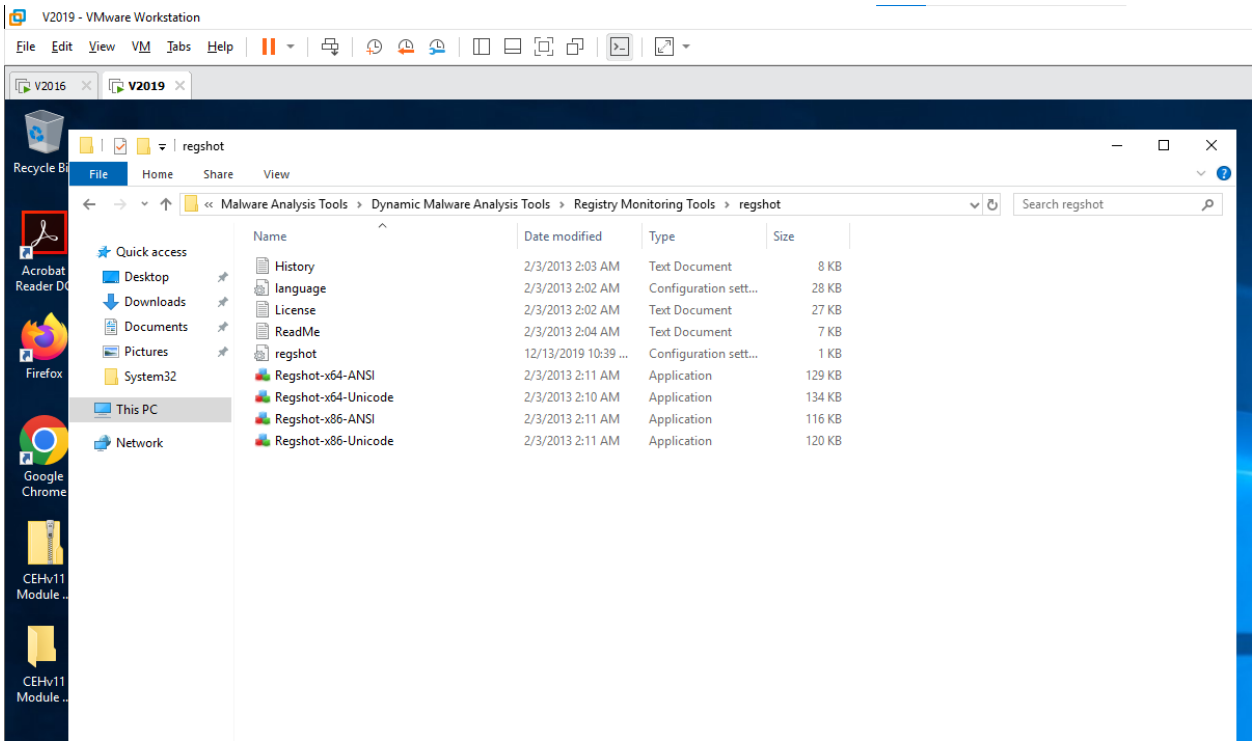

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
10:18:... vmtoolsd.exe 4900 CreateFile C:\ProgramData\Microsoft\Windows\St... NAME NOT FOUND Desired Access: G...
10:18:... vmtoolsd.exe 4900 QueryDirectory C:\ProgramData\Microsoft\Windows\St... NO MORE FILES
10:18:... vmtoolsd.exe 4900 CloseFile C:\ProgramData\Microsoft\Windows\St... SUCCESS
10:18:... Trojan.exe 1136 RegQueryValue HKCU\Software\Microsoft\Windows\C... NAME NOT FOUND Length: 144
10:18:... Trojan.exe 1136 RegQueryKey HKCU SUCCESS Query: HandleTag...
10:18:... Trojan.exe 1136 RegQueryKey HKCU SUCCESS Query: Name
10:18:... Trojan.exe 1136 RegOpenKey HKCU\Software\Microsoft\Windows\C... SUCCESS Desired Access: R...
10:18:... Trojan.exe 1136 RegSetInfoKey HKCU\SOFTWARE\Microsoft\Window... SUCCESS KeySetInformation...
10:18:... Trojan.exe 1136 RegQueryValue HKCU\SOFTWARE\Microsoft\Window... SUCCESS Type: REG_SZ, Le...
10:18:... Trojan.exe 1136 RegQueryKey HKCU\SOFTWARE\Microsoft\Window... SUCCESS Query: HandleTag...
10:18:... Trojan.exe 1136 RegSetValue HKCU\SOFTWARE\Microsoft\Window... SUCCESS Type: REG_SZ, Le...
10:18:... Trojan.exe 1136 RegQueryValue HKLM\Software\Microsoft\Windows\C... NAME NOT FOUND Length: 144
10:18:... Trojan.exe 1136 RegQueryKey HKLM SUCCESS Query: HandleTag...
10:18:... Trojan.exe 1136 RegQueryKey HKLM SUCCESS Query: Name
10:18:... Trojan.exe 1136 RegOpenKey HKLM\Software\WOW6432Node\Micr... SUCCESS Desired Access: R...
10:18:... Trojan.exe 1136 RegSetInfoKey HKLM\SOFTWARE\WOW6432Node\... SUCCESS KeySetInformation...
10:18:... Trojan.exe 1136 RegQueryValue HKLM\SOFTWARE\WOW6432Node\... SUCCESS Type: REG_SZ, Le...
10:18:... Trojan.exe 1136 RegQueryKey HKLM\SOFTWARE\WOW6432Node\... SUCCESS Query: HandleTag...
10:18:... Trojan.exe 1136 RegSetValue HKLM\SOFTWARE\WOW6432Node\... SUCCESS Type: REG_SZ, Le...
10:18:... vmtoolsd.exe 4900 CreateFile C:\Users\Administrator\AppData\Roami... NAME NOT FOUND Desired Access: R...
10:18:... vmtoolsd.exe 4900 CreateFile C:\ProgramData\Microsoft\Windows\St... SUCCESS Desired Access: R...
10:18:... vmtoolsd.exe 4900 QueryDirectory C:\ProgramData\Microsoft\Windows\St... SUCCESS Filter: *, 1: .
10:18:... vmtoolsd.exe 4900 QueryDirectory C:\ProgramData\Microsoft\Windows\St... SUCCESS 0: .., 1: Uninstall W...
10:18:... vmtoolsd.exe 4900 CreateFile C:\ProgramData\Microsoft\Windows\St... NAME NOT FOUND Desired Access: G...
10:18:... vmtoolsd.exe 4900 CreateFile C:\ProgramData\Microsoft\Windows\St... NAME NOT FOUND Desired Access: G...
10:18:... vmtoolsd.exe 4900 CreateFile C:\ProgramData\Microsoft\Windows\St... NAME NOT FOUND Desired Access: G...
10:18:... vmtoolsd.exe 4900 QueryDirectory C:\ProgramData\Microsoft\Windows\St... NO MORE FILES
10:18:... vmtoolsd.exe 4900 CloseFile C:\ProgramData\Microsoft\Windows\St... SUCCESS
10:18:... vmtoolsd.exe 4900 CreateFile C:\Users\Administrator\AppData\Roami... NAME NOT FOUND Desired Access: R...
10:18:... vmtoolsd.exe 4900 CreateFile C:\ProgramData\Microsoft\Windows\St... SUCCESS Desired Access: R...
10:18:... vmtoolsd.exe 4900 QueryDirectory C:\ProgramData\Microsoft\Windows\St... SUCCESS Filter: *, 1: .

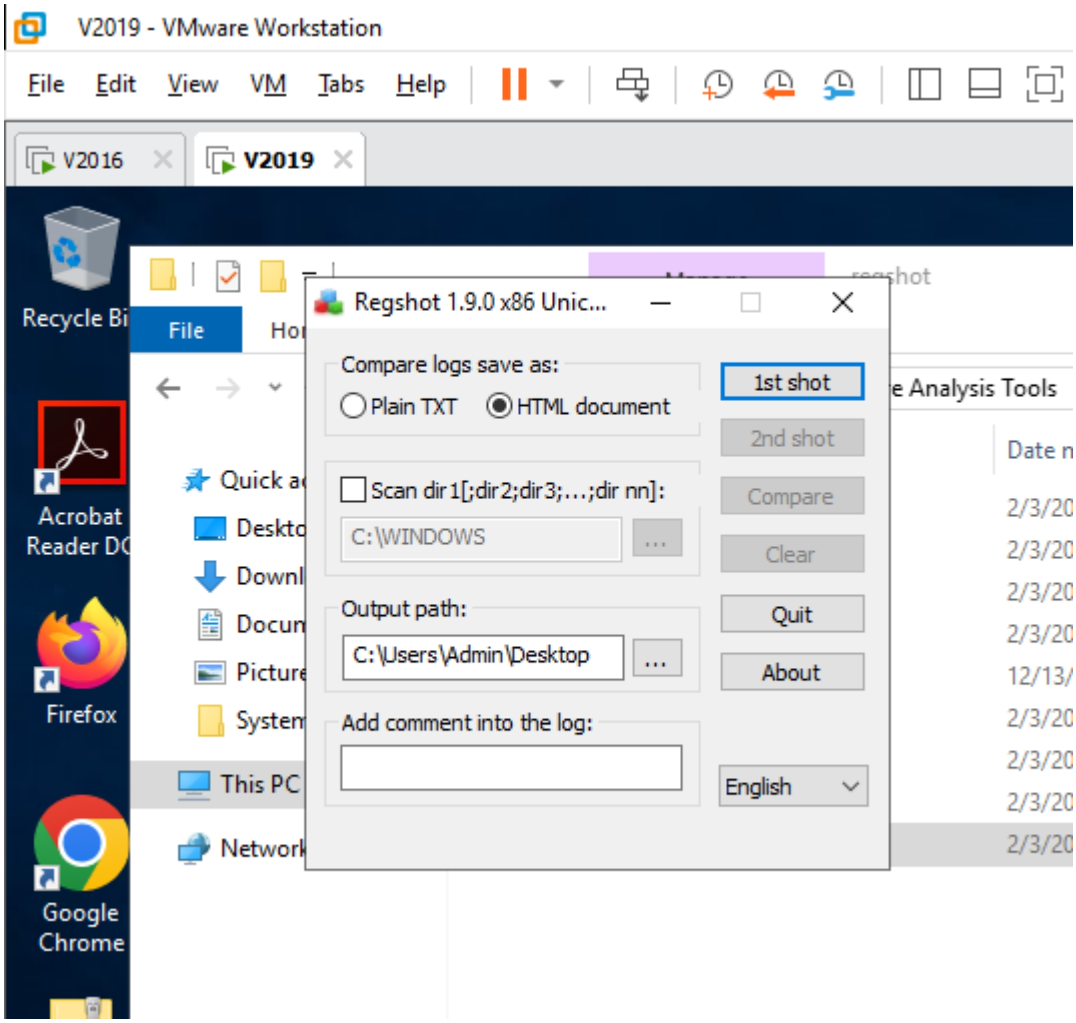

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
10:18:... vmtoolsd.exe 4900 CreateFile C:\ProgramData\Microsoft\Windows\St... NAME NOT FOUND Desired Access: G...
10:18:... vmtoolsd.exe 4900 QueryDirectory C:\ProgramData\Microsoft\Windows\St... NO MORE FILES
Event Properties
Event Process Stack
Date: 10/9/2023 10:18:10.0883160 AM
Thread: 5796
Class: Registry
Operation: RegQueryValue
Result: NAME NOT FOUND
Path: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\bc03afd
Duration: 0.0000116
Length: 144
Next Highlighted
Copy All
Close
10:18:... vmtoolsd.exe 4900 CreateFile C:\ProgramData\Microsoft\Windows\St... SUCCESS Desired Access: G...
10:18:... vmtoolsd.exe 4900 LockFile C:\ProgramData\Microsoft\Windows\St... SUCCESS Exclusive: False, O...

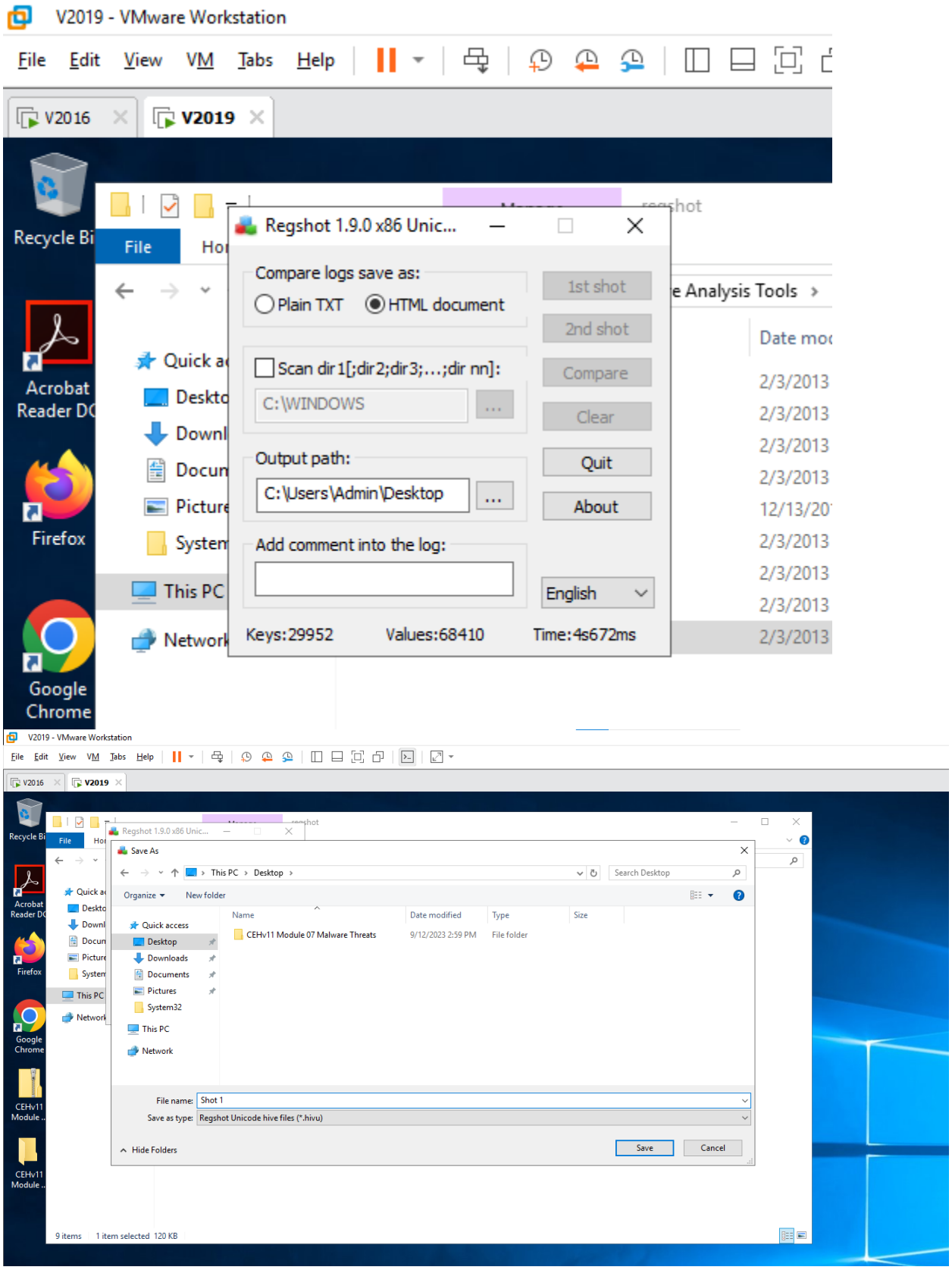

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
10:18:... vmtoolsd.exe 4900 CreateFile C:\ProgramData\Microsoft\Windows\St... NAME NOT FOUND Desired Access: G...
10:18:... vmtoolsd.exe 4900 QueryDirectory C:\ProgramData\Microsoft\Windows\St... NO MORE FILES
Event Properties
Event Process Stack
Image
Name: Trojan.exe
Version:
Path:
C:\Users\Administrator\AppData\Local\Temp\Trojan.exe
Command Line:
"C:\Users\Administrator\AppData\Local\Temp\Trojan.exe"
PID: 1136
Parent PID: 3024
Session ID: 1
User: CEH\Administrator
Auth ID: 00000000:000535ce
Started: 10/9/2023 10:17:52 AM
Architecture: 32-bit
Virtualized: False
Integrity: High
Ended: (Running)
Modules:
Module Address Size Path
Trojan.exe 0xd40000 0xc000 C:\Users\Administrator
kernel32.dll 0x1110000 0xac000 C:\Windows\System32
Next Highlighted
Copy All
Close
10:18:... vmtoolsd.exe 4900 CreateFile C:\ProgramData\Microsoft\Windows\St... SUCCESS
10:18:... vmtoolsd.exe 4900 LockFile C:\ProgramData\Microsoft\Windows\St... SUCCESS
10:18:... vmtoolsd.exe 4900 QueryStandardI... C:\ProgramData\Microsoft\Windows\St... SUCCESS

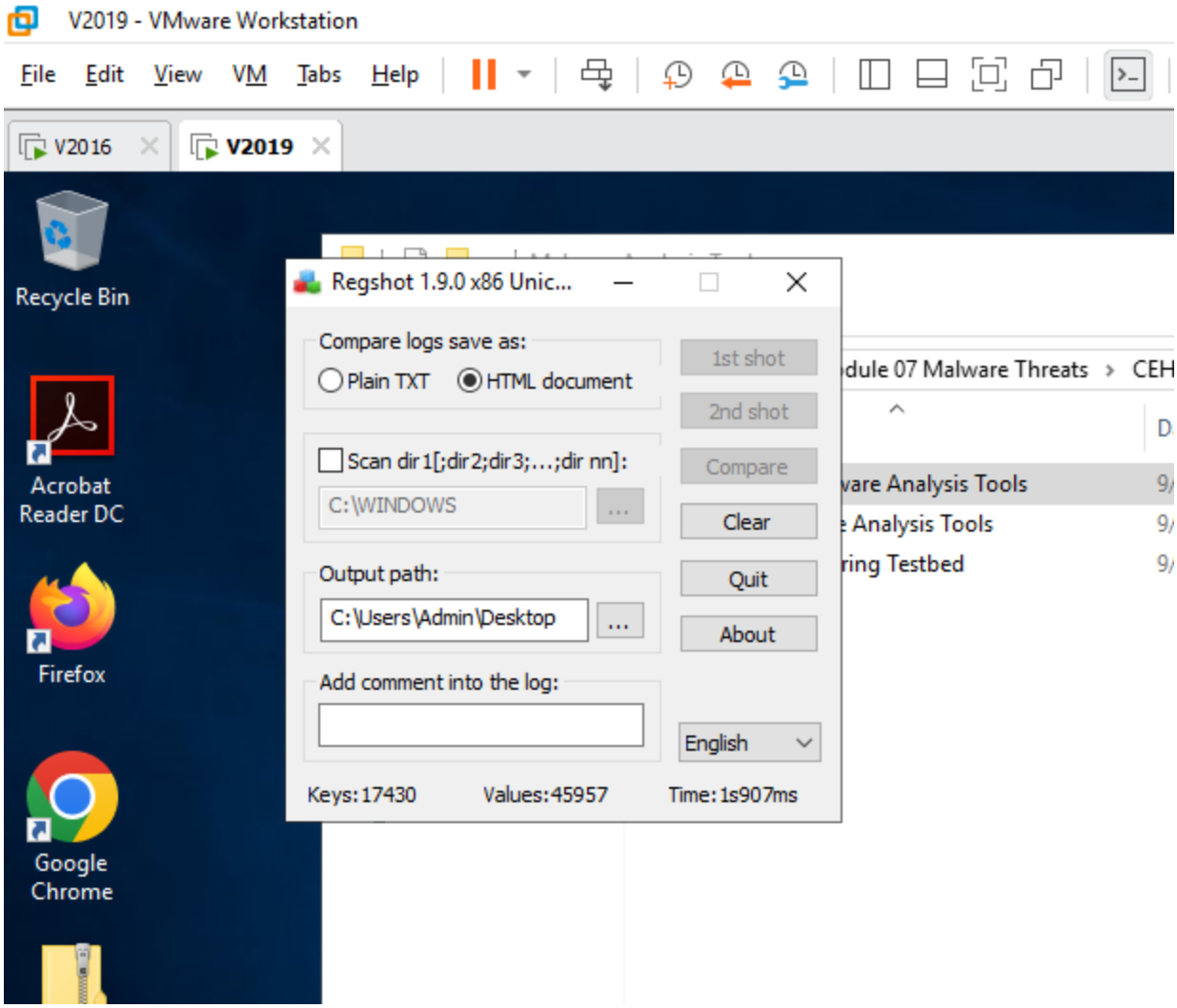


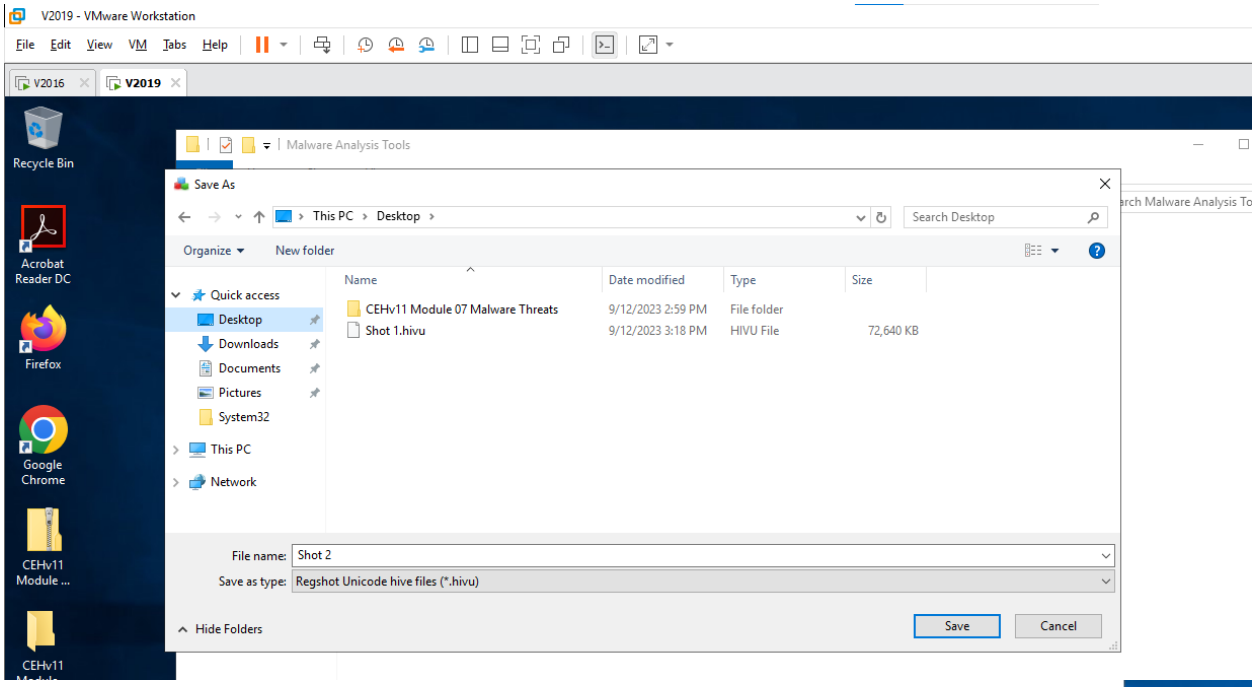

4.3 Perform Registry Monitoring using Regshot and jv16 Power Tools
- Open Windows 10, Windows Server 2016

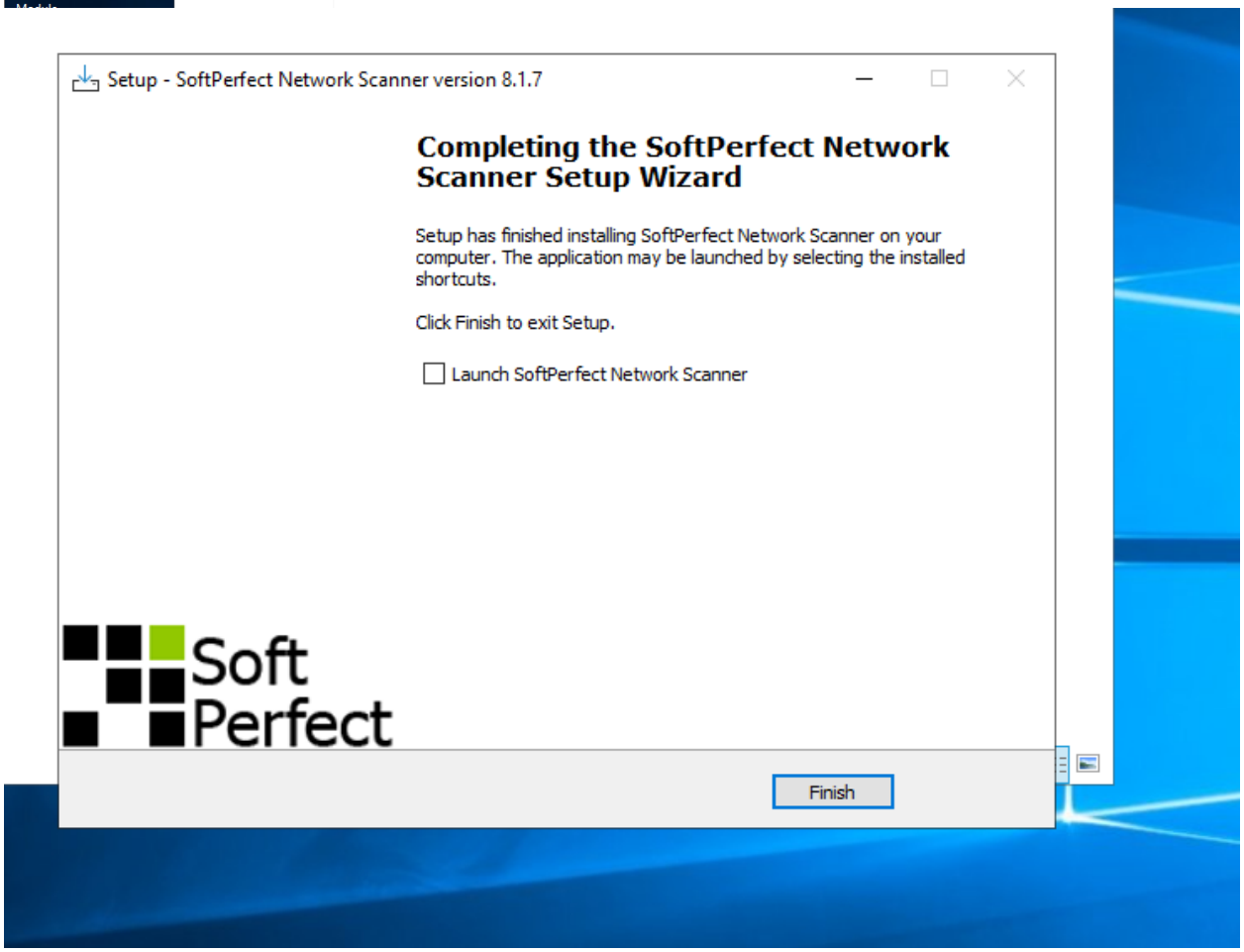

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bi
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ..
CEHv11 Module ..
regshot
File Home Share View
Malware Analysis Tools › Dynamic Malware Analysis Tools › Registry Monitoring Tools › regshot
Search regshot
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
History 2/3/2013 2:03 AM Text Document 8 KB
language 2/3/2013 2:02 AM Configuration sett... 28 KB
License 2/3/2013 2:02 AM Text Document 27 KB
ReadMe 2/3/2013 2:04 AM Text Document 7 KB
regshot 12/13/2019 10:39 ... Configuration sett... 1 KB
Regshot-x64-ANSI 2/3/2013 2:11 AM Application 129 KB
Regshot-x64-Unicode 2/3/2013 2:10 AM Application 134 KB
Regshot-x86-ANSI 2/3/2013 2:11 AM Application 116 KB
Regshot-x86-Unicode 2/3/2013 2:11 AM Application 120 KB

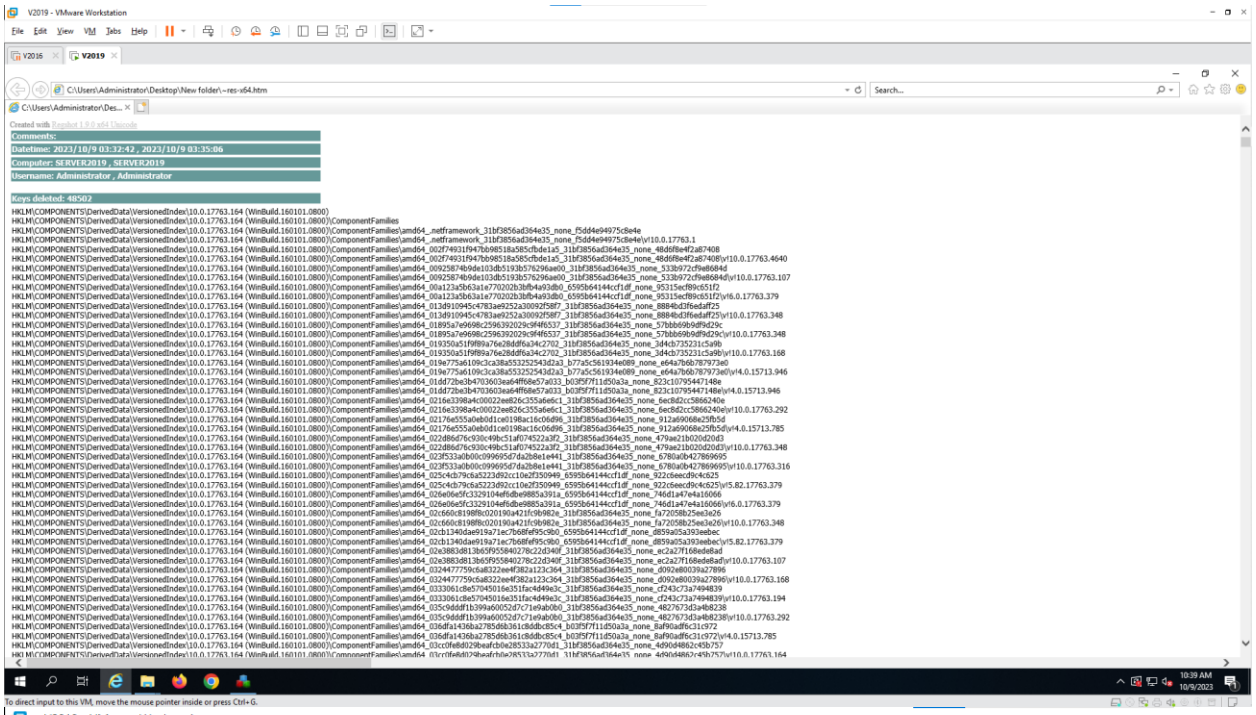

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bi
Acrobat Reader DC
Firefox
Google Chrome
File
Quick a
Deskto
Downl
Docun
Picture
System
This PC
Network
Regshot 1.9.0 x86 Unic...
Compare logs save as:
Plain TXT
HTML document
Scan dir1[;dir2;dir3;...;dir nn]:
C:\WINDOWS
Output path:
C:\Users\Admin\Desktop
Add comment into the log:
1st shot
2nd shot
Compare
Clear
Quit
About
English
e Analysis Tools
Date n
2/3/20
12/13/


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bi
Acrobat Reader DC
Firefox
Google Chrome
Regshot 1.9.0 x86 Unic...
Compare logs save as:
Plain TXT
HTML document
Scan dir1[;dir2;dir3;...;dir nn]:
C:\WINDOWS
Output path:
C:\Users\Admin\Desktop
Add comment into the log:
1st shot
2nd shot
Compare
Clear
Quit
About
English
Keys:29952
Values:68410
Time:4s672ms
Save As
This PC
Desktop
Search Desktop
Organize
New folder
Quick access
Downloads
Documents
Pictures
System32
Network
Name
Date modified
Type
Size
CEHv11 Module 07 Malware Threats
9/12/2023 2:59 PM
File folder
File name:
Shot 1
Save as type:
Regshot Unicode hive files (*.hivu)
Hide Folders
Save
Cancel
9 items
1 item selected 120 KB


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Regshot 1.9.0 x86 Unic...
Compare logs save as:
Plain TXT
HTML document
Scan dir1[;dir2;dir3;...;dir nn]:
C:\WINDOWS
Output path:
C:\Users\Admin\Desktop
Add comment into the log:
1st shot
2nd shot
Compare
Clear
Quit
About
English
Keys: 17430
Values: 45957
Time: 1s907ms
dule 07 Malware Threats
ware Analysis Tools
Analysis Tools
ring Testbed


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
Malware Analysis Tools
Save As
This PC › Desktop ›
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
CEHv11 Module 07 Malware Threats
9/12/2023 2:59 PM
File folder
Shot 1.hivu
9/12/2023 3:18 PM
HIVU File
72,640 KB
File name: Shot 2
Save as type: Regshot Unicode hive files (*.hivu)
Hide Folders
Save
Cancel


Setup - SoftPerfect Network Scanner version 8.1.7
Completing the SoftPerfect Network Scanner Setup Wizard
Setup has finished installing SoftPerfect Network Scanner on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Launch SoftPerfect Network Scanner
Soft Perfect
Finish



V2019 - VMware Workstation

File Edit View VM Tabs Help

V2016 V2019

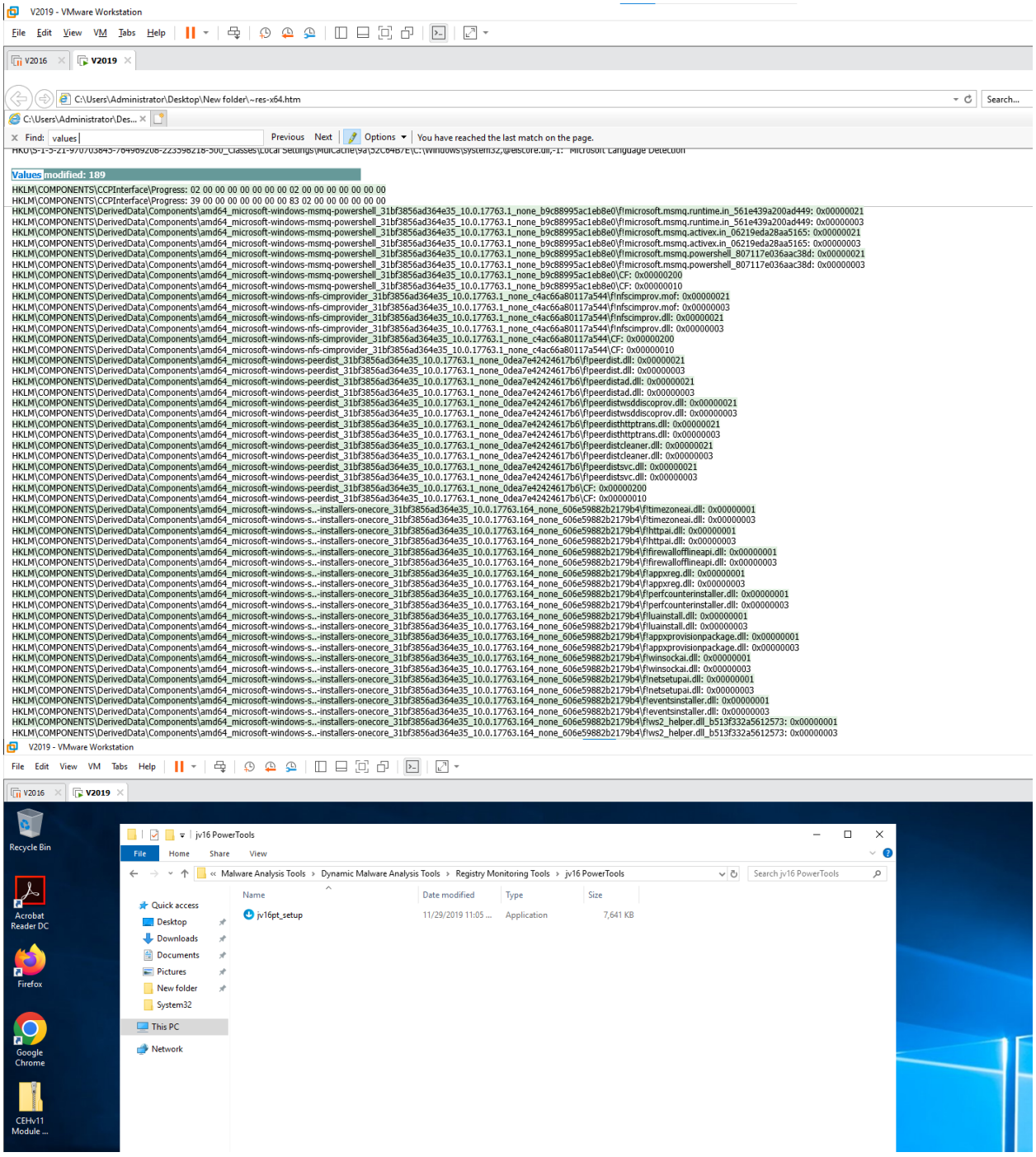
C:\Users\Administrator\Desktop\New folder\~res-x64.htm

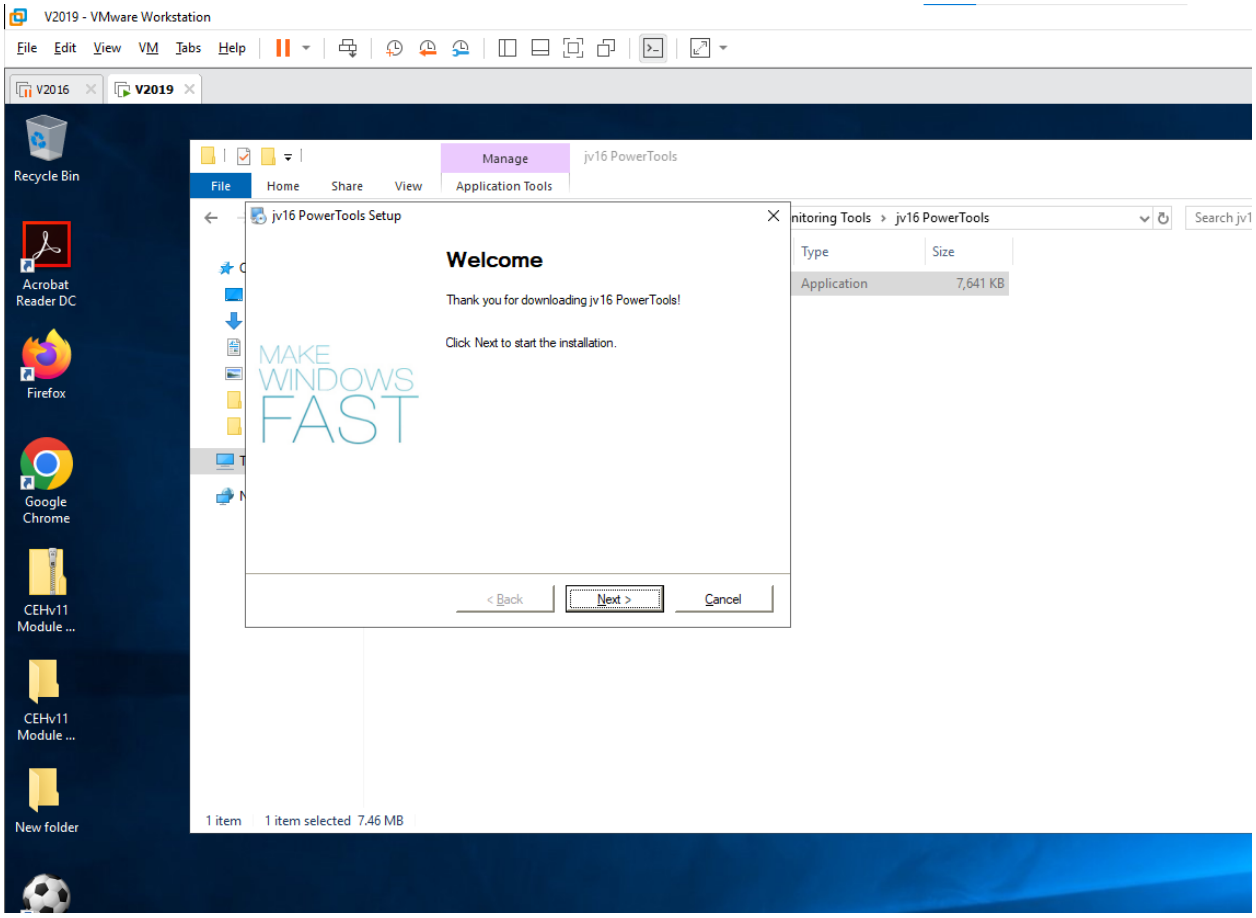
C:\Users\Administrator\Des...

Find: values Previous Next Options 3 matches

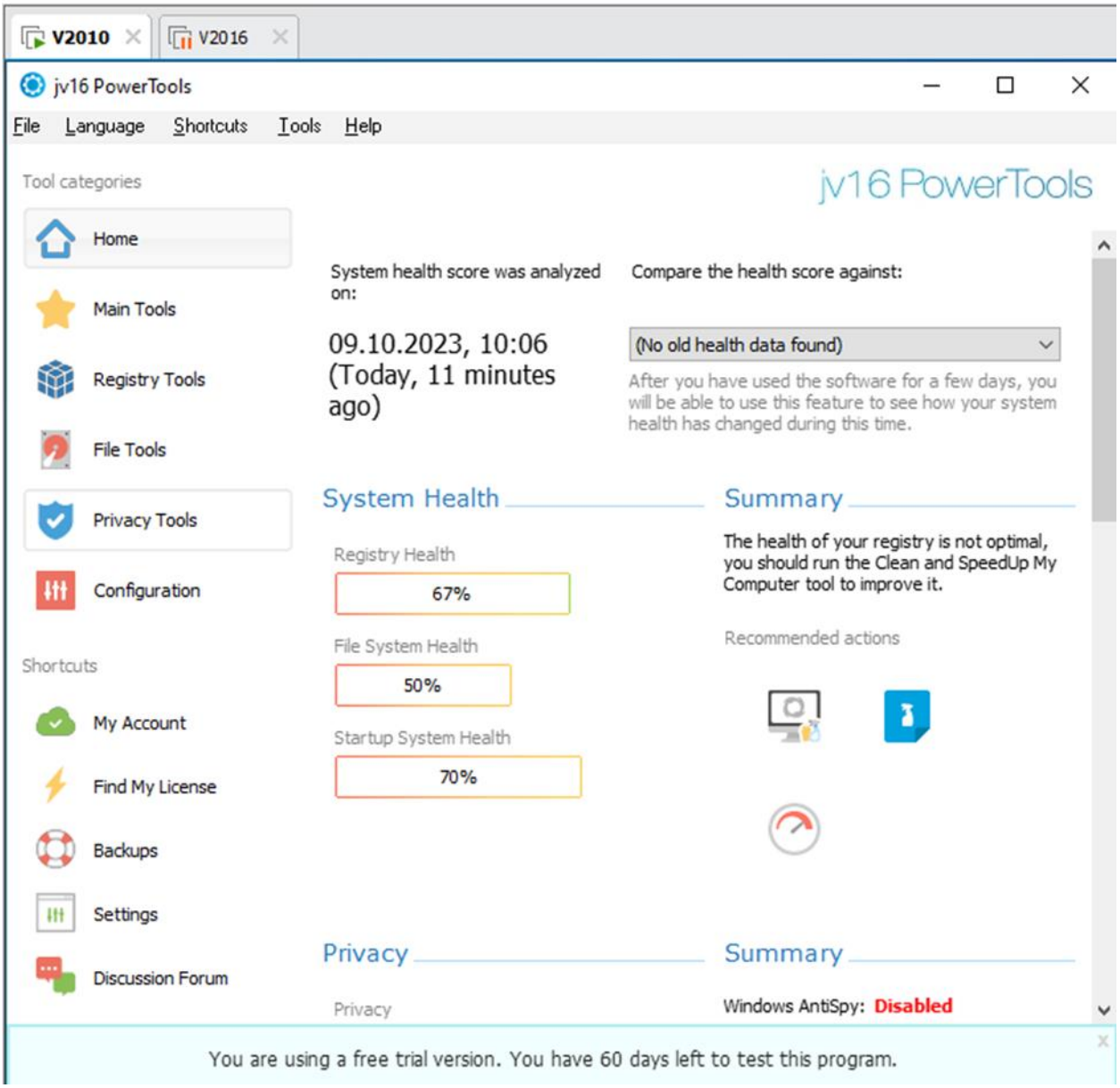
**Values added: 53122**

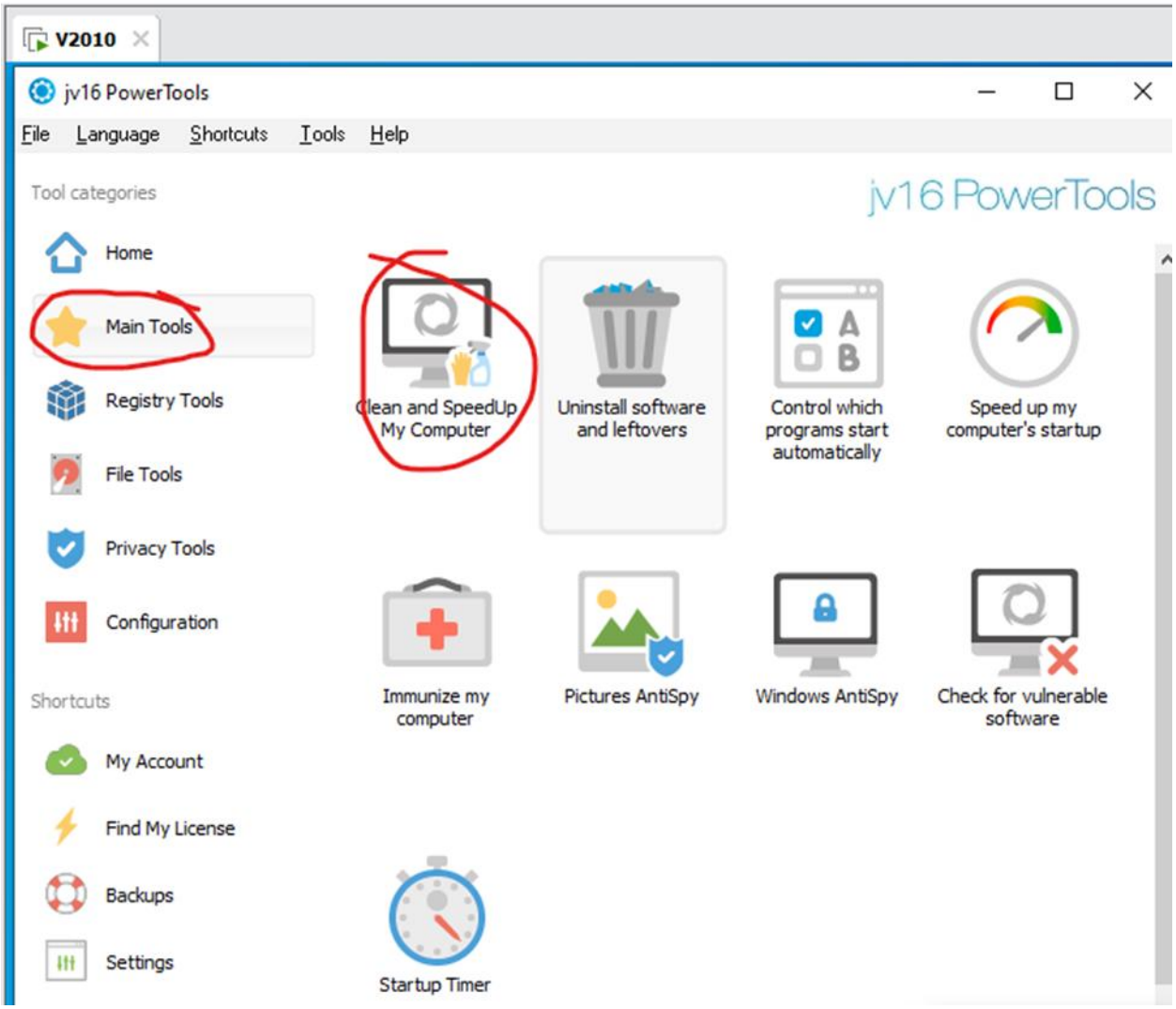
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-msmq-powershell_31bf3856ad364e35_10.0.17763.1_none_b9c88995ac1eb8e0\DV: 7B 01 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-msmq-powershell_31bf3856ad364e35_10.0.17763.1_none_b9c88995ac1eb8e0\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-nfs-cimprovider_31bf3856ad364e35_10.0.17763.1_none_c4ac66a80117a544\DV: 24 01 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-nfs-cimprovider_31bf3856ad364e35_10.0.17763.1_none_c4ac66a80117a544\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e42424617b6\DV: 5C 01 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e42424617b6\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\DV: 20 12 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..cingstack-onecoreds_31bf3856ad364e35_10.0.17763.164_none_290a66b8a7666d07\DV: 20 12 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..cingstack-onecoreds_31bf3856ad364e35_10.0.17763.164_none_290a66b8a7666d07\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..cingstack-onecoreds_31bf3856ad364e35_10.0.17763.164_none_290a66b8a7666d07\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..cingstack.resources_31bf3856ad364e35_10.0.17763.164_en-us_016ba3b61a7e35c9\DV: 20 12 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..cingstack.resources_31bf3856ad364e35_10.0.17763.164_en-us_016ba3b61a7e35c9\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..cingstack.resources_31bf3856ad364e35_10.0.17763.164_en-us_016ba3b61a7e35c9\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..ck-mof-onecoreadmin_31bf3856ad364e35_10.0.17763.164_none_8e73d24eb4d0e1f0\DV: 20 12 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..ck-mof-onecoreadmin_31bf3856ad364e35_10.0.17763.164_none_8e73d24eb4d0e1f0\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..ck-mof-onecoreadmin_31bf3856ad364e35_10.0.17763.164_none_8e73d24eb4d0e1f0\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..formers-shell-extra_31bf3856ad364e35_10.0.17763.164_none_5ec0b59a02e49a43\DV: 20 12 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..formers-shell-extra_31bf3856ad364e35_10.0.17763.164_none_5ec0b59a02e49a43\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..formers-shell-extra_31bf3856ad364e35_10.0.17763.164_none_5ec0b59a02e49a43\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..gstack-boot-onecore_31bf3856ad364e35_10.0.17763.164_none_ca790cc5f636172b\DV: 20 12 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..gstack-boot-onecore_31bf3856ad364e35_10.0.17763.164_none_ca790cc5f636172b\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..gstack-boot-onecore_31bf3856ad364e35_10.0.17763.164_none_ca790cc5f636172b\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..ingstack-base-extra_31bf3856ad364e35_10.0.17763.164_none_93b6d412490ea1cd\DV: 20 12 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..ingstack-base-extra_31bf3856ad364e35_10.0.17763.164_none_93b6d412490ea1cd\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..ingstack-base-extra_31bf3856ad364e35_10.0.17763.164_none_93b6d412490ea1cd\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..k-transformers-core_31bf3856ad364e35_10.0.17763.164_none_e0e583a05b2c1d65\DV: 20 12 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..k-transformers-core_31bf3856ad364e35_10.0.17763.164_none_e0e583a05b2c1d65\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..k-transformers-core_31bf3856ad364e35_10.0.17763.164_none_e0e583a05b2c1d65\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..llers-onecore-extra_31bf3856ad364e35_10.0.17763.164_none_988cac2248f3fa2d\DV: 20 12 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..llers-onecore-extra_31bf3856ad364e35_10.0.17763.164_none_988cac2248f3fa2d\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..llers-onecore-extra_31bf3856ad364e35_10.0.17763.164_none_988cac2248f3fa2d\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..ngstack-onecorebase_31bf3856ad364e35_10.0.17763.164_none_6536debe679f2c45\DV: 20 12 63 45 00 00 0A 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..ngstack-onecorebase_31bf3856ad364e35_10.0.17763.164_none_6536debe679f2c45\CTS: 0x5254CEC8
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..ngstack-onecorebase_31bf3856ad364e35_10.0.17763.164_none_6536debe679f2c45\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..ransformers-onecore_31bf3856ad364e35_10.0.17763.164_none_99089eae813b4697\DV: 20 12 63 45 00 00 0A 00

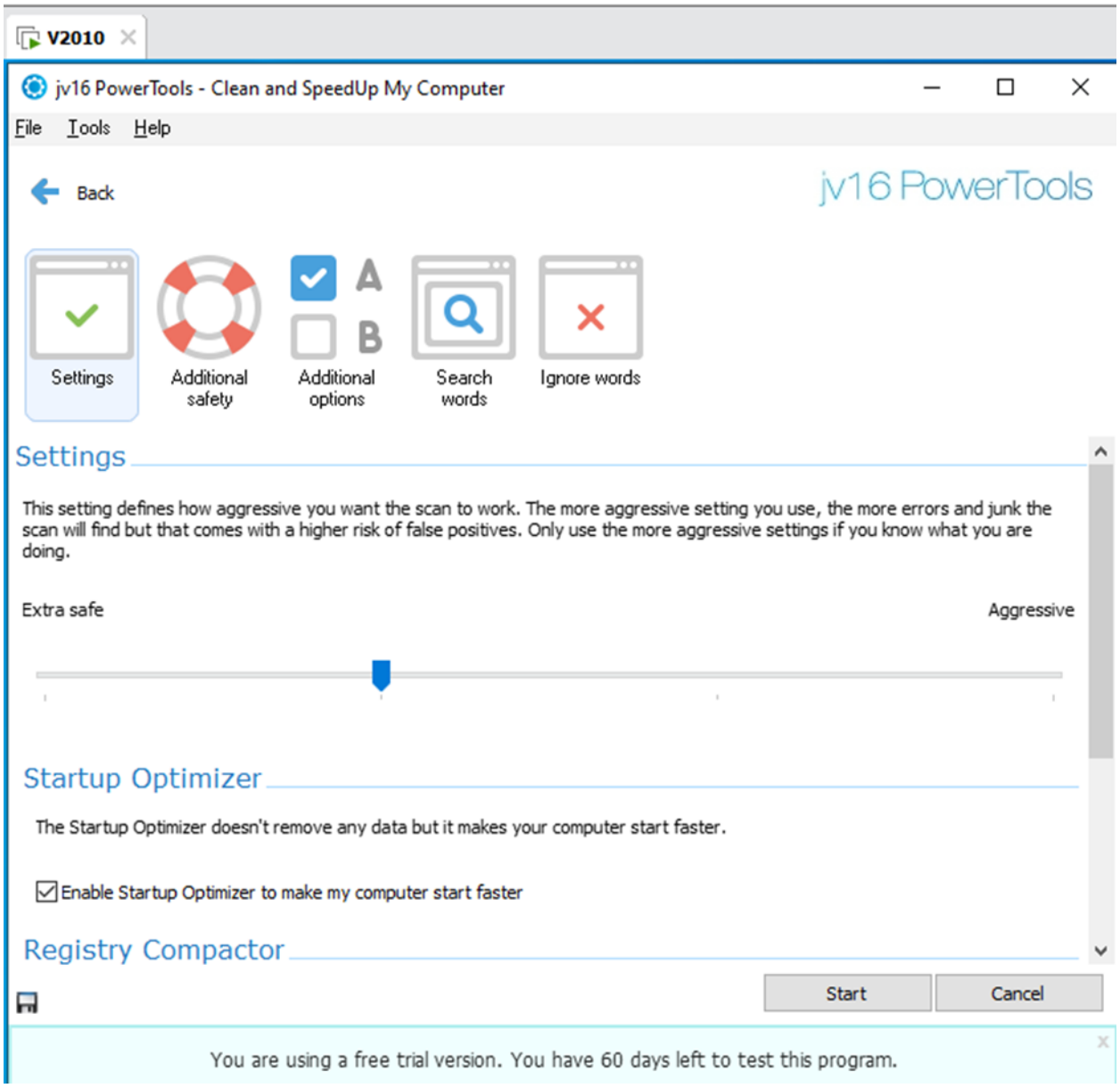

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
C:\Users\Administrator\Desktop\New folder\~res-x64.htm
Search...
C:\Users\Administrator\Des...
Find: values
Previous
Next
Options
You have reached the last match on the page.
Values modified: 189
HKLM\COMPONENTS\CCPInterface\Progress: 02 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00
HKLM\COMPONENTS\CCPInterface\Progress: 39 00 00 00 00 00 00 00 83 02 00 00 00 00 00 00
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-msmq-powershell_31bf3856ad364e35_10.0.17763.1_none_b9c88995ac1eb8e0\fmicrosoft.msmq.runtime.in_561e439a200ad449: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-msmq-powershell_31bf3856ad364e35_10.0.17763.1_none_b9c88995ac1eb8e0\fmicrosoft.msmq.runtime.in_561e439a200ad449: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-msmq-powershell_31bf3856ad364e35_10.0.17763.1_none_b9c88995ac1eb8e0\fmicrosoft.msmq.activex.in_06219eda28aa5165: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-msmq-powershell_31bf3856ad364e35_10.0.17763.1_none_b9c88995ac1eb8e0\fmicrosoft.msmq.activex.in_06219eda28aa5165: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-msmq-powershell_31bf3856ad364e35_10.0.17763.1_none_b9c88995ac1eb8e0\fmicrosoft.msmq.powershell_807117e036aac38d: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-msmq-powershell_31bf3856ad364e35_10.0.17763.1_none_b9c88995ac1eb8e0\fmicrosoft.msmq.powershell_807117e036aac38d: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-msmq-powershell_31bf3856ad364e35_10.0.17763.1_none_b9c88995ac1eb8e0\CF: 0x00000200
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-msmq-powershell_31bf3856ad364e35_10.0.17763.1_none_b9c88995ac1eb8e0\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-nfs-cimprovider_31bf3856ad364e35_10.0.17763.1_none_c4ac66a80117a544\fnfscimprov.mof: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-nfs-cimprovider_31bf3856ad364e35_10.0.17763.1_none_c4ac66a80117a544\fnfscimprov.mof: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-nfs-cimprovider_31bf3856ad364e35_10.0.17763.1_none_c4ac66a80117a544\fnfscimprov.dll: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-nfs-cimprovider_31bf3856ad364e35_10.0.17763.1_none_c4ac66a80117a544\fnfscimprov.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-nfs-cimprovider_31bf3856ad364e35_10.0.17763.1_none_c4ac66a80117a544\CF: 0x00000200
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-nfs-cimprovider_31bf3856ad364e35_10.0.17763.1_none_c4ac66a80117a544\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdist.dll: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdist.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdistad.dll: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdistad.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdistwsddiscoprov.dll: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdistwsddiscoprov.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdisthttptrans.dll: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdisthttptrans.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdistcleaner.dll: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdistcleaner.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdistsvc.dll: 0x00000021
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\fpeerdistsvc.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\CF: 0x00000200
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-peerdist_31bf3856ad364e35_10.0.17763.1_none_0dea7e4242461 7b6\CF: 0x00000010
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\ftimezoneai.dll: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\ftimezoneai.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fhttpai.dll: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fhttpai.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\ffirewallofflineapi.dll: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\ffirewallofflineapi.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fappxreg.dll: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fappxreg.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fperfcounterinstaller.dll: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fperfcounterinstaller.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fluainstall.dll: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fluainstall.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fappxprovisionpackage.dll: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fappxprovisionpackage.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fwinsockai.dll: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fwinsockai.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fnetsetupai.dll: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fnetsetupai.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\feventsinstaller.dll: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\feventsinstaller.dll: 0x00000003
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fws2_helper.dll_b513f332a5612573: 0x00000001
HKLM\COMPONENTS\DerivedData\Components\amd64_microsoft-windows-s..-installers-onecore_31bf3856ad364e35_10.0.17763.164_none_606e59882b2179b4\fws2_helper.dll_b513f332a5612573: 0x00000003
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
jv16 PowerTools
File Home Share View
Malware Analysis Tools › Dynamic Malware Analysis Tools › Registry Monitoring Tools › jv16 PowerTools
Search jv16 PowerTools
Quick access
Desktop
Downloads
Documents
Pictures
New folder
System32
This PC
Network
Name
Date modified
Type
Size
jv16pt_setup
11/29/2019 11:05 ...
Application
7,641 KB

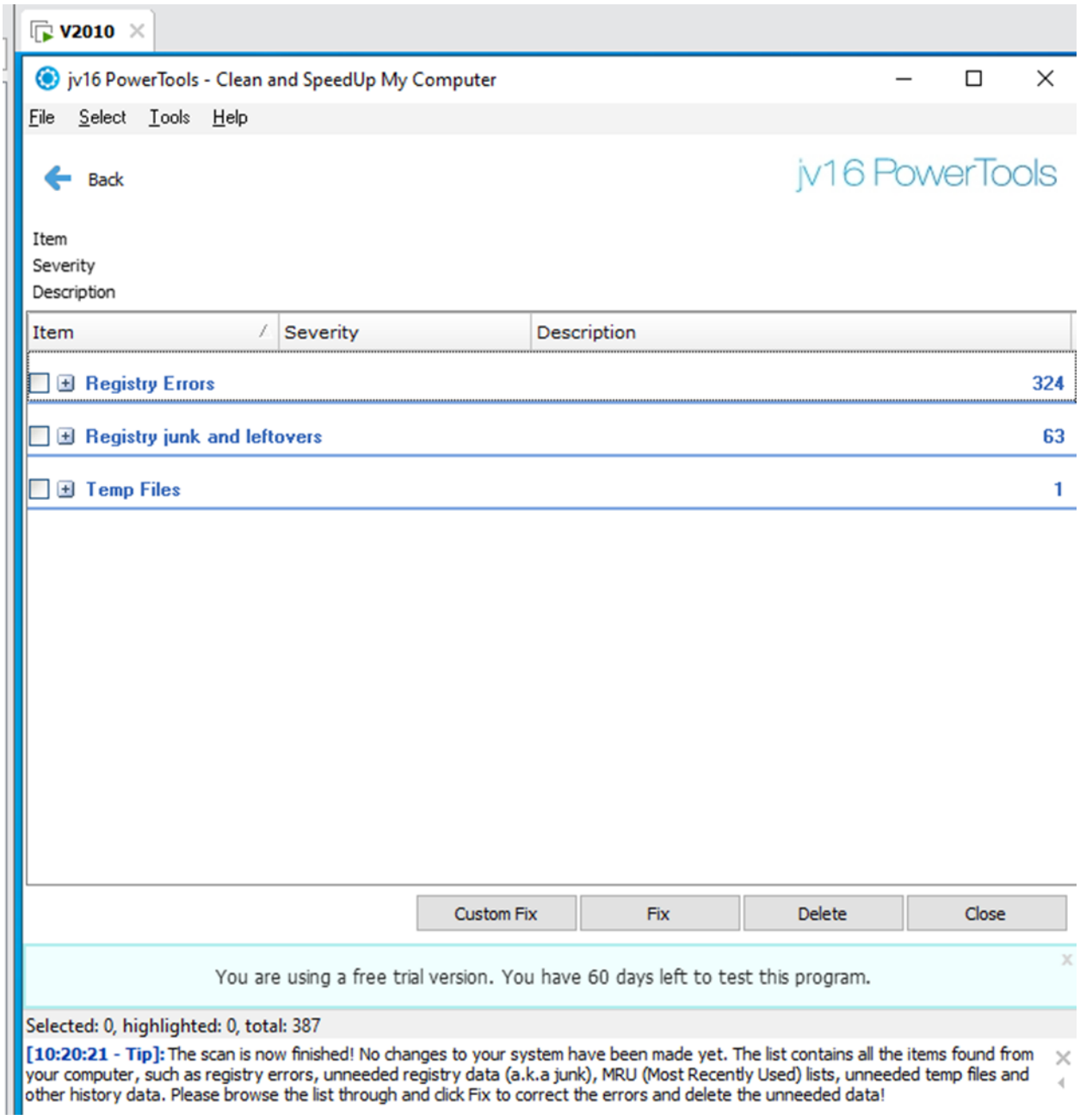

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
New folder
Manage
jv16 PowerTools
File Home Share View Application Tools
jv16 PowerTools Setup
Welcome
Thank you for downloading jv16 PowerTools!
Click Next to start the installation.
MAKE WINDOWS FAST
< Back
Next >
Cancel
nitoring Tools › jv16 PowerTools
Search jv1
Type
Size
Application
7,641 KB
1 item
1 item selected 7.46 MB

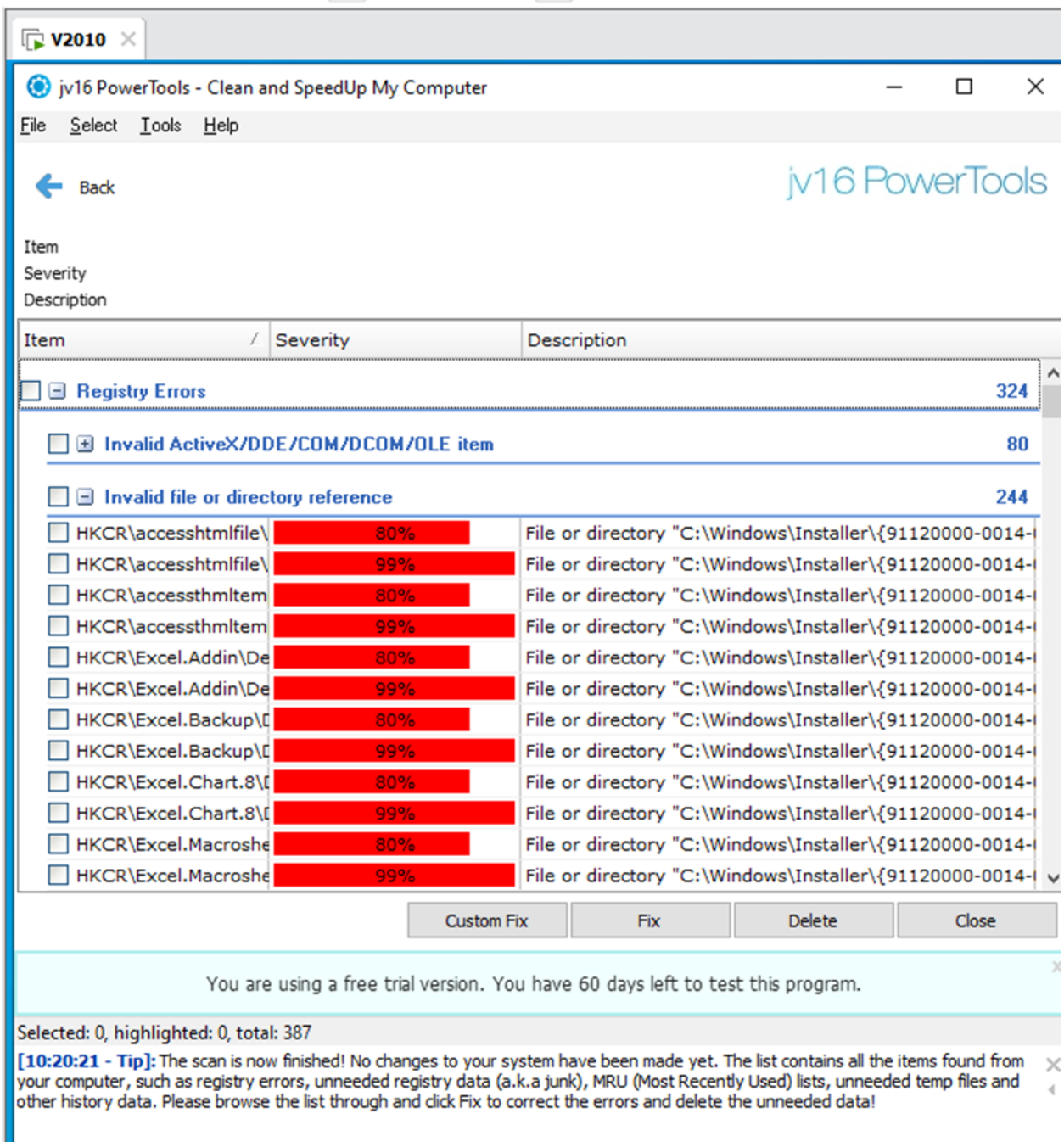

V2010
V2016
jv16 PowerTools - Quick Tutorial
jv16 PowerTools
MAKE
WINDOWS
FAST
Next

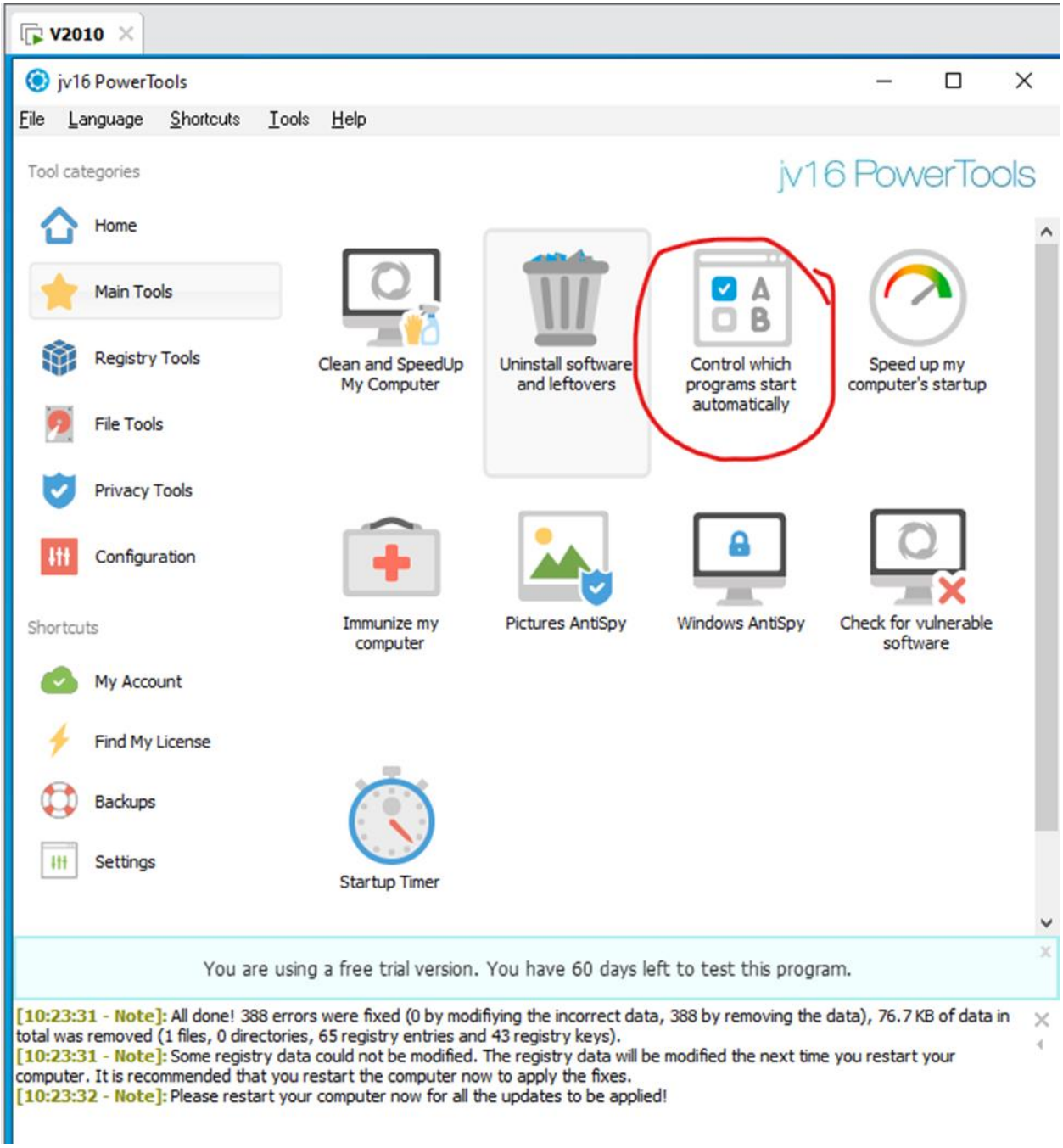

V2010
V2016
jv16 PowerTools
File Language Shortcuts Tools Help
Tool categories
jv16 PowerTools
Home
Main Tools
Registry Tools
File Tools
Privacy Tools
Configuration
Shortcuts
My Account
Find My License
Backups
Settings
Discussion Forum
System health score was analyzed on:
09.10.2023, 10:06 (Today, 11 minutes ago)
Compare the health score against:
(No old health data found)
After you have used the software for a few days, you will be able to use this feature to see how your system health has changed during this time.
System Health
Registry Health
67%
File System Health
50%
Startup System Health
70%
Summary
The health of your registry is not optimal, you should run the Clean and SpeedUp My Computer tool to improve it.
Recommended actions
Privacy
Privacy
Summary
Windows AntiSpy: Disabled
You are using a free trial version. You have 60 days left to test this program.

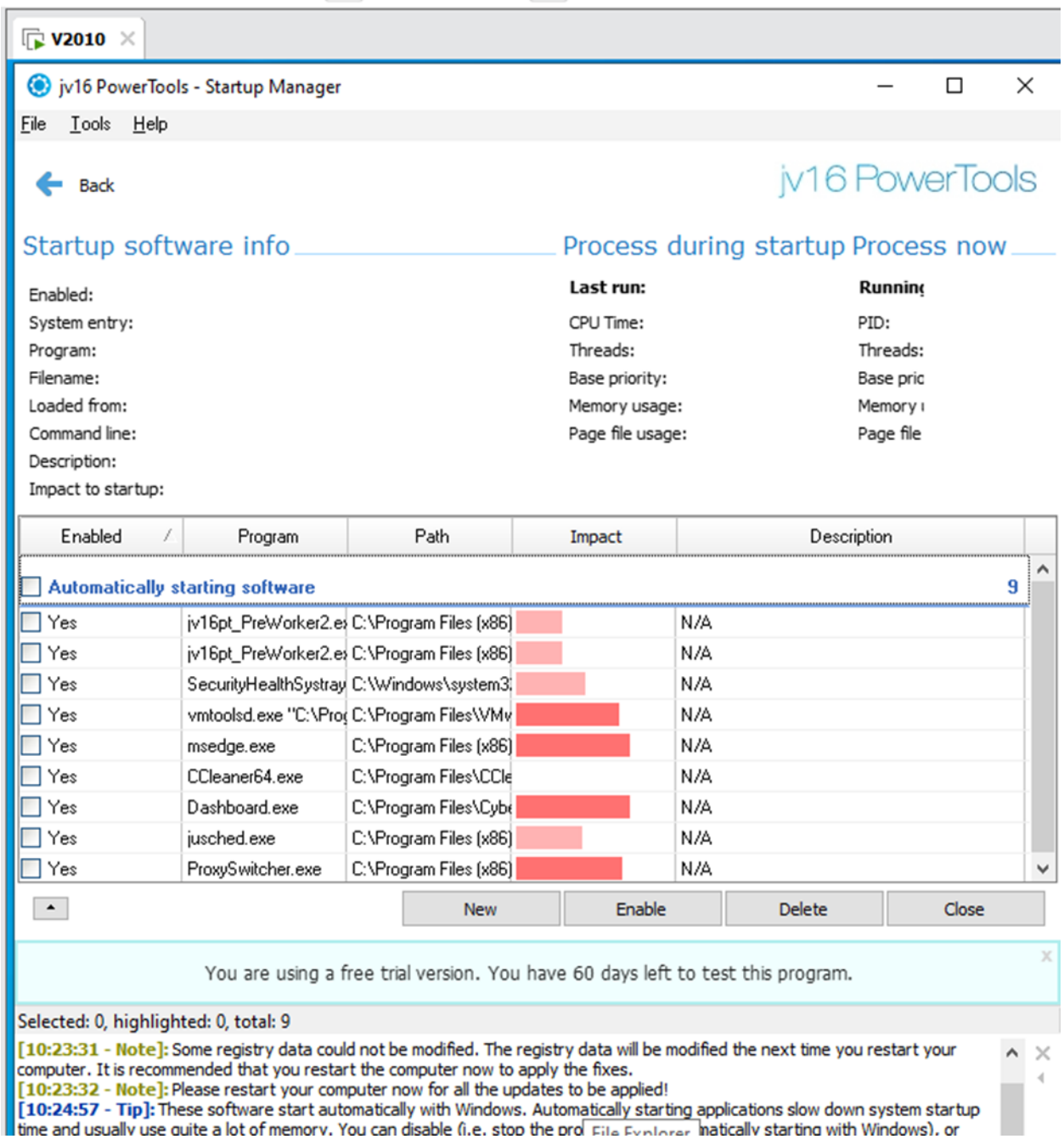

V2010
jv16 PowerTools
File
Language
Shortcuts
Tools
Help
Tool categories
jv16 PowerTools
Home
Main Tools
Registry Tools
File Tools
Privacy Tools
Configuration
Shortcuts
My Account
Find My License
Backups
Settings
Clean and SpeedUp My Computer
Uninstall software and leftovers
Control which programs start automatically
Speed up my computer's startup
Immunize my computer
Pictures AntiSpy
Windows AntiSpy
Check for vulnerable software
Startup Timer

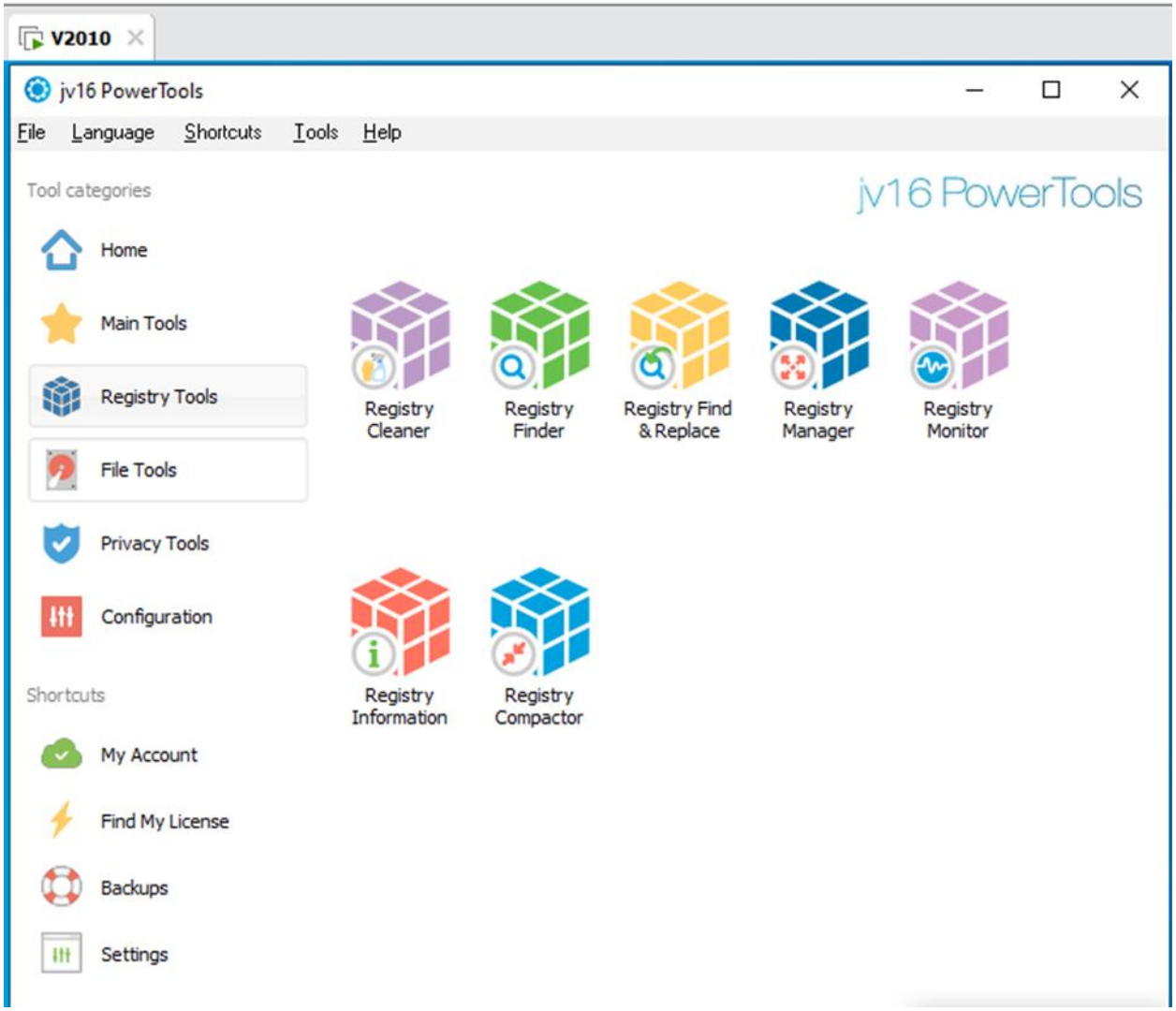

V2010
jv16 PowerTools - Clean and SpeedUp My Computer
File
Tools
Help
Back
jv16 PowerTools
Settings
Additional safety
Additional options
Search words
Ignore words
Settings
This setting defines how aggressive you want the scan to work. The more aggressive setting you use, the more errors and junk the scan will find but that comes with a higher risk of false positives. Only use the more aggressive settings if you know what you are doing.
Extra safe
Aggressive
Startup Optimizer
The Startup Optimizer doesn't remove any data but it makes your computer start faster.
Enable Startup Optimizer to make my computer start faster
Registry Compactor
Start
Cancel
You are using a free trial version. You have 60 days left to test this program.

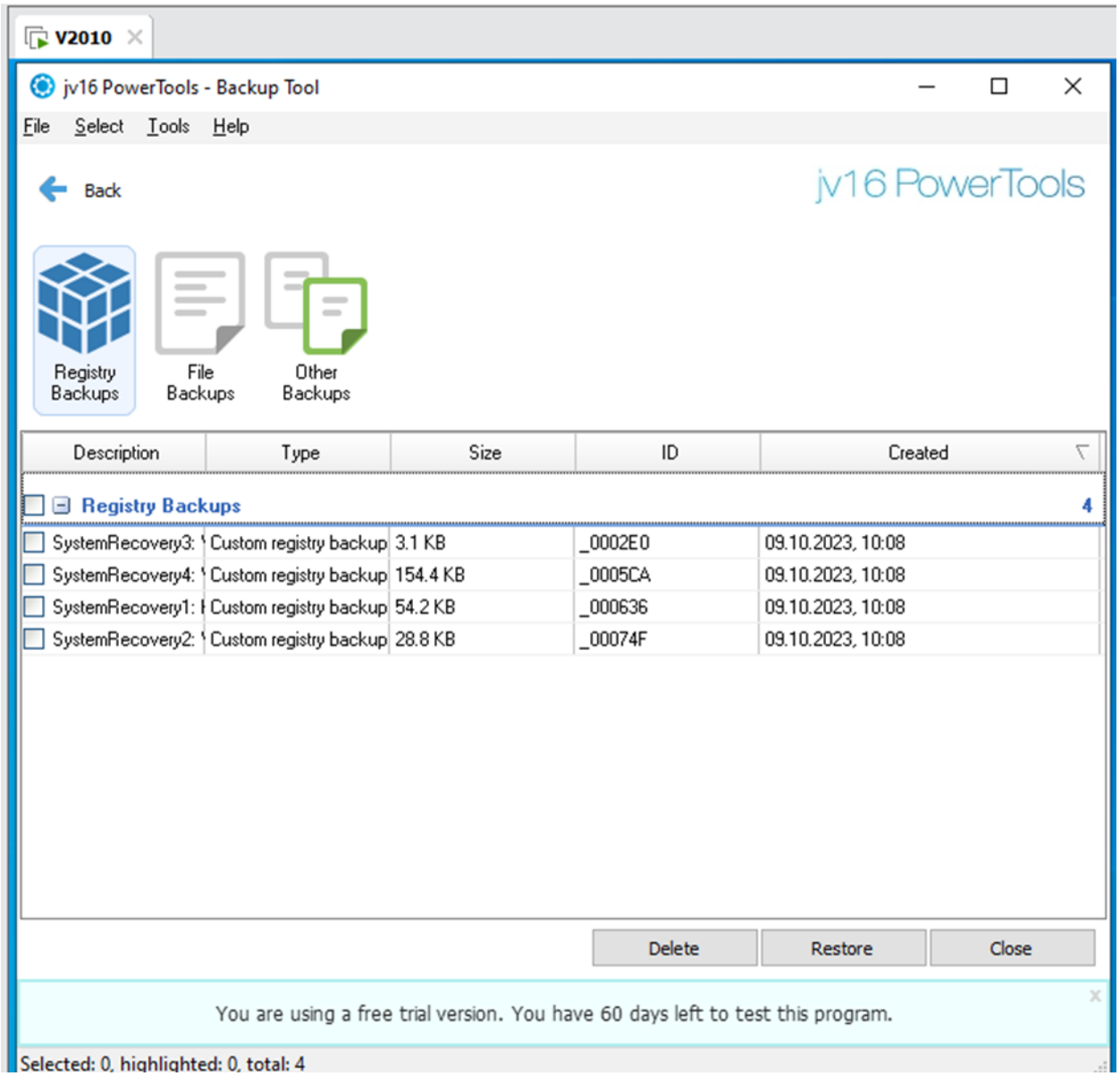

V2010
jv16 PowerTools - Clean and SpeedUp My Computer
File Select Tools Help
Back
jv16 PowerTools
Item
Severity
Description
Item
Severity
Description
Registry Errors 324
Registry junk and leftovers 63
Temp Files 1
Custom Fix
Fix
Delete
Close
You are using a free trial version. You have 60 days left to test this program.
Selected: 0, highlighted: 0, total: 387
[10:20:21 - Tip]: The scan is now finished! No changes to your system have been made yet. The list contains all the items found from your computer, such as registry errors, unneeded registry data (a.k.a junk), MRU (Most Recently Used) lists, unneeded temp files and other history data. Please browse the list through and click Fix to correct the errors and delete the unneeded data!


V2010
jv16 PowerTools - Clean and SpeedUp My Computer
File Select Tools Help
Back
jv16 PowerTools
Item
Severity
Description
Item
Severity
Description
Registry Errors 324
Invalid ActiveX/DDE/COM/DCOM/OLE item 80
Invalid file or directory reference 244
HKCR\accesshtmlfile\ 80% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\accesshtmlfile\ 99% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\accessthmltem 80% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\accessthmltem 99% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\Excel.Addin\De 80% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\Excel.Addin\De 99% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\Excel.Backup\D 80% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\Excel.Backup\D 99% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\Excel.Chart.8\D 80% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\Excel.Chart.8\D 99% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\Excel.Macroshe 80% File or directory "C:\Windows\Installer\{91120000-0014-
HKCR\Excel.Macroshe 99% File or directory "C:\Windows\Installer\{91120000-0014-
Custom Fix
Fix
Delete
Close
You are using a free trial version. You have 60 days left to test this program.
Selected: 0, highlighted: 0, total: 387
[10:20:21 - Tip]: The scan is now finished! No changes to your system have been made yet. The list contains all the items found from your computer, such as registry errors, unneeded registry data (a.k.a junk), MRU (Most Recently Used) lists, unneeded temp files and other history data. Please browse the list through and click Fix to correct the errors and delete the unneeded data!


V2010
jv16 PowerTools
File Language Shortcuts Tools Help
Tool categories
jv16 PowerTools
Home
Main Tools
Registry Tools
File Tools
Privacy Tools
Configuration
Shortcuts
My Account
Find My License
Backups
Settings
Clean and SpeedUp My Computer
Uninstall software and leftovers
Control which programs start automatically
Speed up my computer's startup
Immunize my computer
Pictures AntiSpy
Windows AntiSpy
Check for vulnerable software
Startup Timer
You are using a free trial version. You have 60 days left to test this program.
[10:23:31 - Note]: All done! 388 errors were fixed (0 by modifiying the incorrect data, 388 by removing the data), 76.7 KB of data in total was removed (1 files, 0 directories, 65 registry entries and 43 registry keys).
[10:23:31 - Note]: Some registry data could not be modified. The registry data will be modified the next time you restart your computer. It is recommended that you restart the computer now to apply the fixes.
[10:23:32 - Note]: Please restart your computer now for all the updates to be applied!


V2010
jv16 PowerTools - Startup Manager
File Tools Help
Back
jv16 PowerTools
Startup software info
Process during startup
Process now
Enabled:
System entry:
Program:
Filename:
Loaded from:
Command line:
Description:
Impact to startup:
Last run:
CPU Time:
Threads:
Base priority:
Memory usage:
Page file usage:
Running
PID:
Threads:
Base pric
Memory
Page file
Enabled
Program
Path
Impact
Description
Automatically starting software 9
Yes jv16pt_PreWorker2.e C:\Program Files (x86) N/A
Yes jv16pt_PreWorker2.e C:\Program Files (x86) N/A
Yes SecurityHealthSystray C:\Windows\system3 N/A
Yes vmtoolsd.exe "C:\Pro C:\Program Files\VMv N/A
Yes msedge.exe C:\Program Files (x86) N/A
Yes CCleaner64.exe C:\Program Files\CCle N/A
Yes Dashboard.exe C:\Program Files\Cybe N/A
Yes jusched.exe C:\Program Files (x86) N/A
Yes ProxySwitcher.exe C:\Program Files (x86) N/A
New
Enable
Delete
Close
You are using a free trial version. You have 60 days left to test this program.
Selected: 0, highlighted: 0, total: 9
[10:23:31 - Note]: Some registry data could not be modified. The registry data will be modified the next time you restart your computer. It is recommended that you restart the computer now to apply the fixes.
[10:23:32 - Note]: Please restart your computer now for all the updates to be applied!
[10:24:57 - Tip]: These software start automatically with Windows. Automatically starting applications slow down system startup time and usually use quite a lot of memory. You can disable (i.e. stop the pro File Explorer matically starting with Windows), or


V2010
jv16 PowerTools
File
Language
Shortcuts
Tools
Help
Tool categories
jv16 PowerTools
Home
Main Tools
Registry Tools
File Tools
Privacy Tools
Configuration
Shortcuts
My Account
Find My License
Backups
Settings
Registry Cleaner
Registry Finder
Registry Find & Replace
Registry Manager
Registry Monitor
Registry Information
Registry Compactor


V2010
jv16 PowerTools - Backup Tool
File Select Tools Help
Back
jv16 PowerTools
Registry Backups
File Backups
Other Backups
Description Type Size ID Created
Registry Backups 4
SystemRecovery3: Custom registry backup 3.1 KB _0002E0 09.10.2023, 10:08
SystemRecovery4: Custom registry backup 154.4 KB _0005CA 09.10.2023, 10:08
SystemRecovery1: Custom registry backup 54.2 KB _000636 09.10.2023, 10:08
SystemRecovery2: Custom registry backup 28.8 KB _00074F 09.10.2023, 10:08
Delete
Restore
Close
You are using a free trial version. You have 60 days left to test this program.
Selected: 0, highlighted: 0, total: 4