

Lab 4: Perform Dynamic Malware Analysis

Task 1: Perform Port Monitoring using TCPView and CurrPorts

We know that the Internet uses a software protocol named TCP/IP to format and transfer data. Malware programs corrupt the system and open system input and output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also act as backdoors or communication channels for other types of harmful malware and programs. They open unused ports on the victim's machine to connect back to the malware handlers.

You can identify the malware trying to access a particular port by installing port monitoring tools such as TCPView and CurrPorts.

TCPView TCPView is a Windows program that shows the detailed listings of all the TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpcvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

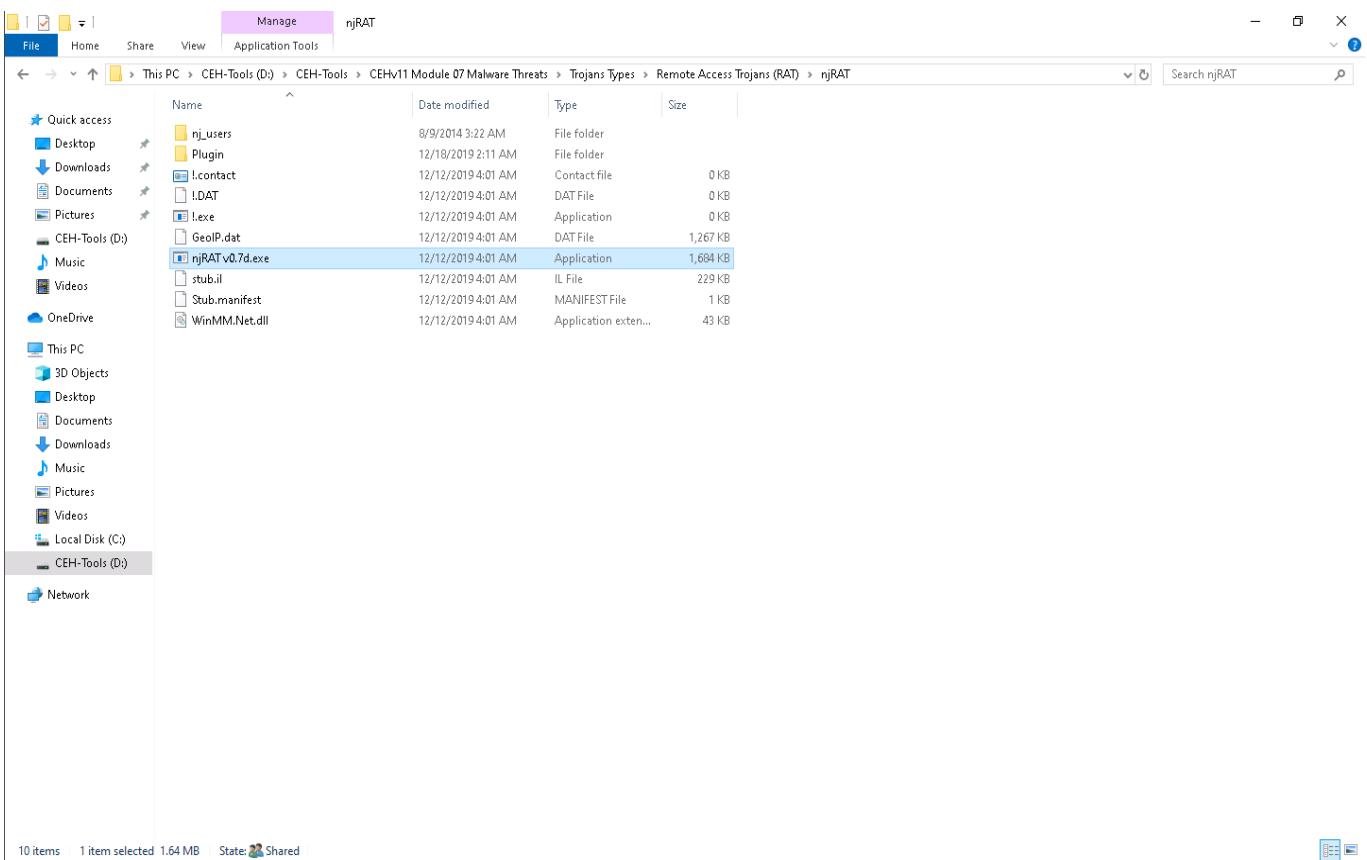
CurrPorts CurrPorts is a piece of network monitoring software that displays a list of all the currently open TCP/IP and UDP ports on a local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, etc.), the time that the process was created, and the user that created it.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP port information to an HTML file, XML file, or to tab-delimited text file.

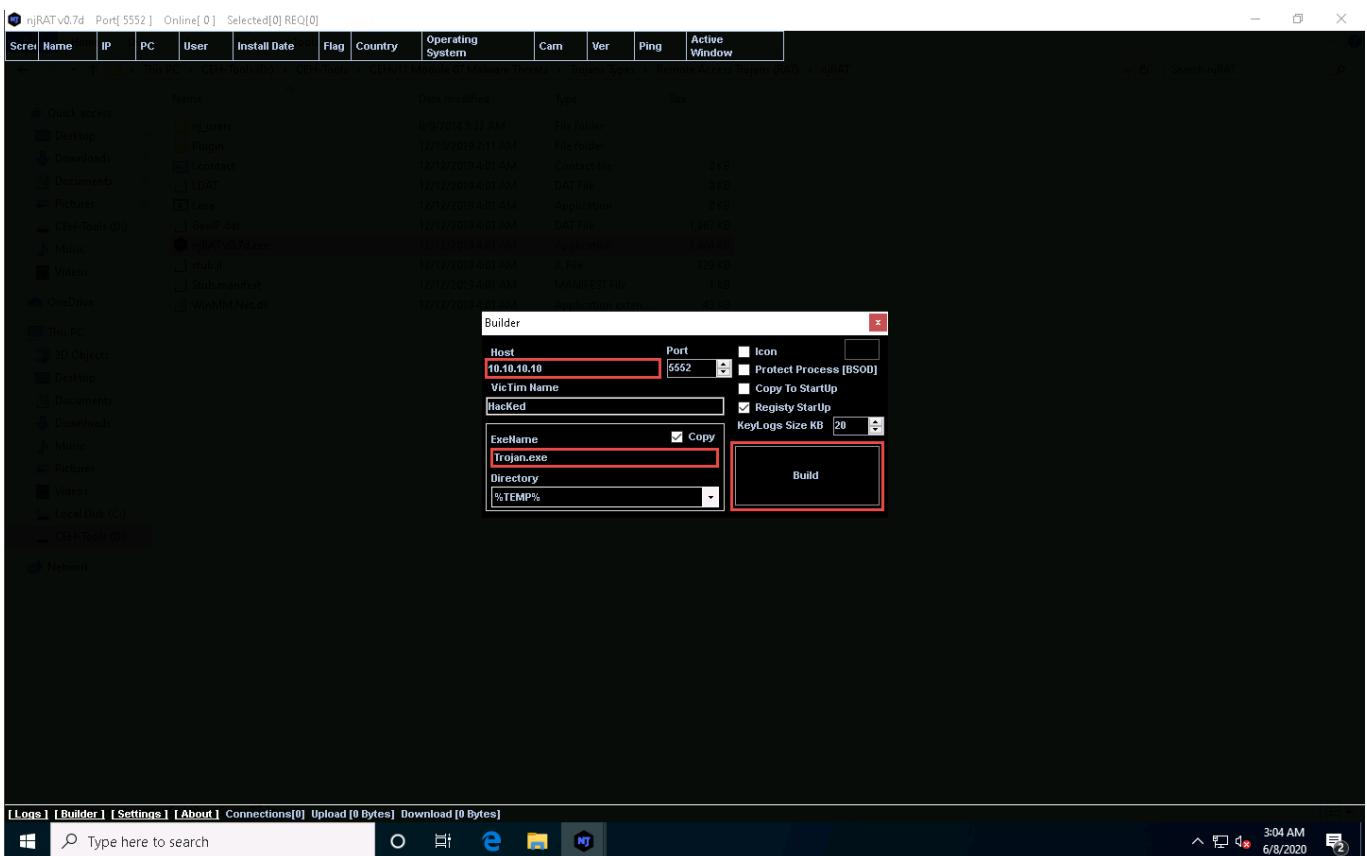
CurrPorts also automatically marks suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons) in pink.

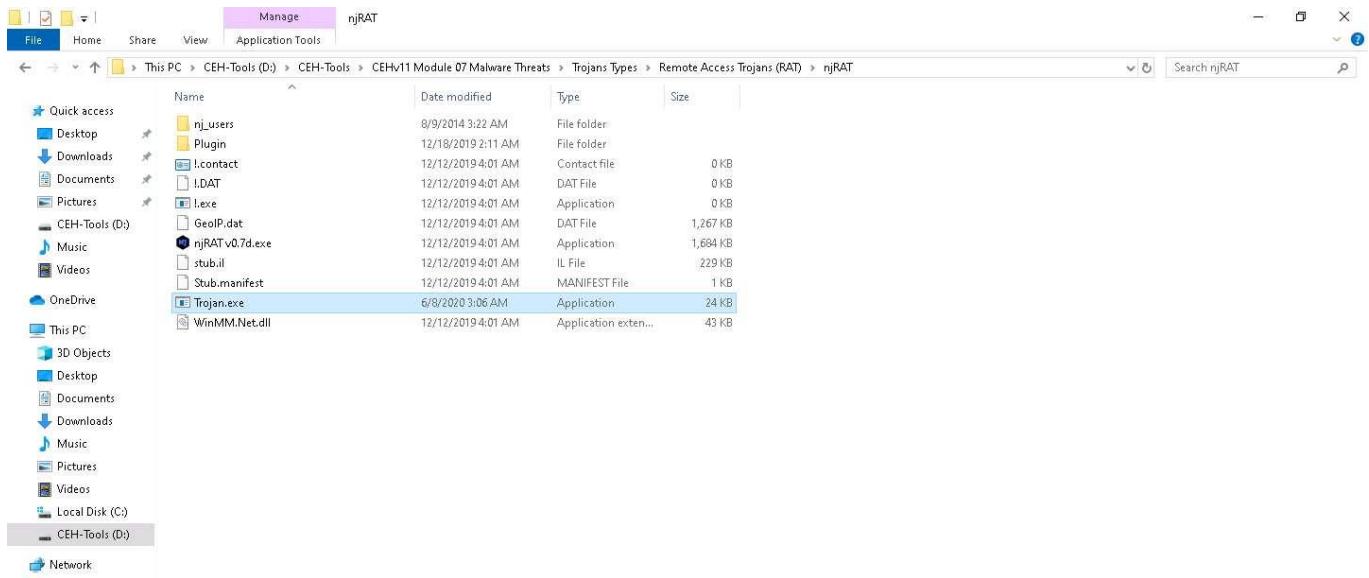
This lab activity demonstrates how to analyze malicious processes running on a machine using TCPView and CurrPorts. Here, you will first create a server using njRAT, and then execute this server from the second machine. Later, you will run the TCPView and CurrPorts applications on the second machine and find that the process associated with the server is running on it.

1. On the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe** to launch **njRAT**.

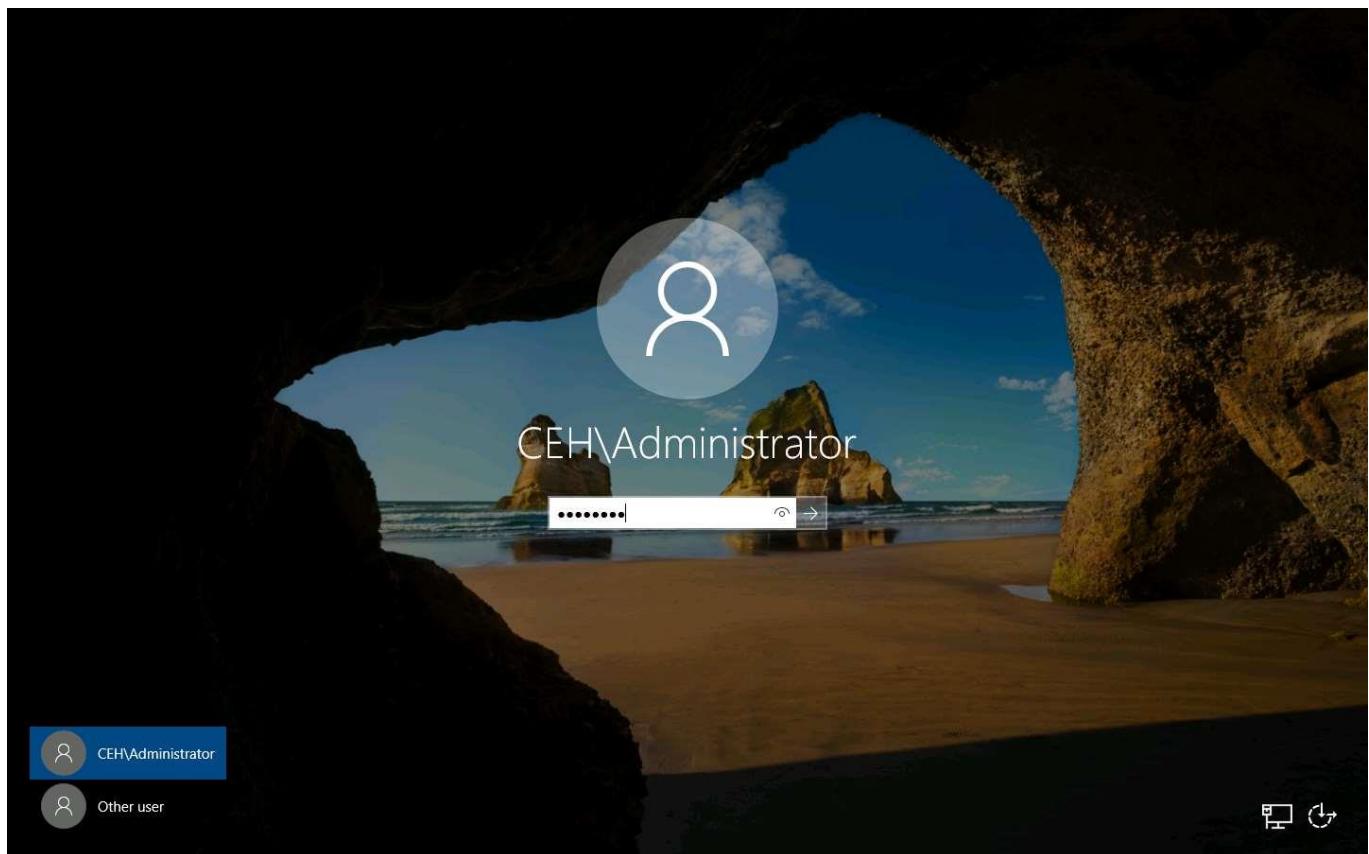


2. Create a server and save it to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.
3. While building the server, assign the server name **Trojan.exe** for demonstration purposes.

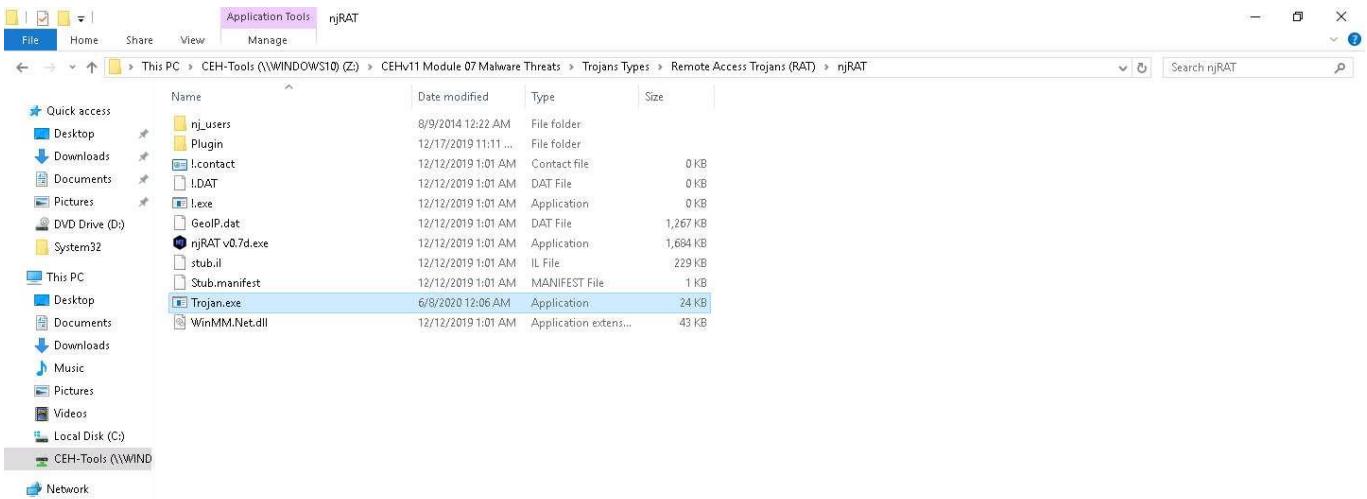




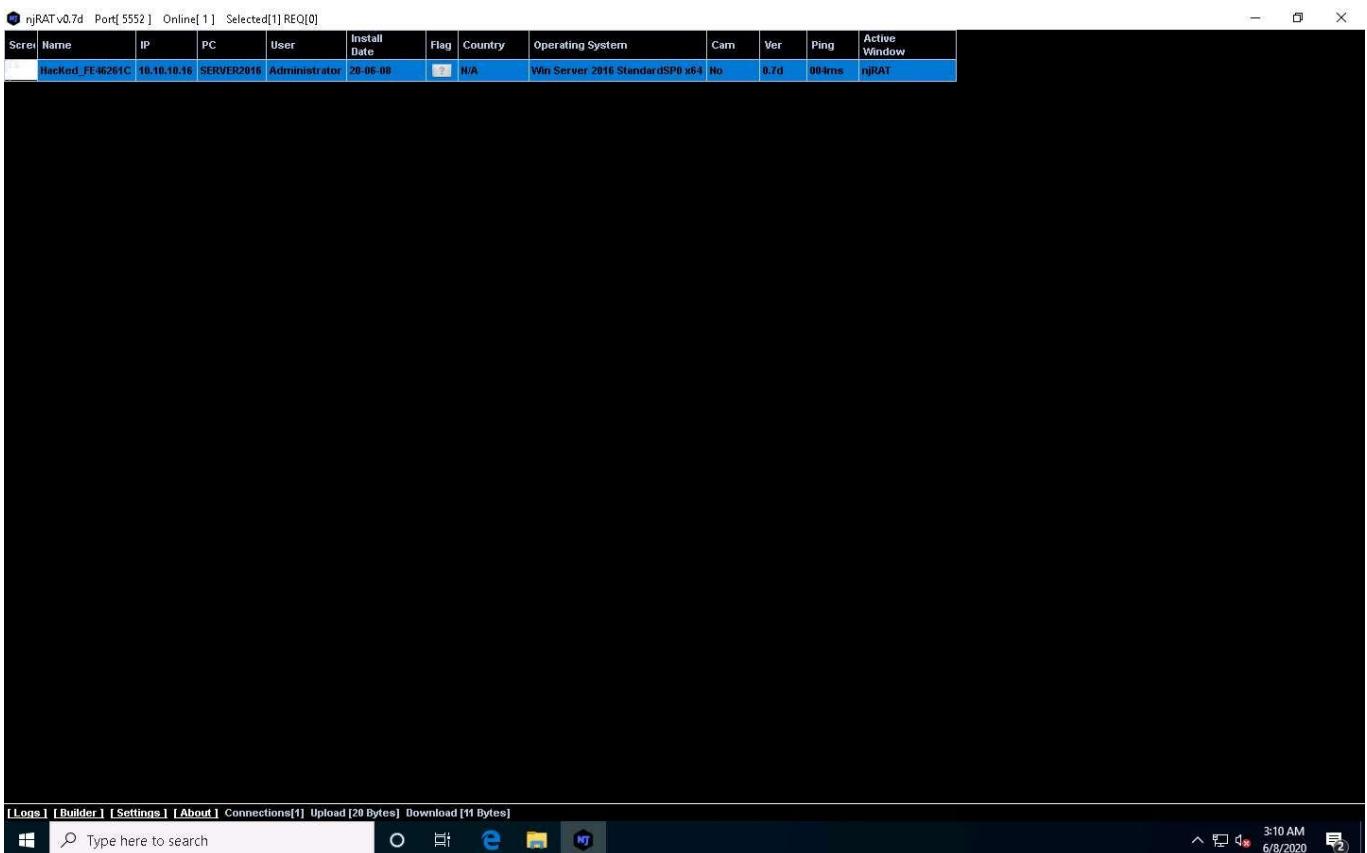
4. Click [Windows Server 2016](#) to switch to the **Windows Server 2016** machine. Click **[Ctrl+Alt+Delete](#)** to activate the machine, by default, **CEH\Administrator** account is selected, click **Pa\$\$w0rd** to enter the password and press **Enter**.



5. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe**.



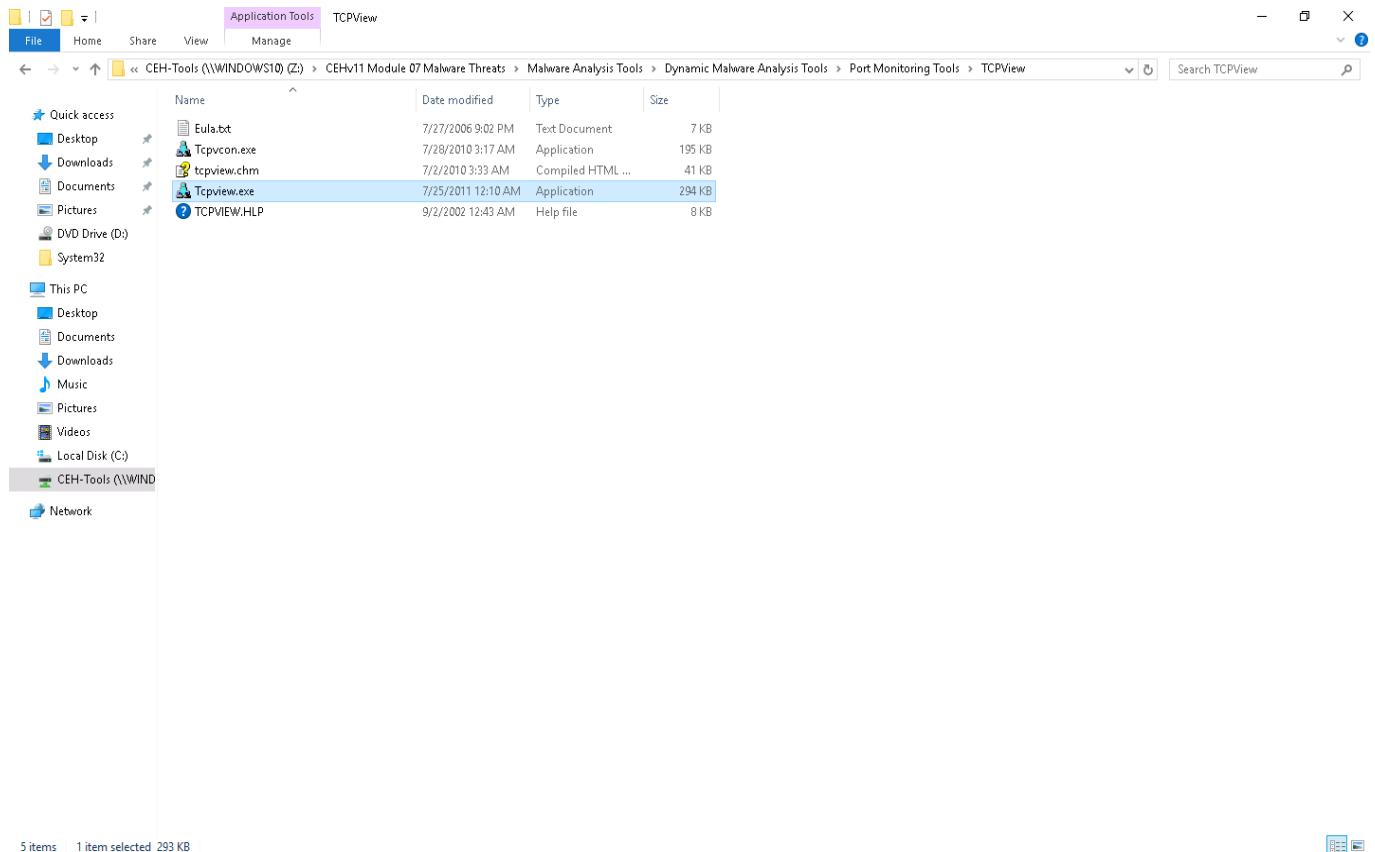
6. Observe that a connection has been established by the njRAT client. Click [Windows 10](#) to switch to the **Windows 10** machine to observe the established connection.



7. Now, let us analyze this process on **Windows Server 2016** using **TCPView** tool. Click [Windows Server 2016](#) to switch back to the **Windows Server 2016** machine.

8. Navigate to Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView and double-click **Tcpview.exe** to launch the application.

If a **User Account Control** pop-up appears, click **Yes**.



9. If a **TCPView License Agreement** window appears, click the **Agree** button to agree to the terms and conditions.
10. The **TCPView** main window appears, displaying the details such as Process, ProcessId, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State, as shown in the screenshot.

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

A →

Process	/	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc]	/	0	TCPV6	[fe80::0:0:e564...]	22816	[fe80::0:0:e564...]	epmap	TIME_WAIT				
[dns.exe]	/	2288	TCP	Server2016	1064	Server2016	0	LISTENING				
[dns.exe]	/	2288	UDP	Server2016	62360	*	*					
[dns.exe]	/	2288	TCPV6	[fe80::0:0:e564...]	1059	[fe80::0:0:e564...]	ldap	ESTABLISHED				
[dns.exe]	/	2288	TCPV6	[fe80::0:0:e564...]	1061	[fe80::0:0:e564...]	1539	ESTABLISHED				
[dns.exe]	/	2288	TCPV6	[fe80::0:0:e564...]	1062	[fe80::0:0:e564...]	ldap	ESTABLISHED				
[dns.exe]	/	2288	TCPV6	[fe80::0:0:e564...]	1064	[0:0:0:0:0:0]	0	LISTENING				
[dssvc.exe]	/	2436	TCPV6	[fe80::0:0:e564...]	1578	[fe80::0:0:e564...]	1539	ESTABLISHED				
[dns.exe]	/	2192	TCP	server2016.ceh.com	domain	Server2016	0	LISTENING				
[dns.exe]	/	2192	TCP	Server2016	1574	Server2016	0	LISTENING				
[dns.exe]	/	2192	UDP	server2016.ceh.com	domain	*	*					
[dns.exe]	/	2192	UDP	Server2016	49787	*	*					
[dns.exe]	/	2192	UDP	Server2016	50784	*	*					
[dns.exe]	/	2192	UDP	Server2016	50785	*	*					
[dns.exe]	/	2192	UDP	Server2016	50786	*	*					
[dns.exe]	/	2192	UDP	Server2016	50787	*	*					
[dns.exe]	/	2192	UDP	Server2016	50788	*	*					
[dns.exe]	/	2192	UDP	Server2016	50789	*	*					
[dns.exe]	/	2192	UDP	Server2016	50790	*	*					
[dns.exe]	/	2192	UDP	Server2016	50791	*	*					
[dns.exe]	/	2192	UDP	Server2016	50792	*	*					
[dns.exe]	/	2192	UDP	Server2016	50793	*	*					
[dns.exe]	/	2192	UDP	Server2016	50794	*	*					
[dns.exe]	/	2192	UDP	Server2016	50795	*	*					
[dns.exe]	/	2192	UDP	Server2016	50796	*	*					
[dns.exe]	/	2192	UDP	Server2016	50797	*	*					
[dns.exe]	/	2192	UDP	Server2016	50798	*	*					
[dns.exe]	/	2192	UDP	Server2016	50799	*	*					
[dns.exe]	/	2192	UDP	Server2016	50800	*	*					
[dns.exe]	/	2192	UDP	Server2016	50801	*	*					
[dns.exe]	/	2192	UDP	Server2016	50802	*	*					
[dns.exe]	/	2192	UDP	Server2016	50803	*	*					
[dns.exe]	/	2192	UDP	Server2016	50804	*	*					
[dns.exe]	/	2192	UDP	Server2016	50805	*	*					
[dns.exe]	/	2192	UDP	Server2016	50806	*	*					
[dns.exe]	/	2192	UDP	Server2016	50807	*	*					
[dns.exe]	/	2192	UDP	Server2016	50812	*	*					
[dns.exe]	/	2192	UDP	Server2016	50813	*	*					
[dns.exe]	/	2192	UDP	Server2016	50814	*	*					
[dns.exe]	/	2192	UDP	Server2016	50815	*	*					
[dns.exe]	/	2192	UDP	Server2016	50816	*	*					
[dns.exe]	/	2192	UDP	Server2016	50817	*	*					
[dns.exe]	/	2192	UDP	Server2016	50818	*	*					
[dns.exe]	/	2192	UDP	Server2016	50819	*	*					
[dns.exe]	/	2192	UDP	Server2016	50820	*	*					
[dns.exe]	/	2192	UDP	Server2016	50821	*	*					
[dns.exe]	/	2192	UDP	Server2016	50822	*	*					
[dns.exe]	/	2192	UDP	Server2016	50823	*	*					
[dns.exe]	/	2192	UDP	Server2016	50824	*	*					
[dns.exe]	/	2192	UDP	Server2016	50825	*	*					
[dns.exe]	/	2192	UDP	Server2016	50826	*	*					
[dns.exe]	/	2192	UDP	Server2016	50827	*	*					
[dns.exe]	/	2192	UDP	Server2016	50828	*	*					
[dns.exe]	/	2192	UDP	Server2016	50829	*	*					
[dns.exe]	/	2192	UDP	Server2016	50830	*	*					
[dns.exe]	/	2192	UDP	Server2016	50831	*	*					
[dns.exe]	/	2192	UDP	Server2016	50832	*	*					

Windows Taskbar: TCPView, File Explorer, Internet Explorer, Mozilla Firefox, FileZilla, Task View, Start button, Search, Task View icon, Date/Time: 12:16 AM, Date: 6/8/2020, Taskbar icon.

11. TCPView performs **Port monitoring**. Click the **Local Port** tab to view the ports in serial order.

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

A →

Process	/	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc]	/	0	TCPV6	[fe80::0:0:e564...]	22816	[fe80::0:0:e564...]	epmap	TIME_WAIT				
[dns.exe]	/	2288	TCP	Server2016	1064	Server2016	0	LISTENING				
[dns.exe]	/	2288	UDP	Server2016	62360	*	*					
[dns.exe]	/	2288	TCPV6	[fe80::0:0:e564...]	1059	[fe80::0:0:e564...]	ldap	ESTABLISHED				
[dns.exe]	/	2288	TCPV6	[fe80::0:0:e564...]	1061	[fe80::0:0:e564...]	1539	ESTABLISHED				
[dns.exe]	/	2288	TCPV6	[fe80::0:0:e564...]	1062	[fe80::0:0:e564...]	ldap	ESTABLISHED				
[dns.exe]	/	2288	TCPV6	[fe80::0:0:e564...]	1064	[0:0:0:0:0:0]	0	LISTENING				
[dssvc.exe]	/	2436	TCPV6	[fe80::0:0:e564...]	1578	[fe80::0:0:e564...]	1539	ESTABLISHED				
[dns.exe]	/	2192	TCP	server2016.ceh.com	domain	Server2016	0	LISTENING				
[dns.exe]	/	2192	TCP	Server2016	1574	Server2016	0	LISTENING				
[dns.exe]	/	2192	UDP	server2016.ceh.com	domain	*	*					
[dns.exe]	/	2192	UDP	Server2016	49787	*	*					
[dns.exe]	/	2192	UDP	Server2016	50784	*	*					
[dns.exe]	/	2192	UDP	Server2016	50785	*	*					
[dns.exe]	/	2192	UDP	Server2016	50786	*	*					
[dns.exe]	/	2192	UDP	Server2016	50787	*	*					
[dns.exe]	/	2192	UDP	Server2016	50788	*	*					
[dns.exe]	/	2192	UDP	Server2016	50789	*	*					
[dns.exe]	/	2192	UDP	Server2016	50790	*	*					
[dns.exe]	/	2192	UDP	Server2016	50791	*	*					
[dns.exe]	/	2192	UDP	Server2016	50792	*	*					
[dns.exe]	/	2192	UDP	Server2016	50793	*	*					
[dns.exe]	/	2192	UDP	Server2016	50794	*	*					
[dns.exe]	/	2192	UDP	Server2016	50795	*	*					
[dns.exe]	/	2192	UDP	Server2016	50796	*	*					
[dns.exe]	/	2192	UDP	Server2016	50797	*	*					
[dns.exe]	/	2192	UDP	Server2016	50798	*	*					
[dns.exe]	/	2192	UDP	Server2016	50799	*	*					
[dns.exe]	/	2192	UDP	Server2016	50800	*	*					
[dns.exe]	/	2192	UDP	Server2016	50801	*	*					
[dns.exe]	/	2192	UDP	Server2016	50802	*	*					
[dns.exe]	/	2192	UDP	Server2016	50803	*	*					
[dns.exe]	/	2192	UDP	Server2016	50804	*	*					
[dns.exe]	/	2192	UDP	Server2016	50805	*	*					
[dns.exe]	/	2192	UDP	Server2016	50806	*	*					
[dns.exe]	/	2192	UDP	Server2016	50807	*	*					
[dns.exe]	/	2192	UDP	Server2016	50812	*	*					
[dns.exe]	/	2192	UDP	Server2016	50813	*	*					
[dns.exe]	/	2192	UDP	Server2016	50814	*	*					
[dns.exe]	/	2192	UDP	Server2016	50815	*	*					
[dns.exe]	/	2192	UDP	Server2016	50816	*	*					
[dns.exe]	/	2192	UDP	Server2016	50817	*	*					
[dns.exe]	/	2192	UDP	Server2016	50818	*	*					
[dns.exe]	/	2192	UDP	Server2016	50819	*	*					
[dns.exe]	/	2192	UDP	Server2016	50820	*	*					
[dns.exe]	/	2192	UDP	Server2016	50821	*	*					
[dns.exe]	/	2192	UDP	Server2016	50822	*	*					
[dns.exe]	/	2192	UDP	Server2016	50823	*	*					
[dns.exe]	/	2192	UDP	Server2016	50824	*	*					
[dns.exe]	/	2192	UDP	Server2016	50825	*	*					

Windows Taskbar: TCPView, File Explorer, Internet Explorer, Mozilla Firefox, FileZilla, Task View, Start button, Search, Task View icon, Date/Time: 12:18 AM, Date: 6/8/2020, Taskbar icon.

12. Observe the protocols running on different ports under the **Protocol** column.

TCPView - Sysinternals: www.sysinternals.com

Process /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc... 0		TCPV6	[fe80::0:e564:3...	22816	[fe80::0:e564:3...	epmap	TIME_WAIT				
dfsvc.exe 2288	TCP	Server2016	1064		Server2016	0	LISTENING				
dfsvc.exe 2288	UDP	Server2016	62360	x		x					
dfsvc.exe 2288	TCPV6	[fe80::0:e564:3...	1059		[fe80::0:e564:3...	ldaps	ESTABLISHED				
dfsvc.exe 2288	TCPV6	[fe80::0:e564:3...	1061		[fe80::0:e564:3...	1539	ESTABLISHED				
dfsvc.exe 2288	TCPV6	[fe80::0:e564:3...	1062		[fe80::0:e564:3...	ldaps	ESTABLISHED				
dfsvc.exe 2288	TCPV6	[0.0.0.0.0.0]	1064		[0.0.0.0.0.0]	0	LISTENING				
dfsvc.exe 2436	TCPV6	[fe80::0:e564:3...	1578		[fe80::0:e564:3...	1539	ESTABLISHED				
dns.exe 2192	TCP	server2016.ceh.com	domain		Server2016	0	LISTENING				
dns.exe 2192	TCP	Server2016	domain		Server2016	0	LISTENING				
dns.exe 2192	TCP	Server2016	1574		Server2016	0	LISTENING				
dns.exe 2192	UDP	server2016.ceh.com	domain		x	x					
dns.exe 2192	UDP	Server2016	50787		x	x					
dns.exe 2192	UDP	Server2016	49787		x	x					
dns.exe 2192	UDP	Server2016	50793		x	x					
dns.exe 2192	UDP	Server2016	50784		x	x					
dns.exe 2192	UDP	Server2016	50785		x	x					
dns.exe 2192	UDP	Server2016	50796		x	x					
dns.exe 2192	UDP	Server2016	50787		x	x					
dns.exe 2192	UDP	Server2016	50788		x	x					
dns.exe 2192	UDP	Server2016	50789		x	x					
dns.exe 2192	UDP	Server2016	50790		x	x					
dns.exe 2192	UDP	Server2016	50791		x	x					
dns.exe 2192	UDP	Server2016	50792		x	x					
dns.exe 2192	UDP	Server2016	50793		x	x					
dns.exe 2192	UDP	Server2016	50794		x	x					
dns.exe 2192	UDP	Server2016	50795		x	x					
dns.exe 2192	UDP	Server2016	50796		x	x					
dns.exe 2192	UDP	Server2016	50798		x	x					
dns.exe 2192	UDP	Server2016	50789		x	x					
dns.exe 2192	UDP	Server2016	50799		x	x					
dns.exe 2192	UDP	Server2016	50800		x	x					
dns.exe 2192	UDP	Server2016	50801		x	x					
dns.exe 2192	UDP	Server2016	50802		x	x					
dns.exe 2192	UDP	Server2016	50803		x	x					
dns.exe 2192	UDP	Server2016	50804		x	x					
dns.exe 2192	UDP	Server2016	50805		x	x					
dns.exe 2192	UDP	Server2016	50806		x	x					
dns.exe 2192	UDP	Server2016	50807		x	x					
dns.exe 2192	UDP	Server2016	50812		x	x					
dns.exe 2192	UDP	Server2016	50813		x	x					
dns.exe 2192	UDP	Server2016	50814		x	x					
dns.exe 2192	UDP	Server2016	50815		x	x					
dns.exe 2192	UDP	Server2016	50816		x	x					
dns.exe 2192	UDP	Server2016	50817		x	x					
dns.exe 2192	UDP	Server2016	50818		x	x					
dns.exe 2192	UDP	Server2016	50819		x	x					
dns.exe 2192	UDP	Server2016	50820		x	x					
dns.exe 2192	UDP	Server2016	50821		x	x					
dns.exe 2192	UDP	Server2016	50822		x	x					
dns.exe 2192	UDP	Server2016	50823		x	x					
dns.exe 2192	UDP	Server2016	50824		x	x					
dns.exe 2192	UDP	Server2016	50825		x	x					

Windows taskbar: TCPView, File Explorer, Edge, Firefox, Task View, 12:18 AM, 6/8/2020

13. As you have executed a malicious application, now search for the **Trojan.exe** process in the TCPView.
14. You can observe that the **Trojan.exe** malicious program is running on the **Windows Server 2016** machine. You can see details such as **Remote Address** and **Remote Port**.

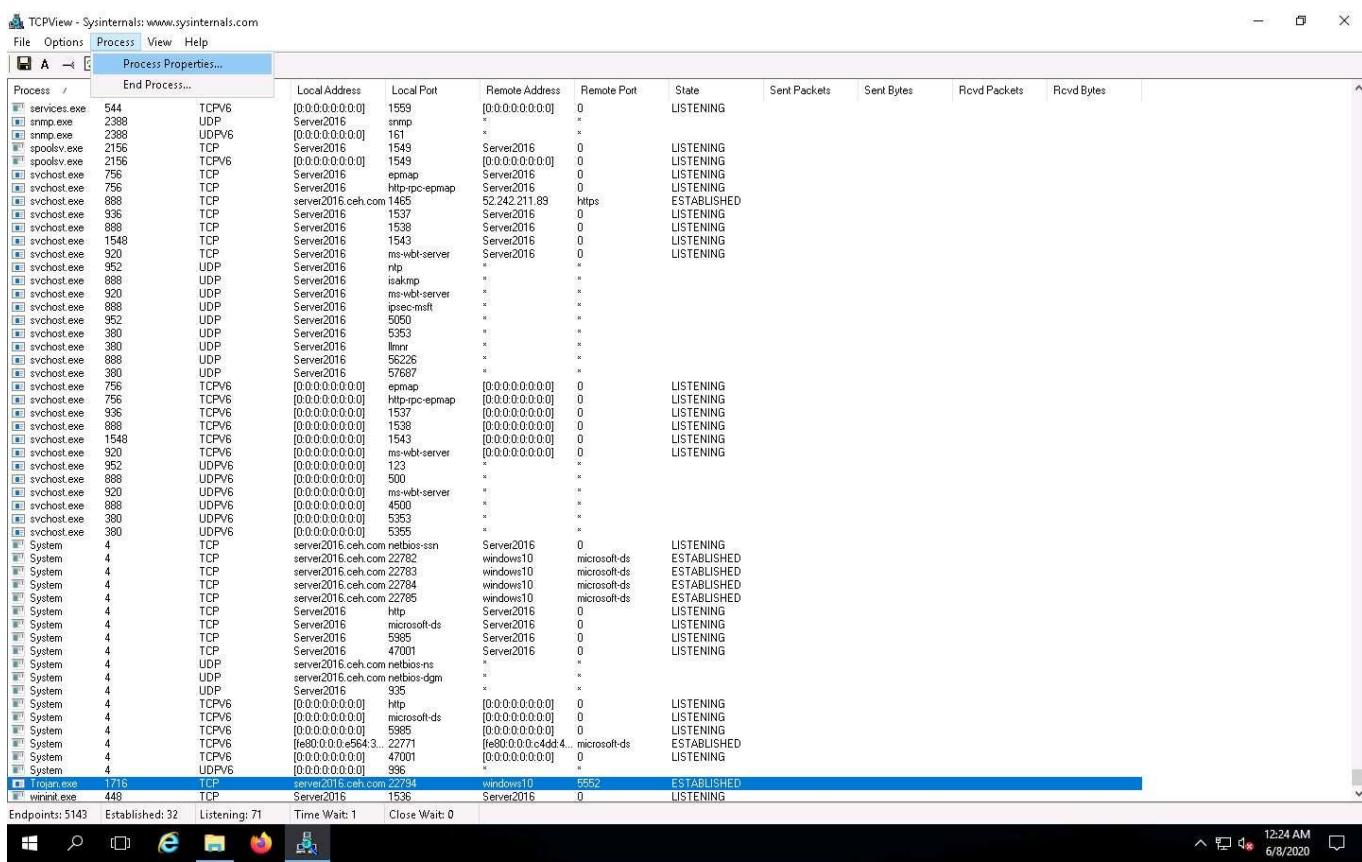
TCPView - Sysinternals: www.sysinternals.com

Process /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[svchost.exe 756	TCP	Server2016	epmap		Server2016	0	LISTENING				
svchost.exe 756	TCP	Server2016	http-epmap		Server2016	0	LISTENING				
svchost.exe 888	TCP	server2016.ceh.com	1455		52.242.211.89	https	ESTABLISHED				
svchost.exe 936	TCP	Server2016	1537		Server2016	0	LISTENING				
svchost.exe 888	TCP	Server2016	1538		Server2016	0	LISTENING				
svchost.exe 1548	TCP	Server2016	1543		Server2016	0	LISTENING				
svchost.exe 920	TCP	Server2016	ms-wbt-server		Server2016	0	LISTENING				
svchost.exe 952	UDP	Server2016	nt		x	x					
svchost.exe 888	UDP	Server2016	isakmp		x	x					
svchost.exe 920	UDP	Server2016	ms-wbt-server		x	x					
svchost.exe 888	UDP	Server2016	ipsec-msft		x	x					
svchost.exe 952	UDP	Server2016	5050		x	x					
svchost.exe 380	UDP	Server2016	5353		x	x					
svchost.exe 888	UDP	Server2016	lmm		x	x					
svchost.exe 380	UDP	Server2016	56226		x	x					
svchost.exe 756	TCPV6	[0.0.0.0.0.0]	epmap		[0.0.0.0.0.0]	0	LISTENING				
svchost.exe 756	TCPV6	[0.0.0.0.0.0]	Http-epmap		[0.0.0.0.0.0]	0	LISTENING				
svchost.exe 936	TCPV6	[0.0.0.0.0.0]	1537		[0.0.0.0.0.0]	0	LISTENING				
svchost.exe 888	TCPV6	[0.0.0.0.0.0]	1538		[0.0.0.0.0.0]	0	LISTENING				
svchost.exe 1548	TCPV6	[0.0.0.0.0.0]	1543		[0.0.0.0.0.0]	0	LISTENING				
svchost.exe 920	TCPV6	[0.0.0.0.0.0]	ms-wbt-server		[0.0.0.0.0.0]	0	LISTENING				
svchost.exe 952	UDPV6	[0.0.0.0.0.0]	123		x	x					
svchost.exe 888	UDPV6	[0.0.0.0.0.0]	500		x	x					
svchost.exe 920	UDPV6	[0.0.0.0.0.0]	ms-wbt-server		x	x					
svchost.exe 888	UDPV6	[0.0.0.0.0.0]	4500		x	x					
svchost.exe 380	UDPV6	[0.0.0.0.0.0]	5353		x	x					
svchost.exe 380	UDPV6	[0.0.0.0.0.0]	5355		x	x					
svchost.exe 888	TCP	server2016.ceh.com	22828		server2016.ceh.com	ldaps	ESTABLISHED				
svchost.exe 888	TCPV6	[fe80::0:e564:3...	22826		[fe80::0:e564:3...	ldaps	ESTABLISHED				
System 4	TCP	server2016.ceh.com	netbios-ssn		Server2016	0	LISTENING				
System 4	TCP	server2016.ceh.com	22782		windows10	microsoft-ds	ESTABLISHED				
System 4	TCP	server2016.ceh.com	22784		windows10	microsoft-ds	ESTABLISHED				
System 4	TCP	server2016.ceh.com	22785		windows10	microsoft-ds	ESTABLISHED				
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-dgm		x	x					
System 4	UDP	Server2016	935		x	x					
System 4	TCPV6	[0.0.0.0.0.0]	http		[0.0.0.0.0.0]	0	LISTENING				
System 4	TCPV6	[0.0.0.0.0.0]	microsoft-ds		[fe80::0:e564:3...	22829	ESTABLISHED				
System 4	TCPV6	[0.0.0.0.0.0]	5985			x	LISTENING				
System 4	TCPV6	[0.0.0.0.0.0]	22771		[fe80::0:c4d4...	microsoft-ds	ESTABLISHED				
System 4	TCPV6	[0.0.0.0.0.0]	47001		[0.0.0.0.0.0]	0	LISTENING				
System 4	UDPV6	[0.0.0.0.0.0]	995		x	x					
System 4	TCPV6	[fe80::0:e564:3...	22829		[fe80::0:e564:3...	microsoft-ds	ESTABLISHED				
Trojan.exe 1716	TCP	server2016.ceh.com	22794		windows10	5552	ESTABLISHED				
virbind.exe 448	TCP	Server2016	1536		Server2016	0	LISTENING				
virbind.exe 448	TCPV6	[0.0.0.0.0.0]	1536		[0.0.0.0.0.0]	0	LISTENING				

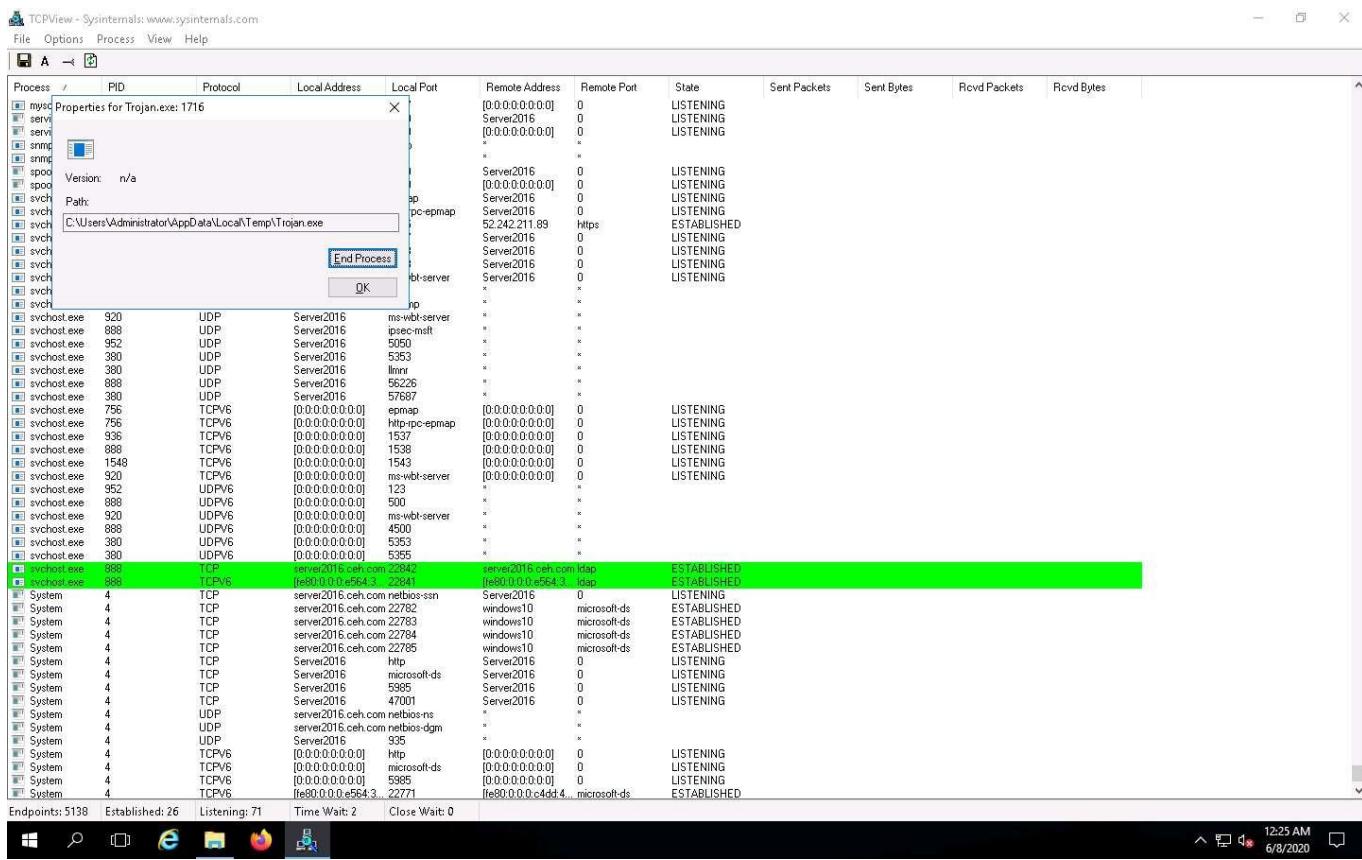
Endpoints: 5147 Established: 35 Listening: 71 Time Wait: 1 Close Wait: 0

Windows taskbar: TCPView, File Explorer, Edge, Firefox, Task View, 12:22 AM, 6/8/2020

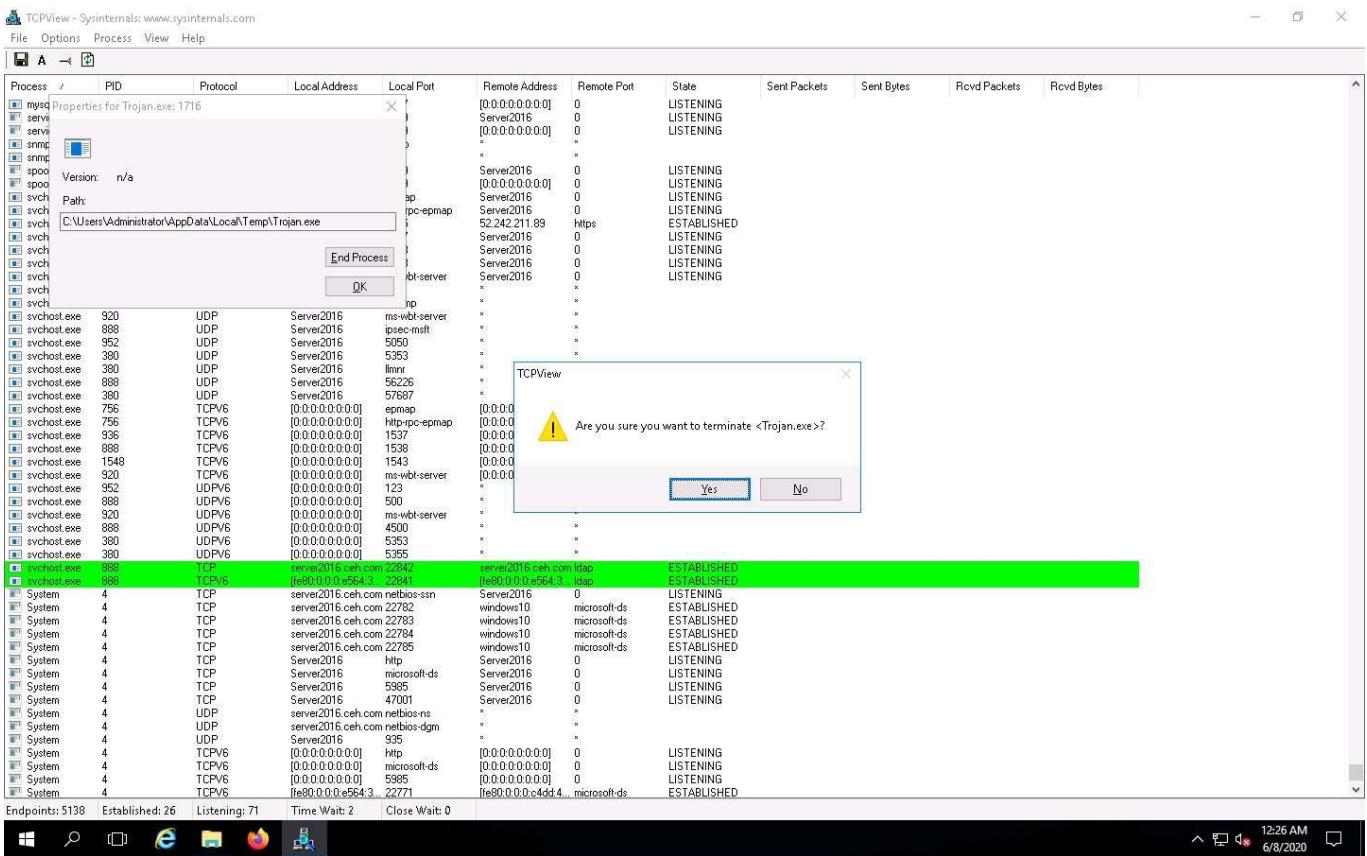
15. To see the process properties, navigate to **Process**, and then click **Process Properties**.



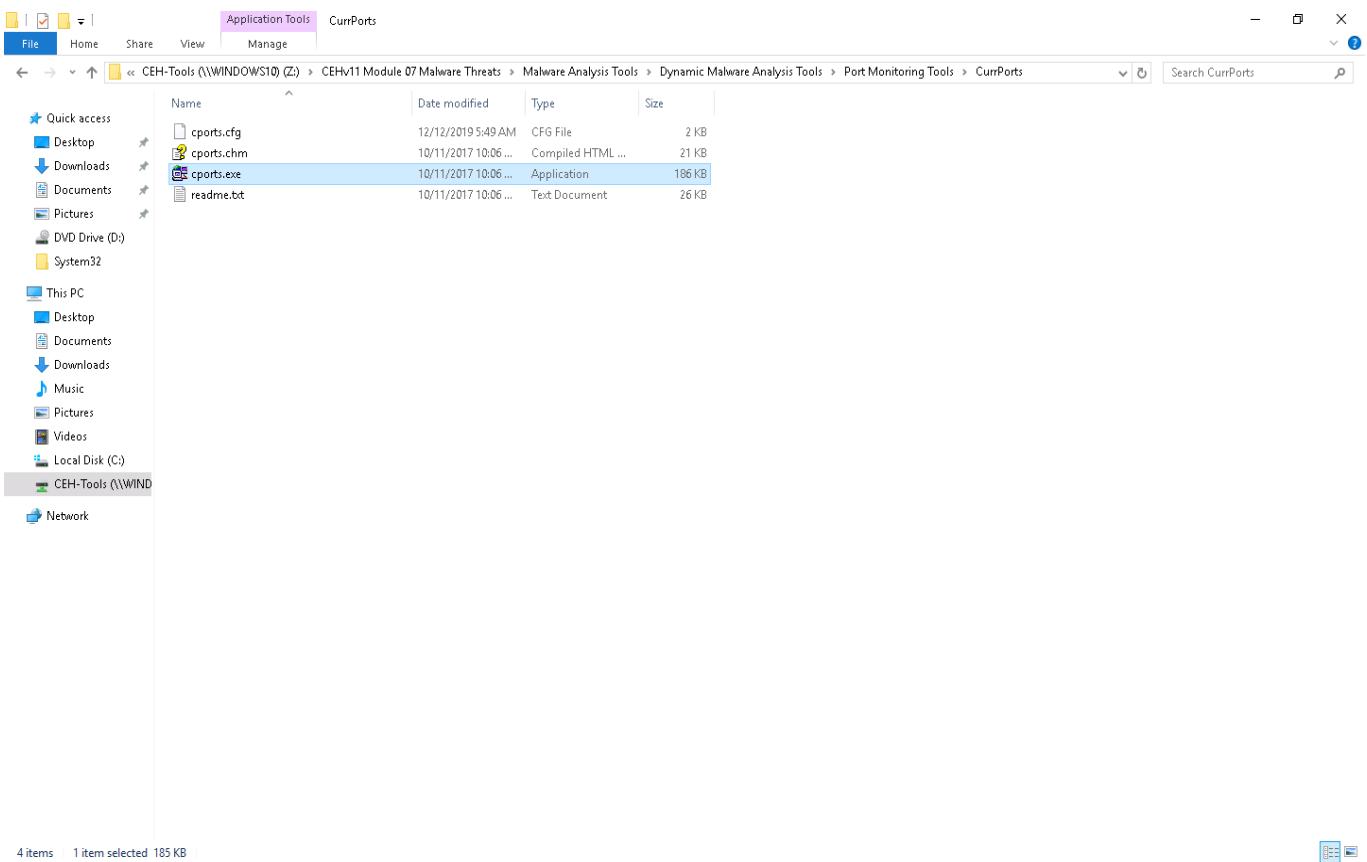
16. The properties for the selected process window appears (here, **Trojan.exe**); click **End Process** to kill the process. This will end the running process.



17. Normally, if a **TCPView** dialog box appears, click **Yes** to terminate the process. However, for this lab, do not Kill the process in this step as we are going to use this running process for the next task; click **No**.



18. This way, you can view all processes running on the machine and stop unwanted or malicious processes that may affect your system. If you are unable to stop a process, you can view the port on which it is running and add a firewall rule to block the port.
19. Close the **TCPView** window.
20. Now, let us analyze this process on **Windows Server 2016** using **CurrPorts**.
21. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts** and double-click **cports.exe**.

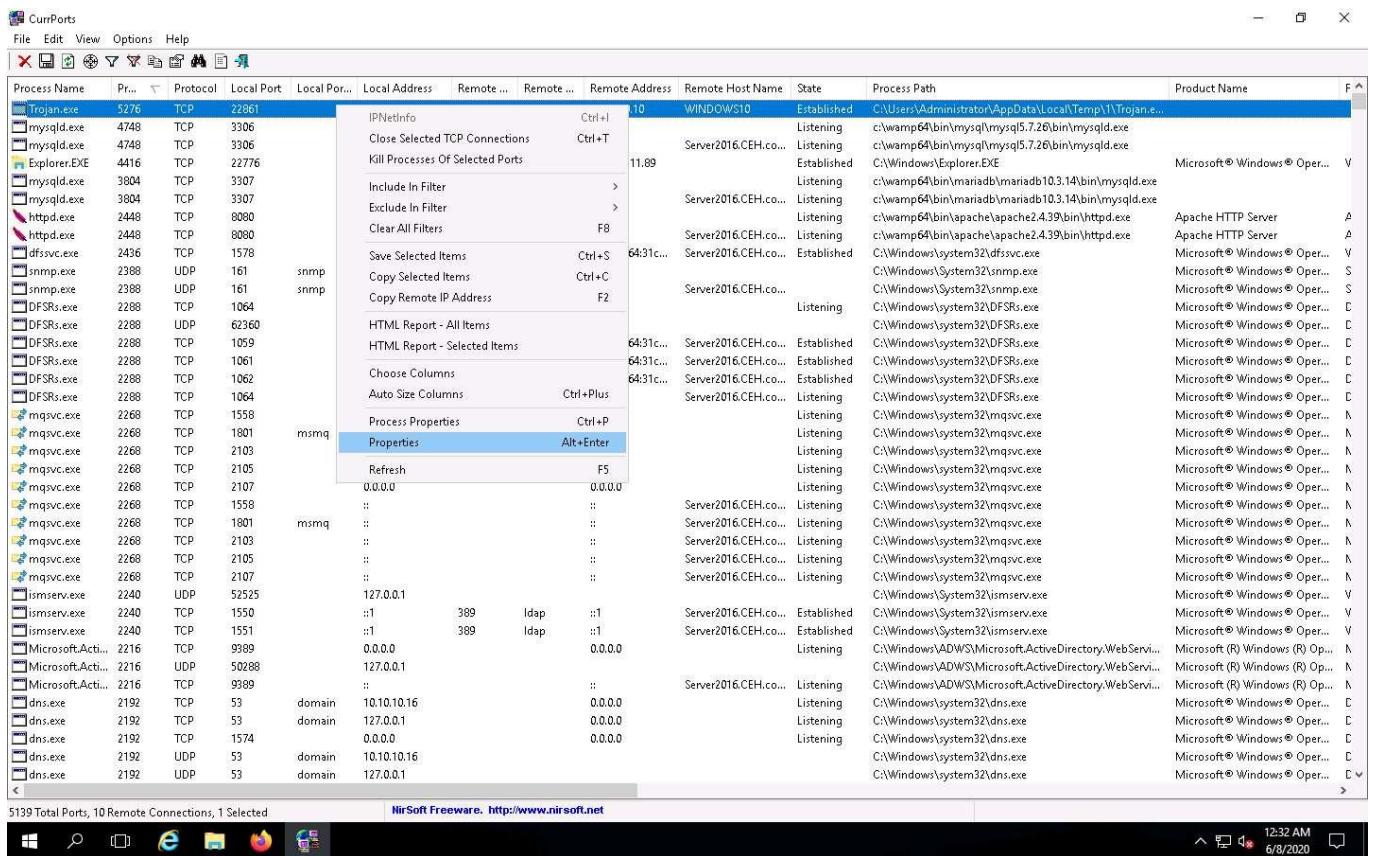


22. The **CurrPorts** window appears, displaying a list of currently open TCP/IP and UDP ports on the machine. Here, you can observe the **Trojan.exe** process running on the machine, as shown in the screenshot.

Process Name	Pr...	Protocol	Local Port	Local Port...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Process Path	Product Name
Trojan.exe	5276	TCP	22861		10.10.10.16	5552		10.10.10.10	WINDOWS10	Established	C:\Users\Administrator\AppData\Local\Temp\1\Trojan.e...	
mysqld.exe	4748	TCP	3306		0.0.0.0			0.0.0.0		Listening	c:\wamp64\bin\mysql\mysql5.7.26\bin\mysqld.exe	
mysqld.exe	4748	TCP	3306		:			:	Server2016.CEH.co...	Listening	c:\wamp64\bin\mysql\mysql5.7.26\bin\mysqld.exe	
Explorer.EXE	4416	TCP	22776		10.10.10.16	443	https	52.242.211.89		Established	C:\Windows\Explorer.EXE	Microsoft® Windows® Oper...
mysqld.exe	3804	TCP	3307		0.0.0.0			0.0.0.0		Listening	c:\wamp64\bin\mysql\mysql5.7.26\bin\mysqld.exe	
mysqld.exe	3804	TCP	3307		:			:	Server2016.CEH.co...	Listening	c:\wamp64\bin\mysql\mysql5.7.26\bin\mysqld.exe	
httpd.exe	2448	TCP	8080		0.0.0.0			0.0.0.0		Listening	c:\wamp64\bin\apache\apache2.4.39\bin\httpd.exe	Apache HTTP Server
httpd.exe	2448	TCP	8080		:			:	Server2016.CEH.co...	Listening	c:\wamp64\bin\apache\apache2.4.39\bin\httpd.exe	Apache HTTP Server
dfsvc.exe	2436	TCP	1578		f80:e564:31c...	1539		f80:e564:31c...	Server2016.CEH.co...	Established	C:\Windows\system32\dfsvc.exe	Microsoft® Windows® Oper...
snmp.exe	2388	UDP	161	snmp	0.0.0.0					Listening	C:\Windows\System32\snmp.exe	Microsoft® Windows® Oper...
snmp.exe	2388	UDP	161	snmp	:				Server2016.CEH.co...	Listening	C:\Windows\System32\snmp.exe	Microsoft® Windows® Oper...
DFSRs.exe	2288	TCP	1064		0.0.0.0			0.0.0.0		Listening	C:\Windows\system32\DFSRs.exe	Microsoft® Windows® Oper...
DFRSr.exe	2288	UDP	62360		127.0.0.1					Listening	C:\Windows\system32\DFRSr.exe	Microsoft® Windows® Oper...
DFSRs.exe	2288	TCP	1059		f80:e564:31c...	389	ldap	f80:e564:31c...	Server2016.CEH.co...	Established	C:\Windows\system32\DFSRs.exe	Microsoft® Windows® Oper...
DFRSr.exe	2288	TCP	1061		f80:e564:31c...	1539		f80:e564:31c...	Server2016.CEH.co...	Established	C:\Windows\system32\DFRSr.exe	Microsoft® Windows® Oper...
DFRSr.exe	2288	TCP	1062		f80:e564:31c...	389	ldap	f80:e564:31c...	Server2016.CEH.co...	Established	C:\Windows\system32\DFRSr.exe	Microsoft® Windows® Oper...
DFRSr.exe	2288	TCP	1064		:			:	Server2016.CEH.co...	Listening	C:\Windows\system32\DFRSr.exe	Microsoft® Windows® Oper...
mqsvc.exe	2268	TCP	1558		0.0.0.0			0.0.0.0		Listening	C:\Windows\system32\mqsvc.exe	Microsoft® Windows® Oper...
mqsvc.exe	2268	TCP	1801	mssql	0.0.0.0			0.0.0.0		Listening	C:\Windows\system32\mqsvc.exe	Microsoft® Windows® Oper...
mqsvc.exe	2268	TCP	2103		0.0.0.0			0.0.0.0		Listening	C:\Windows\system32\mqsvc.exe	Microsoft® Windows® Oper...
mqsvc.exe	2268	TCP	2105		0.0.0.0			0.0.0.0		Listening	C:\Windows\system32\mqsvc.exe	Microsoft® Windows® Oper...
mqsvc.exe	2268	TCP	2107		0.0.0.0			0.0.0.0		Listening	C:\Windows\system32\mqsvc.exe	Microsoft® Windows® Oper...
mqsvc.exe	2268	TCP	1558		:			:	Server2016.CEH.co...	Listening	C:\Windows\system32\mqsvc.exe	Microsoft® Windows® Oper...
mqsvc.exe	2268	TCP	1801	mssql	:			:	Server2016.CEH.co...	Listening	C:\Windows\system32\mqsvc.exe	Microsoft® Windows® Oper...
mqsvc.exe	2268	TCP	2103		:			:	Server2016.CEH.co...	Listening	C:\Windows\system32\mqsvc.exe	Microsoft® Windows® Oper...
mqsvc.exe	2268	TCP	2105		:			:	Server2016.CEH.co...	Listening	C:\Windows\system32\mqsvc.exe	Microsoft® Windows® Oper...
mqsvc.exe	2268	TCP	2107		:			:	Server2016.CEH.co...	Listening	C:\Windows\system32\mqsvc.exe	Microsoft® Windows® Oper...
lsmserver.exe	2240	UDP	52525		127.0.0.1					Listening	C:\Windows\System32\lsmserver.exe	Microsoft® Windows® Oper...
lsmserver.exe	2240	TCP	1550		:1	389	ldap	:1	Server2016.CEH.co...	Established	C:\Windows\System32\lsmserver.exe	Microsoft® Windows® Oper...
lsmserver.exe	2240	TCP	1551		:1	389	ldap	:1	Server2016.CEH.co...	Established	C:\Windows\System32\lsmserver.exe	Microsoft® Windows® Oper...
Microsoft.Acti...	2216	TCP	9589		0.0.0.0			0.0.0.0		Listening	C:\Windows\ADWS\Microsoft\ActiveDirectory\WebServ...	Microsoft (R) Windows...
Microsoft.Acti...	2216	UDP	50288		127.0.0.1					Listening	C:\Windows\ADWS\Microsoft\ActiveDirectory\WebServ...	Microsoft (R) Windows...
Microsoft.Acti...	2216	TCP	9589		:			:	Server2016.CEH.co...	Listening	C:\Windows\ADWS\Microsoft\ActiveDirectory\WebServ...	Microsoft (R) Windows...
dns.exe	2192	TCP	53	domain	10.10.10.16			0.0.0.0		Listening	C:\Windows\system32\dns.exe	Microsoft® Windows® Oper...
dns.exe	2192	TCP	53	domain	127.0.0.1			0.0.0.0		Listening	C:\Windows\system32\dns.exe	Microsoft® Windows® Oper...
dns.exe	2192	TCP	1574		0.0.0.0			0.0.0.0		Listening	C:\Windows\system32\dns.exe	Microsoft® Windows® Oper...
dns.exe	2192	UDP	53	domain	10.10.10.16					Listening	C:\Windows\system32\dns.exe	Microsoft® Windows® Oper...
dns.exe	2192	UDP	53	domain	127.0.0.1					Listening	C:\Windows\system32\dns.exe	Microsoft® Windows® Oper...

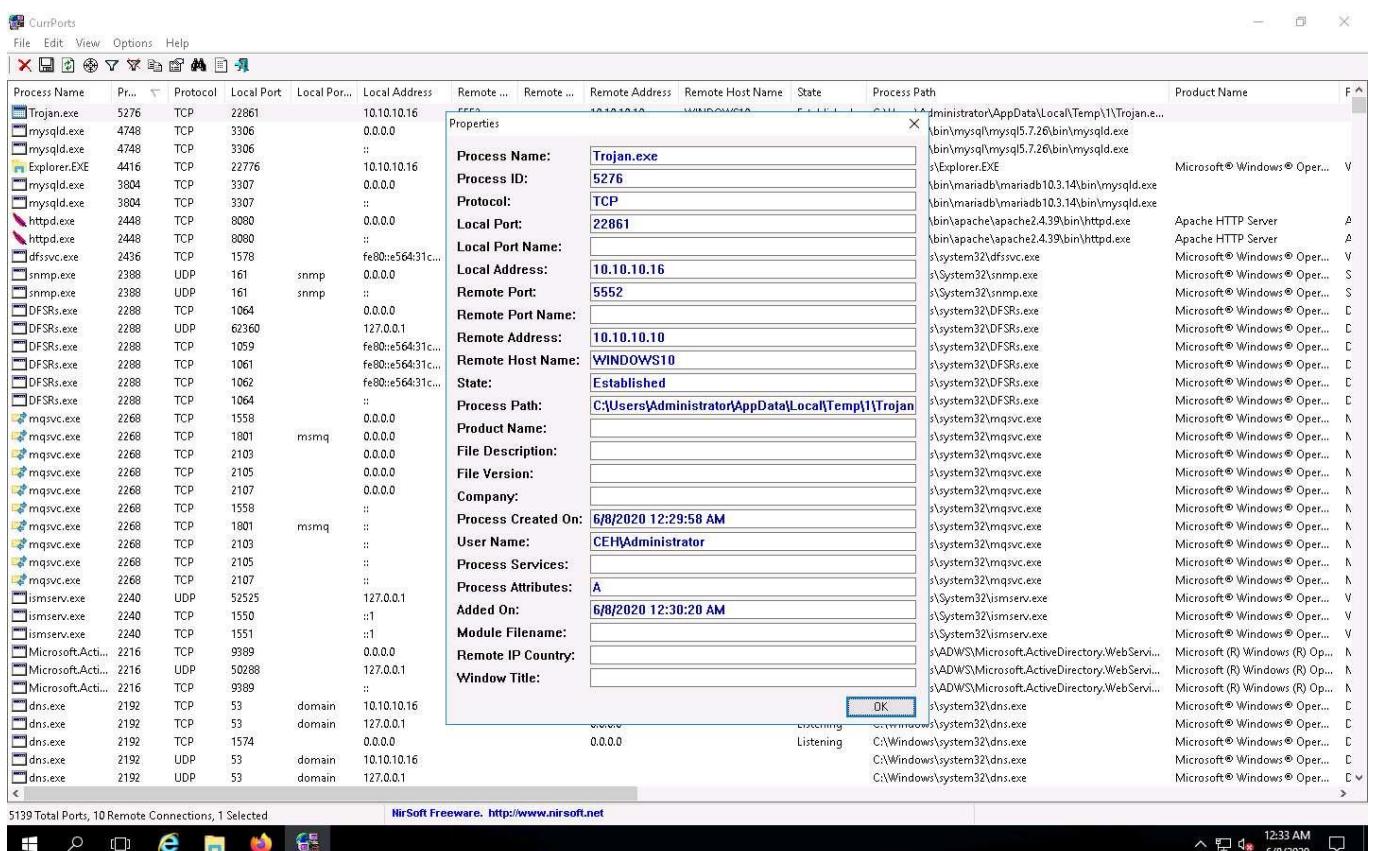
23. It is evident from the above screenshot that the process is connected to the machine on **port 5552**.

24. You can view the properties of the process by right-clicking on the process and clicking **Properties** from the **Context** menu.

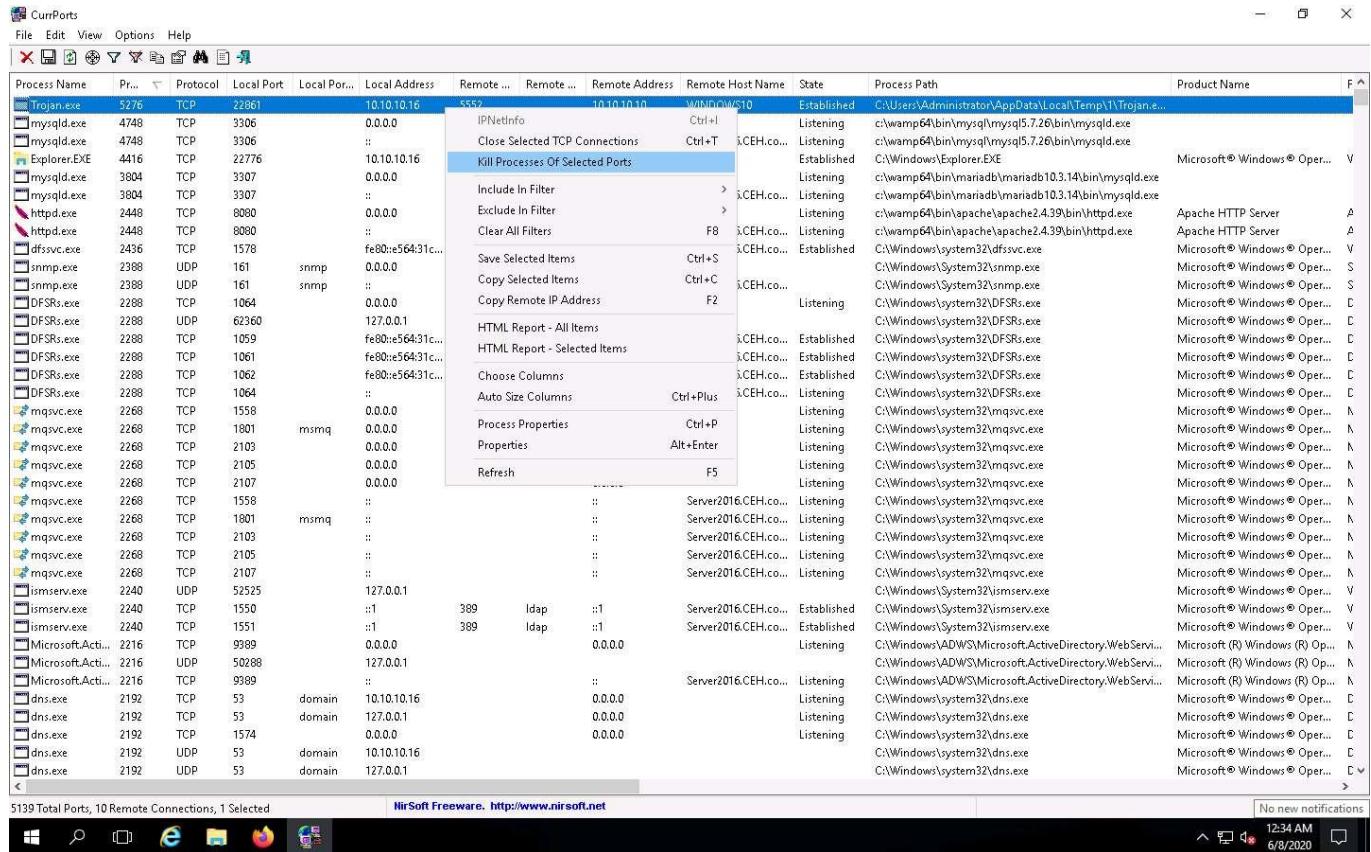


25. The **Properties** window appears, displaying information related to the process such as the name of the process, its process ID, Remote Address, Process Path, Remote Host Name, and other details.

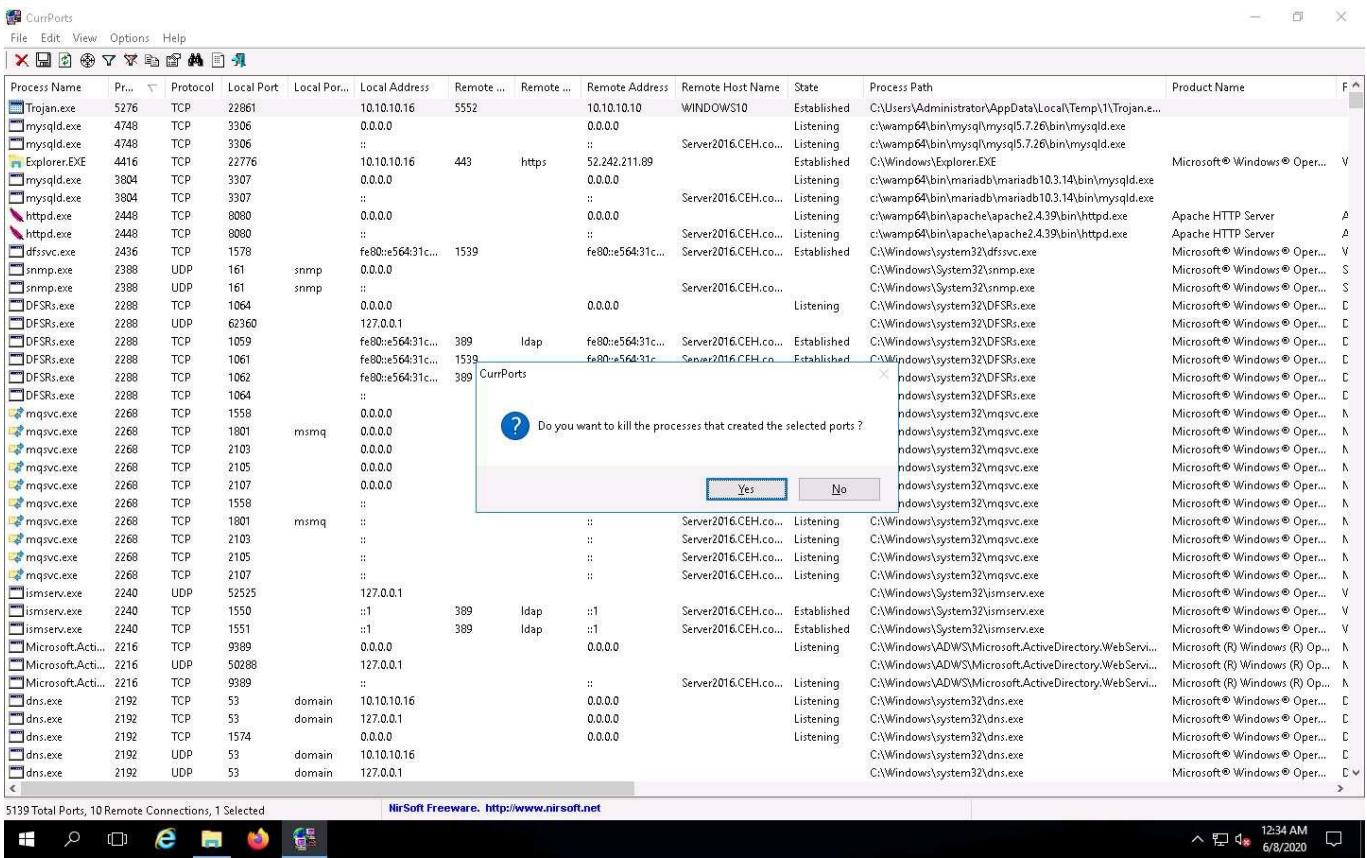
26. Once you are done examining the properties associated with the process, click **OK**.



27. Because **Trojan.exe** is a malicious process, you may end the process by right-clicking on it and selecting **Kill Processes Of Selected Ports** from the context menu.
28. Alternatively, you may select **Close Selected TCP Connections**, so that the port closes, and the attacker can never regain connection through the port unless you open it.



29. Normally, when the **CurrPorts** dialog-box appears, you would click **Yes** to close the connection. However, do not Kill the process at this step, as this running process will be used for the next task; click **No**.



- This way, you can analyze the ports open on a machine and the processes running on it.
- If a process is found to be suspicious, you may either kill the process or close the port.
- Close all open windows.
- You can also use other port monitoring tools such as **Port Monitor** (<https://www.port-monitor.com>), **CurrPorts** (<https://www.nirsoft.net>), **TCP Port Monitoring** (<https://www.dotcom-monitor.com>), or **PortExpert** (<http://www.kcsoftwares.com>) to perform port monitoring.

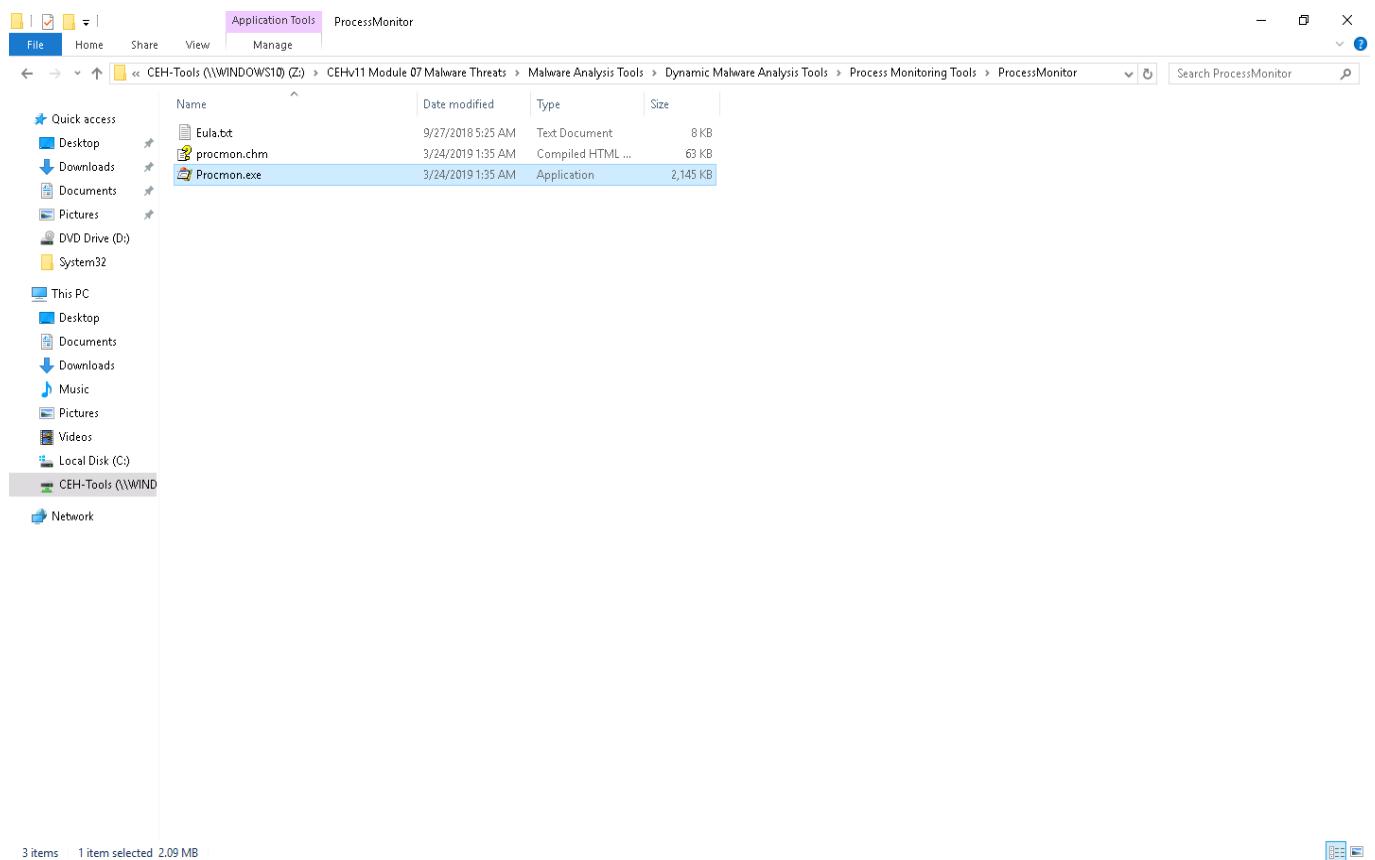
Task 2: Perform Process Monitoring using Process Monitor

Process monitoring will help in understanding the processes that malware initiates and takes over after execution. You should also observe the child processes, associated handles, loaded libraries, functions, and execution flow of boot time processes to define the entire nature of a file or program, gather information about processes running before the execution of the malware, and compare them with the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all processes that malware starts.

Process Monitor is a monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon. It adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, and simultaneous logging to a file. Unique features of Process Monitor make it a core utility in system troubleshooting and vital to the malware hunting toolkit.

Here, we will use the Process Monitor tool to detect suspicious processes.

1. On the **Windows Server 2016** machine, navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor** and double-click **Procmon.exe** to launch the Process Monitor tool.

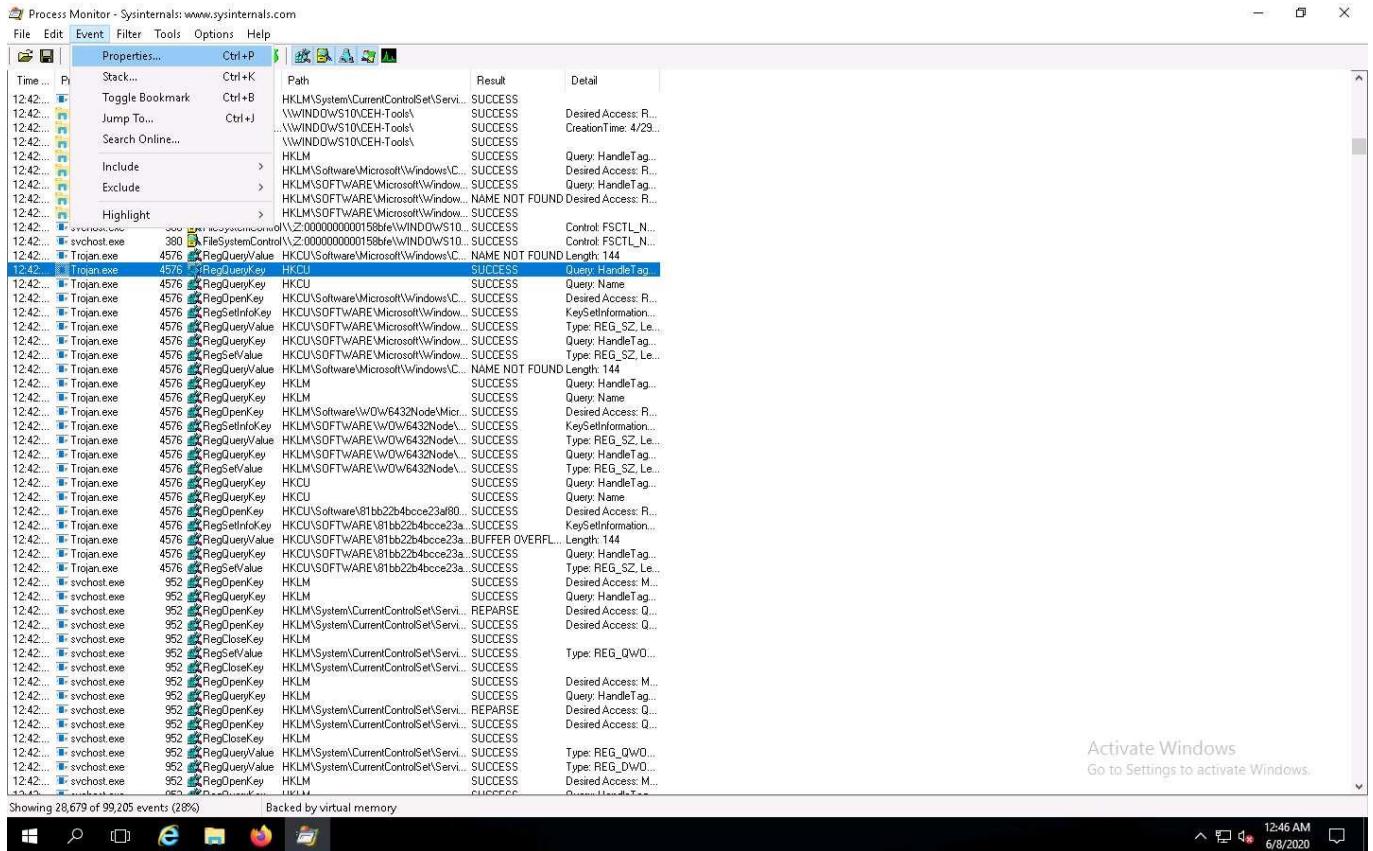


2. The **Process Monitor License Agreement** window appears; click **Agree**.
3. The **Process Monitor** main window appears, as shown in the screenshot, with the processes running on the machine.

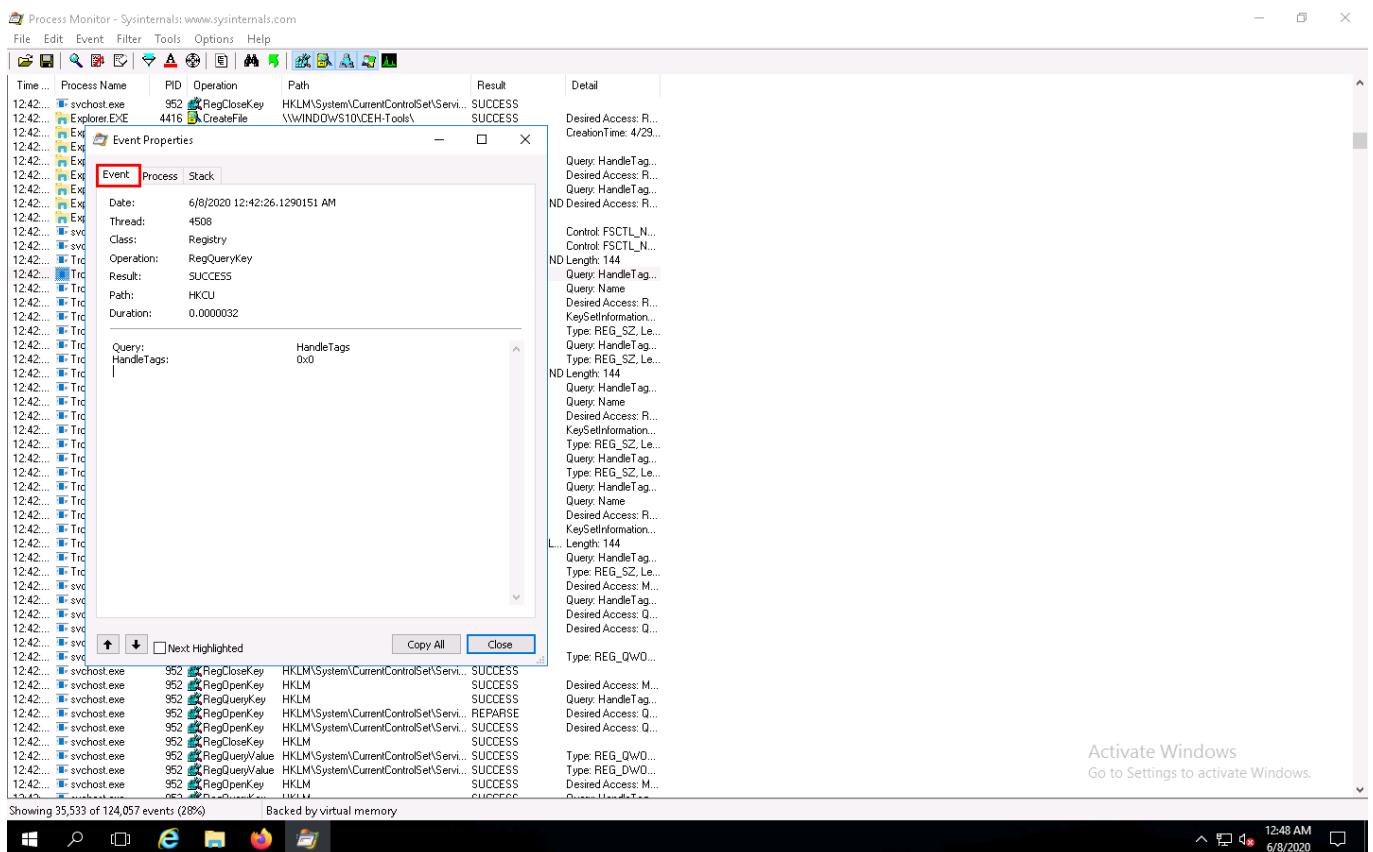
4. Look for the **Trojan.exe** process that was executed in the previous task. If you killed the process at the end of the task, then navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe** to re-execute the malicious program.
 5. Observe that the **Trojan.exe** process is running on the machine. Process Monitor shows the running process details such as the PID, Operation, Path, Result, and Details.

Time ...	Process Name	PID	Operation	Path	Result	Detail
12:42...	svchost.exe	952	RegCloseKey	HKEY\SYSTEM\CurrentControlSet\Serv...	SUCCESS	
12:42...	Explorer.exe	4416	CreateFile	\Windows\10\CEH-Tools\	SUCCESS	Desired Access: R...
12:42...	Explorer.exe	4416	QueryBasicInfo	\Windows\10\CEH-Tools\	SUCCESS	CreationTime: 4/29...
12:42...	Explorer.exe	4416	CloseFile	\Windows\10\CEH-Tools\	SUCCESS	
12:42...	Explorer.exe	4416	RegQueryKey	HKEY...	SUCCESS	Query: HandleTag...
12:42...	Explorer.exe	4416	RegOpenKey	HKEY\Software\Microsoft\Windows\...	SUCCESS	Desired Access: R...
12:42...	Explorer.exe	4416	RegQueryKey	HKEY\Software\Microsoft\Windows\...	SUCCESS	Query: HandleTag...
12:42...	Explorer.exe	4416	RegOpenKey	HKEY\Software\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: R...
12:42...	Explorer.exe	4416	RegCloseKey	HKEY\Software\Microsoft\Windows\...	SUCCESS	
12:42...	svchost.exe	380	FileSystemControl\Z:\000000000158be\Windows10...	SUCCESS	Control: FSCTL_N...	
12:42...	svchost.exe	380	FileSystemControl\Z:\000000000158be\Windows10...	SUCCESS	Control: FSCTL_N...	
12:42...	Trojan.exe	4576	RegQueryValue	HKEY\Software\Microsoft\Windows\...	NAME NOT FOUND	Length: 144
12:42...	Trojan.exe	4576	RegQueryKey	HKEY...	SUCCESS	Query: HandleTag...
12:42...	Trojan.exe	4576	RegOpenKey	HKEY\Software\Microsoft\Windows\...	SUCCESS	Query: Name
12:42...	Trojan.exe	4576	RegSetValue	HKEY\Software\Microsoft\Windows\...	SUCCESS	Desired Access: R...
12:42...	Trojan.exe	4576	RegGetValue	HKEY\Software\Microsoft\Windows\...	SUCCESS	KeySetInformation...
12:42...	Trojan.exe	4576	RegQueryValue	HKEY\Software\Microsoft\Windows\...	SUCCESS	Type: REG_SZ Le...
12:42...	Trojan.exe	4576	RegQueryKey	HKEY\Software\Microsoft\Windows\...	SUCCESS	Query: HandleTag...
12:42...	Trojan.exe	4576	RegQueryValue	HKEY\Software\Microsoft\Windows\...	SUCCESS	Type: REG_SZ Le...
12:42...	Trojan.exe	4576	RegQueryValue	HKEY\Software\Microsoft\Windows\...	NAME NOT FOUND	Length: 144
12:42...	Trojan.exe	4576	RegQueryKey	HKEY...	SUCCESS	Query: HandleTag...
12:42...	Trojan.exe	4576	RegOpenKey	HKEY\Software\WOW6432Node\Mic...	SUCCESS	Query: Name
12:42...	Trojan.exe	4576	RegSetValue	HKEY\Software\WOW6432Node\...	SUCCESS	Desired Access: R...
12:42...	Trojan.exe	4576	RegGetValue	HKEY\Software\WOW6432Node\...	SUCCESS	KeySetInformation...
12:42...	Trojan.exe	4576	RegQueryValue	HKEY\Software\WOW6432Node\...	SUCCESS	Type: REG_SZ Le...
12:42...	Trojan.exe	4576	RegQueryKey	HKEY\Software\WOW6432Node\...	SUCCESS	Query: HandleTag...
12:42...	Trojan.exe	4576	RegSetValue	HKEY\Software\WOW6432Node\...	SUCCESS	Type: REG_SZ Le...
12:42...	Trojan.exe	4576	RegQueryKey	HKEY...	SUCCESS	Query: HandleTag...
12:42...	Trojan.exe	4576	RegQueryValue	HKEY\Software\WOW6432Node\...	SUCCESS	Query: Name
12:42...	Trojan.exe	4576	RegOpenKey	HKEY\Software\WOW6432Node\...	SUCCESS	Desired Access: R...
12:42...	Trojan.exe	4576	RegSetValue	HKEY\Software\WOW6432Node\...	SUCCESS	KeySetInformation...
12:42...	Trojan.exe	4576	RegQueryValue	HKEY\Software\WOW6432Node\...	SUCCESS	Type: REG_QWORD...
12:42...	Trojan.exe	4576	RegQueryKey	HKEY\Software\WOW6432Node\...	SUCCESS	Query: HandleTag...
12:42...	svchost.exe	952	RegOpenKey	HKEY...	SUCCESS	Desired Access: M...
12:42...	svchost.exe	952	RegQueryKey	HKEY...	SUCCESS	Query: HandleTag...
12:42...	svchost.exe	952	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Se...	REPARSE	Desired Access: Q...
12:42...	svchost.exe	952	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Se...	SUCCESS	Desired Access: Q...
12:42...	svchost.exe	952	RegCloseKey	HKEY...	SUCCESS	
12:42...	svchost.exe	952	RegSetValue	HKEY\SYSTEM\CurrentControlSet\Se...	SUCCESS	Type: REG_QWORD...
12:42...	svchost.exe	952	RegCloseKey	HKEY\SYSTEM\CurrentControlSet\Se...	SUCCESS	
12:42...	svchost.exe	952	RegOpenKey	HKEY...	SUCCESS	Desired Access: M...
12:42...	svchost.exe	952	RegQueryKey	HKEY...	SUCCESS	Query: HandleTag...
12:42...	svchost.exe	952	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Se...	REPARSE	Desired Access: Q...
12:42...	svchost.exe	952	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Se...	SUCCESS	Desired Access: Q...
12:42...	svchost.exe	952	RegCloseKey	HKEY...	SUCCESS	
12:42...	svchost.exe	952	RegQueryValue	HKEY\SYSTEM\CurrentControlSet\Se...	SUCCESS	Type: REG_QWORD...
12:42...	svchost.exe	952	RegQueryValue	HKEY\SYSTEM\CurrentControlSet\Se...	SUCCESS	Type: REG_DWORD...
12:42...	svchost.exe	952	RegOpenKey	HKEY...	SUCCESS	Desired Access: M...
12:42...	svchost.exe	952	RegQueryKey	HKEY...	SUCCESS	Query: HandleTag...

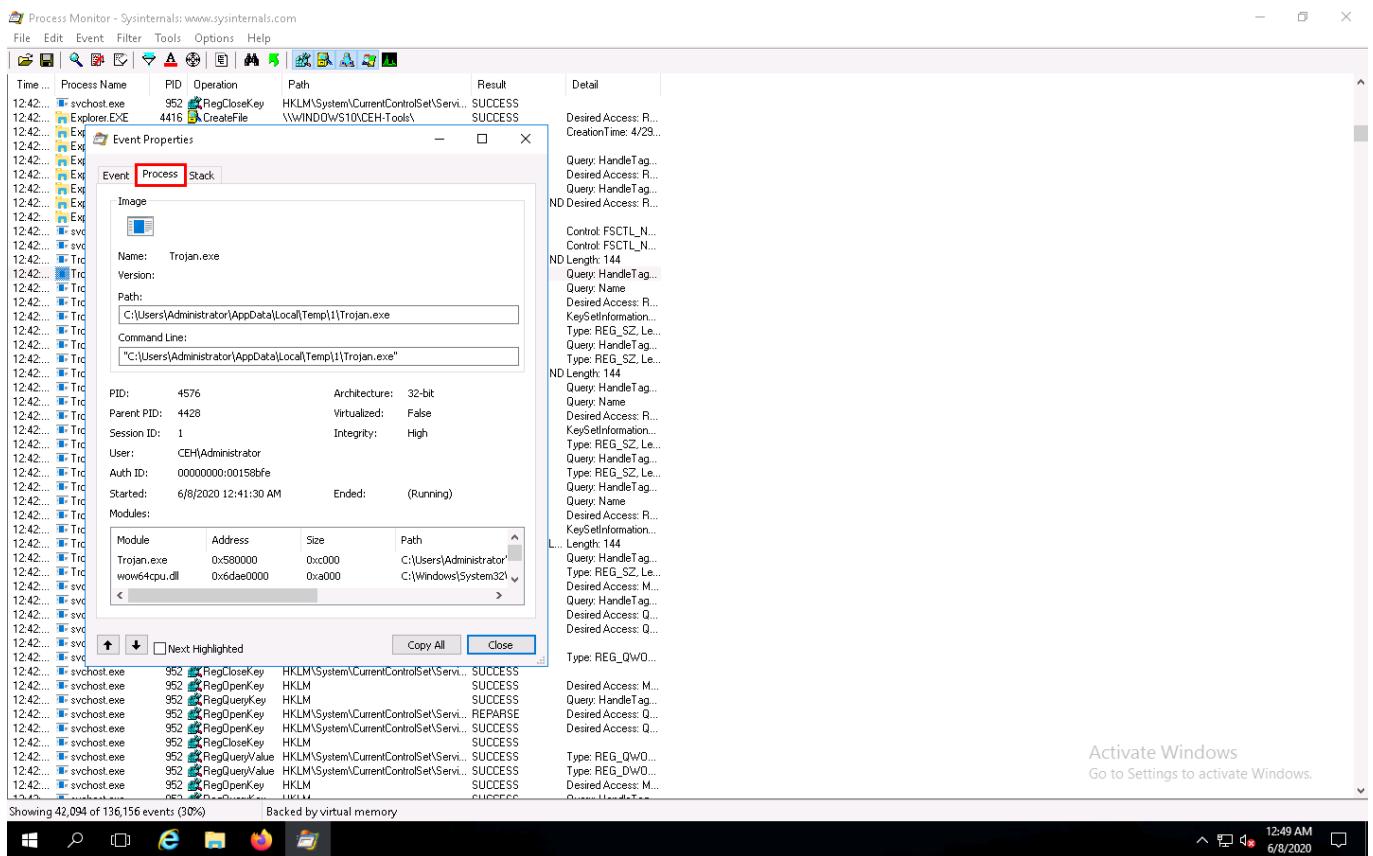
6. To view the properties of a running process, select the process (here, **Trojan.exe**), navigate to **Event**, and click **Properties** from the menu.



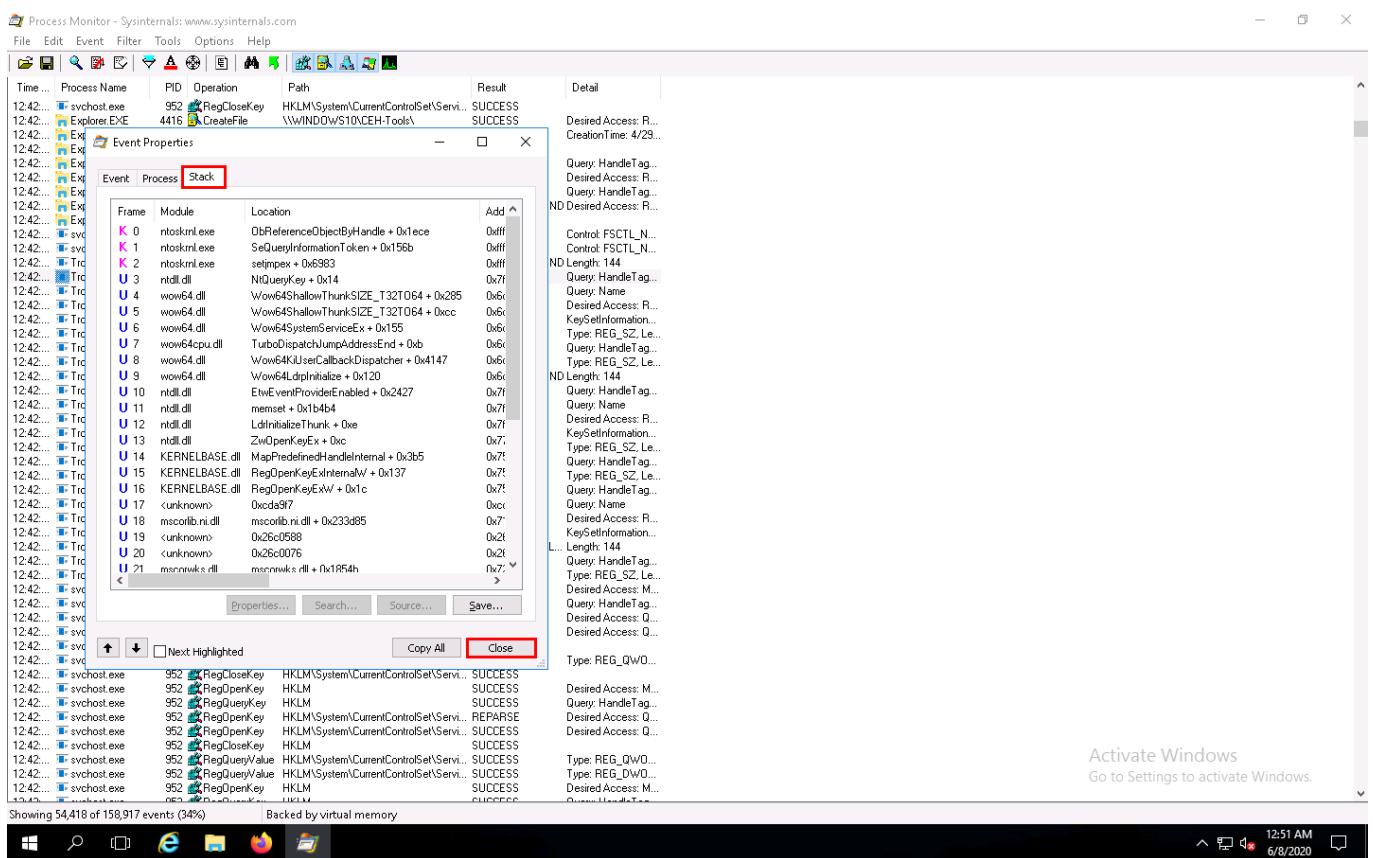
7. The **Event Properties** window appears with the details of the chosen process.
 8. In the **Event** tab, you can see the complete details of the running process such as Date, Thread, Class, Operation, Result, Path, and Duration.



9. Once the analysis is complete, click the **Process** tab.
10. The **Process** tab shows the complete details of the process running, as shown in the screenshot.



11. Click the **Stack** tab to view the supported DLLs of the selected process. Once the analysis is done, click **Close**.



12:51 AM
6/8/2020

12. This way, you can analyze the processes running on a machine.
 13. If a process is found to be suspicious, you may either kill the process or close the port.
 14. Close all windows on the **Windows 10** and **Windows Server 2016** machines.
 15. You can also use other process monitoring tools such as **Process Explorer** (<https://docs.microsoft.com>), **OpManager** (<https://www.manageengine.com>), **Monit** (<https://monit.com>), or **ESET SysInspector** (<https://www.eset.com>) to perform process monitoring.
-

Task 3: Perform Registry Monitoring using Regshot and jv16 PowerTools

The Windows registry stores OS and program configuration details such as settings and options. If the malware is a program, the registry stores its functionality. When an attacker installs a type of malware on the victim's machine, it generates a registry entry. One must have a fair knowledge of the Windows registry, its contents, and inner workings to analyze the presence of malware. Scanning for suspicious registries will help to detect malware. While most computer users generally do not do this, monitoring the registry entries is a great way to track any modifications made to your system.

Registry monitoring tools such as Regshot and jv16 PowerTools provide a simple way to perform the interesting task of tracking registry modifications, which proves to be useful in troubleshooting and monitoring background changes.

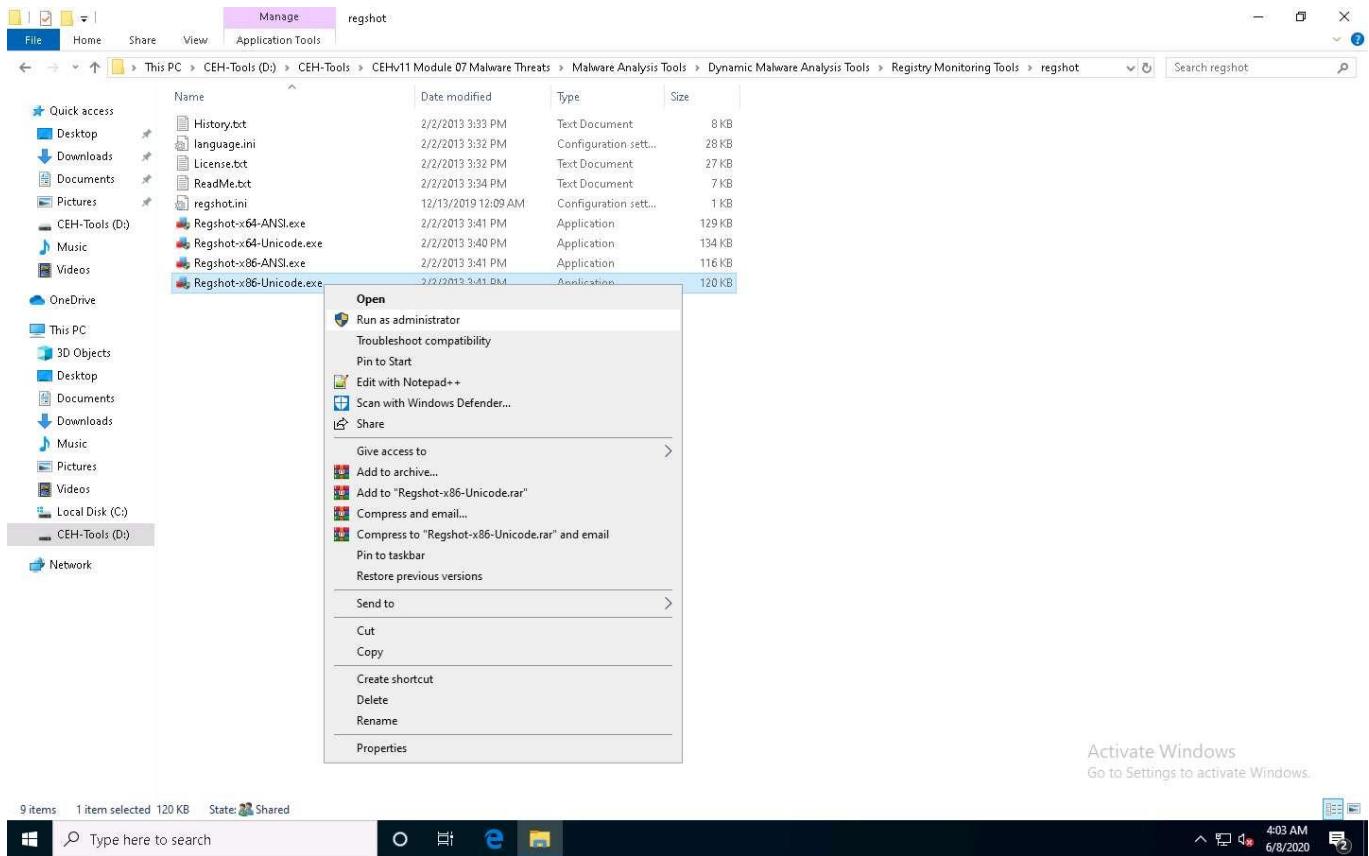
Regshot Regshot is a registry compare utility that helps to compare changes in registry entries after installing or uninstalling a program or manually modifying the registry. The purpose of this utility is to compare your registry at two separate points by taking a snapshot of the registry before and after any program or settings are added, removed, or otherwise modified.

jv16 PowerTools jv16 PowerTools is a PC system utility software that works by cleaning out unneeded files and data, cleaning the Windows registry, automatically fixing system errors, and applying optimization to your system. It allows the user to scan and monitor the Registry.

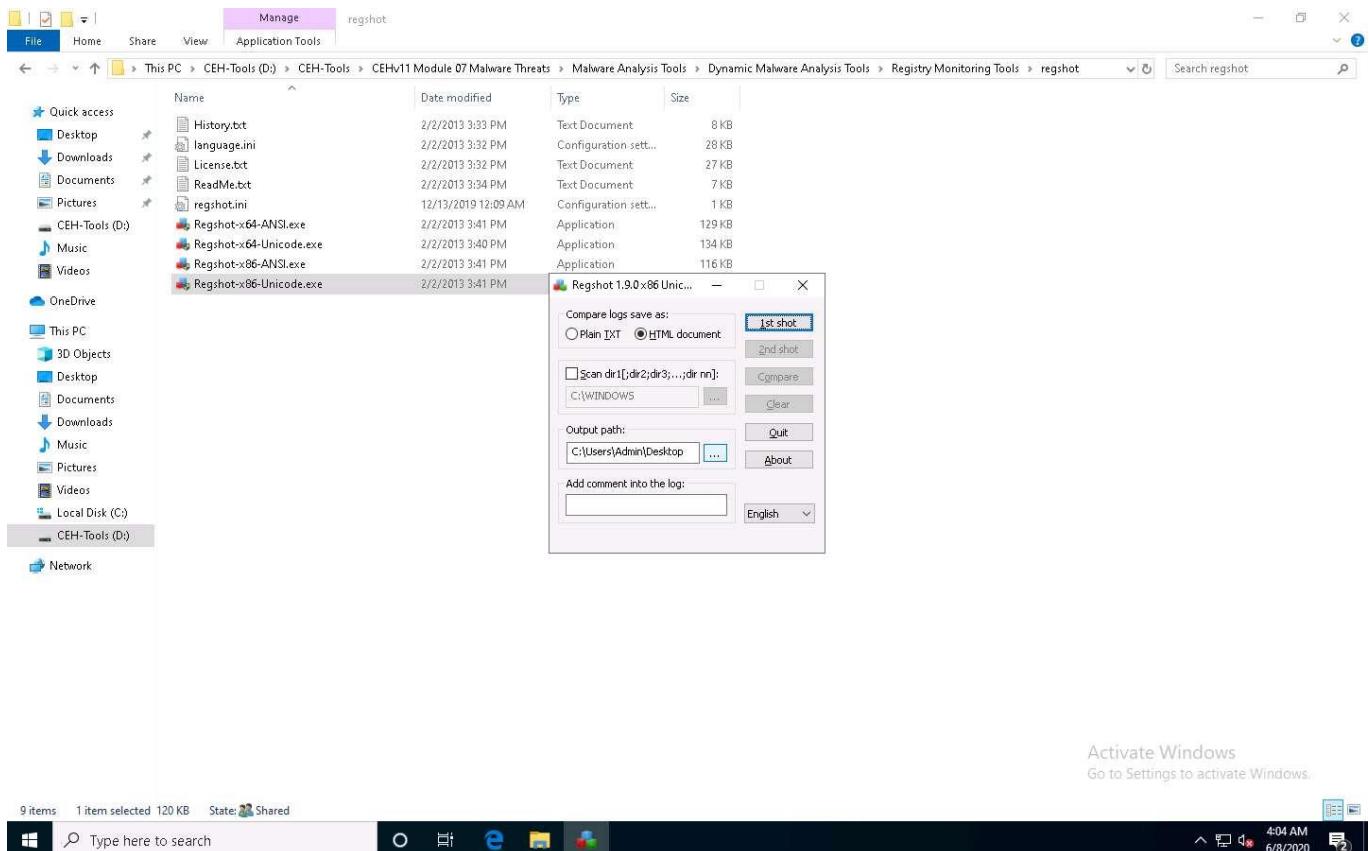
Further, jv16 helps in detecting registry entries created by malware. The "Clean and Speedup My Computer" feature of the Registry Cleaner in jv16 PowerTools is a solution for fixing registry errors and system errors, cleaning registry leftovers, as well as managing unneeded files such as old log files and temporary files.

Here, we will use the registry monitoring tools Regshot and jv16 PowerTools to scan the registry values for any suspicious entries that may indicate a malware infection.

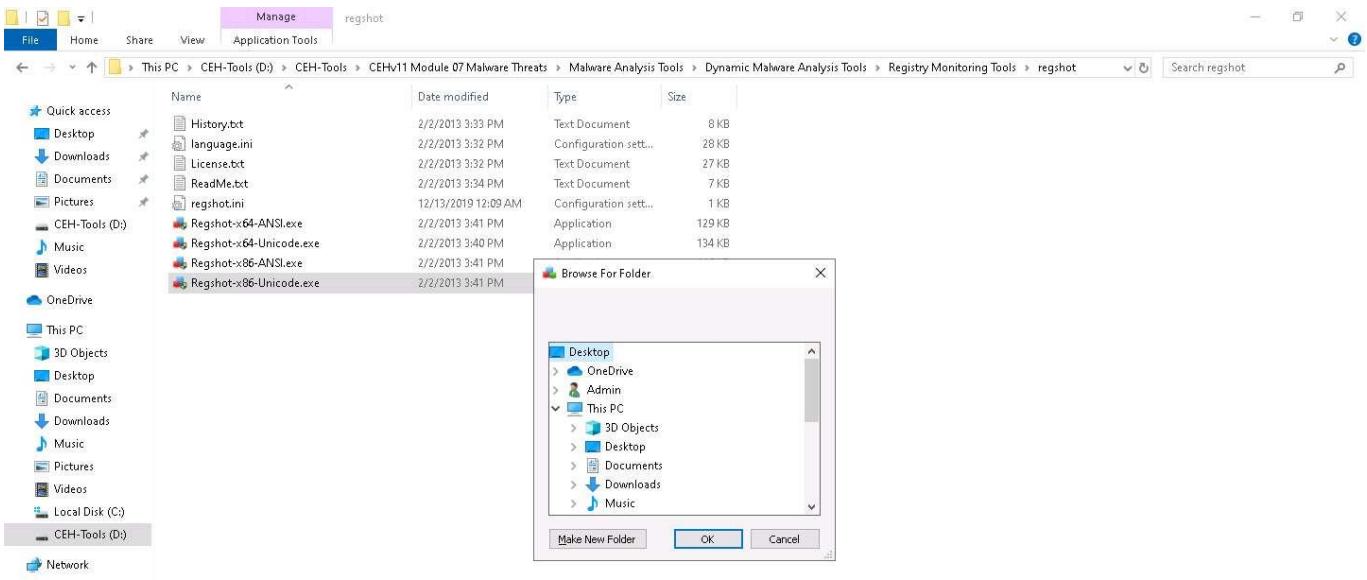
1. Click [Windows 10](#) to switch to the **Windows 10** machine and navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\regshot**. Right-click **Regshot-x86-Unicode.exe** and choose **Run as administrator** from the context menu, as shown in the screenshot.
2. If a **User Account Control** window appears, click **Yes**.



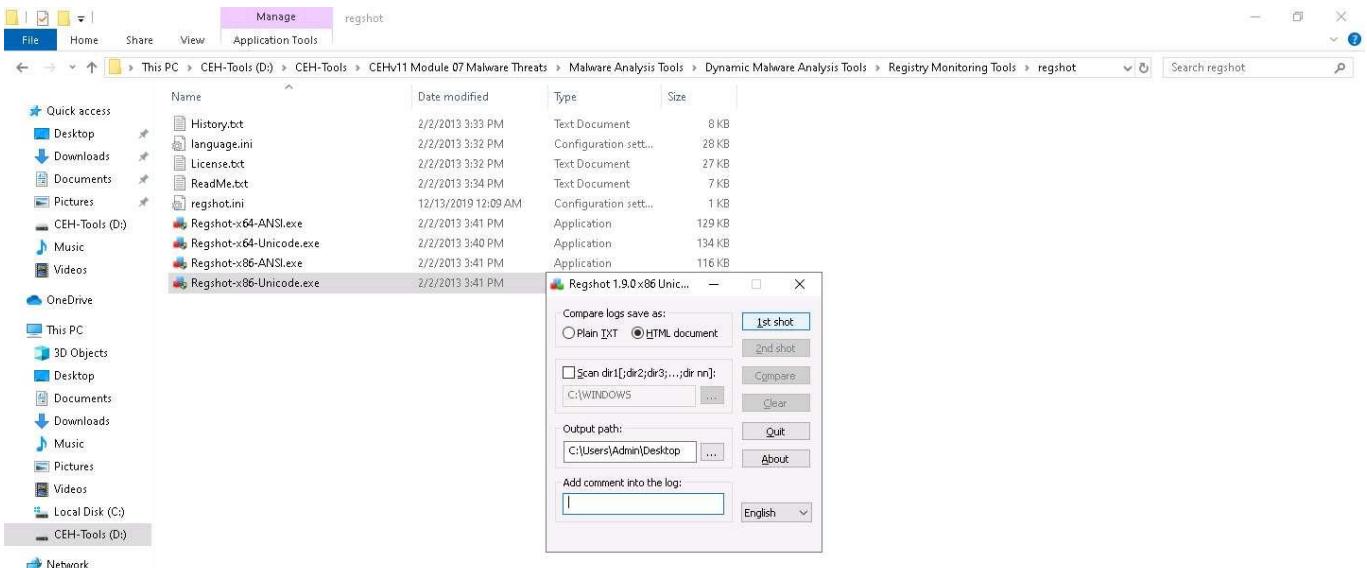
3. The **Regshot** application window opens, select the **HTML document** radio button, and in the **Output path** menu, click the ellipsis button.



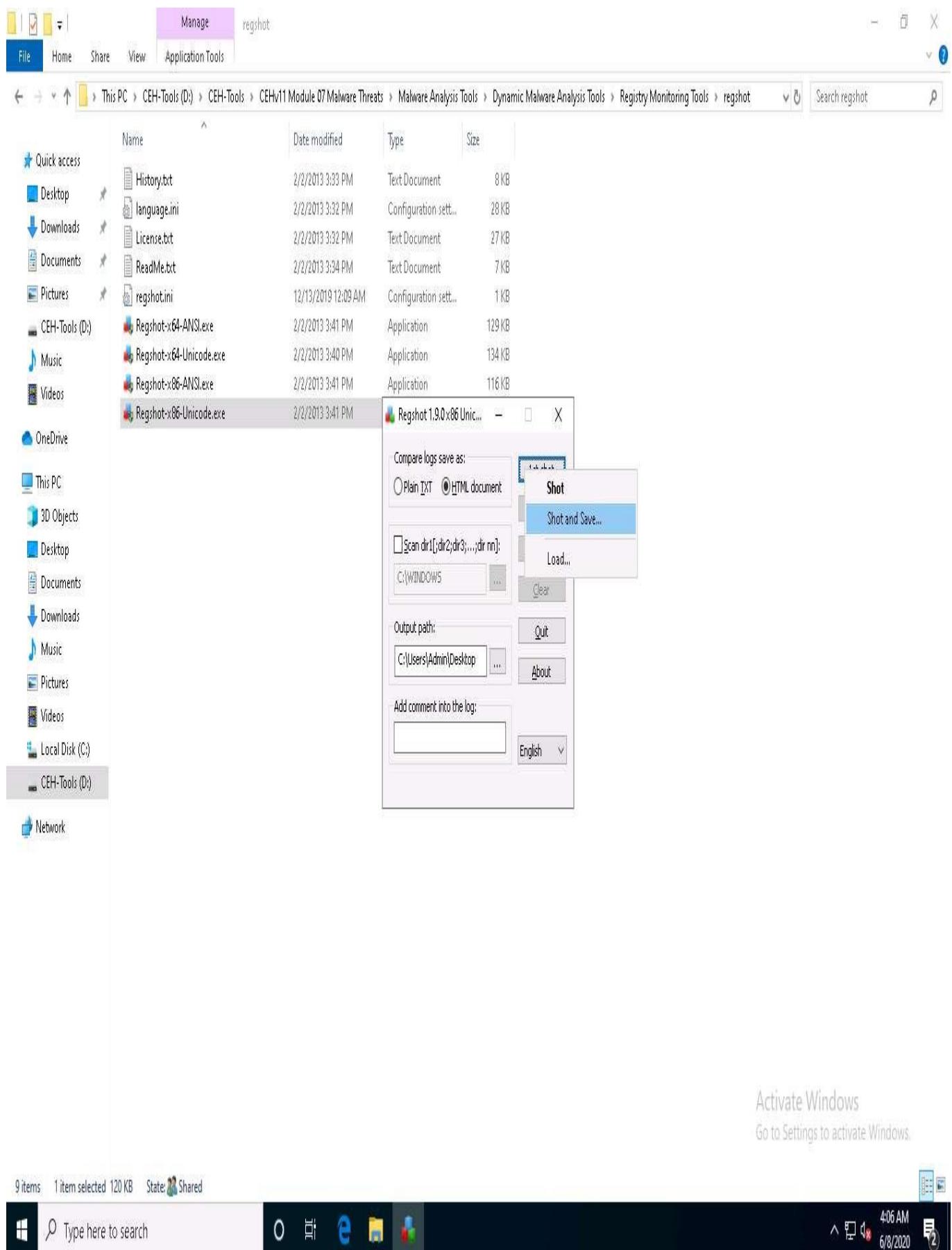
4. The **Browse For Folder** window appears; choose **Desktop**, and then click **OK**, as shown in the screenshot.



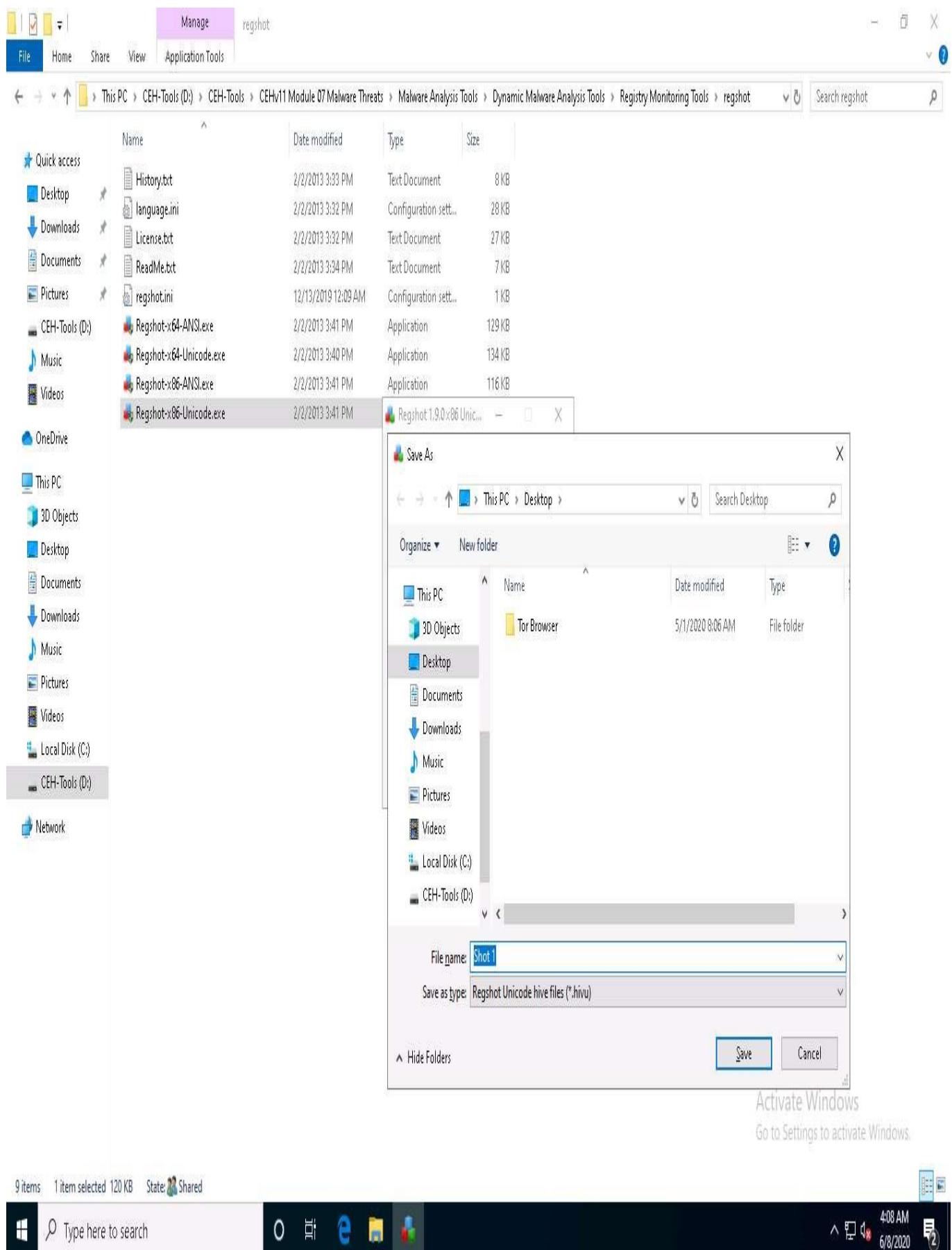
5. In Regshot's main window, click the **1st shot** button, as shown in the screenshot.



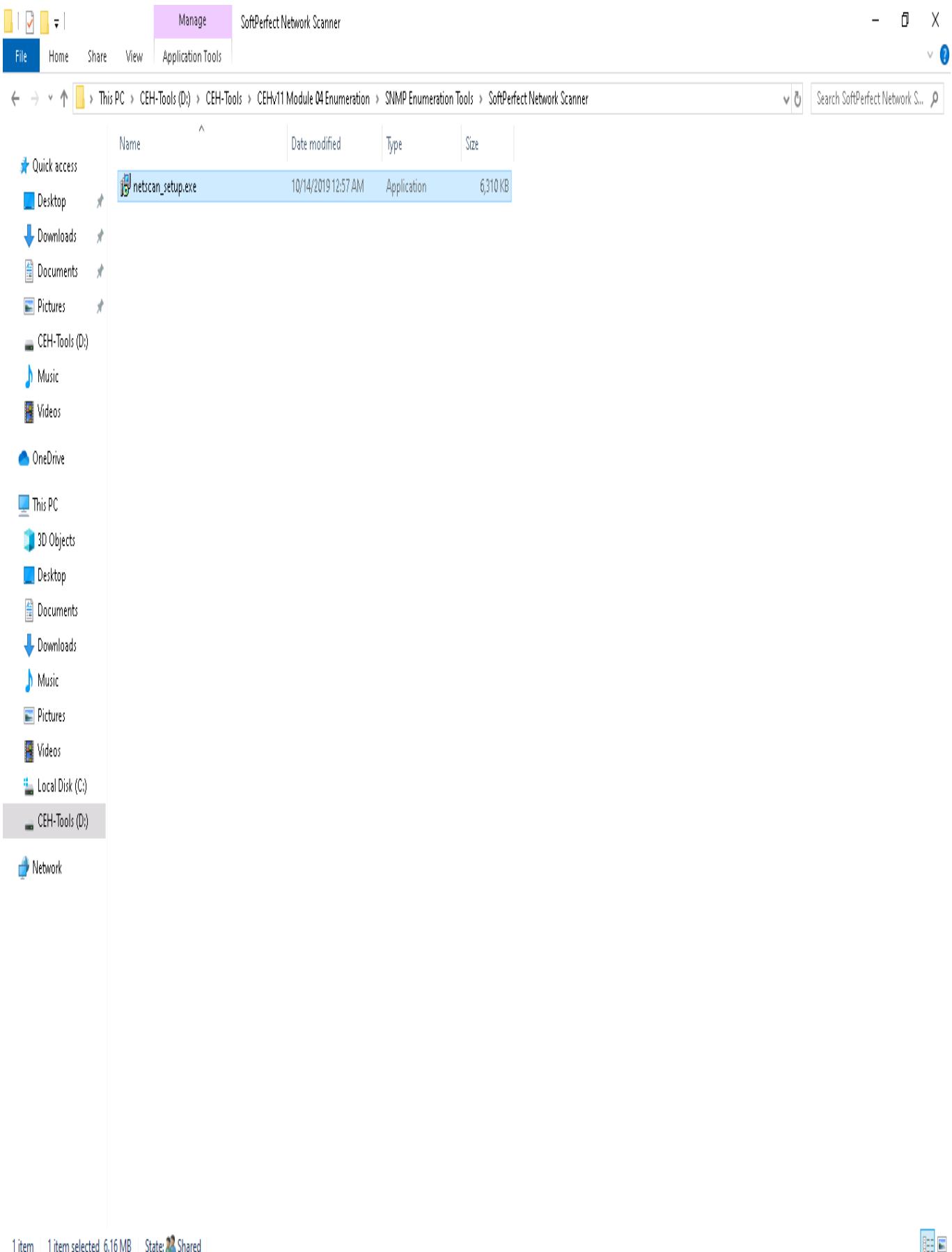
6. A context menu appears; click **Shot and Save....**



7. The **Save As** window appears; enter the file name (here **Shot 1**) and set the location to **Desktop**. Then, click **Save**, as shown in the screenshot.

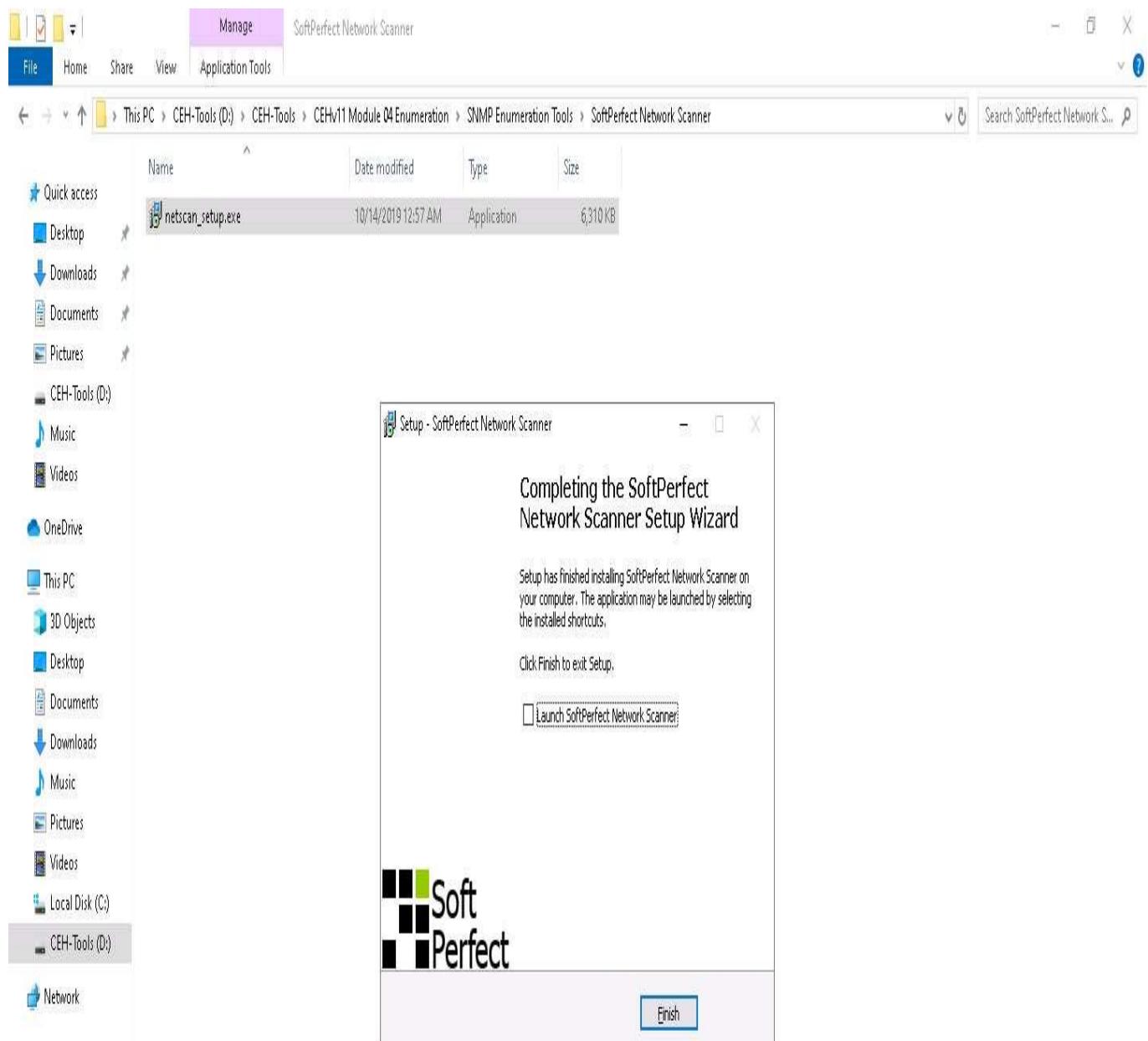


8. Now to demonstrate a change in the registry, install an application (here, **SoftPerfect Network Scanner**).
9. Navigate to **D:\CEH-Tools\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.



10. If a **User Account Control** window appears, click **Yes**.
11. Follow the wizard-driven installation steps to install the SoftPerfect Network Scanner.
12. Once the installation is complete, uncheck the **Launch SoftPerfect Network Scanner** option and click **Finish**.

You can install any application to view the changes in the registry. For demonstration purposes, we have installed the SoftPerfect Network Scanner.

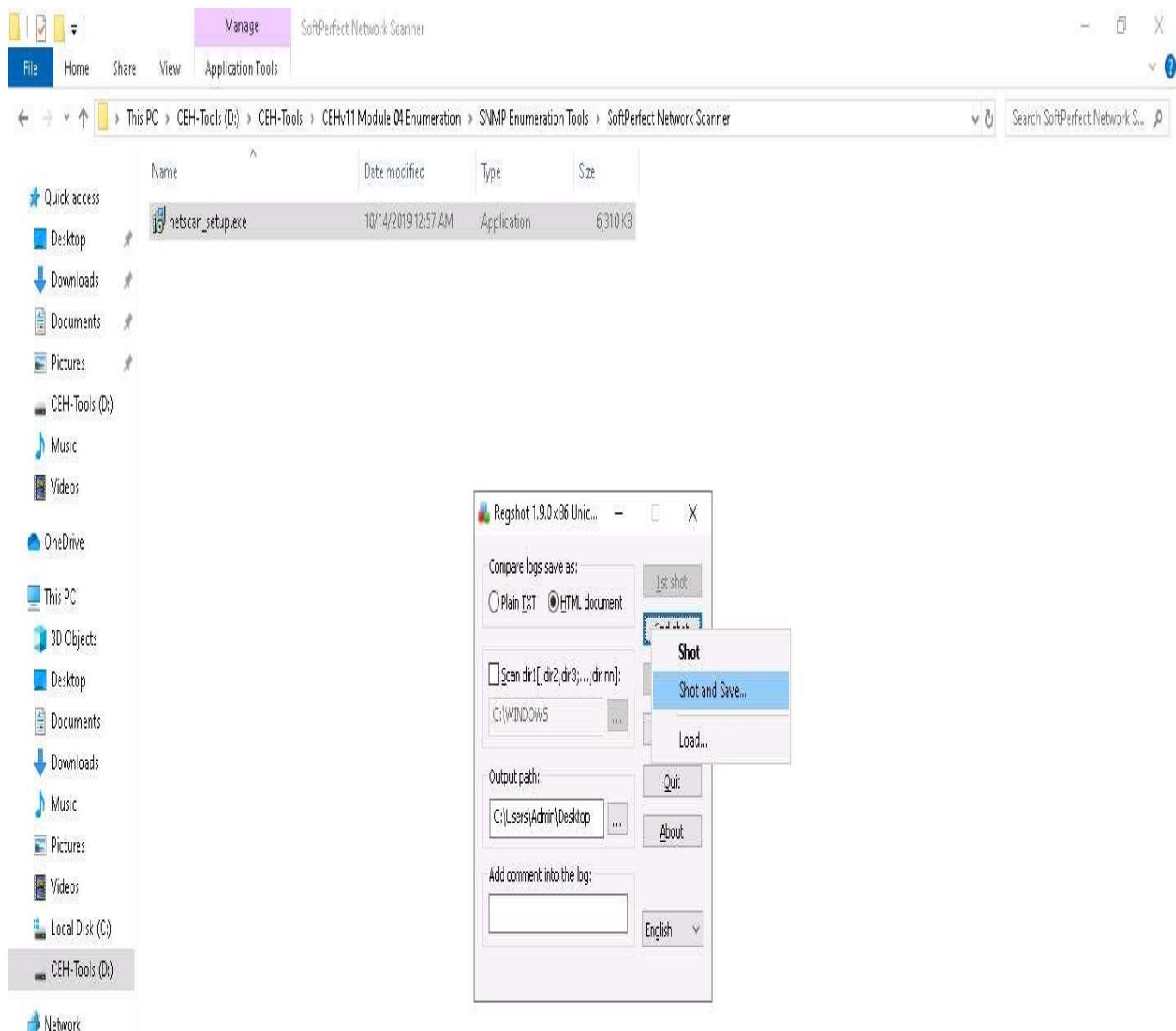


Activate Windows
Go to Settings to activate Windows.



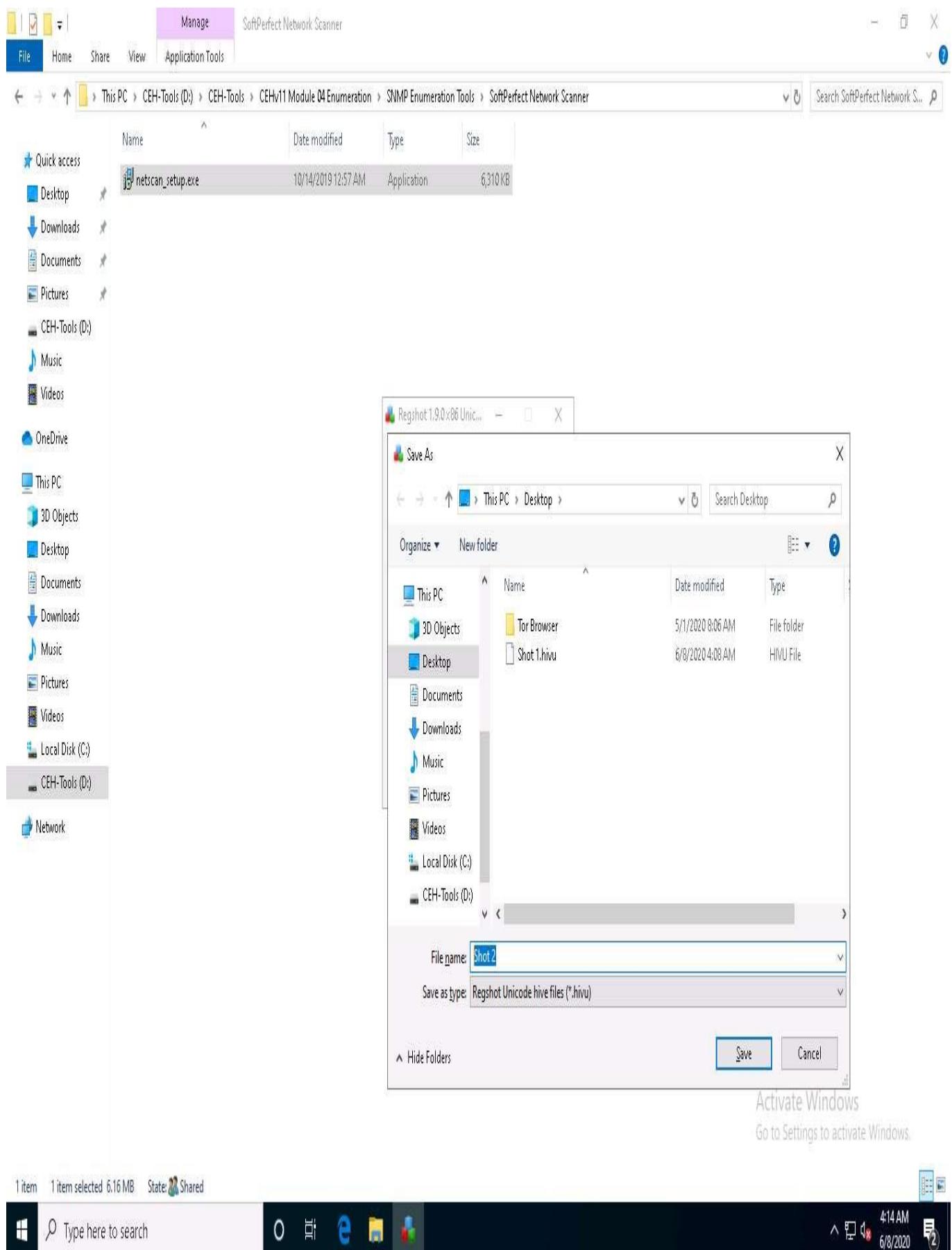
13. Switch to the **Regshot** application window; leave all settings to default, and click **2nd shot**.

14. A context menu appears; click **Shot and Save...**, as shown in the screenshot.



15. The **Save As** window appears; enter the file name (here **Shot 2**) and set the location to **Desktop**. Then, click **Save**, as shown in the screenshot.

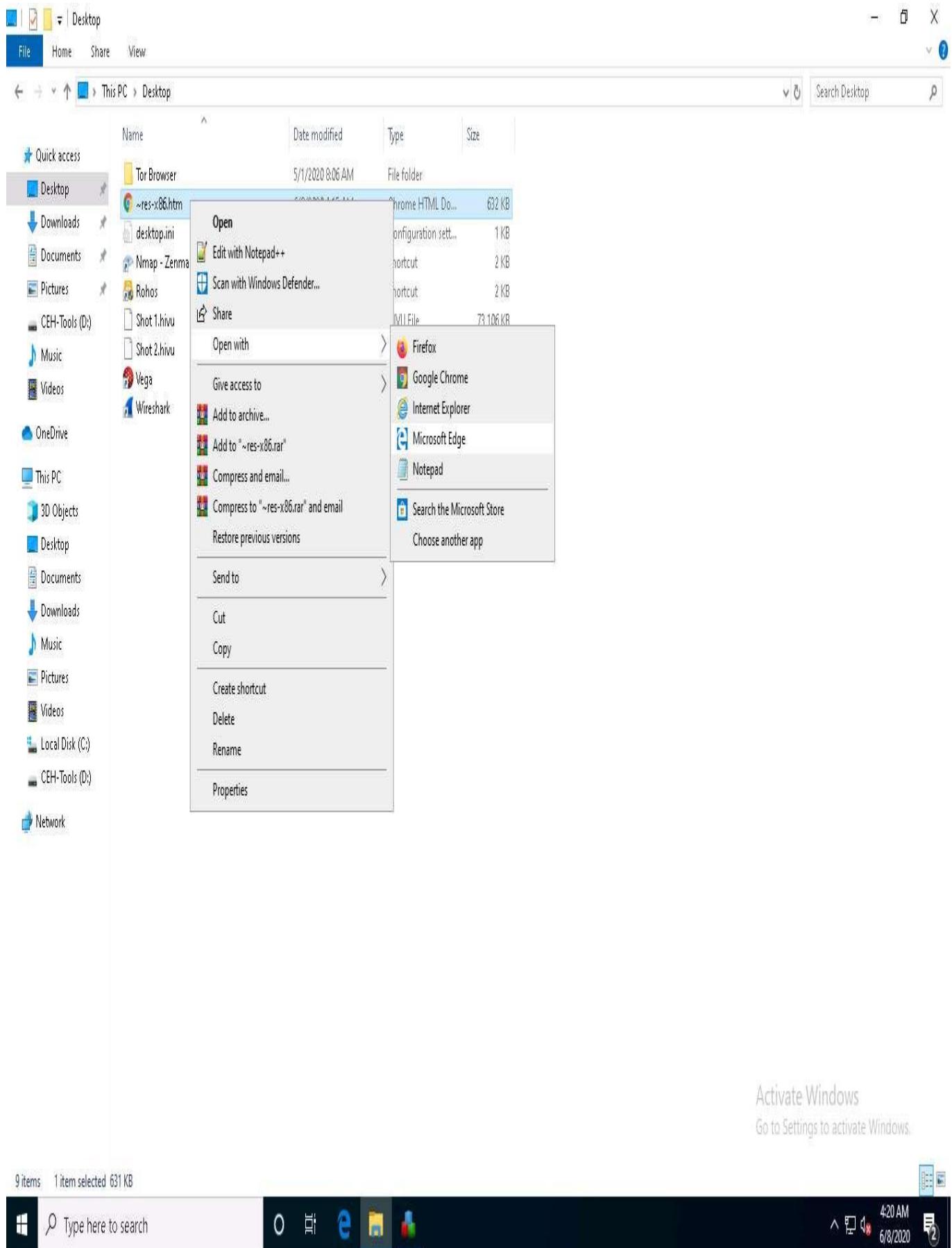




16. Now, return to the **Regshot** application window and click **Compare**, as shown in the screenshot.



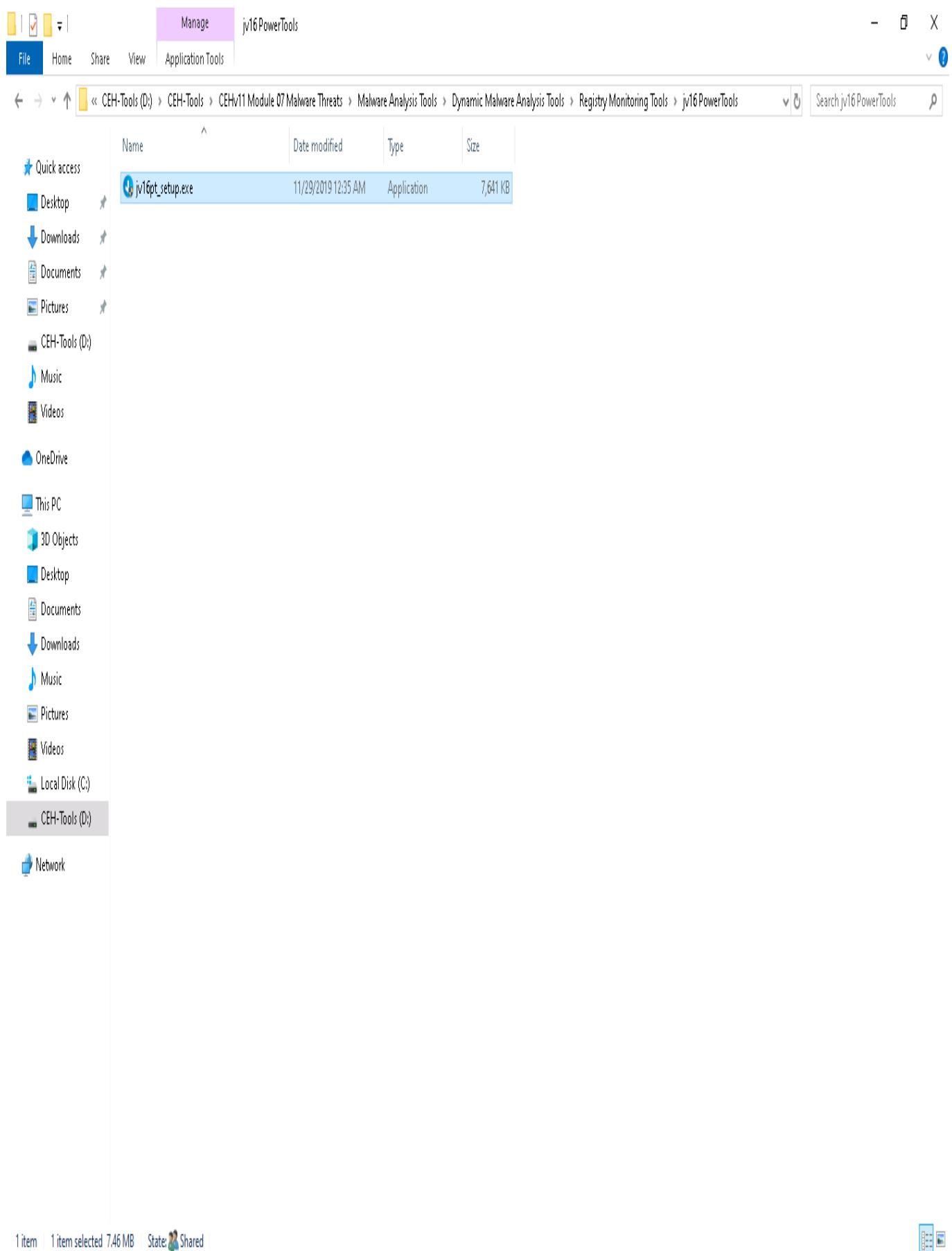
17. The comparison of both shots opens in a default browser window (here, **Google Chrome**), close the browser.
18. Navigate to the **Desktop** right-click **~res-x86.htm**, navigate to **Open with --> Microsoft Edge**.



19. Observe the registry entries that have been modified by comparing the 1st and the 2nd shots, as shown in the screenshot.

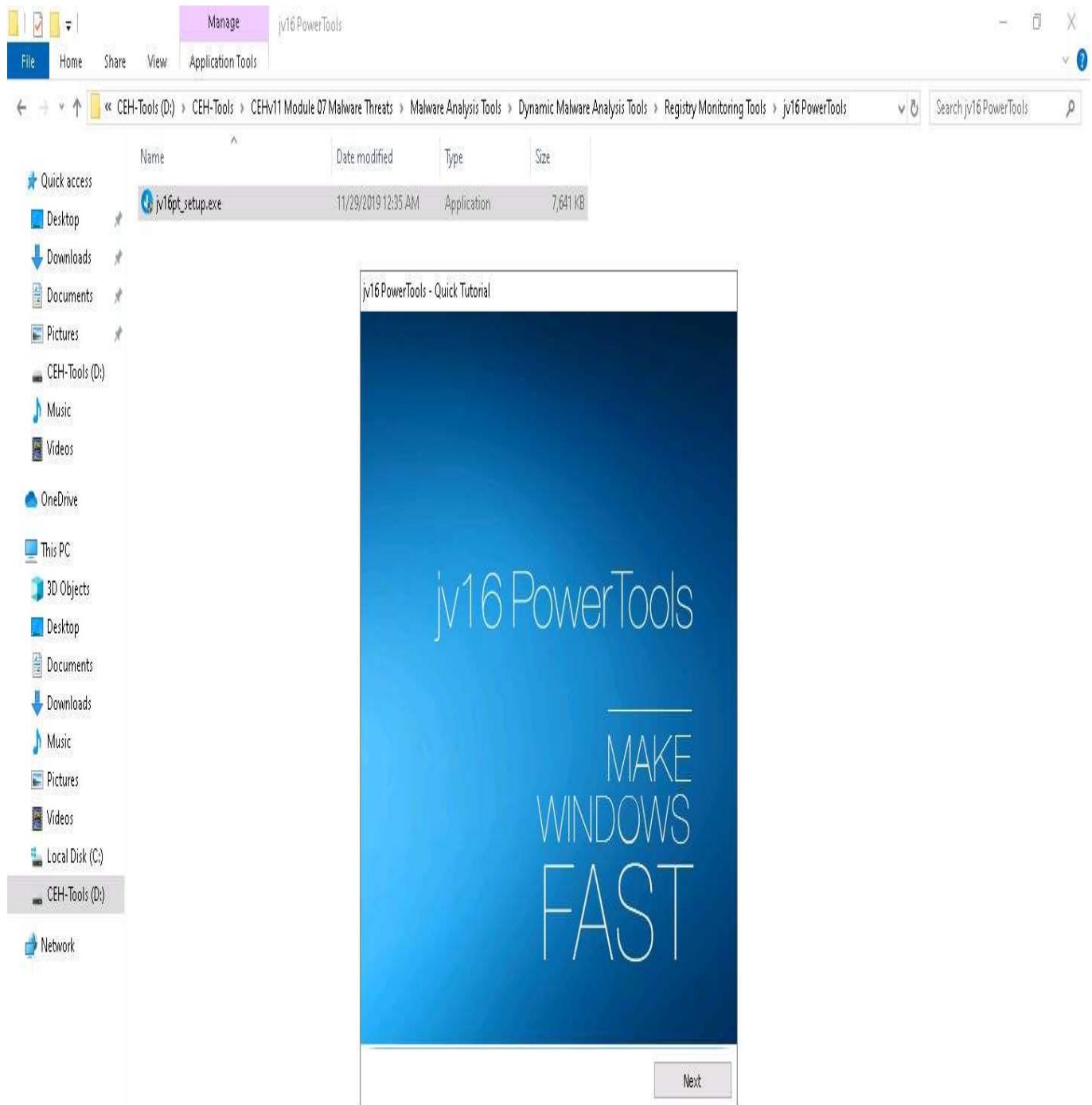
20. By examining modified registry entries in the result, you can find any unwanted registry entries on the machine and stop or delete them manually.
 21. Close all open windows on the **Windows 10** machine.
 22. Now, we will perform an intensive scan for unwanted resources using iv16 PowerTools.

23. On the Windows 10 machine, navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\jv16 PowerTools** and double-click **jv16pt_setup.exe**.

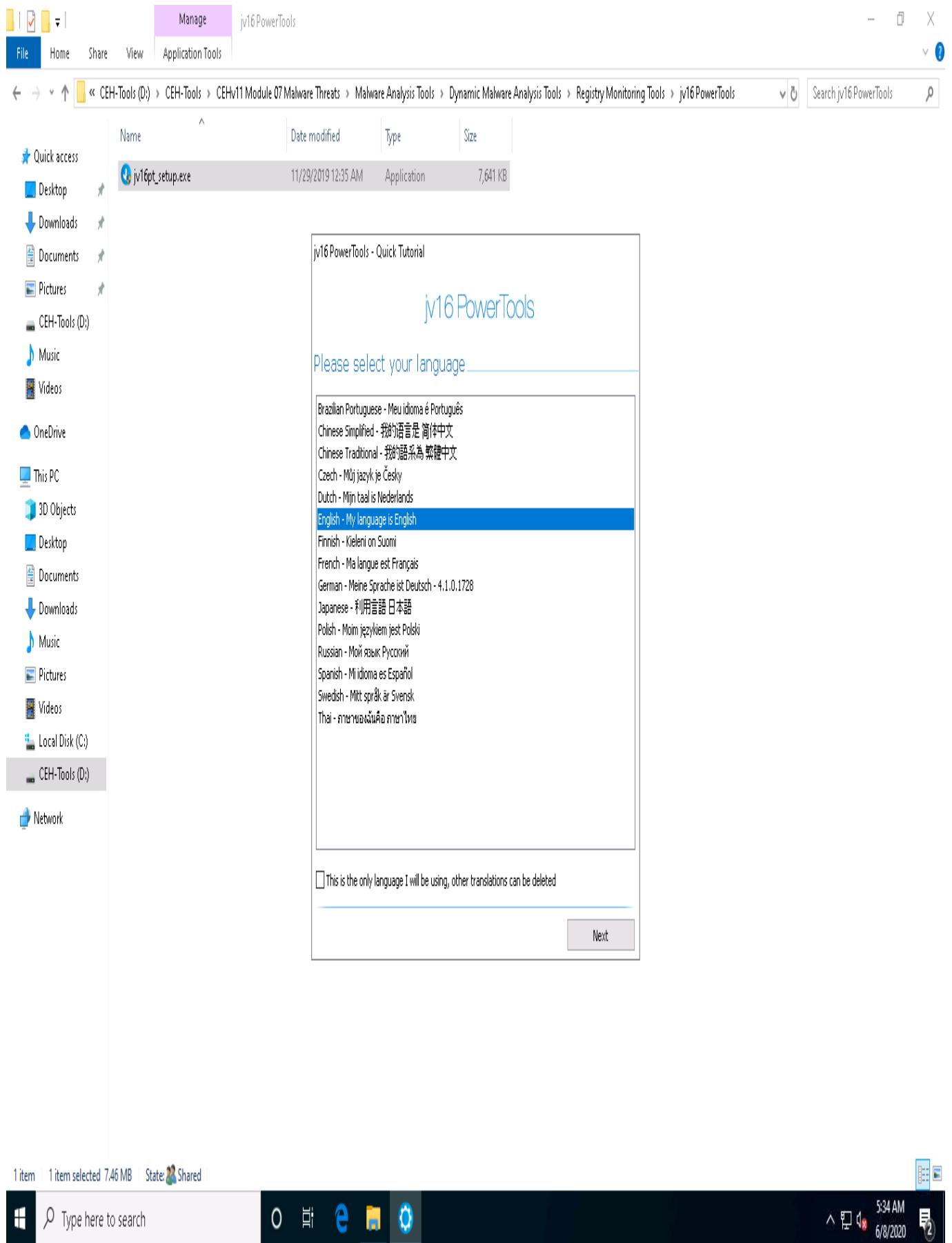


24. If the **User Account Control** window appears, click **Yes**.
25. Follow the wizard-driven installation steps to install jv16 Power Tools.
26. The **jv16 PowerTools Quick Tutorial** window appears; click **Next**.

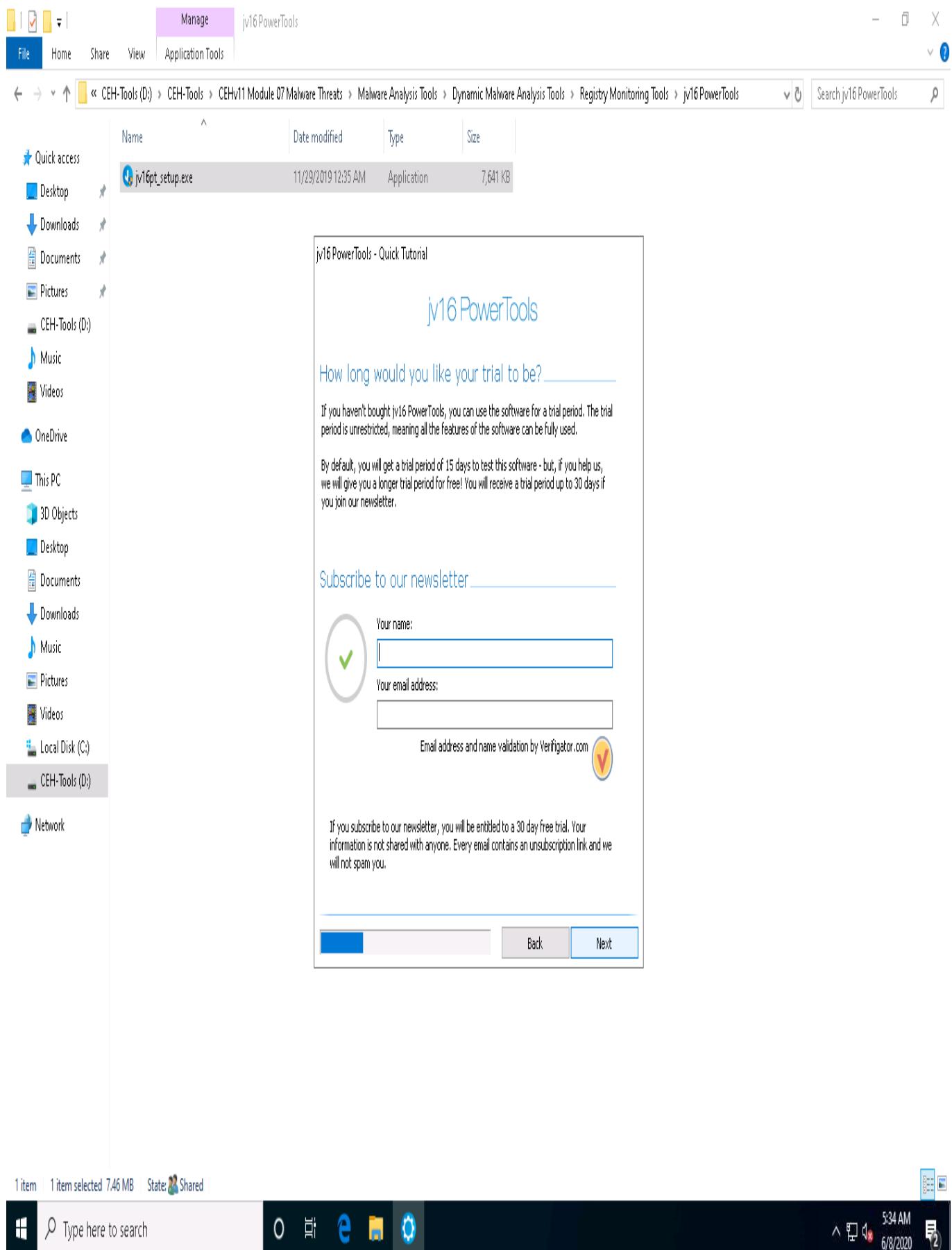
If the **jv16 PowerTools Quick Tutorial** window does not appear, then double-click the **jv16 PowerTools** short-cut icon on **Desktop** to launch the application.



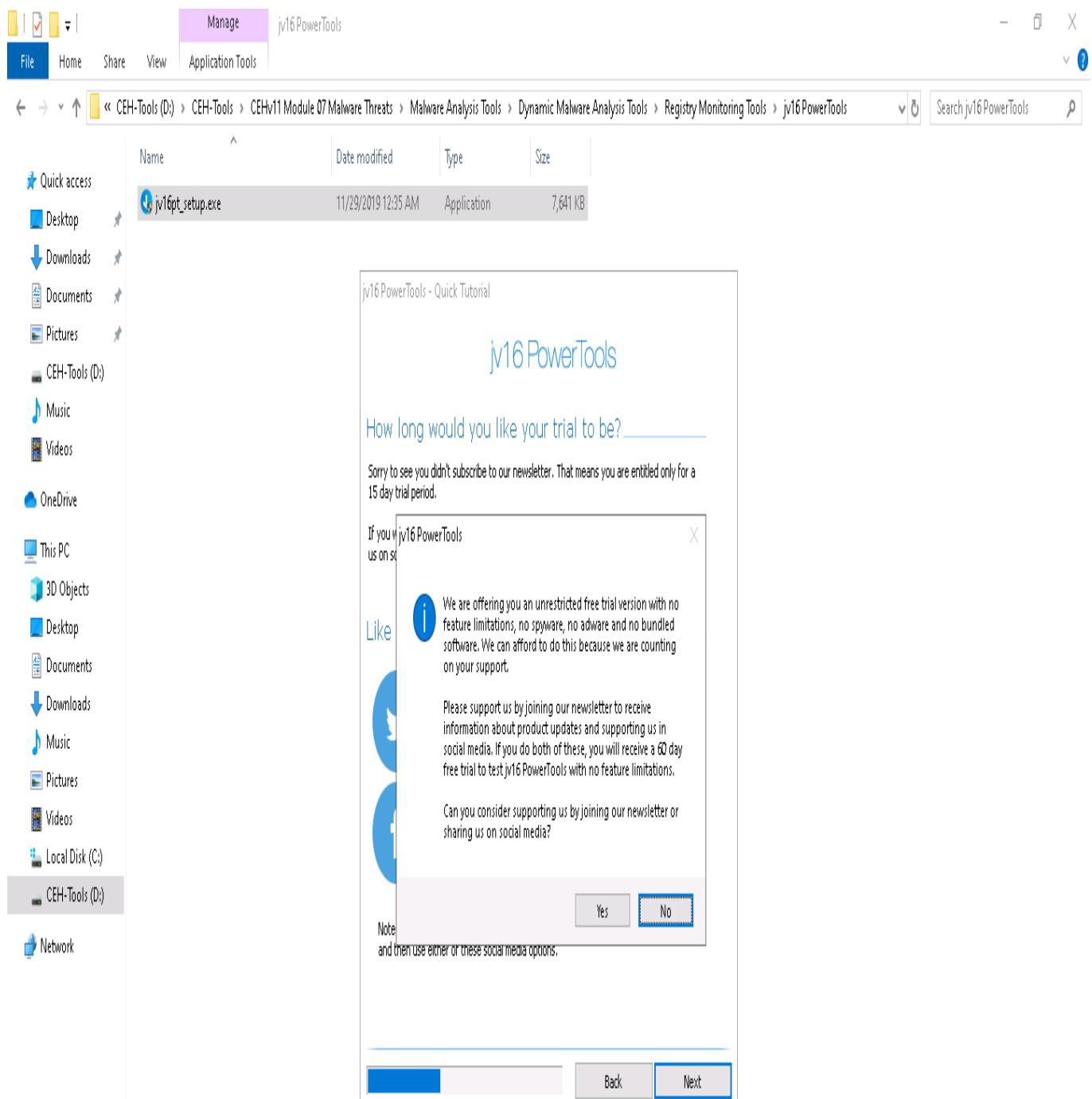
27. In the **Please select your language** wizard, choose a language (here, **English**) and click **Next**.



28. The **How long would you like your trial to be?** wizard appears; leave the fields blank and click **Next**.

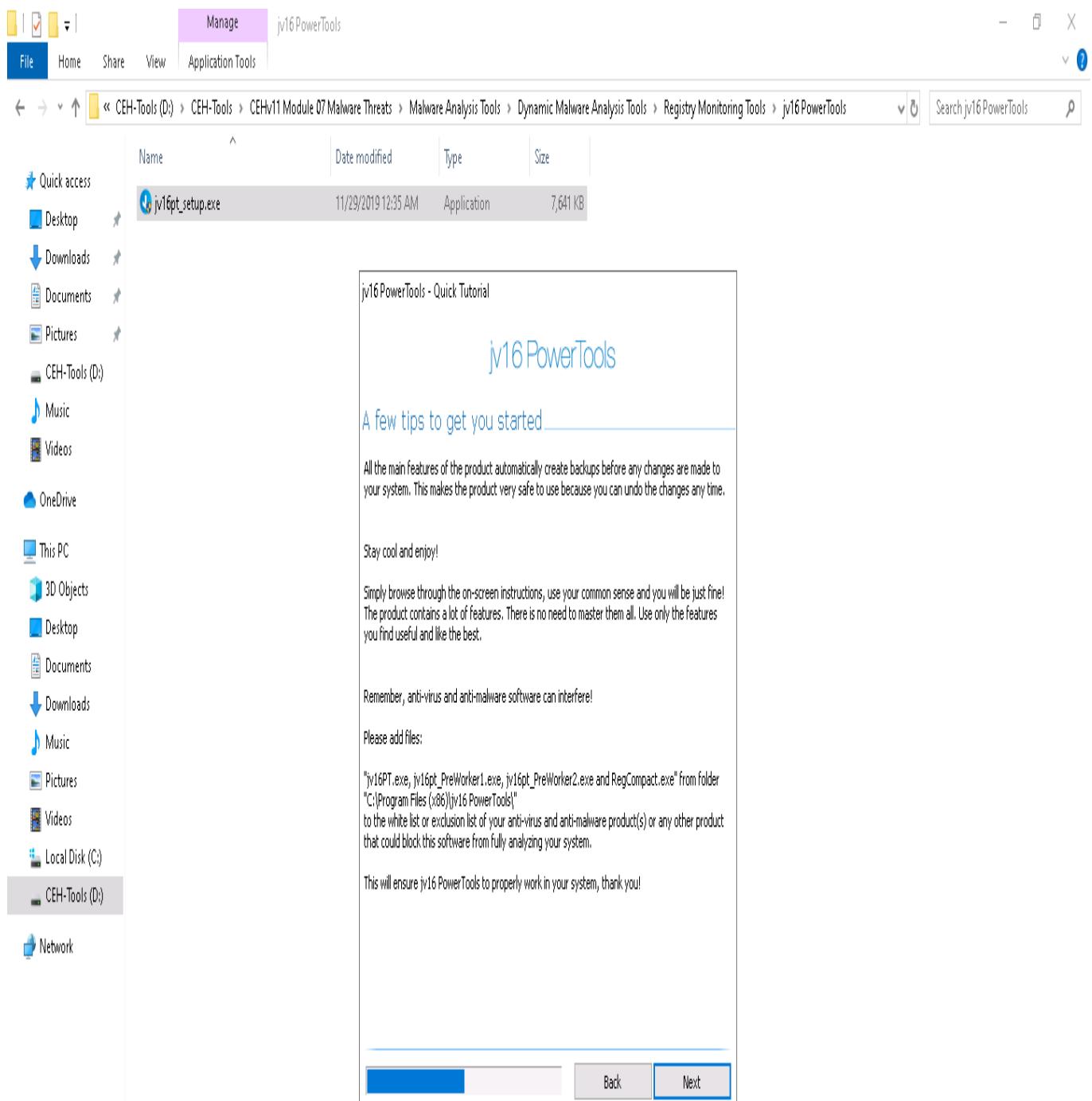


29. In the next **How long would you like your trial to be?** wizard screen, leave the fields blank and click **Next**.
30. The **jv16 PowerTools** pop-up appears; click **No**.

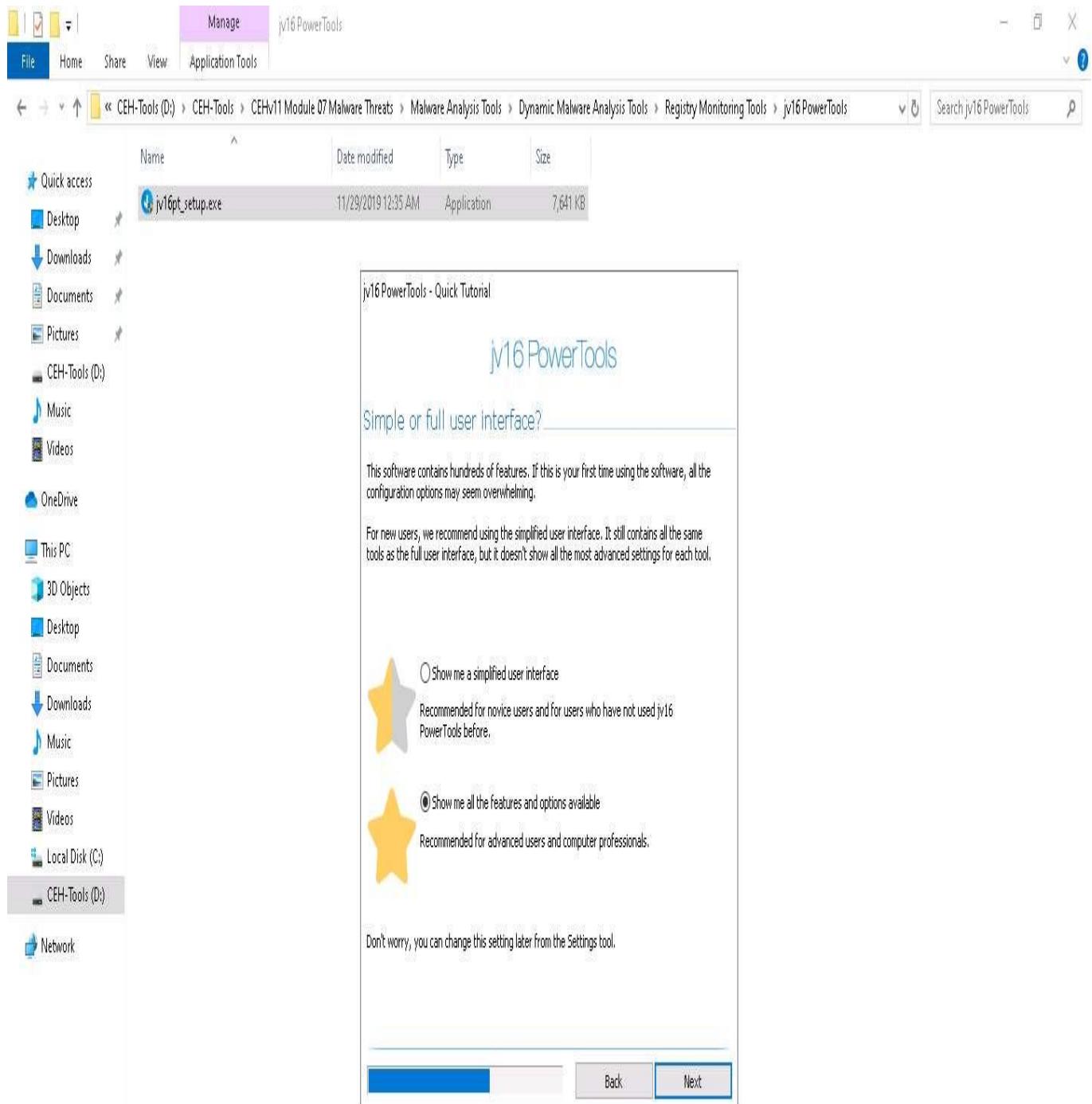


31. The **A few tips to get you started** wizard appears; click **Next**.





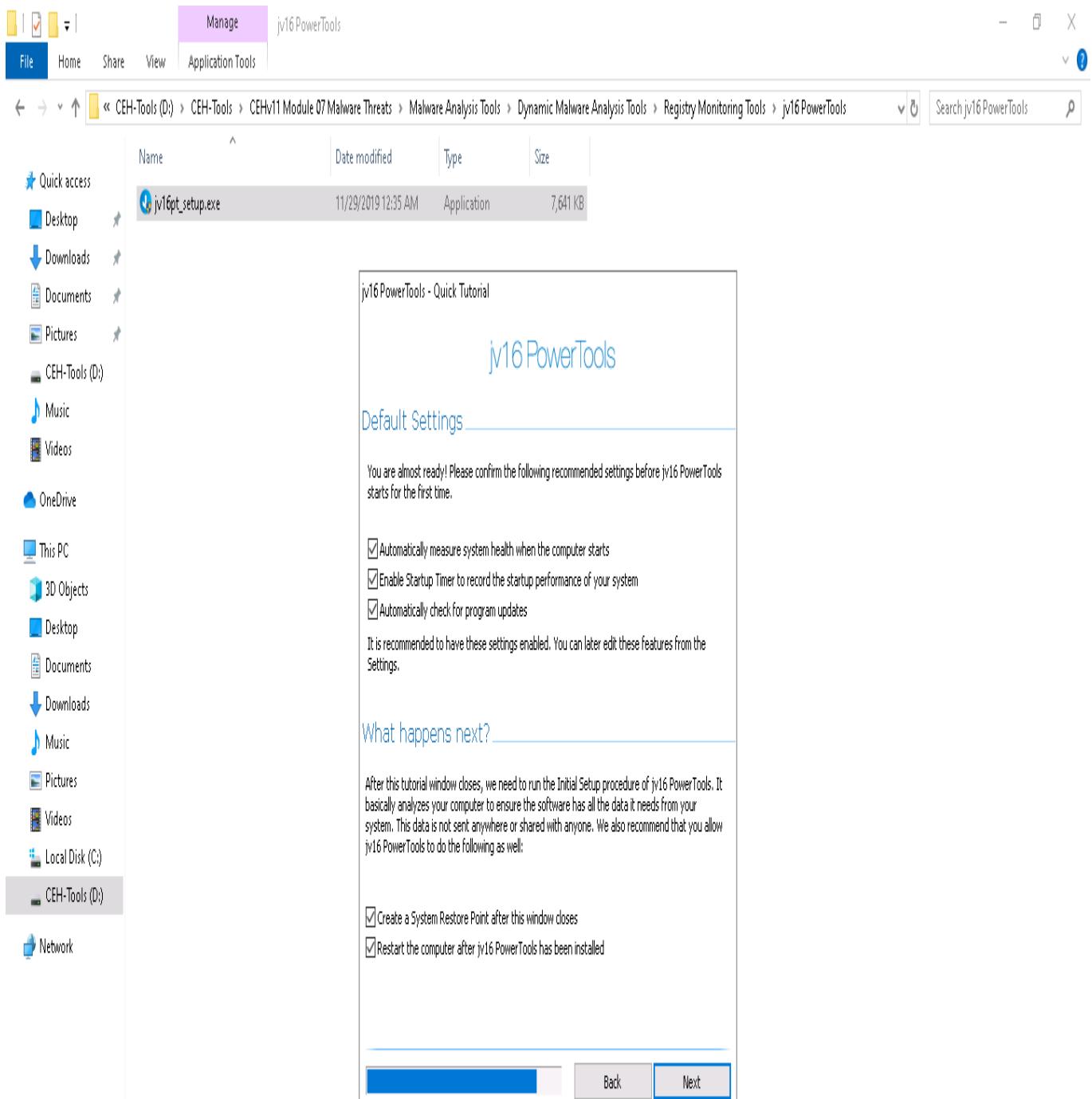
32. The **Simple or full user interface** wizard appears; choose the **Show me all the features and options available** radio button, and then click **Next**.



Activate Windows
Go to Settings to activate Windows.



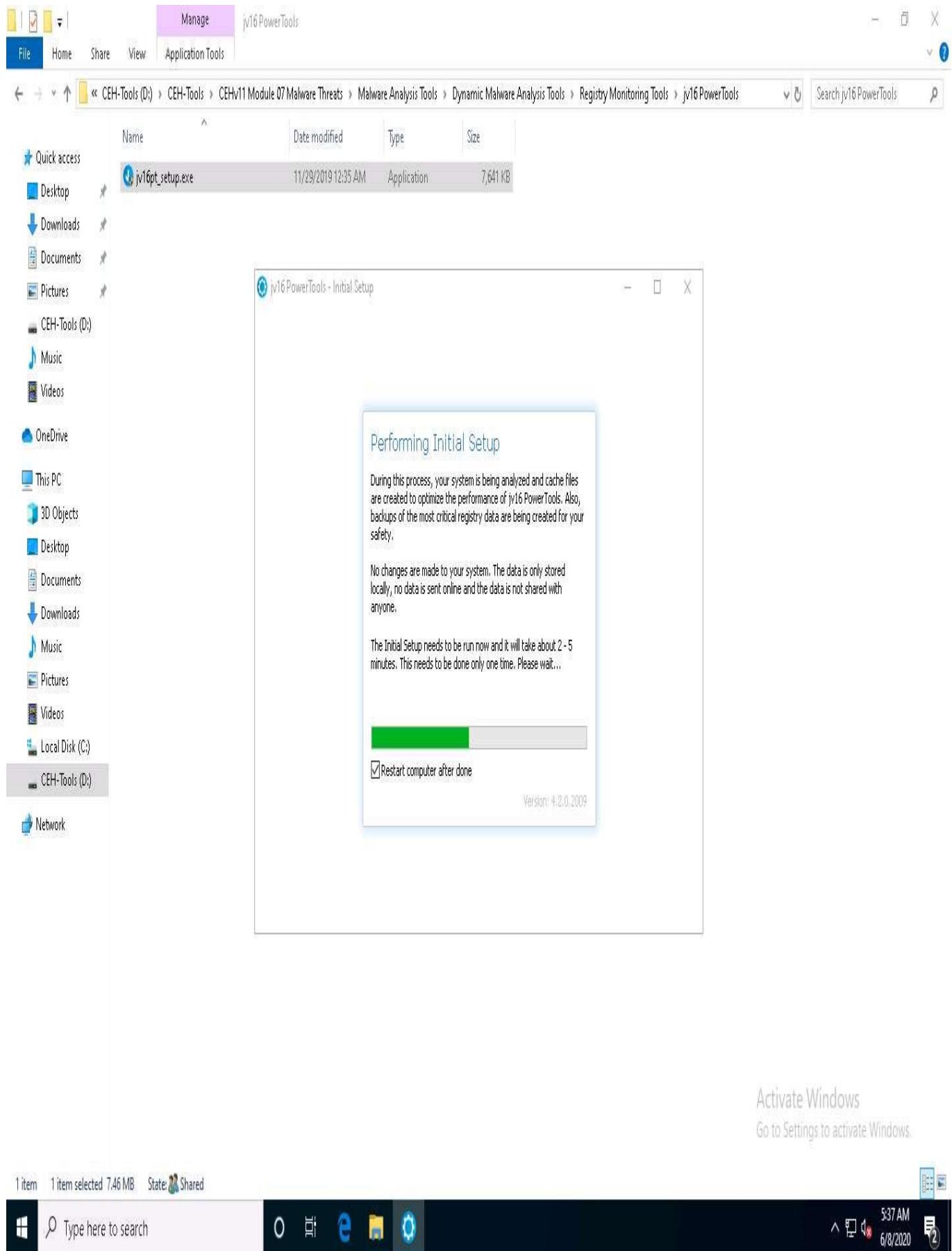
33. Click **Next** in the **Global Ignore List** wizard.
34. In the **Default Settings** wizard, leave all settings set to default, and then click **Next**.



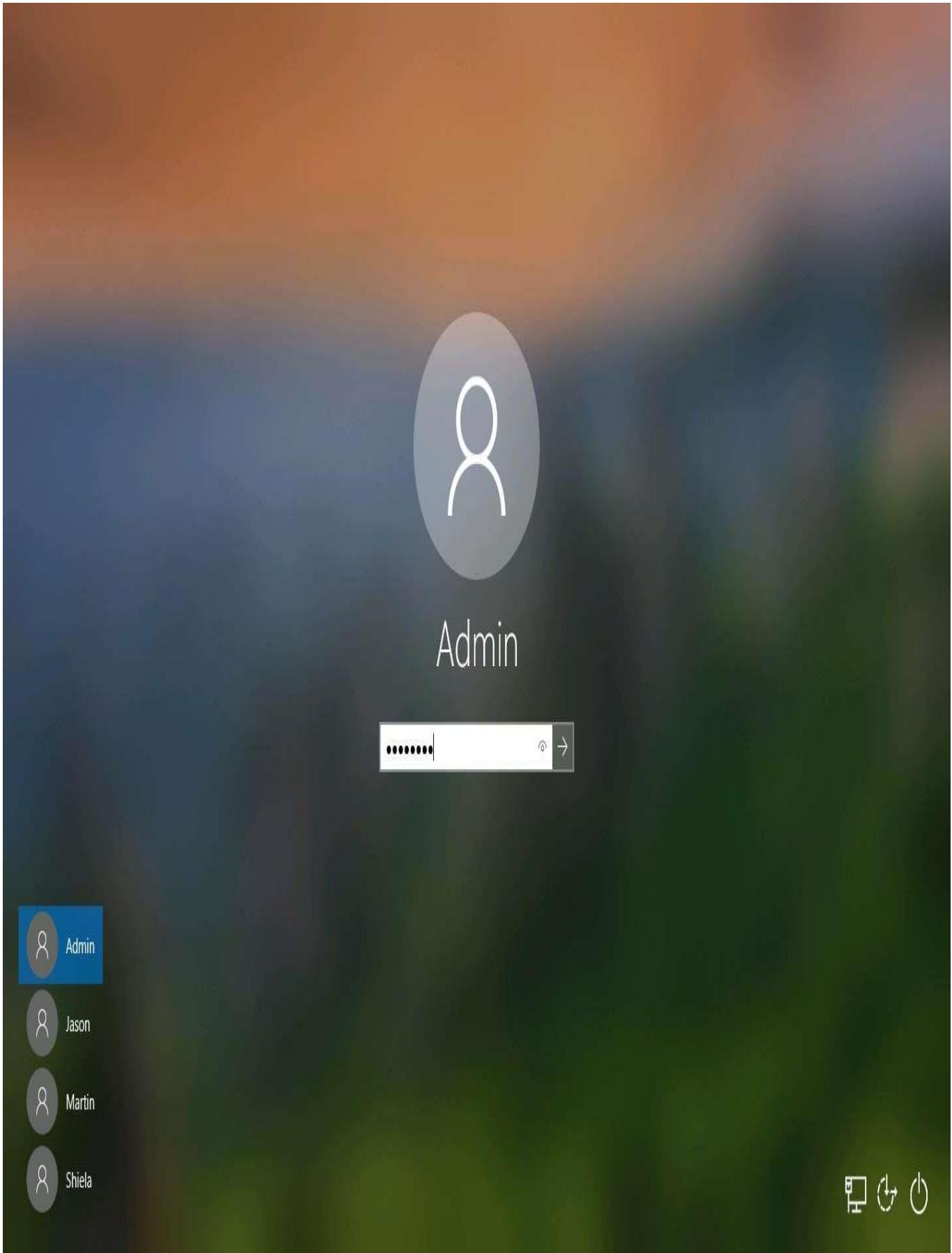
1 item 1 item selected 7.46 MB State: Shared



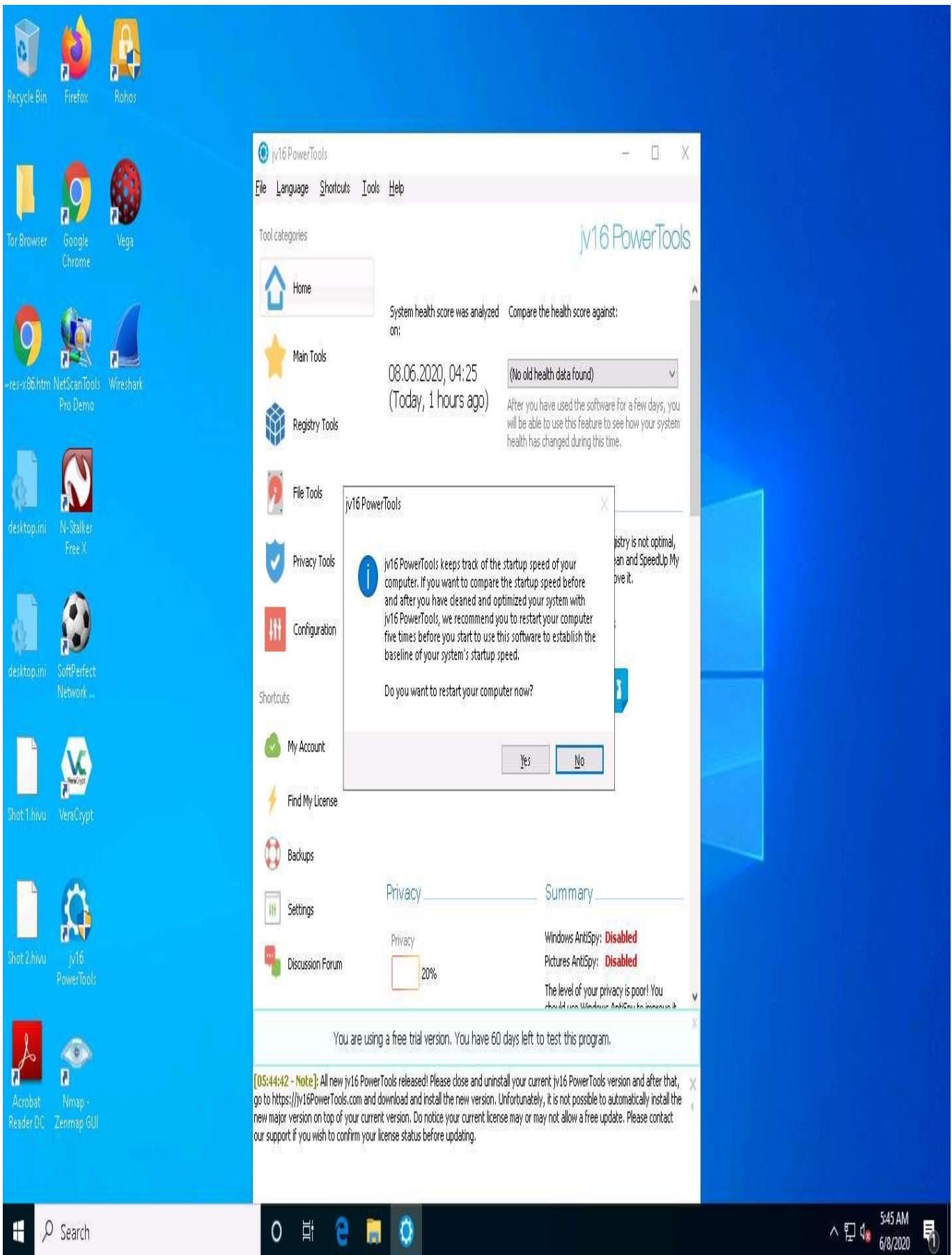
35. The **Performing Initial Setup** window appears. Make sure that the **Restart computer after done** option is checked. Once the setup is done, the machine will automatically restart.



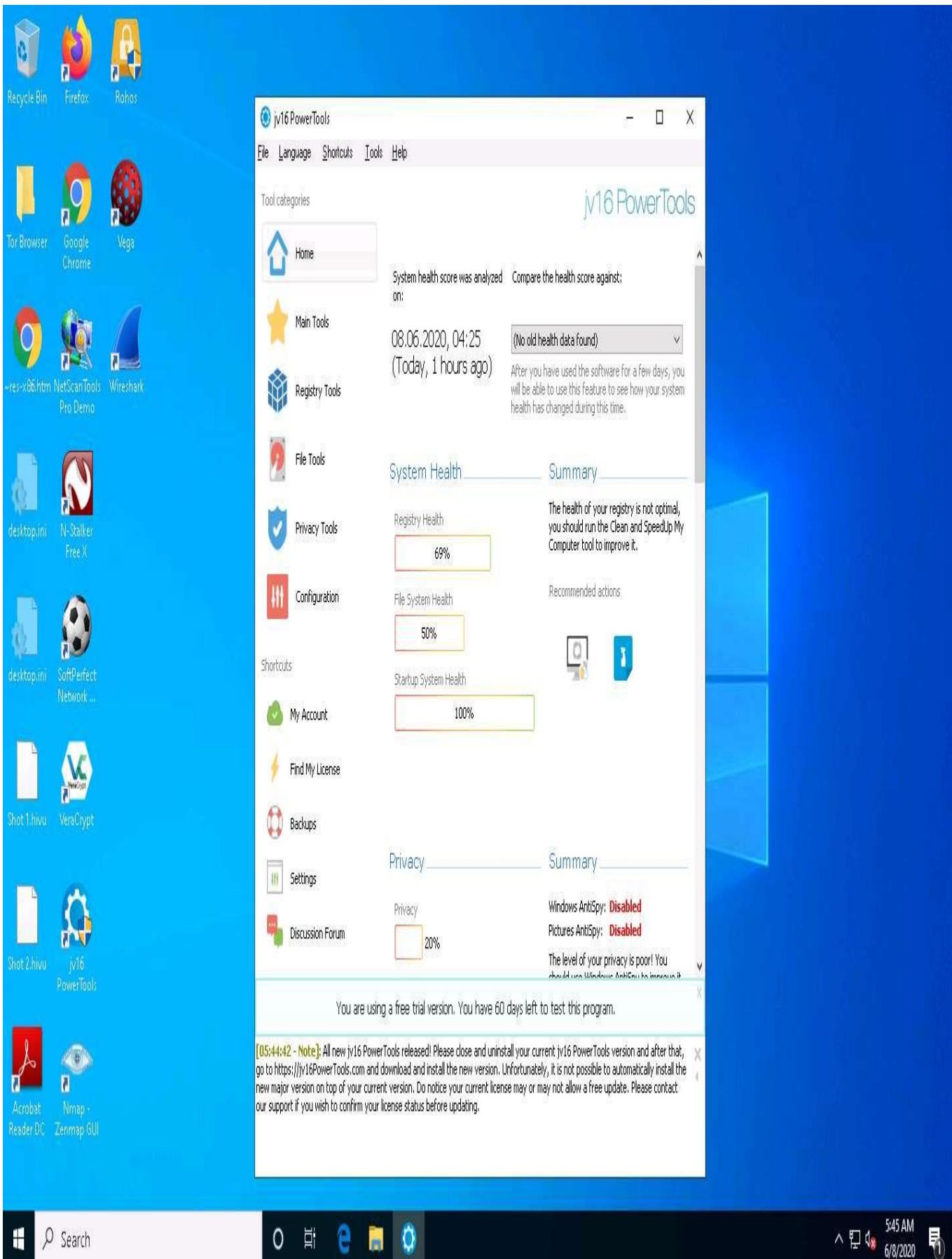
36. Once the machine has restarted, click [Ctrl+Alt+Delete](#) to activate the machine. By default, **Admin** user account is selected, click **Pa\$\$w0rd** to enter the password and press **Enter** to log in.



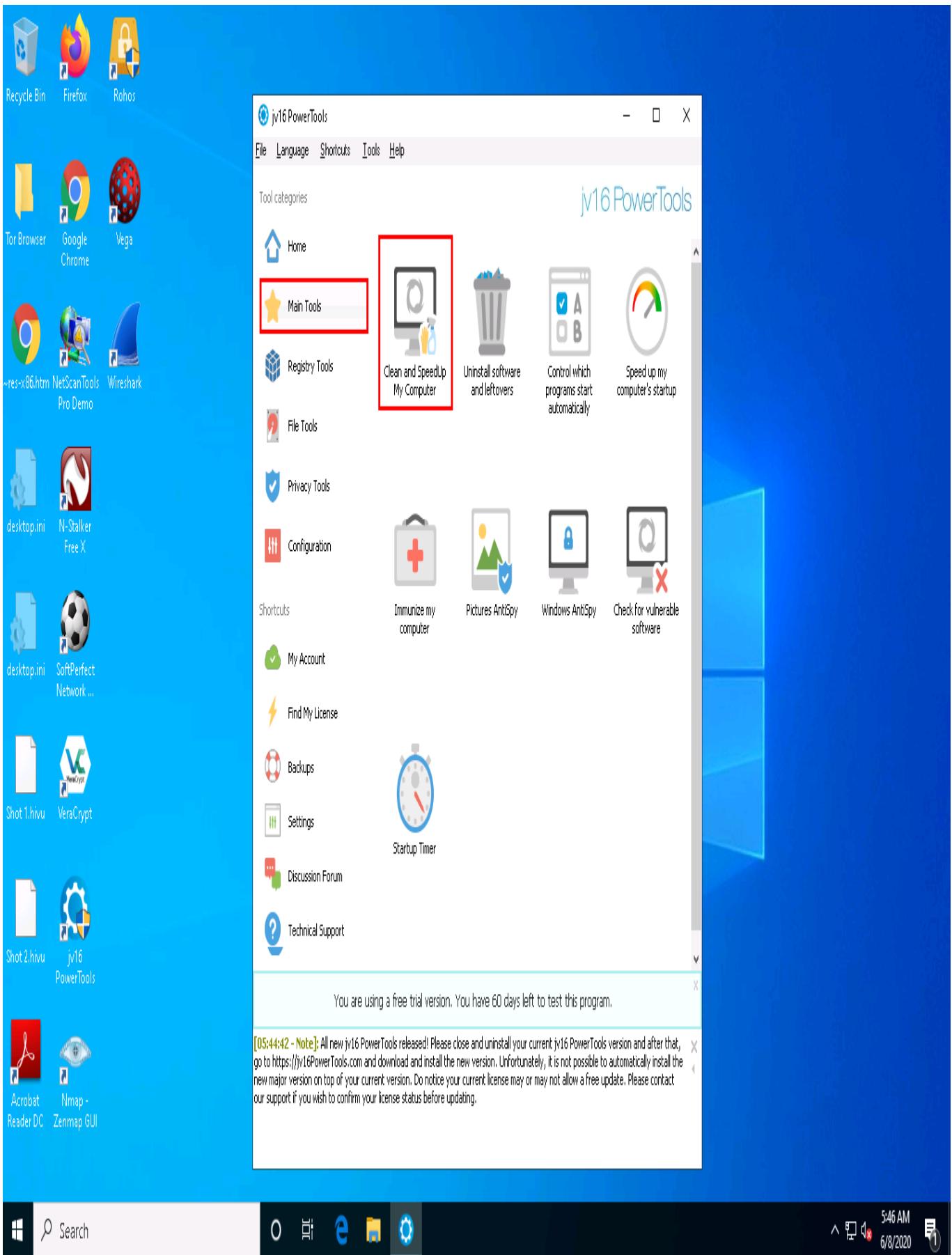
37. Observe that the jv16 PowerTools application launches automatically, along with a **jv16 PowerTools** pop-up; click **No**.



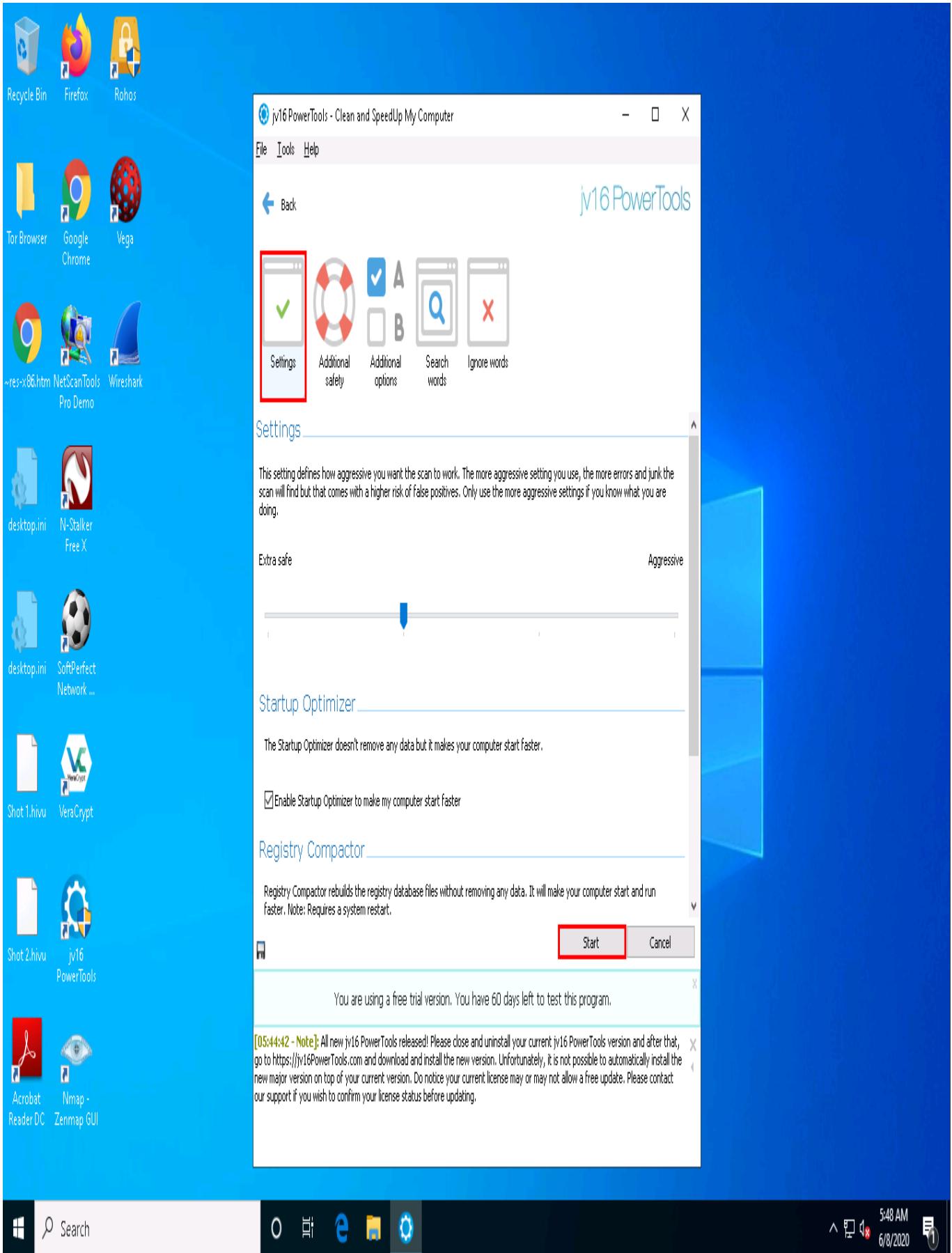
38. The **jv16 PowerTools** main window appears, as shown in the screenshot. By default, the **Home** option is selected, which displays the System Health, Privacy, Registry Integrity, and System Startup Times Summaries.



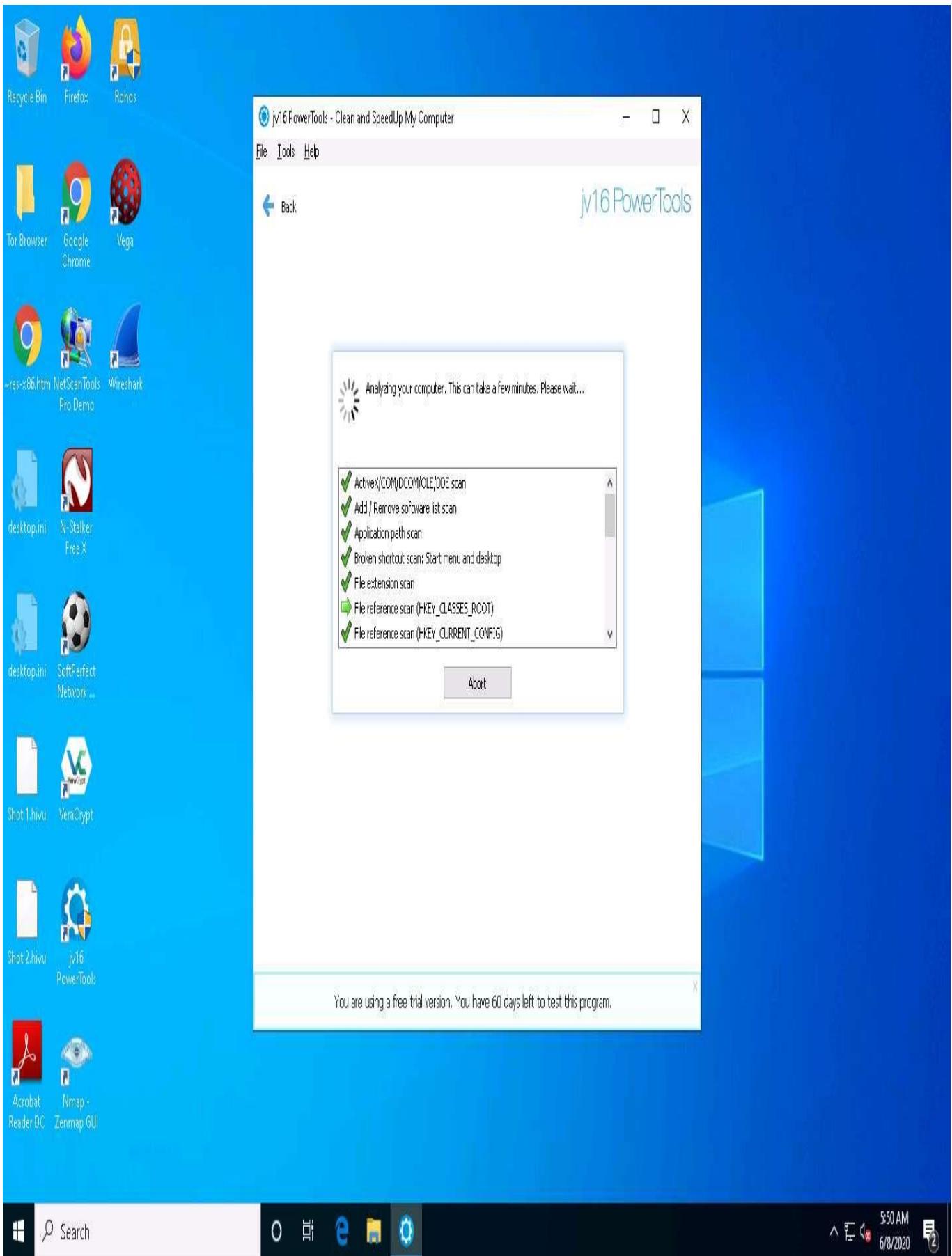
39. Click the **Main Tools** section from the left pane to view the available tools in jv16 PowerTools. The **Main Tools** section lists out all available tool features, as shown in the screenshot.
40. Click the **Clean and SpeedUp My Computer** icon.



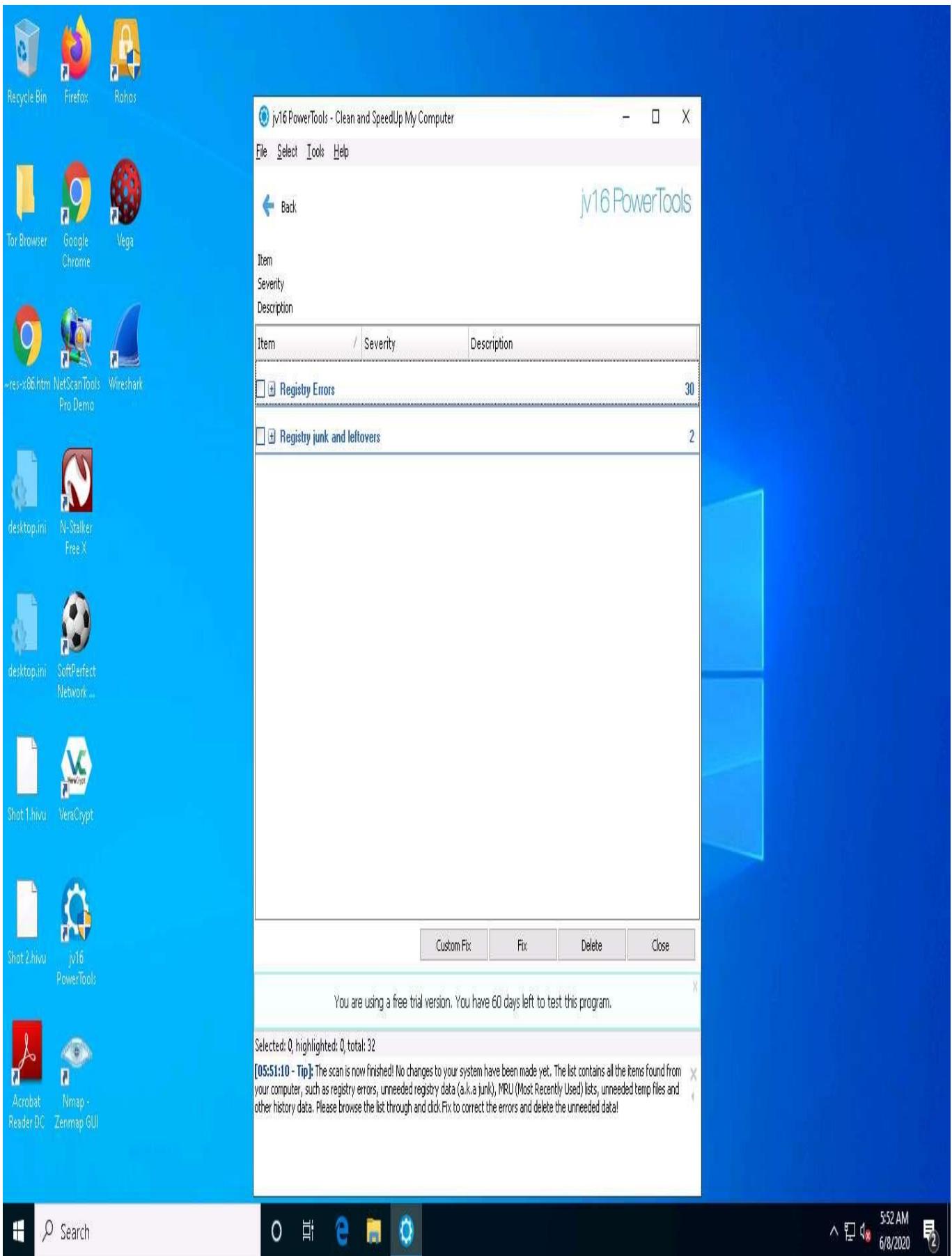
41. The **Clean and SpeedUp My Computer** wizard appears. Click the **Settings** and click **Start**.



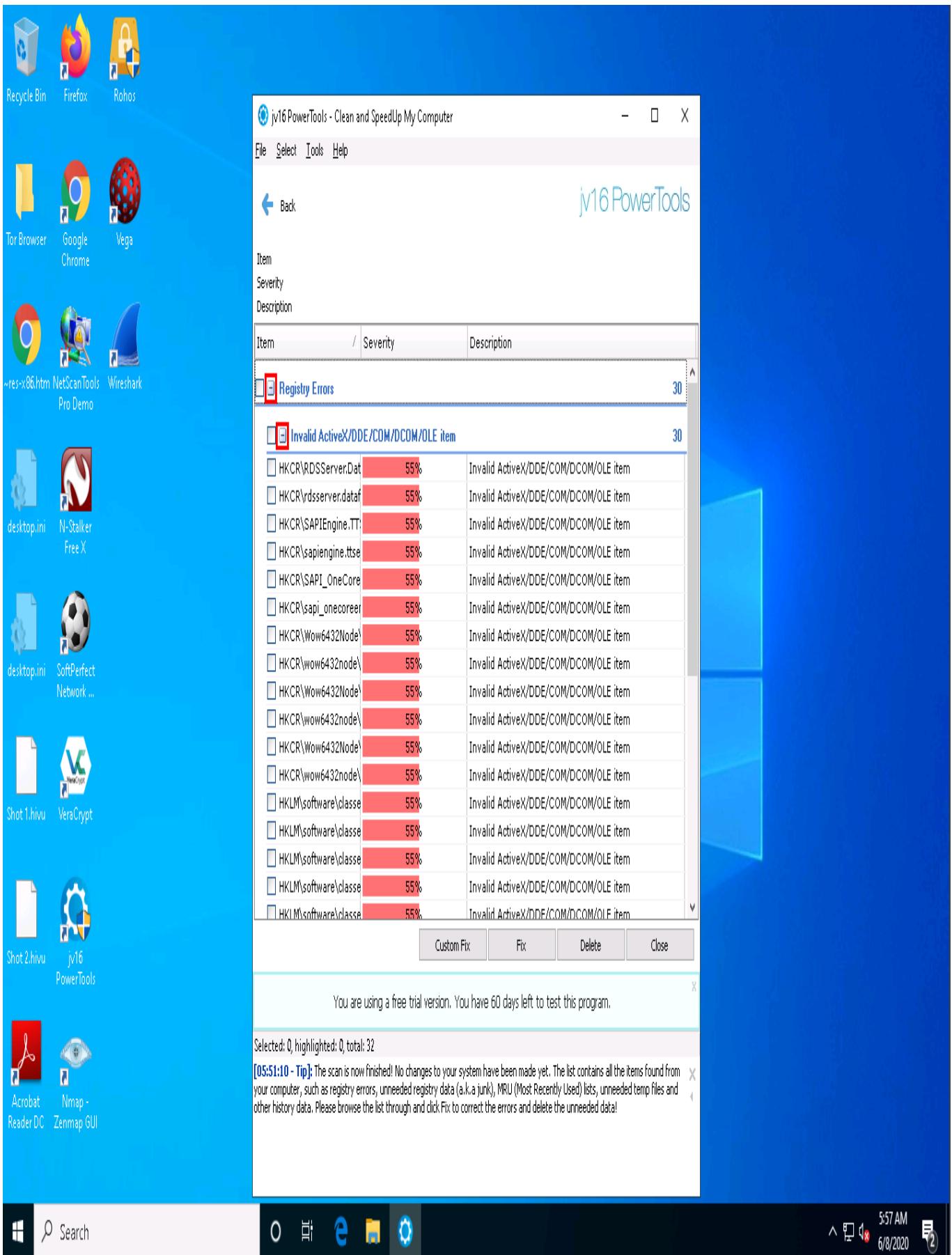
42. The tool starts analyzing the machine. The process takes a few minutes.



43. Once the scanning is complete, JV16 PowerTools displays the **Registry Errors**, **Temp Files**, and other results.

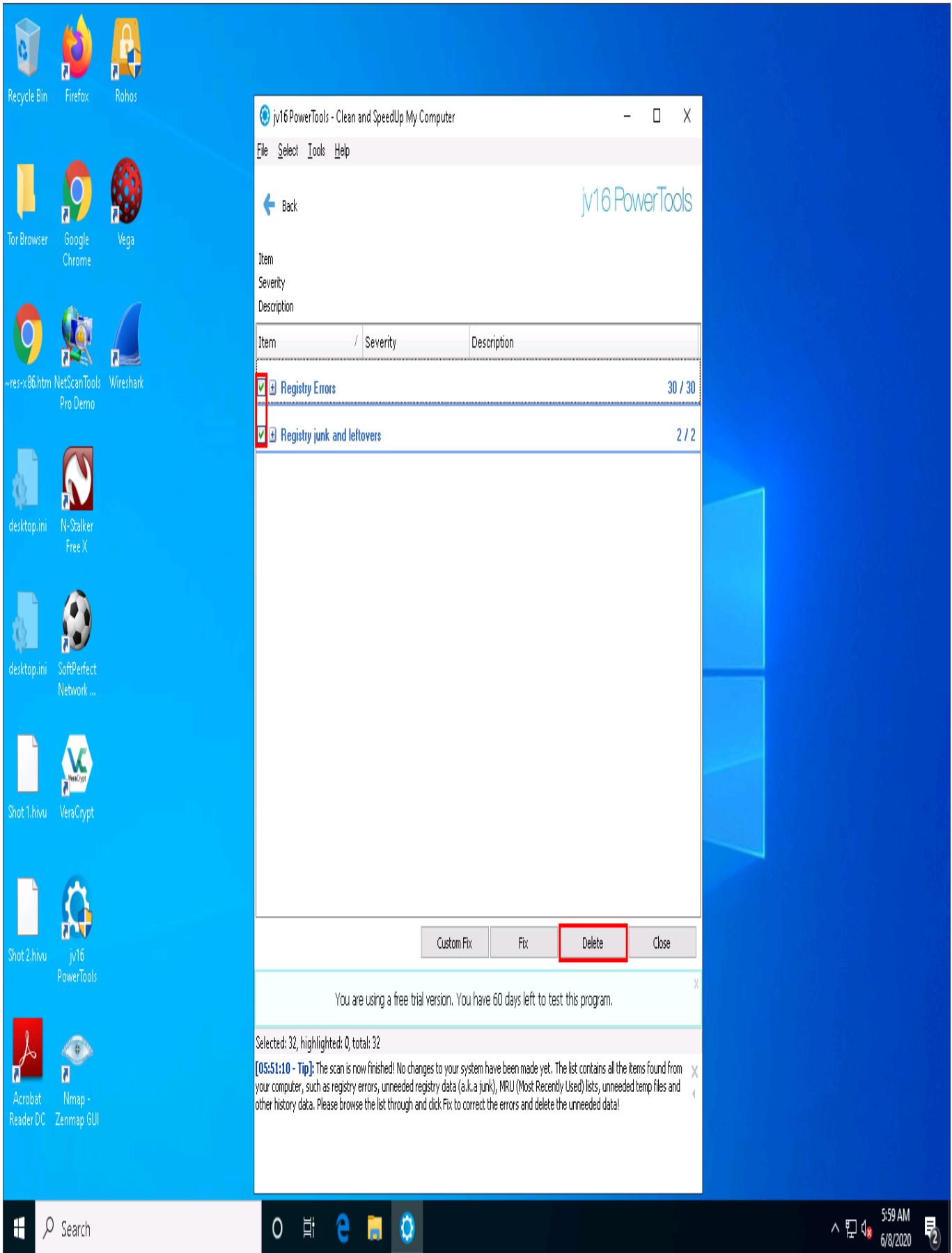


44. To view the registry errors, expand the **Registry Errors** node, and then expand the **Invalid ActiveX/DDE/COM/DCOM/OLE** item node.

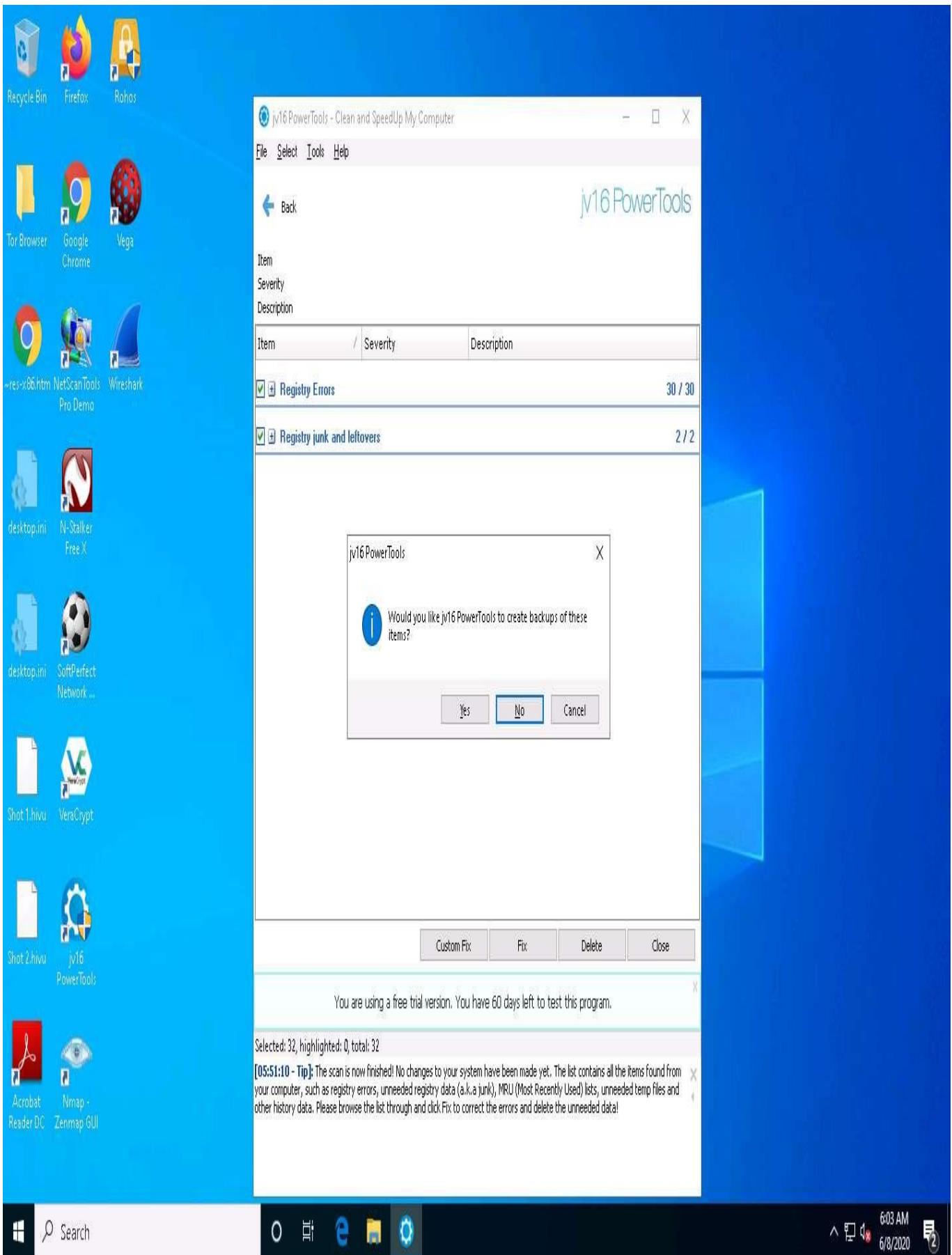


45. In the same way, expand the other items in the list to view all temporary files, log files, and other data.
46. Select all items in the application window, and then click **Delete**.

The registry errors might differ in your lab.

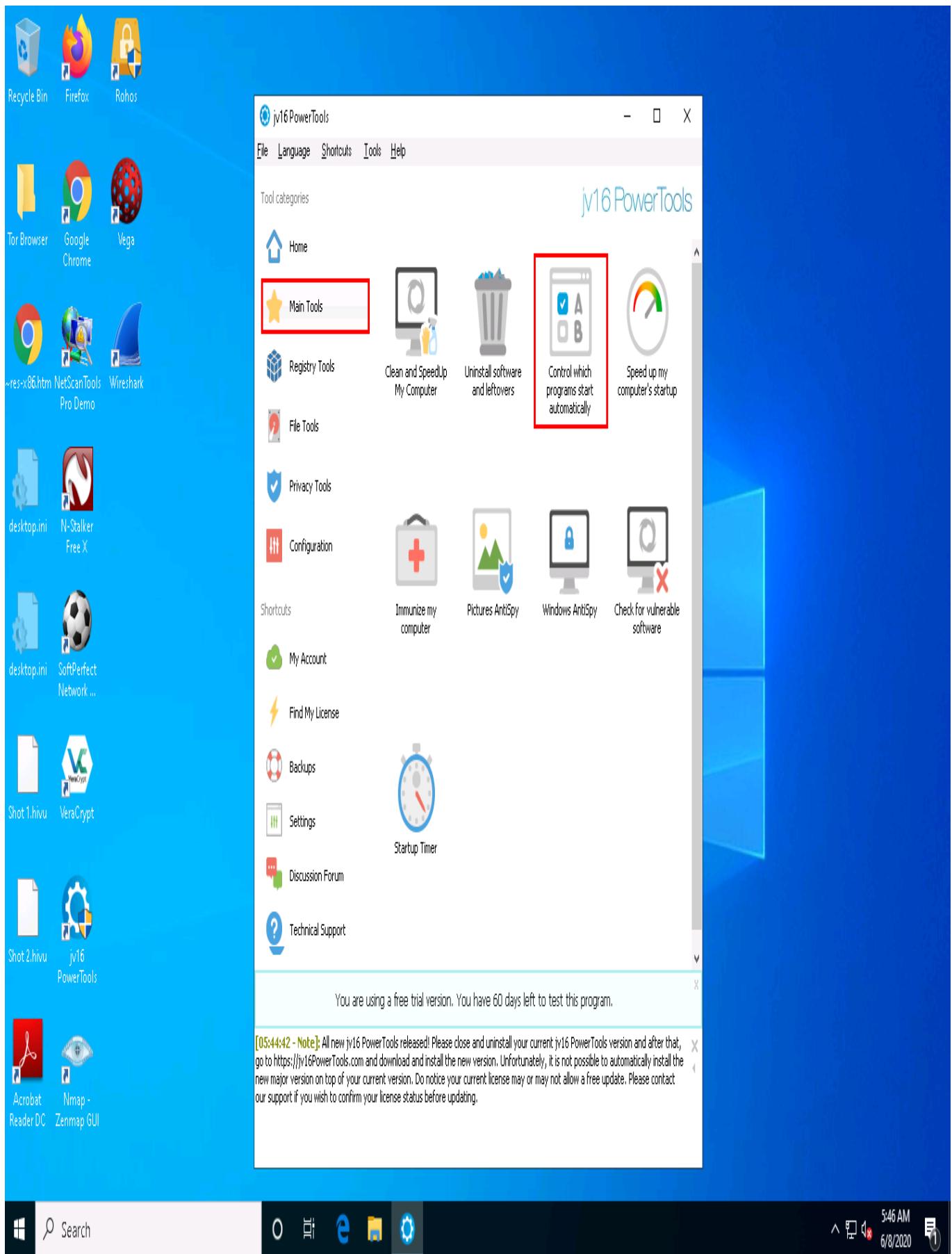


47. The **jv16 PowerTools** pop-up appears. If you want to create a backup, click **Yes**. In this lab, we have selected the **No** option, which deletes all files.

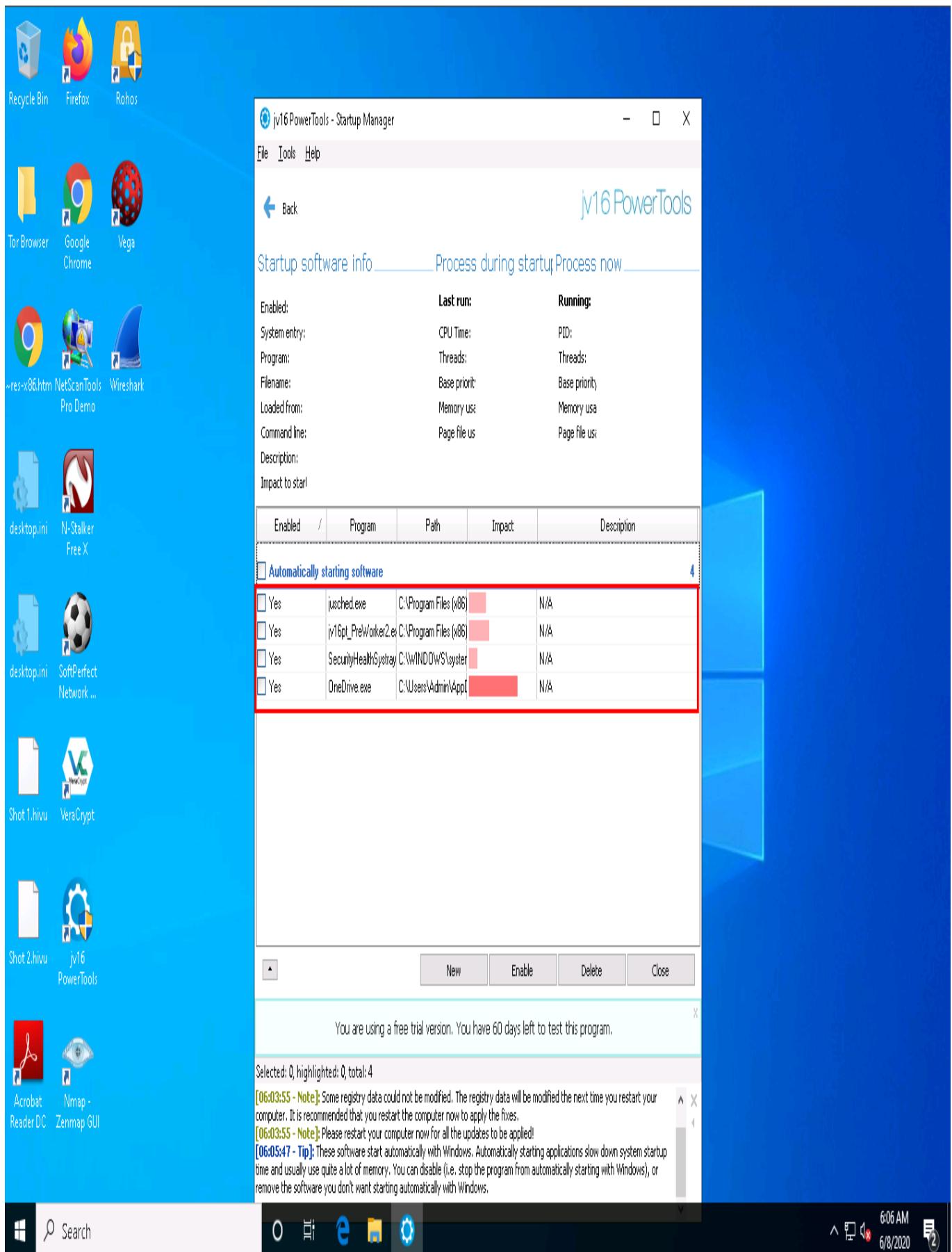


48. This deletes all unwanted or harmful registries, logs, temporary files, and other identified files, ensuring the safety of your computer.
49. If a **jv16 Power Tools** pop-up appears, asking you to restart the computer, click **No**.
50. If a **Clean and Fix My Computer** dialogue-box appears, close it.

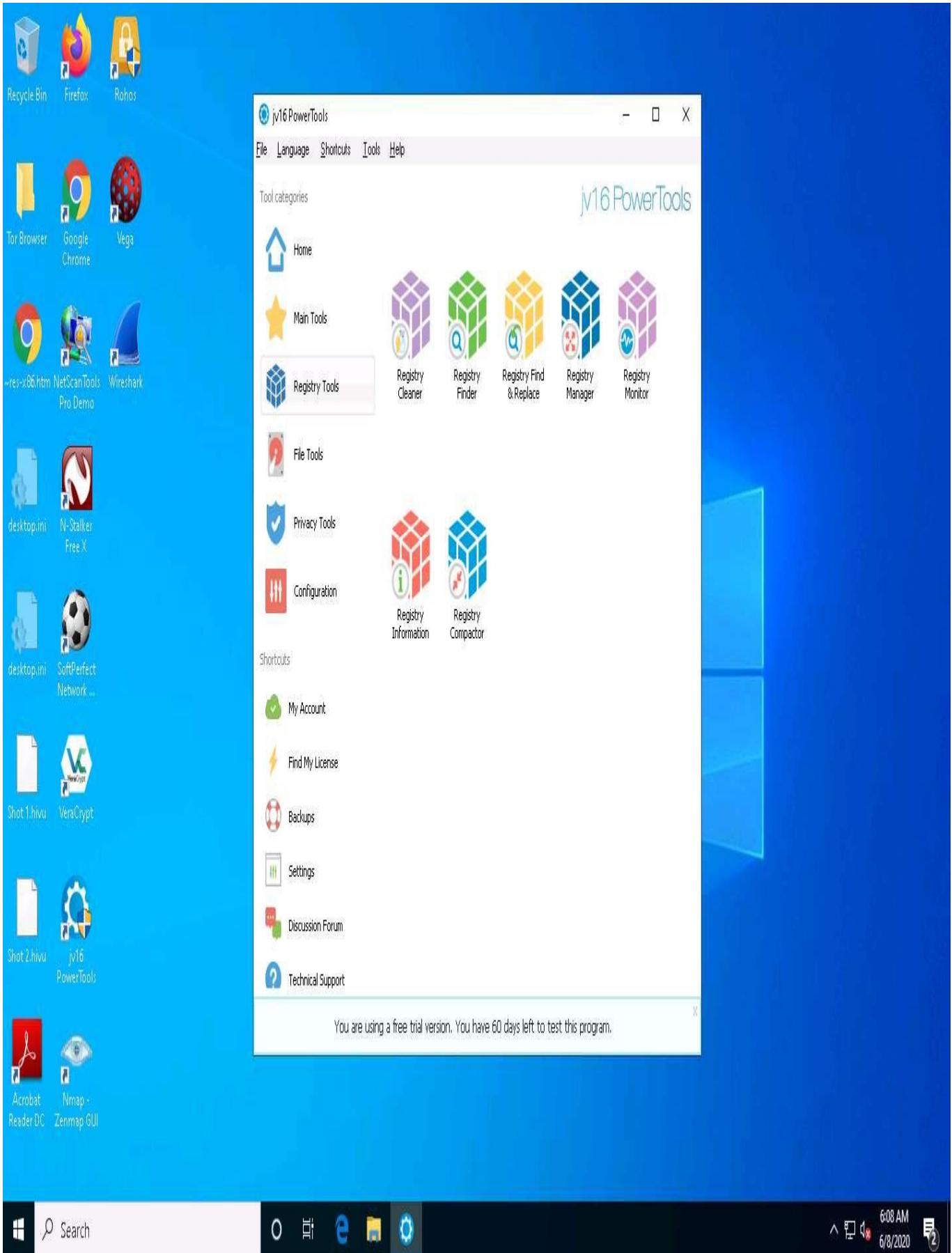
51. jv16 PowerTools redirects you to the **Main Tools** section; click **Control which programs start automatically**.



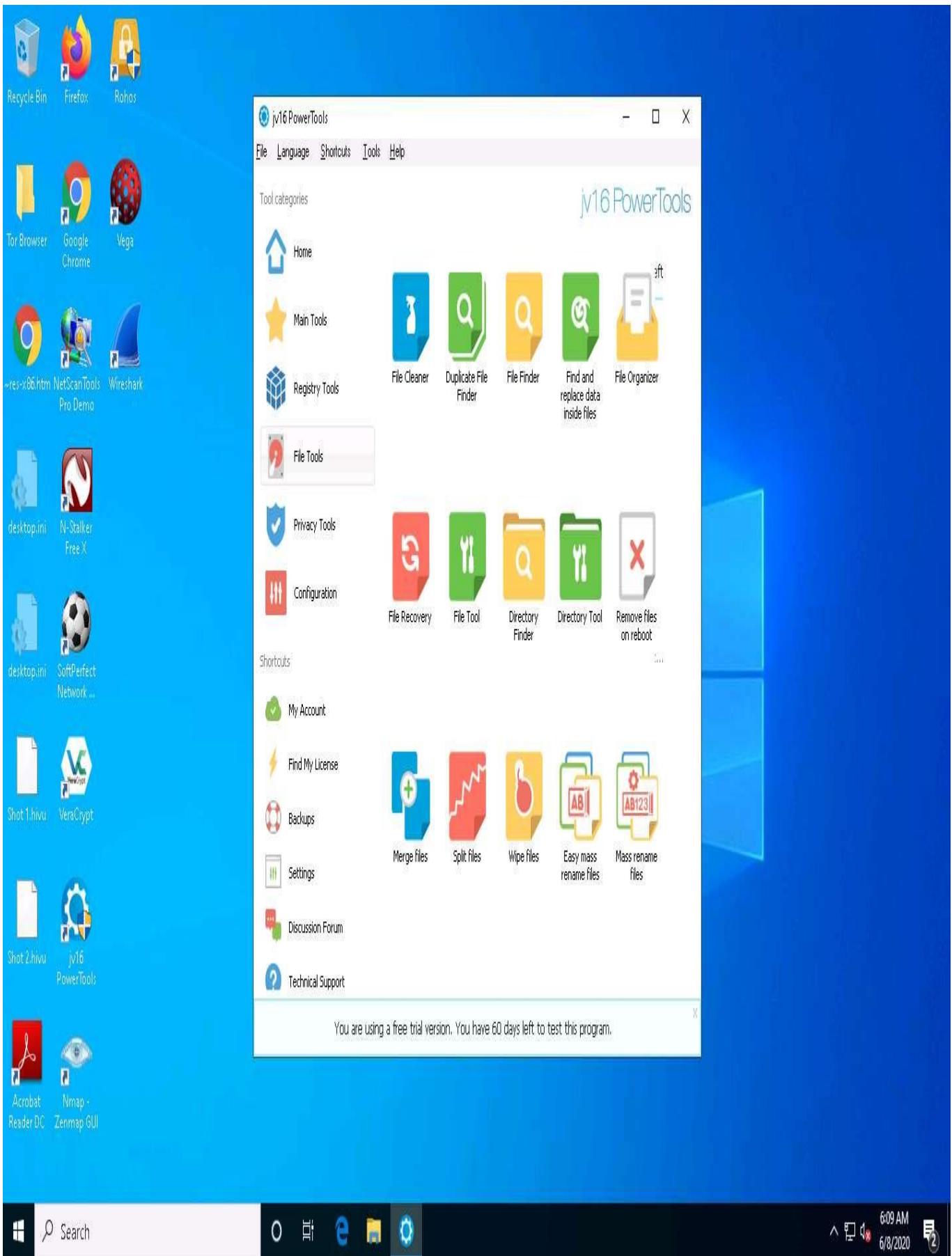
52. Select the software of your choice in the **Startup Manager** and assign the appropriate action for the software you check.



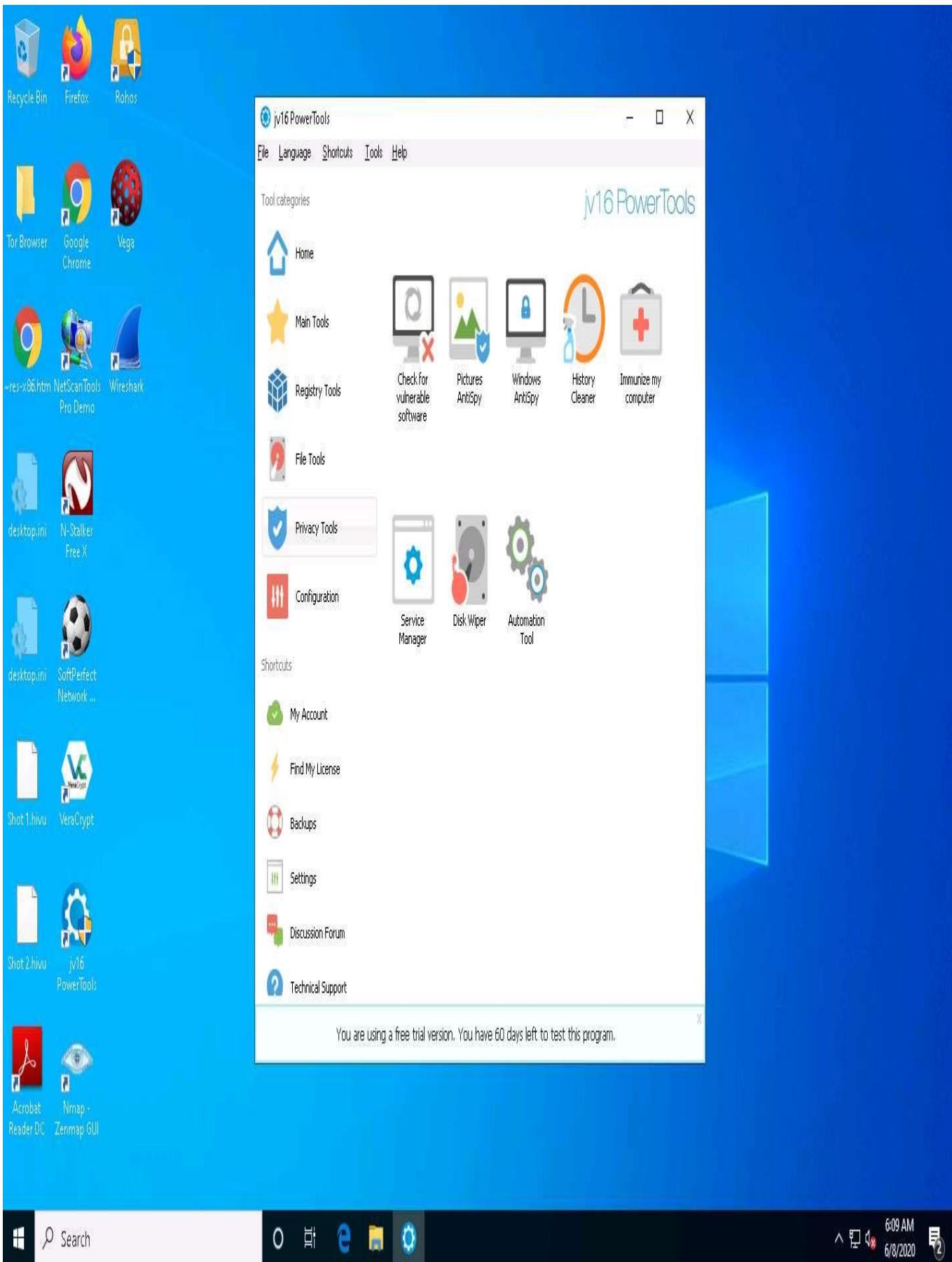
53. Thus, you could find any Trojans or malicious files running at system startup and choose the appropriate actions against them. Click **Close** in the **Startup Manager** wizard, which will redirect you to the **Main Tools** section of jv16 PowerTools.
54. Select **Registry Tools** to view Registry-related functions.
55. This section helps you to find, manage, monitor, compress, clean, or replace **registry files**.



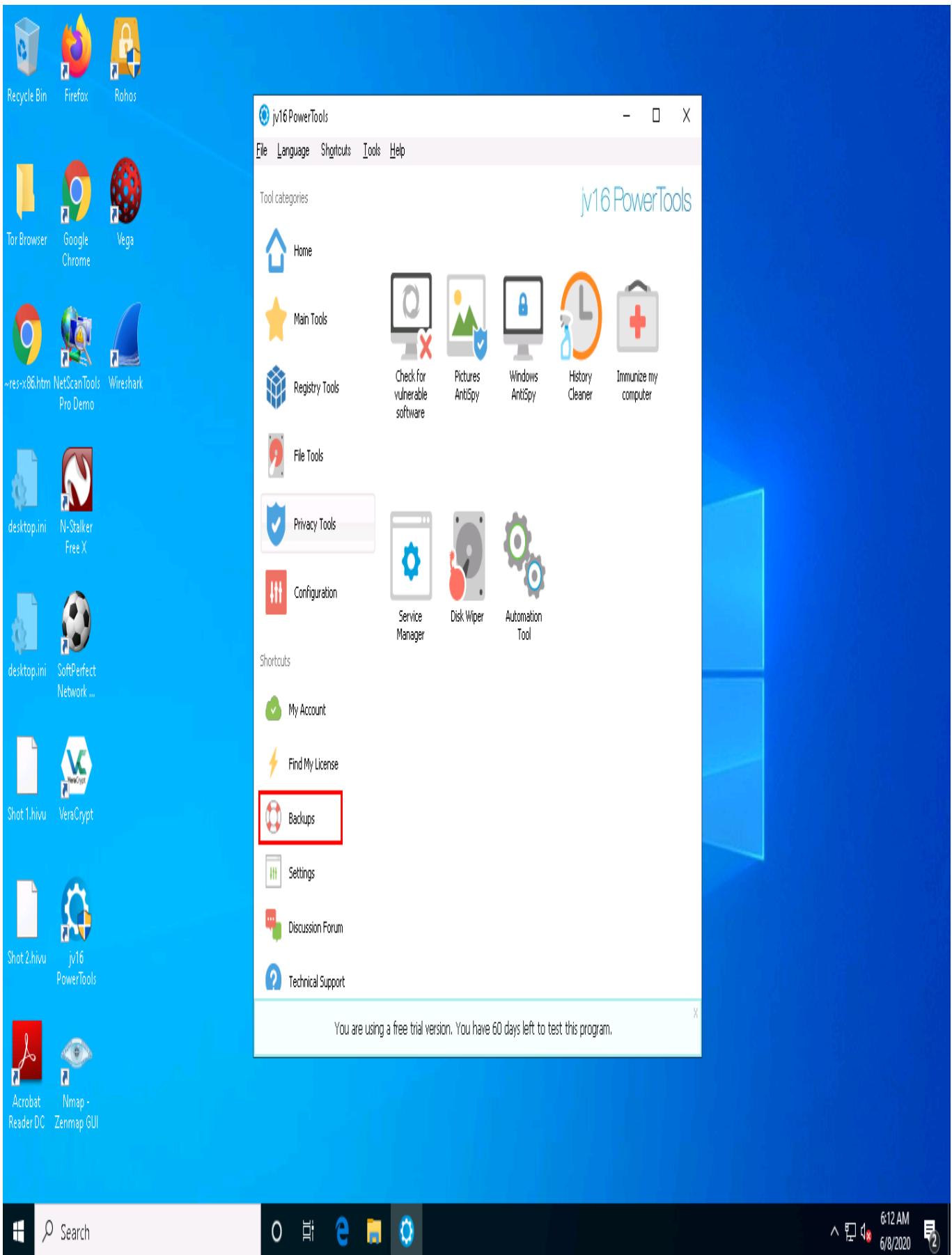
56. Click **File Tools** to view file-related functions.
57. This section helps you to find, recover, clean, organize, or merge files or directories.



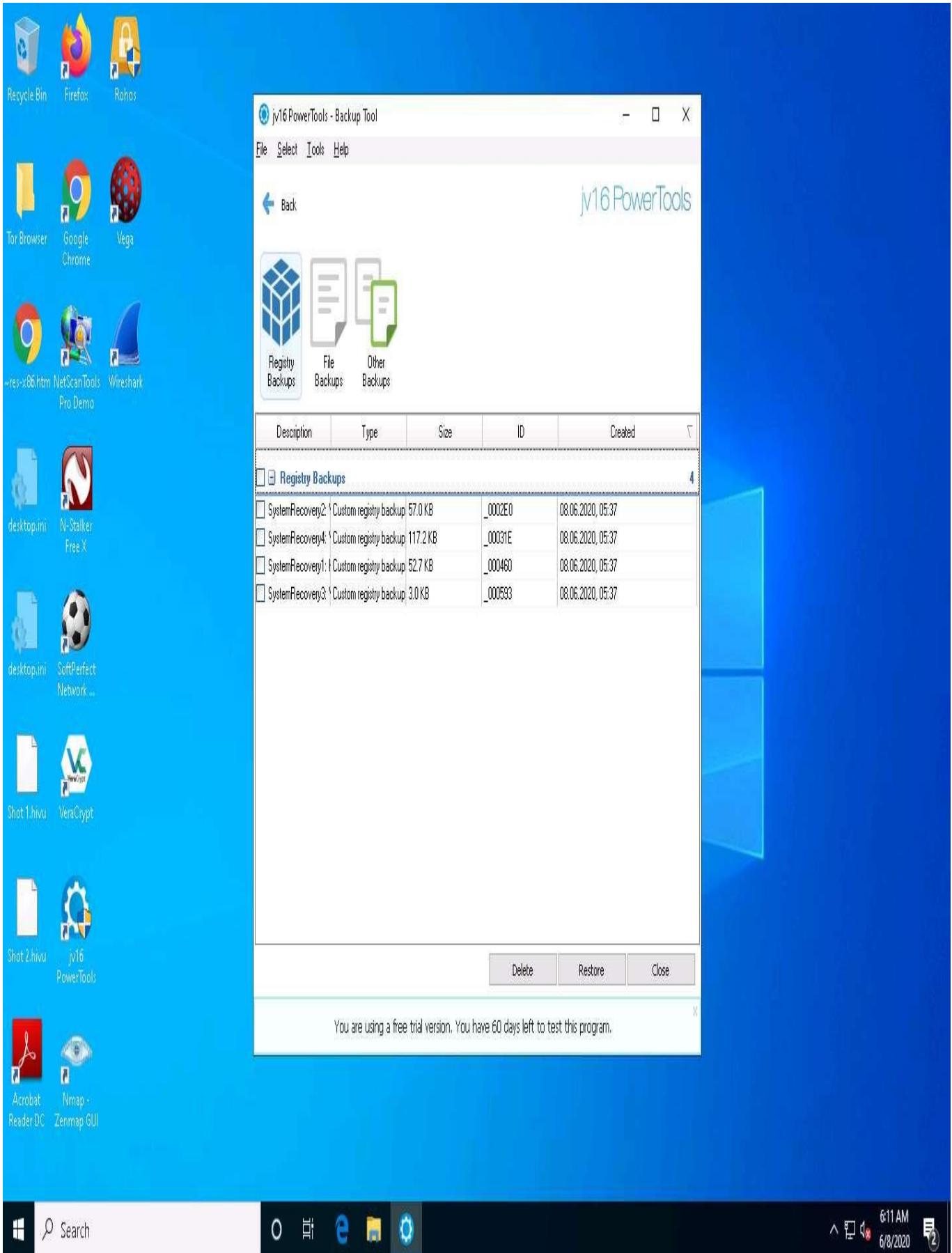
58. Select **Privacy Tools** to view privacy-related functions.
59. This section helps you to check for vulnerable software, spyware, clear your history, and perform other tasks.



60. The **Disk Wiper** option wipes the disk—this is not recommended.
61. Select **Backups** to view the system-related backups.



62. The **Jv16 PowerTools - Backup Tool** window appears, displaying the **registry**, **file**, and **other backups**.



63. You can choose whether to delete or restore backups in this window.
64. Click **Close** on the **Jv16 PowerTools - Backup Tool** window; this will redirect you to the **Main Tools** section of jv16 PowerTools.

If a restart prompt appears, then restart the machine.

65. Examining the result of the jv16 PowerTools scan reveals unwanted registry entries and other suspicious activities on the machine and allows the user to stop or delete them.
 66. Close the **jv16 PowerTools** main window.
 67. You can also use other registry monitoring tools such as **Reg Organizer** (<https://www.chemtable.com>), **Registry Viewer** (<https://accessdata.com>), **RegScanner** (<https://www.nirsoft.net>), or **Registrar Registry Manager** (<https://www.resplendence.com>) to perform registry monitoring.
-

Task 4: Perform Windows Services Monitoring using Windows Service Manager (SrvMan)

Attackers design malware and other malicious code in such a way that they install and run on a computer device in the form of a service. As most services run in the background to support processes and applications, malicious services are invisible, even when they are performing harmful activities on the system, and can even function without intervention or input. Malware spawns Windows services that allow attackers to control the victim machine and pass malicious instructions remotely. Malware may also employ rootkit techniques to manipulate the following registry keys to hide their processes and services.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services These malicious services run as the SYSTEM account or another privileged account, which provides more access compared to regular user accounts, making them more dangerous than common malware and executable code. Attackers also try to conceal their actions by naming the malicious services with the names similar to genuine Windows services to avoid detection.

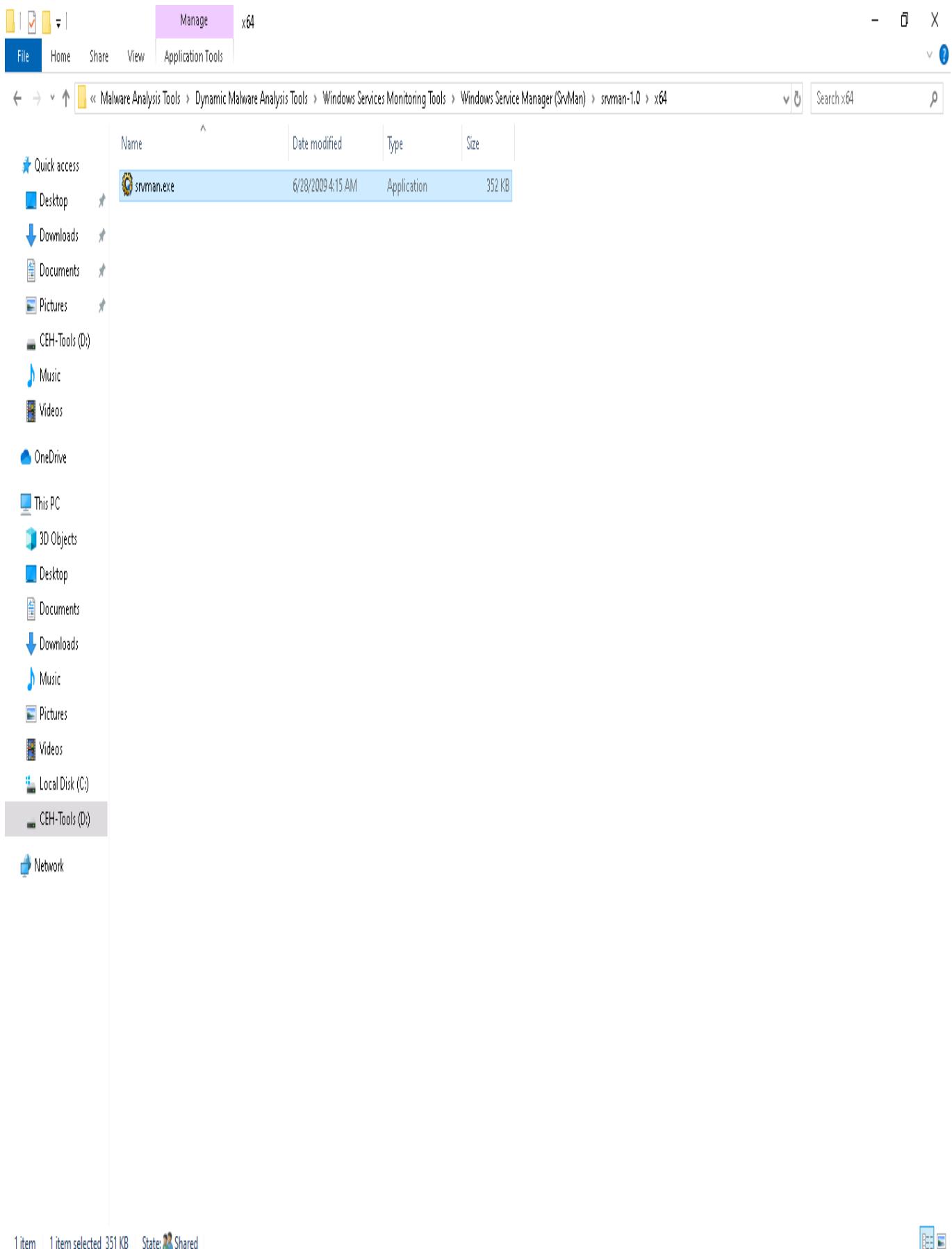
You can trace malicious services initiated by the suspect file during dynamic analysis by using Windows service monitoring tools such as Windows Service Manager (SrvMan), which can detect changes in services and scan for suspicious Windows services.

SrvMan has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window automatically closes).

Here, we will use the SrvMan tool to check for suspicious windows services.

1. On the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\srvman-1.0\x64** and double-click **srvman.exe**.

You can choose any of the executable files for the Windows Service Manager according to your computer and OS design.



2. If a **User Account Control** window appears, click **Yes**.
3. The **Service Manager** main window appears, listing all services available or running on the machine, as shown in the screenshot.

Service Manager

- X

File View Service Help

Internal name	State	Type	Display name	Start type	Executable
1394ohci	stopped	driver	1394 OHCI Compliant Host Controller	manual	\SystemRoot\System32\drivers\1394ohci.sys
3ware	stopped	driver	3ware	manual	\SystemRoot\System32\drivers\3ware.sys
AarSvc_8...	stopped	unknown	Agent Activation Runtime_83253	manual	C:\WINDOWS\system32\svchost.exe -k Aar...
ACPI	running	driver	Microsoft ACPI Driver	boot	\SystemRoot\System32\drivers\ACPI.sys
AcpiDev	stopped	driver	ACPI Devices driver	manual	\SystemRoot\System32\drivers\AcpiDev.sys
acpixe	running	driver	Microsoft ACPIEx Driver	boot	\SystemRoot\System32\Drivers\acpixe.sys
acpipagr	stopped	driver	ACPI Processor Aggregator Driver	manual	\SystemRoot\System32\drivers\acpipagr.sys
AcpiPmI	stopped	driver	ACPI Power Meter Driver	manual	\SystemRoot\System32\drivers\acippmi.sys
Acpitime	stopped	driver	ACPI Wake Alarm Driver	manual	\SystemRoot\System32\drivers\acpitime.sys
Acx01000	stopped	driver	Acx01000	manual	system32\drivers\Acx01000.sys
AdobeAR...	running	win32	Adobe Acrobat Update Service	auto	'C:\Program Files (x86)\Common Files\Adobe...
ADP80XX	stopped	driver	ADP80XX	manual	\SystemRoot\System32\drivers\ADP80XX.SYS
AFD	running	driver	Ancillary Function Driver for Winsock	system	\SystemRoot\system32\drivers\afd.sys
afunix	running	driver	afunix	system	\SystemRoot\system32\drivers\afunix.sys
ahcache	running	driver	Application Compatibility Cache	system	system32\DRIVERS\ahcache.sys
AllJoyn Router	stopped	shared	AllJoyn Router Service	manual	C:\WINDOWS\system32\svchost.exe -k Loc...
ALG	stopped	win32	Application Layer Gateway Service	manual	C:\WINDOWS\System32\alg.exe
amdgpio2	stopped	driver	AMD GPIO Client Driver	manual	\SystemRoot\System32\drivers\amdgpio2.sys
amdi2c	stopped	driver	AMD I2C Controller Service	manual	\SystemRoot\System32\drivers\amdi2c.sys
AmdK8	stopped	driver	AMD K8 Processor Driver	manual	\SystemRoot\System32\drivers\amdk8.sys
AmdPPM	stopped	driver	AMD Processor Driver	manual	\SystemRoot\System32\drivers\amdpmm.sys
amdsata	stopped	driver	amdsata	manual	\SystemRoot\System32\drivers\amdsata.sys
amdsbs	stopped	driver	amdsbs	manual	\SystemRoot\System32\drivers\amdsbs.sys
amdiata	stopped	driver	amdiata	manual	\SystemRoot\System32\drivers\amdiata.sys
AppHostS...	running	unknown	Application Host Helper Service	auto	C:\WINDOWS\system32\svchost.exe -k app...
ApplID	stopped	driver	ApplID Driver	manual	system32\drivers\applid.sys
ApplDSvc	stopped	shared	Application Identity	manual	C:\WINDOWS\system32\svchost.exe -k Loc...
Appinfo	running	unknown	Application Information	manual	C:\WINDOWS\system32\svchost.exe -k nets...
applocker	stopped	driver	Smartlocker Filter Driver	manual	system32\drivers\applockerfltr.sys
AppMgmt	stopped	shared	Application Management	manual	C:\WINDOWS\System32\svchost.exe -k nets...
AppReadi...	stopped	shared	App Readiness	manual	C:\WINDOWS\System32\svchost.exe -k App...
AppVClient	stopped	win32	Microsoft AppV Client	disabled	C:\WINDOWS\System32\AppClient.exe
AppvStm	stopped	FS driver	AppvStm	manual	\SystemRoot\System32\drivers\AppvStm.sys
AppvVmgr	stopped	FS driver	AppvVmgr	manual	\SystemRoot\System32\drivers\AppvVmgr.sys
AppvVs	stopped	FS driver	AppvVs	manual	\SystemRoot\System32\drivers\AppvVs.sys
AppxSvc	running	unknown	AppX Deployment Service (AppXVC)	manual	C:\WINDOWS\system32\svchost.exe -k woa...
arcas	stopped	driver	Adaptec SAS/SATA-II RAID Storage Port...	manual	\SystemRoot\System32\drivers\arcas.sys
Assigned...	stopped	shared	AssignedAccessManager Service	manual	C:\WINDOWS\system32\svchost.exe -k Assi...
AsyncMac	stopped	driver	RAS Asynchronous Media Driver	manual	\SystemRoot\System32\drivers\asyncmac.sys
atapi	running	driver	IDE Channel	boot	\SystemRoot\System32\drivers\atapi.sys
AudioEnd...	running	unknown	Windows Audio Endpoint Builder	auto	C:\WINDOWS\System32\svchost.exe -k Loc...
Audiosrv	running	win32	Windows Audio	auto	C:\WINDOWS\System32\svchost.exe -k Loc...

Properties...

Start service

Restart service

Add service

Delete service

Exit



Search



8:19 AM
6/8/2020

- The Service Manager shows the **Internal name**, **State**, **Type**, **Display name**, **Start type**, and **Executable** data of the services.
- Here, you can choose any unwanted service that is running on your computer, and **Stop** or **Delete** that service by choosing the appropriate action.

6. You can view the properties of the selected service by clicking on **Properties**.
7. To Start a stopped service, click the **Start service** button. To stop a running service, click **Stop service**.
8. To restart any running service, click the **Restart service** button.
9. To add a new service to your machine, click the **Add service** button.
10. To delete any running or stopped service, click the **Delete service** button.

Service Manager

File View Service Help

Internal name	State	Type	Display name	Start type	Executable
1394ohci	stopped	driver	1394 OHCI Compliant Host Controller	manual	\SystemRoot\System32\drivers\1394ohci.sys
3ware	stopped	driver	3ware	manual	\SystemRoot\System32\drivers\3ware.sys
AarSvc_8...	stopped	unknown	Agent Activation Runtime_83253	manual	C:\WINDOWS\system32\svchost.exe -k Aar...
ACPI	running	driver	Microsoft ACPI Driver	boot	\SystemRoot\System32\drivers\ACPI.sys
AcpiDev	stopped	driver	ACPI Devices driver	manual	\SystemRoot\System32\drivers\AcpiDev.sys
acpiex	running	driver	Microsoft ACPIEx Driver	boot	\SystemRoot\System32\Drivers\acpiex.sys
acpipagr	stopped	driver	ACPI Processor Aggregator Driver	manual	\SystemRoot\System32\drivers\acpipagr.sys
AcpiPmI	stopped	driver	ACPI Power Meter Driver	manual	\SystemRoot\System32\drivers\acippmi.sys
acpitime	stopped	driver	ACPI Wake Alarm Driver	manual	\SystemRoot\System32\drivers\acpitime.sys
Acx01000	stopped	driver	Acx01000	manual	system32\drivers\Acx01000.sys
AdobeARe...	running	win32	Adobe Acrobat Update Service	auto	"C:\Program Files (x86)\Common Files\Adobe...
ADP80XX	stopped	driver	ADP80XX	manual	\SystemRoot\System32\drivers\ADP80XX.SYS
AFD	running	driver	Ancillary Function Driver for Winsock	system	\SystemRoot\system32\drivers\afd.sys
afunix	running	driver	afunix	system	\SystemRoot\system32\drivers\afunix.sys
ahcache	running	driver	Application Compatibility Cache	system	system32\DRIVERS\ahcache.sys
AllJoyn Router	stopped	shared	AllJoyn Router Service	manual	C:\WINDOWS\system32\svchost.exe -k Loc...
ALG	stopped	win32	Application Layer Gateway Service	manual	C:\WINDOWS\System32\alg.exe
amdgpio2	stopped	driver	AMD GPIO Client Driver	manual	\SystemRoot\System32\drivers\amdgpio2.sys
amdi2c	stopped	driver	AMD I2C Controller Service	manual	\SystemRoot\System32\drivers\amdi2c.sys
AmdK8	stopped	driver	AMD K8 Processor Driver	manual	\SystemRoot\System32\drivers\amdk8.sys
AmdFPM	stopped	driver	AMD Processor Driver	manual	\SystemRoot\System32\drivers\amdpmp.sys
amdsata	stopped	driver	amdsata	manual	\SystemRoot\System32\drivers\amdsata.sys
amdsbs	stopped	driver	amdsbs	manual	\SystemRoot\System32\drivers\amdsbs.sys
amdkata	stopped	driver	amdkata	manual	\SystemRoot\System32\drivers\amdkata.sys
AppHost\$...	running	unknown	Application Host Helper Service	auto	C:\WINDOWS\system32\svchost.exe -k app...
AppID	stopped	driver	AppID Driver	manual	system32\drivers\appid.sys
ApplDSvc	stopped	shared	Application Identity	manual	C:\WINDOWS\system32\svchost.exe -k Loc...
AppInfo	running	unknown	Application Information	manual	C:\WINDOWS\system32\svchost.exe -k nets...
applocker...	stopped	driver	Smartlocker Filter Driver	manual	system32\drivers\applockerfltr.sys
AppMgmt	stopped	shared	Application Management	manual	C:\WINDOWS\system32\svchost.exe -k nets...
AppReadi...	stopped	shared	App Readiness	manual	C:\WINDOWS\system32\svchost.exe -k App...
AppVClient	stopped	win32	Microsoft AppV Client	disabled	C:\WINDOWS\system32\appv\Client.exe
AppvStrm	stopped	FS driver	AppvStrm	manual	\SystemRoot\System32\drivers\appvstrm.sys
AppvVemgr	stopped	FS driver	AppvVemgr	manual	\SystemRoot\System32\drivers\appvvemgr.sys
AppvVfs	stopped	FS driver	AppvVfs	manual	\SystemRoot\System32\drivers\appvvfs.sys
AppXSvc	stopped	unknown	AppX Deployment Service (AppXVC)	manual	C:\WINDOWS\system32\svchost.exe -k wsa...
arcas	stopped	driver	Adaptec SAS/SATA-II RAID Storport...	manual	\SystemRoot\System32\drivers\arcas.sys
Assigned...	stopped	shared	AssignedAccessManager Service	manual	C:\WINDOWS\system32\svchost.exe -k Assi...
AsyncMac	stopped	driver	RAS Asynchronous Media Driver	manual	\SystemRoot\System32\drivers\asyncmac.sys
atapi	running	driver	IDE Channel	boot	\SystemRoot\System32\drivers\atapi.sys
AudioEnd...	running	unknown	Windows Audio Endpoint Builder	auto	C:\WINDOWS\system32\svchost.exe -k Loc...
Audiosrv	running	win32	Windows Audio	auto	C:\WINDOWS\System32\svchost.exe -k Loc...

Properties... Stop service

Add service Delete service Restart service

Exit

Search

8:22 AM 6/8/2020

11. Thus, you can monitor the unwanted services running on the machine using the Windows Service Manager.
12. Close the **Service Manager** window.

13. You can also use other Windows service monitoring tools such as **Advanced Windows Service Manager** (<https://securityxploded.com>), **Process Hacker** (<https://processhacker.sourceforge.io>), **Netwrix Service Monitor** (<https://www.netwrix.com>), or **AnVir Task Manager** (<https://www.anvir.com>) to perform Windows services monitoring.
-

Task 5: Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol

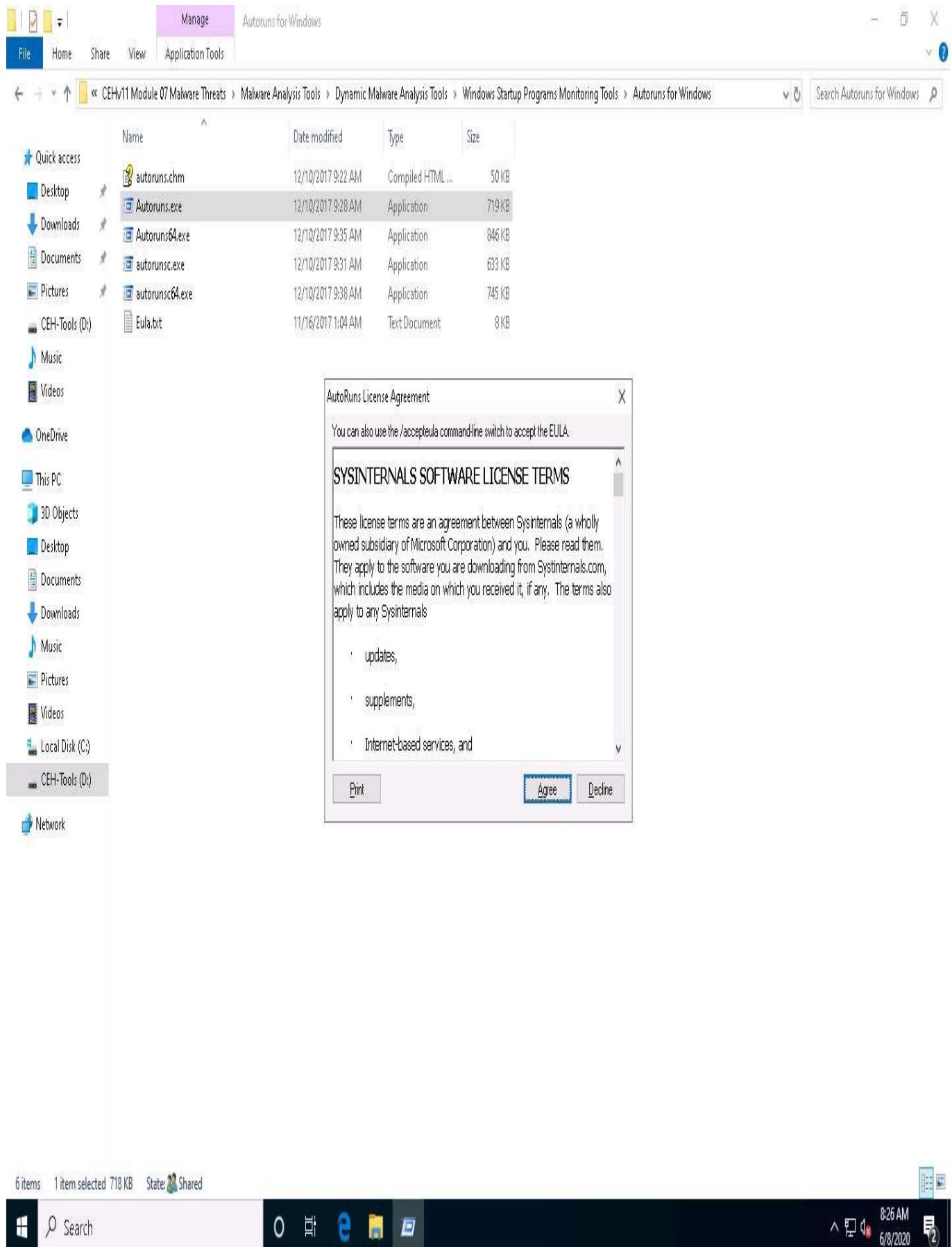
Startup programs are applications or processes that start when your system boots up. Attackers make many malicious programs such as Trojans and worms in such a way that they are executed during startup, and the user is unaware of the malicious program running in the background.

An ethical hacker or penetration tester must identify the applications or processes that start when a system boots up and remove any unwanted or malicious programs that can breach privacy or affect a system's health. Therefore, scanning for suspicious startup programs manually or using startup program monitoring tools like Autoruns for Windows and WinPatrol is essential for detecting malware.

Autoruns for Windows This utility can auto-start the location of any startup monitor, display which programs are configured to run during system bootup or login, and show the entries in the order Windows processes them. As soon as this program is included in the startup folder, Run, RunOnce, and other Registry keys, users can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services. Autoruns' Hide Signed Microsoft Entries option helps the user zoom in on third-party auto-starting images that add to the users' system, and it has support for looking at the auto-starting images configured for other accounts configured on the system.

WinPatrol WinPatrol provides the user with 14 different tabs to help in monitoring the system and its files. This security utility gives the user a chance to look for programs that are running in the background of a system so that the user can take a closer look and control the execution of legitimate and malicious programs.

1. On the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows** and double-click **Autoruns.exe**.
2. The **AutoRuns License Agreement** window appears; click **Agree**.



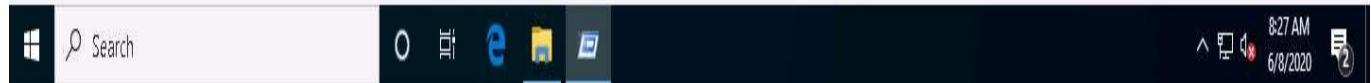
3. The **Autoruns** main window appears. It displays all **processes**, **dll's**, and **services**, as shown in the screenshot.

The application lists displayed under all the tabs may vary in your lab environment.

Autorun - Sysinternals: www.sysinternals.com					
File Entry Options Help					
Print Monitors		LSA Providers		Network Providers	
Everything	Logon	Explorer	Internet Explorer	Scheduled Tasks	Services
Drivers	Codecs	Boot Execute	Image Hijacks	Sidebar Gadgets	Office
AppInit	KnownDLLs	Winlogon	Winsock Providers		
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				4/14/2020 3:52 AM	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	12/28/1914 2:19 AM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				6/8/2020 6:16 AM	
<input checked="" type="checkbox"/> jv16 PT (System Sta...)			c:\program files (x86)\jv16 power...	5/18/2018 3:57 AM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				6/8/2020 5:37 AM	
<input checked="" type="checkbox"/> SunJavaUpdateSch... Java Update Scheduler	Oracle Corporation		c:\program files (x86)\common fil...	12/11/2019 7:56 AM	
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				4/14/2020 4:47 AM	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\admin\appdata\local\m...	3/2/1912 12:36 AM	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				4/14/2020 9:29 AM	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	Google LLC	c:\program files (x86)\google\chr...	5/15/2020 8:06 PM	
<input checked="" type="checkbox"/> n/a	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	10/26/1908 7:35 AM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				4/14/2020 9:29 AM	
<input checked="" type="checkbox"/> n/a	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\syswow64\rundll32...	10/20/1921 4:00 PM	
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				4/14/2020 6:29 AM	
<input checked="" type="checkbox"/> Java(TM) Plug-In 2 S... Java(TM) Platform SE binary	Oracle Corporation		c:\program files (x86)\java\jre1.8...	12/11/2019 6:43 AM	
<input checked="" type="checkbox"/> Java(TM) Plug-In SG... Java(TM) Platform SE binary	Oracle Corporation		c:\program files (x86)\java\jre1.8...	12/11/2019 6:46 AM	
Task Scheduler					
<input checked="" type="checkbox"/> Adobe Acrobat Up... Adobe Reader and Acrobat Man...	Adobe Systems		c:\program files (x86)\common fil...	2/25/2020 5:41 PM	
<input checked="" type="checkbox"/> Microsoft\Windows... Windows host process (Rundll32)	Microsoft Corporation		c:\windows\system32\rundll32.exe	10/26/1908 7:35 AM	
<input checked="" type="checkbox"/> Microsoft\Windows... Windows host process (Rundll32)	Microsoft Corporation		c:\windows\system32\rundll32.exe	10/26/1908 7:35 AM	
<input type="checkbox"/> Microsoft\Windows... Windows host process (Rundll32)	Microsoft Corporation		c:\windows\system32\rundll32.exe	10/26/1908 7:35 AM	
<input checked="" type="checkbox"/> Microsoft\Windows... Windows host process (Rundll32)	Microsoft Corporation		c:\windows\system32\rundll32.exe	10/26/1908 7:35 AM	
<input checked="" type="checkbox"/> OneDrive Standalone Updater	Microsoft Corporation		c:\users\admin\appdata\local\m...	10/18/2002 1:59 PM	
HKLM\System\CurrentControlSet\Services				6/8/2020 7:44 AM	
<input type="checkbox"/> AdobeARMservice	Adobe Acrobat Update Service: ...	Adobe Systems	c:\program files (x86)\common fil...	2/25/2020 5:40 PM	
HKLM\System\CurrentControlSet\Services				6/8/2020 7:44 AM	
<input checked="" type="checkbox"/> 3ware	3ware: LSI 3ware SCSI Storport ...	LSI	c:\windows\system32\drivers\3...	5/18/2015 6:28 PM	
<input checked="" type="checkbox"/> ADP80XX	ADP80XX: PMC-Sierra Storport ...	PMC-Sierra	c:\windows\system32\drivers\ad...	4/9/2015 4:49 PM	
<input checked="" type="checkbox"/> amdgpio2	AMD GPIO Client Driver: AMD G...	Advanced Micro Devices, Inc	c:\windows\system32\drivers\am...	2/7/2019 5:32 AM	
<input checked="" type="checkbox"/> amdi2c	AMD I2C Controller Service: AM...	Advanced Micro Devices, Inc	c:\windows\system32\drivers\am...	6/13/2018 1:25 AM	
<input checked="" type="checkbox"/> amdsata	amdsata: AHCI 1.3 Device Driver	Advanced Micro Devices	c:\windows\system32\drivers\am...	5/14/2015 8:14 AM	
<input checked="" type="checkbox"/> amdsbs	amdsbs: AMD Technology AHCI ...	AMD Technologies Inc.	c:\windows\system32\drivers\am...	12/11/2012 5:21 PM	
<input checked="" type="checkbox"/> amdkata	amdkata: Storage Filter Driver	Advanced Micro Devices	c:\windows\system32\drivers\am...	4/30/2015 8:55 PM	
<input checked="" type="checkbox"/> arcas	Adaptec SAS/SATA-II RAID Stor...	PMC-Sierra, Inc.	c:\windows\system32\drivers\ar...	4/9/2015 3:12 PM	
<input checked="" type="checkbox"/> b06bdrv	QLogic Network Adapter VBD: Q...	QLogic Corporation	c:\windows\system32\drivers\bx...	5/25/2016 3:03 AM	
<input checked="" type="checkbox"/> bcmfr2	bcmfr2 Service: BCM Function 2...	Windows (R) Win 7 DDK provider	c:\windows\system32\drivers\bc...	10/31/2016 10:09 PM	

(Escape to cancel) Scanning..

Windows Entries Hidden.



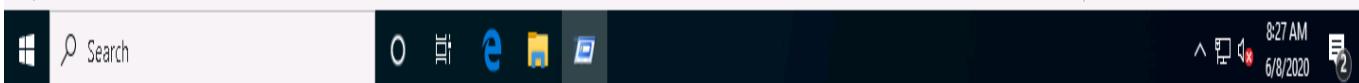
4. Click the **Logon** tab to view the applications that run automatically during login.

File Entry Options Help

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	KnownDLLs	Winlogon	Winsock Providers
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal								
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				4/14/2020 3:52 AM									
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	12/28/1914 2:19 AM									
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				6/8/2020 6:16 AM									
<input checked="" type="checkbox"/> jv16 PT (System Sta...			c:\program files (x86)\jv16 power...	5/18/2018 3:57 AM									
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				6/8/2020 5:37 AM									
<input checked="" type="checkbox"/> SunJavaUpdateScheduler	Java Update Scheduler	Oracle Corporation	c:\program files (x86)\common fil...	12/11/2019 7:56 AM									
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				4/14/2020 4:47 AM									
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\admin\appdata\local\m...	3/2/1912 12:36 AM									
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				4/14/2020 9:29 AM									
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	Google LLC	c:\program files (x86)\google\chr...	5/15/2020 8:06 PM									
<input checked="" type="checkbox"/> n/a	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	10/26/1908 7:35 AM									
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				4/14/2020 9:29 AM									
<input checked="" type="checkbox"/> n/a	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\syswow64\rundll32....	10/20/1921 4:00 PM									

Ready.

Windows Entries Hidden.



5. Click the **Explorer** tab to view the explorer applications that run automatically at system startup.

Autoruns - Sysinternals: www.sysinternals.com						-	X								
File	Entry	Options	Help												
		Filter: []													
		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	KnownDLLs	Winlogon	Winsock Providers
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal										
HKLM\Software\Classes\ShellEx\ContextMenuHandlers				4/14/2020 5:46 AM											
<input checked="" type="checkbox"/> ANotepad++64	ShellHandler for Notepad++ (64 bit)	c:\program files (x86)\notepad++\	5/12/2014 5:49 AM												
<input checked="" type="checkbox"/> EPP	Microsoft Security Client Shell Ext... Microsoft Corporation	c:\program files\windows defend...	2/15/2029 1:37 PM												
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension	Alexander Roshal	c:\program files\winrar\varext.dll	3/26/2020 6:02 AM											
HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				4/14/2020 3:52 AM											
<input checked="" type="checkbox"/> EPP	Microsoft Security Client Shell Ext... Microsoft Corporation	c:\program files\windows defend...	2/15/2029 1:37 PM												
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers				4/14/2020 3:52 AM											
<input checked="" type="checkbox"/> EPP	Microsoft Security Client Shell Ext... Microsoft Corporation	c:\program files\windows defend...	2/15/2029 1:37 PM												
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers				4/14/2020 5:38 AM											
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension	Alexander Roshal	c:\program files\winrar\varext.dll	3/26/2020 6:02 AM											
HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers				4/14/2020 5:38 AM											
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension	Alexander Roshal	c:\program files\winrar\varext.dll	3/26/2020 6:02 AM											

6. Clicking the **Services** tab displays all services that run automatically at system startup.

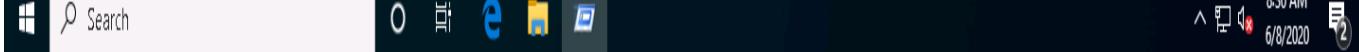
File Entry Options Help

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\System\CurrentControlSet\Services				6/8/2020 7:44 AM	
AdobeARMservice	Adobe Acrobat Update Service... Adobe Systems	c:\program files (x86)\common fl...	2/25/2020 5:40 PM		
GoogleChromeEleva...	Google Chrome Elevation Servic... Google LLC	c:\program files (x86)\google\chr...	5/15/2020 8:06 PM		
gupdate	Google Update Service (gupdate... Google LLC	c:\program files (x86)\google\up...	3/2/2020 7:22 PM		
gupdateam	Google Update Service (gupdate... Google LLC	c:\program files (x86)\google\up...	3/2/2020 7:22 PM		
MozillaMaintenance	Mozilla Maintenance Service: Th... Mozilla Foundation	c:\program files (x86)\mozilla mai...	4/3/2020 2:52 PM		
rpcapd	Remote Packet Capture Protocol... Riverbed Technology, Inc.	c:\program files (x86)\winpcap\...	2/28/2013 9:28 PM		
Sense	Windows Defender Advanced T... Microsoft Corporation	c:\program files\windows defend...	12/23/1980 6:21 AM		
Tenable Nessus	Tenable Nessus: Tenable Nessu... Tenable, Inc.	c:\program files\tenable\nessus\...	3/10/2020 9:35 AM		
WdNisSvc	Windows Defender Antivirus Net... Microsoft Corporation	c:\programdata\microsoft\windo...	4/8/1936 1:55 PM		
WinDefend	Windows Defender Antivirus Ser... Microsoft Corporation	c:\programdata\microsoft\windo...	10/2/2020 11:00 AM		
WMPNetworkSvc	Windows Media Player Network ... Microsoft Corporation	c:\program files\windows media...	8/27/2031 3:43 PM		

Ready. Windows Entries Hidden.

Ready.

Windows Entries Hidden.



7. Click the **Drivers** tab to view all application drivers that run automatically at system startup.
8. Click any driver to display its size, version, and the time at which it was automatically run at system startup (for the first time).

The list displayed under this tab may vary in your lab environment.

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

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 KnownDLLs Winlogon Winsock Providers

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKEY_LOCAL_MACHINE\CurrentControlSet\Services				6/8/2020 7:44 AM	
<input checked="" type="checkbox"/> 3ware	3ware: LSI 3ware SCSI Stopor... LSI		c:\windows\system32\drivers\3... 5/18/2015 6:28 PM		
<input checked="" type="checkbox"/> ADP80XX	ADP80XX: PMC-Sierra Stopor ... PMC-Sierra		c:\windows\system32\drivers\ad... 4/9/2015 4:49 PM		
<input checked="" type="checkbox"/> andgpiod2	AMD GPIO Client Driver AMD G... Advanced Micro Devices, Inc		c:\windows\system32\drivers\am... 2/7/2013 5:32 AM		
<input checked="" type="checkbox"/> amdI2c	AMD I2C Controller Service AM... Advanced Micro Devices, Inc		c:\windows\system32\drivers\am... 6/13/2018 1:25 AM		
<input checked="" type="checkbox"/> amdsata	amdsata: AHCI 1.3 Device Driver Advanced Micro Devices		c:\windows\system32\drivers\am... 5/14/2015 8:14 AM		
<input checked="" type="checkbox"/> amdsbs	amdsbs: AMD Technology AHCI ... AMD Technologies Inc.		c:\windows\system32\drivers\am... 12/11/2012 5:21 PM		
<input checked="" type="checkbox"/> amdkata	amdkata: Storage Filter Driver Advanced Micro Devices		c:\windows\system32\drivers\am... 4/30/2015 8:55 PM		
<input checked="" type="checkbox"/> arcosas	Adaptec SAS/SATA-II RAID Stor... PMC-Sierra, Inc.		c:\windows\system32\drivers\ar... 4/9/2015 3:12 PM		
<input checked="" type="checkbox"/> b06bdv	QLogic Network Adapter VBD: Q... QLogic Corporation		c:\windows\system32\drivers\bx... 5/25/2016 3:03 AM		
<input checked="" type="checkbox"/> bcmfn2	bcmfn2 Service: BCM Function 2... Windows [R] Win 7 DDK provider		c:\windows\system32\drivers\bc... 10/31/2016 10:09 PM		
<input checked="" type="checkbox"/> cht4iscsi	cht4iscsi: Chelsio iSCSI VMimport... Chelsio Communications		c:\windows\system32\drivers\ch... 5/8/2018 9:27 AM		
<input checked="" type="checkbox"/> cht4vbd	Chelsio Virtual Bus Driver: Virtual ... Chelsio Communications		c:\windows\system32\drivers\ch... 5/8/2018 9:23 AM		
<input checked="" type="checkbox"/> ebdrv	QLogic 10 Gigabit Ethernet Adap... QLogic Corporation		c:\windows\system32\drivers\ev... 5/25/2016 3:01 AM		
<input checked="" type="checkbox"/> HpSAMD	HpSAMD: Smart Array SAS/SAT... Hewlett-Packard Company		c:\windows\system32\drivers\hp... 3/26/2013 5:36 PM		
<input checked="" type="checkbox"/> iaggio	Intel Serial IO GPIO Controller Di... Intel(R) Corporation		c:\windows\system32\drivers\ia... 7/23/2018 5:04 AM		
<input checked="" type="checkbox"/> iai2c	Intel(R) Serial IO I2C Host Control... Intel(R) Corporation		c:\windows\system32\drivers\ia... 7/23/2018 5:04 AM		
<input checked="" type="checkbox"/> ialPSS2_GPIO2	Intel(R) Serial IO GPIO Driver v2... Intel Corporation		c:\windows\system32\drivers\ia... 4/19/2018 3:53 AM		
<input checked="" type="checkbox"/> ialPSS2_GPIO2_B...	Intel(R) Serial IO GPIO Driver v2... Intel Corporation		c:\windows\system32\drivers\ia... 4/17/2018 5:25 AM		
<input checked="" type="checkbox"/> ialPSS2_GPIO2_C...	Intel(R) Serial IO GPIO Driver v2... Intel Corporation		c:\windows\system32\drivers\ia... 4/17/2018 3:07 AM		
<input checked="" type="checkbox"/> ialPSS2_GPIO2_G...	Intel(R) Serial IO GPIO Driver v2... Intel Corporation		c:\windows\system32\drivers\ia... 5/16/2018 1:46 AM		
<input checked="" type="checkbox"/> ialPSS2_I2C	Intel(R) Serial IO I2C Driver v2: In... Intel Corporation		c:\windows\system32\drivers\ia... 4/19/2018 3:52 AM		
<input checked="" type="checkbox"/> ialPSS2_I2C_BKT_P	Intel(R) Serial IO I2C Driver v2: In... Intel Corporation		c:\windows\system32\drivers\ia... 4/17/2018 5:24 AM		
<input checked="" type="checkbox"/> ialPSS2_I2C_CNL	Intel(R) Serial IO I2C Driver v2: In... Intel Corporation		c:\windows\system32\drivers\ia... 4/17/2018 3:06 AM		
<input checked="" type="checkbox"/> ialPSS2_I2C_GLK	Intel(R) Serial IO I2C Driver v2: In... Intel Corporation		c:\windows\system32\drivers\ia... 5/16/2018 1:46 AM		
<input checked="" type="checkbox"/> ialPSS1_GPIO	Intel(R) Serial IO GPIO Controller ... Intel Corporation		c:\windows\system32\drivers\ia... 2/2/2015 5:00 AM		
<input checked="" type="checkbox"/> ialPSS1_I2C	Intel(R) Serial IO I2C Controller Dr... Intel Corporation		c:\windows\system32\drivers\ia... 2/24/2015 11:52 AM		
<input checked="" type="checkbox"/> iaStorAVC	Intel Chipset SATA RAID Controll... Intel Corporation		c:\windows\system32\drivers\ia... 2/7/2018 7:53 AM		
<input checked="" type="checkbox"/> iaStorV	Intel RAID Controller Windows 7... Intel Corporation		c:\windows\system32\drivers\ia... 4/11/2011 2:48 PM		
<input checked="" type="checkbox"/> ibbus	Mellanox InfiniBand Bus/AL/Flite... Mellanox		c:\windows\system32\drivers\ia... 4/25/2018 12:29 PM		
<input checked="" type="checkbox"/> IISas35i	IISas35i: Avago SAS Gen3.5 Dri... Avago Technologies		c:\windows\system32\drivers\ia... 5/3/2018 5:57 AM		
<input checked="" type="checkbox"/> LSI_SAS	LSI_SAS: LSI Fusion-MPT SAS ... LSI Corporation		c:\windows\system32\drivers\ls... 3/25/2015 3:36 PM		
<input checked="" type="checkbox"/> LSI_SAS2i	LSI_SAS2i: LSI SAS Gen2 Driver... LSI Corporation		c:\windows\system32\drivers\ls... 8/2/2017 9:29 AM		
<input checked="" type="checkbox"/> LSI_SAS3i	LSI_SAS3i: Avago SAS Gen3 Dri... Avago Technologies		c:\windows\system32\drivers\ls... 5/2/2018 5:40 AM		
<input checked="" type="checkbox"/> LSI_SSS	LSI_SSS: LSI SSS PCIe/Flash D... LSI Corporation		c:\windows\system32\drivers\ls... 3/15/2013 7:39 PM		
<input checked="" type="checkbox"/> megasas	megasas: MEGASAS RAID Contr... Avago Technologies		c:\windows\system32\drivers\m... 3/4/2015 10:36 PM		

Ready. Windows Entries Hidden.

Search

8:32 AM 6/8/2020

9. Click the **KnownDLLs** tab to view all known DLLs that start automatically at system startup.

File Entry Options Help

Filter:

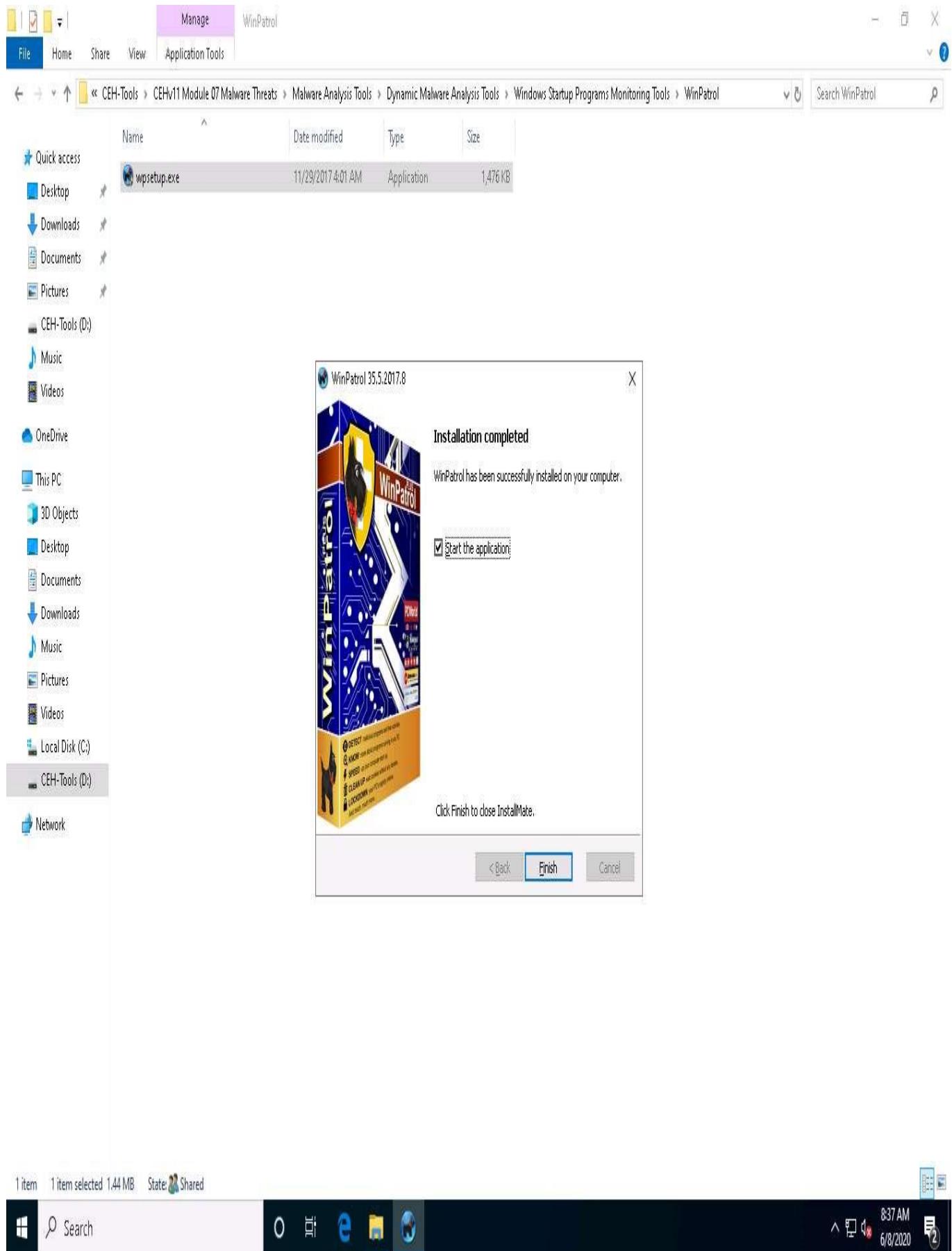
Print Monitors	LSA Providers	Network Providers	WMI	Sidebar Gadgets	Office								
Everything	Logon	Explorer	Internet Explorer	Scheduled Tasks	Services	Drivers	Codecs	Boot Execute	Image Hijacks	AppInit	KnownDLLs	Winlogon	Winsock Providers
Autorun Entry	Description	Publisher	ImagePath	Timestamp	VirusTotal								
HKLM\System\CurrentControlSet\Control\Session Manager\KnownDLLs				4/14/2020 7:48 AM									
<input checked="" type="checkbox"/> _Wow64			File not found: C:\WINDOWS\S...										
<input checked="" type="checkbox"/> _Wow64cpu			File not found: C:\WINDOWS\S...										
<input checked="" type="checkbox"/> _Wow64win			File not found: C:\WINDOWS\S...										
<input checked="" type="checkbox"/> _wowamhw			File not found: C:\WINDOWS\S...										
<input checked="" type="checkbox"/> _wowamhw			File not found: C:\WINDOWS\S...										
<input checked="" type="checkbox"/> _x86it			File not found: C:\WINDOWS\S...										
<input checked="" type="checkbox"/> _x86it			File not found: C:\WINDOWS\S...										
<input checked="" type="checkbox"/> _wow64			File not found: C:\WINDOWS\S...										
<input checked="" type="checkbox"/> _wow64win			File not found: C:\WINDOWS\S...										

Ready. Windows Entries Hidden.

Search 8:33 AM 6/8/2020

10. By examining all these tabs, you can find any unwanted processes or applications running on the machine when the system boots up and stop or delete them manually.
11. Close the **Autoruns** main window.

12. Now, we will find out which applications or processes start when the system boots up using the WinPatrol tool.
13. On the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\WinPatrol**. Double-click **wpsetup.exe** to launch the setup.
14. If a **User Account Control** window appears, click **Yes**.
15. Follow the wizard-driven installation steps to install WinPatrol.
16. In the **Installation completed** wizard, make sure that the **Start the application** options is checked, and then click **Finish**. This will automatically launch the application.



17. The WinPatrol application window appears with the **PLUS** tab open by default. Click the **Startup Programs** tab.
18. Select any program that affects your system bootup (here, **OneDrive**) and click **Disable**, as shown in the screenshot.

The screenshot may differ from the image on the screen in your lab environment

WinPatrol [FREE Edition]

PLUS REQUIRED

Startup Programs Delayed Start IE Helpers Scheduled Tasks 1.0 Services Active Tasks Cookies File Types Hidden Files File Size Monitor Recent PLUS REQUIRED

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.

?

Display

Title	Command	Status	Company	Type	First Detected
SecurityHealth	SecurityHealt...	Micros...	HKLM_RUN	06/08/2020 8:39 AM	
jv16 PT (System Startu...			HKLM_RUN	06/08/2020 8:39 AM	
OneDrive	OneDrive.exe...	Running	Micros...	HKCU_RUN	06/08/2020 8:39 AM
WinPatrol [FREE Edition]	winpatrol.exe	Running	Ruiware	HKCU_RUN	06/08/2020 8:38 AM
SunJavaUpdateSched	jusched.exe	Running	Oracle ...	x64_RUN	06/08/2020 8:38 AM

Info... Add Remove Disable Close

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Search 8:39 AM 6/8/2020

19. A popup appears, as shown in the screenshot. Click **Yes** to proceed.

PLUS REQUIRED

Startup Programs Delayed Start IE Helpers Scheduled Tasks 1.0 Services Active Tasks Cookies File Types Hidden Files File Size Monitor Recent **PLUS REQUIRED**

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	06/08/2020 8:39 AM
jv16 PT (System Startu...				HKLM_RUN	06/08/2020 8:39 AM
OneDrive	OneDrive.ex...	Running	Micros...	HKCU_RUN	06/08/2020 8:39 AM
WinPatrol [FREE Edition]	wingpatrol.exe	Running	Ruiware	HKCU_RUN	06/08/2020 8:38 AM
SunJavaUpdateSched	jusched.exe	Running	Oracle ...	x64_RUN	06/08/2020 8:38 AM

WinPatrol [FREE Edition]

OneDrive 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

HKCU\Software\Microsoft\Windows\CurrentVersion\Run



20. The OneDrive program will be deleted from the Startup Programs list. This is how to manage the Startup Programs for a Windows machine.

21. Now, switch to the **IE Helpers** tab. It shows all toolbars and links loaded by IE or other windows component. Select duplicate or non-required programs (here **Java(tm) Plug-In SSV Helper**), and then click **Remove**.

If a popup appears, as shown in the screenshot. Click **Yes** to proceed.

WinPatrol [FREE Edition]

PLUS REQUIRED

IE Helpers

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	06/08/2020 8:38 AM
Java(tm) Plug-In 2 SSV Helper	jp2ssv.dll	Oracle Corporation	BHO	06/08/2020 8:38 AM

Info... **Remove** **Close**

Java(TM) Platform SE binary

Search

8:41 AM
6/8/2020



22. Switch to the **Services** tab to display the installed services on your system. Select any service and click **Info...**, as shown in the screenshot.

WinPatrol [FREE Edition]

PLUS REQUIRED

Startup Programs Delayed Start IE Helpers Scheduled Tasks 1.0 Services Active Tasks Cookies File Types Hidden Files File Size Monitor Recent PLUS REQUIRED

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.

?

Clock

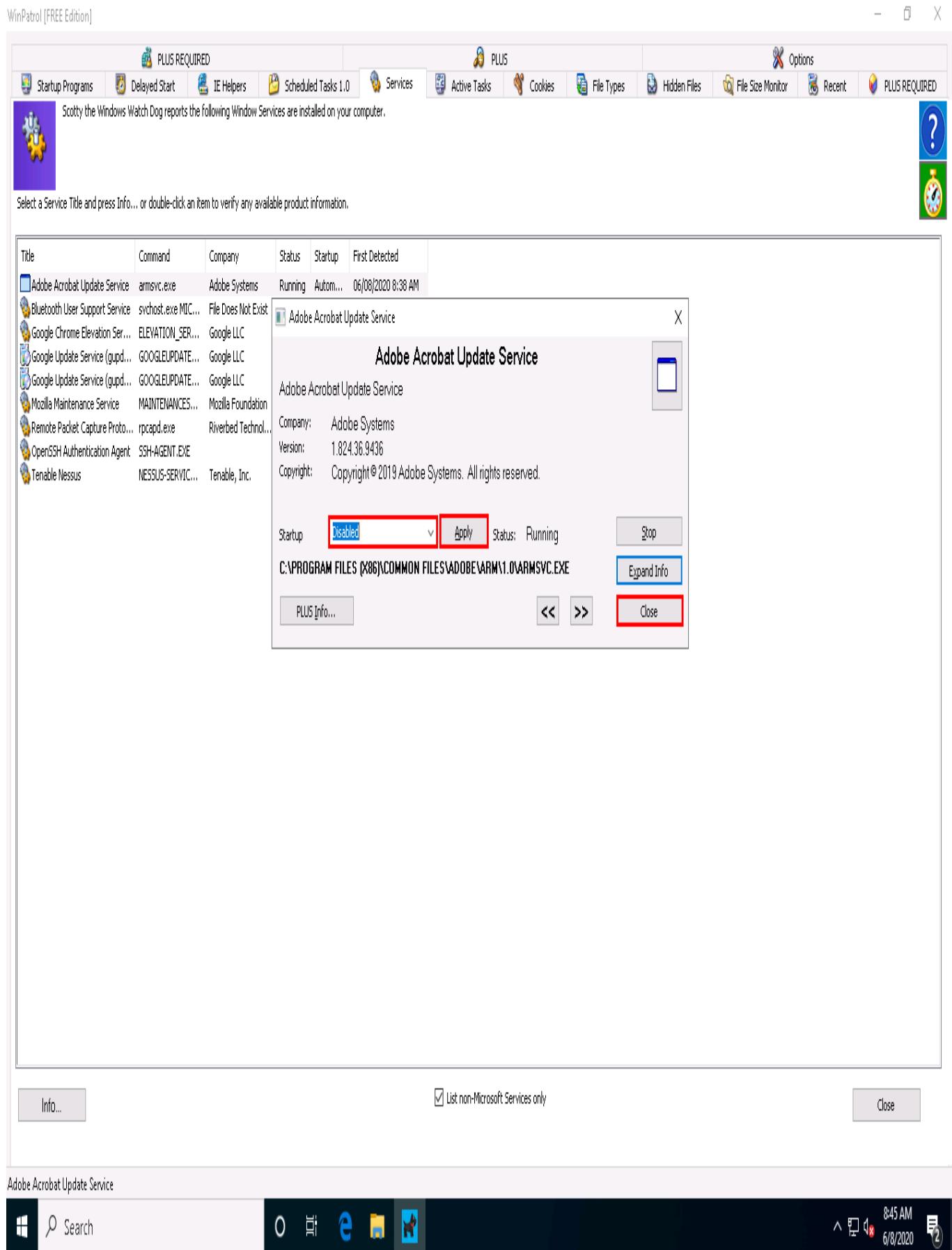
Title	Command	Company	Status	Startup	First Detected
Adobe Acrobat Update Service	armsvc.exe	Adobe Systems	Running	Autom...	06/08/2020 8:38 AM
Bluetooth User Support Service	svchost.exe MIC...	File Does Not Exist	Stopped	Manual	06/08/2020 8:43 AM
Google Chrome Elevation Ser...	ELEVATION_SER...	Google LLC	Stopped	Manual	06/08/2020 8:38 AM
Google Update Service (gupd...	GOOGLEUPDATE...	Google LLC	Stopped	Delaye...	06/08/2020 8:43 AM
Google Update Service (gupd...	GOOGLEUPDATE...	Google LLC	Stopped	Manual	06/08/2020 8:43 AM
Mozilla Maintenance Service	MAINTENANCES...	Mozilla Foundation	Stopped	Manual	06/08/2020 8:38 AM
Remote Packet Capture Proto...	rpcapd.exe	Riverbed Technol...	Stopped	Manual	06/08/2020 8:43 AM
OpenSSH Authentication Agent	SSH-AGENT.EXE		Stopped	Disabled	06/08/2020 8:38 AM
Tenable Nessus	NESSUS-SERVIC...	Tenable, Inc.	Running	Autom...	06/08/2020 8:38 AM

Info... List non-Microsoft Services only Close

Adobe Acrobat Update Service

Search 8:43 AM 6/8/2020

23. A window showing the service information appears. To disable a service, select **Disabled** from the drop-down list and click **Apply**, as shown in the screenshot. Click **Close** to exit the window.



24. Switch to the **File Types** tab to view the programs associated with a file. Select a program and click **Info...** to view the available information.

WinPatrol [FREE Edition]

PLUS REQUIRED

Startup Programs Delayed Start IE Helpers Scheduled Tasks 1.0 Services Active Tasks Cookies File Types Options Hidden Files File Size Monitor Recent PLUS REQUIRED

Scotty the Windows Watch Dog reports that the following programs are associated with particular file types.

Select a Program Title and press Info... or double-click an item to verify any available product information.

Title	Command	Company	Class	Extension	Type
Windows Batch File	Executable		batfile	.BAT	System
Security Catalog	CRYPTTEXT.DLL	Microsoft Corporation	CATFile	.CAT	System
Compiled HTML Help file	HH.EXE	Microsoft Corporation	chmfile	.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	infile	.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	WindowsURL	User D...
WinRAR archive	WINRAR.EXE	Alexander Roshal	WinRAR	.CAB	System
Video Clip	WMPPLAYER.EXE	Microsoft Corporation	WMP11.A...	.AVI	System
MIDI Sequence	WMPPLAYER.EXE	Microsoft Corporation	WMP11.A...	.MID	System
MP3 Format Sound	WMPPLAYER.EXE	Microsoft Corporation	WMP11.A...	.MP3	System
Windows Script File	WSCRIPT.EXE	Microsoft Corporation	WSFFile	.WSF	System
Windows Script Host Settings ...	WSCRIPT.EXE	Microsoft Corporation	WSHFile	.WSH	System

Info... Add Remove Close

%1%* 8:46 AM 6/8/2020

Search

25. The **Windows Batch File** window appears, as shown in the screenshot. Click **Expand Info** to view the full info about the program.

WinPatrol [FREE Edition]

PLUS REQUIRED

Startup Programs Delayed Start IE Helpers Scheduled Tasks 1.0 Services Active Tasks Cookies File Types Hidden Files File Size Monitor Recent PLUS REQUIRED

Scotty the Windows Watch Dog reports that the following programs are associated with particular file types.

Select a Program Title and press Info... or double-click an item to verify any available product information.

?

Windows Batch File

No Icon

Status: File Does Not Exist

Expand Info

<< >>

Close

Title	Command	Company	Class	Extension	Type
Windows Batch File	Executable		batfile	.BAT	System
Security Catalog	CRYPTTEXT.DLL	Microsoft Corporation	Windows Batch File		
Compiled HTML Help file	HH.EXE	Microsoft Corporation			
Windows Command Script	Executable				
MS-DOS Application	Executable				
Application	Executable				
Setup Information	NOTEPAD.EXE	Microsoft Corporation	Company:		
JavaScript File	WSCRIPT.EXE	Microsoft Corporation	Version:		
Windows Installer Package	MSIEXEC.EXE	Microsoft Corporation	Copyright:		
Shortcut to MS-DOS Program	Executable				
Registration Entries	REGEDIT.EXE	Microsoft Corporation			
Rich Text Document	WORDPAD.EXE	Microsoft Corporation			
Screen saver	Executable		%1 %*		
Text Document	NOTEPAD.EXE	Microsoft Corporation			
Text Document	NOTEPAD.EXE	Microsoft Corporation			
VBScript Encoded File	WSCRIPT.EXE	Microsoft Corporation			
VBScript Script File	WSCRIPT.EXE	Microsoft Corporation	VBSFile	.VBS	System
Windows host process (Rundll...)	IEFRAME.DLL	Microsoft Corporation	WindowsURL	User D...
WinRAR archive	WINRAR.EXE	Alexander Roshal	WinRAR	.CAB	System
Video Clip	WMPPLAYER.EXE	Microsoft Corporation	WMP11.A...	.AVI	System
MIDI Sequence	WMPPLAYER.EXE	Microsoft Corporation	WMP11.A...	.MID	System
MP3 Format Sound	WMPPLAYER.EXE	Microsoft Corporation	WMP11.A...	.MP3	System
Windows Script File	WSCRIPT.EXE	Microsoft Corporation	WSFFile	.WSF	System
Windows Script Host Settings ...	WSCRIPT.EXE	Microsoft Corporation	WSHFile	.WSH	System

Info... Add Remove Close

%1 %*

Search

8:48 AM 6/8/2020

26. The expanded view shows all information related to the program and its associated file, as demonstrated in the screenshot. Analyze the info and close the window.

WinPatrol [FREE Edition]

PLUS REQUIRED

Startup Programs Delayed Start IE Helpers Scheduled Tasks 1.0 Services Active Tasks Cookies File Types Hidden Files File Size Monitor Recent PLUS REQUIRED

Scotty the Windows Watch Dog reports that the following programs are associated with particular file types.

Select a Program Title and press Info... or double-click an item to verify any available product information.

?

Windows Batch File

Title	Command	Company	Class	Extension	Type
Windows Batch File	Executable		batfile	.BAT	System
Security Catalog	CRYPTTEXT.DLL	Microsoft Corporation	Windows Batch File		
Compiled HTML Help file	HH.EXE	Microsoft Corporation			
Windows Command Script	Executable				
MS-DOS Application	Executable				
Application	Executable				
Setup Information	NOTEPAD.EXE	Microsoft Corporation	Company:		
JavaScript File	WSCRIPT.EXE	Microsoft Corporation	Version:		
Windows Installer Package	MSIEXEC.EXE	Microsoft Corporation	Copyright:		
Shortcut to MS-DOS Program	Executable				
Registration Entries	REGEDIT.EXE	Microsoft Corporation			
Rich Text Document	WORDPAD.EXE	Microsoft Corporation			
Screen saver	Executable				
Text Document	NOTEPAD.EXE	Microsoft Corporation	Date Created	Last Saved	File Size
Text Document	NOTEPAD.EXE	Microsoft Corporation			Detectd by WinPatrol
VBScript Encoded File	WSCRIPT.EXE	Microsoft Corporation			
VBScript Script File	WSCRIPT.EXE	Microsoft Corporation			
Windows host process (Rundll...)	IEFRAME.DLL	Microsoft Corporation			
WinRAR archive	WINRAR.EXE	Alexander Roshal			
Video Clip	WMPPLAYER.EXE	Microsoft Corporation			
MIDI Sequence	WMPPLAYER.EXE	Microsoft Corporation			
MP3 Format Sound	WMPPLAYER.EXE	Microsoft Corporation			
Windows Script File	WSCRIPT.EXE	Microsoft Corporation			
Windows Script Host Settings ...	WSCRIPT.EXE	Microsoft Corporation			

No Icon

Status: File Does Not Exist

Shrink Window

%1%

File Type Extension: .BAT

PLUS Info... Create Note << >> Close

Info... Add Remove Close

%1%

Search

8:49 AM 6/8/2020

27. Now, switch to the **Active Tasks** tab to view the current tasks running on your computer. Select any task and click **Kill Task** to end the task, as shown in the screenshot.

WinPatrol [FREE Edition]

PLUS REQUIRED

Startup Programs Delayed Start IE Helpers Scheduled Tasks 1.0 Services Active Tasks Options PLUS Cookies File Types Hidden Files File Size Monitor Recent PLUS REQUIRED

Scotty the Windows Watch Dog has sniffed out the following programs which are currently running on your computer.

Select a program and press Properties, or double click an item to verify any available product information.
[64 bit processes available to PLUS customers only]

Module	Program Description	Company	First Detected	File Size	Proces...
jusched.exe	Java Update Scheduler	Oracle Corporat...	06/08/2020 8:3...	646,160	7120
jucheck.exe	Java Update Checker	Oracle Corporat...	06/08/2020 8:3...	961,040	4292
WINPATROL.EXE	WinPatrol [FREE Edition]	Ruiware	06/08/2020 8:3...	1,223,...	820
WINPATROLEX.EXE	WinPatrol [FREE Edition]	Ruiware	06/08/2020 8:3...	1,981,...	7568

Info... Refresh Kill Task Kill By Name [PLUS ONLY] Close

Java Update Scheduler

Search 8:50 AM 6/8/2020

28. By examining all these tabs, you can find any unwanted process or application running on the machine when the system boots up and manually stop or delete them.
 29. Close all open windows on the **Windows 10** machine.
 30. You can also use other Windows startup programs monitoring tools such as **Autorun Organizer** (<https://www.chemtable.com>), **Quick Startup** (<https://www.glarysoft.com>), **StartEd Pro** (<http://www.outertech.com>), or **Chameleon Startup Manager** (<http://www.chameleon-managers.com>) to perform startup programs monitoring.
-

Task 6: Perform Installation Monitoring using Mirekusoft Install Monitor

When the system or users install or uninstall any software application, there is a chance that it will leave traces of the application data on the system. Installation monitoring help to detect hidden and background installations that malware performs.

Mirekusoft Install Monitor automatically monitors what gets placed on your system and allows you to uninstall it completely. Install Monitor works by monitoring what resources such as file and registry, are created when a program is installed. It provides detailed information about the software installed, including how much disk space, CPU, and memory your programs are using. It also provides information about how often you use different programs. A program tree is a useful tool that can show you which programs were installed together.

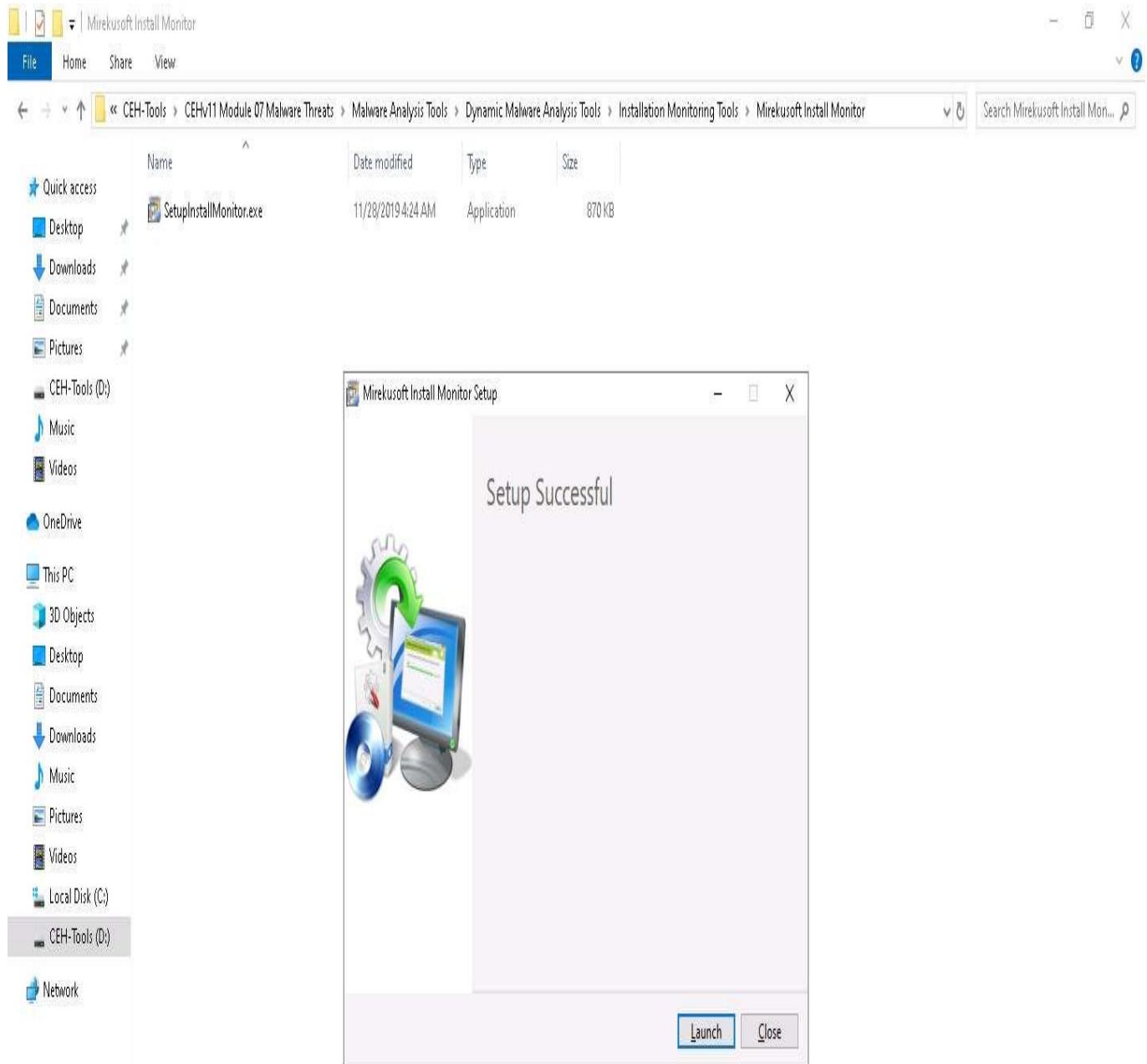
Here, we will use the Mirekusoft Install Monitor tool to detect hidden and background installations.

1. On the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools** and double-click **SetupInstallMonitor.exe**.

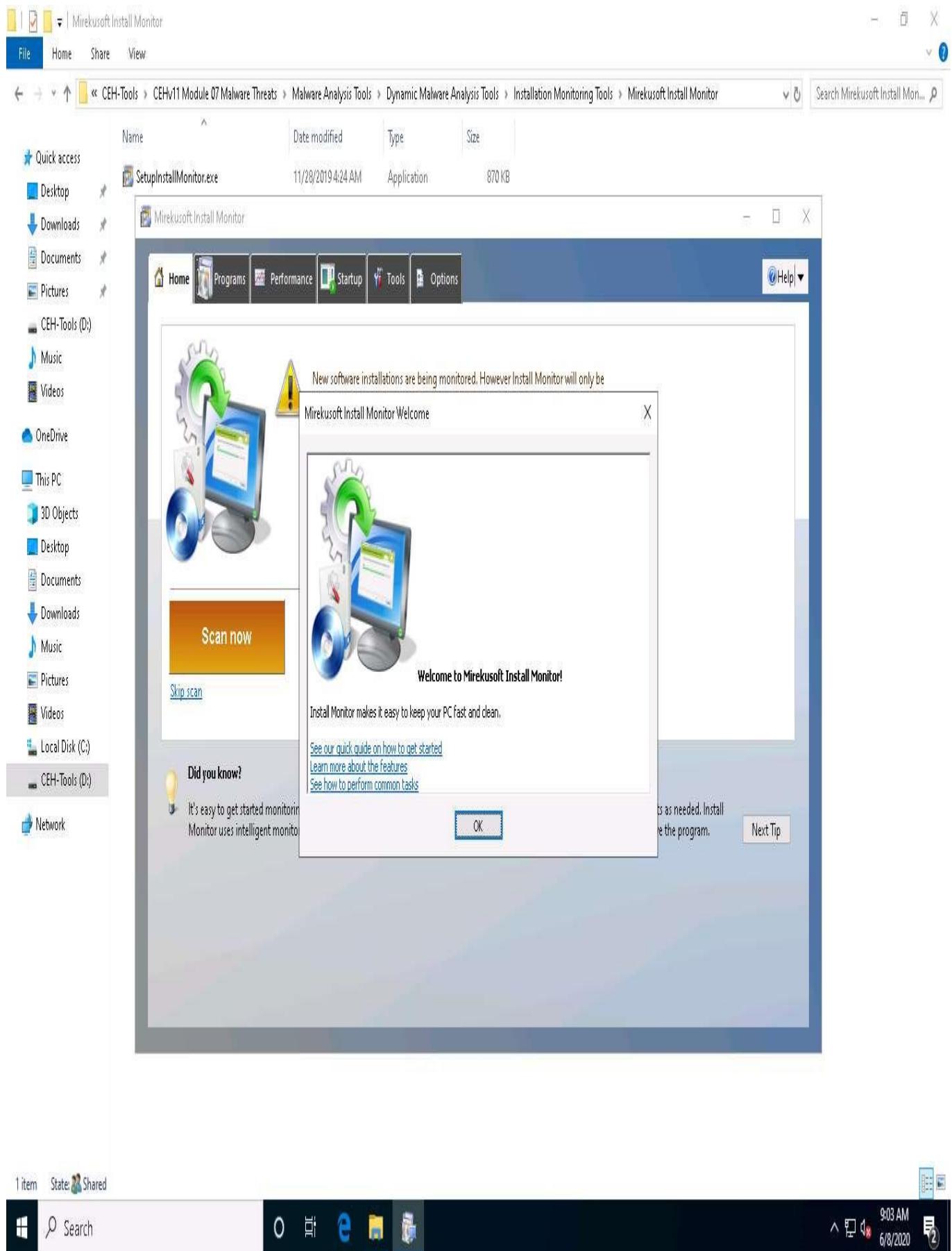
If **Update Available** wizard appears, click **Update** button.

If a **User Account Control** window appears, click **Yes**.

2. Follow the installation steps to install **Mirekusoft Install Monitor**.
3. The **Setup Successful** wizard appears; click **Launch**.



4. If a **User Account Control** window appears, click **Yes**.
5. The **Mirekusoft Install Monitor** main window appears, along with a **Welcome** pop-up, click **OK**. Click **Skip scan** in the **Home** tab.



6. Click the **Programs** tab to view the programs installed on your machine. You can choose any unwanted or unused application and click **Uninstall** to remove it from your machine. In this task, we are choosing the **WinPatrol** application.

The **WinPatrol** pop-up appears; click **Reject Change**.

Mirekusoft Install Monitor

Programs

Manage and uninstall programs. Select multiple programs to batch uninstall.

Name	Publisher	Installed	Size	Version	Last Used	Usage
Mirekusoft Install Monitor	Mirekusoft	6/8/20 9:02 AM	861 KB	4.6.1055.1		
Microsoft SQL Server Compact 4.0 SP1 x64 ENU	Microsoft Corporation	6/8/20 9:01 AM	19.1 MB	4.0.8876.1		
WinPatrol	Ruiware	6/8/20 8:36 AM	4.05 MB	35.5.2017.8		
j16PowerTools	Macecraft Software	6/8/20 4:23 AM	18.4 MB			
SoftPerfect Network Scanner version 7.2.6	SoftPerfect Pty Ltd	6/8/20 4:11 AM	16.1 MB	7.2.6		
ID4 Freeware v7.0	Hex-Rays SA	6/8/20 12:58 AM	63.7 MB			
Adobe Acrobat Reader DC	Adobe Systems Incorporated	6/8/20 12:25 AM	337 MB	20.09.20067		
Microsoft OneDrive	Microsoft Corporation	6/8/20 12:14 AM	34.1 MB	20.064.0329.00...		
Google Chrome	Google LLC	6/7/20 11:50 PM	402 MB	83.0.4103.61		
Tenable Nessus (x64)	Tenable, Inc.	5/2/20 2:28 PM	131 MB	8.7.2.20213		
Microsoft Visual C++ 2015 Redistributable (x86) - 1...	Microsoft Corporation	5/1/20 8:44 AM	517 KB	14.0.24123.0		
Rohos Disk 3.0	SafeJKA SRL	5/1/20 8:44 AM	21.5 MB	3.0		
VeraCrypt	IDRIX	5/1/20 8:43 AM	34.2 MB	1.24-Hotfix1		
N-Stalker Web Application Security Scanner X (Free...)	N-Stalker, Inc	5/1/20 8:40 AM	56.9 KB	10.14.1.34		
Vega 1.0	Subgraph	5/1/20 8:39 AM	48.2 KB	1.0		
Cain & Abel 4.9.56		5/1/20 8:32 AM	146 KB			
NetScanTools Pro Demo 11.863	Northwest Performance Softwa...	5/1/20 8:17 AM	155 MB	11.863		
Microsoft Visual C++ 2008 Redistributable - x86 9.0...	Microsoft Corporation	5/1/20 8:13 AM	222 KB	9.0.30729.6161		
Nmap 7.80	Nmap Project	5/1/20 8:12 AM	77.2 KB	7.80		
Microsoft Visual C++ 2013 Redistributable (x86) - 1...	Microsoft Corporation	5/1/20 8:12 AM	444 KB	12.0.21005.1		
Wireshark 3.0.5 64-bit	The Wireshark developer comm...	5/1/20 8:10 AM	175 MB	3.0.5		
Npcap 0.9983	Nmap Project	5/1/20 8:10 AM	232 KB	0.9983		
Microsoft Visual C++ 2017 Redistributable (x64) - 1...	Microsoft Corporation	5/1/20 8:09 AM	881 KB	14.16.27033.0		
Lab on Demand Hyper-V Integration Service	Learn on Demand Systems	4/14/20 10:46 AM	10.7 MB	1.0.9		
Java 8 Update 241	Oracle Corporation	4/14/20 6:29 AM	239 MB	8.0.2410.7		
WinPcap 4.1.3	Riverbed Technology, Inc.	4/14/20 6:00 AM	118 KB	4.1.0.2980		
Mozilla Maintenance Service	Mozilla	4/14/20 5:54 AM	88.8 KB	75.0		
Mozilla Firefox 75.0 (64-bit) (S)	Mozilla	4/14/20 5:54 AM	189 MB	75.0		

WinPatrol

Publisher: Ruiware Version: 35.5.2017.8

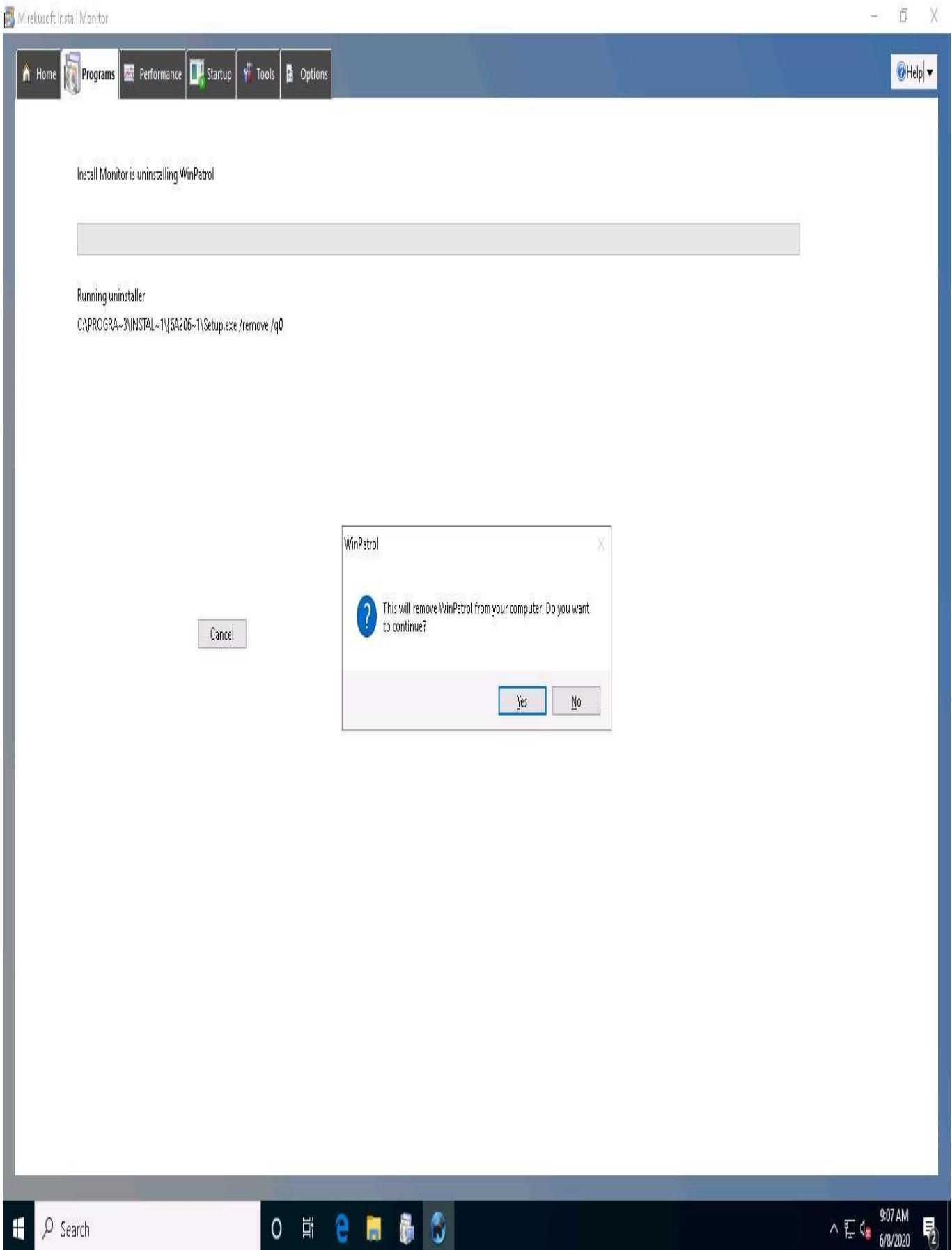
Date: Today, June 8, 2020, 29 minutes ago
 Size: 4.05 MB (4,253,847 bytes) Size of registry: 1.52 KB (1,566 bytes) Contains: 23 Files, Registry: 2 Keys, 33 Values
 About: <https://www.winpatrol.com>

[Uninstall](#)

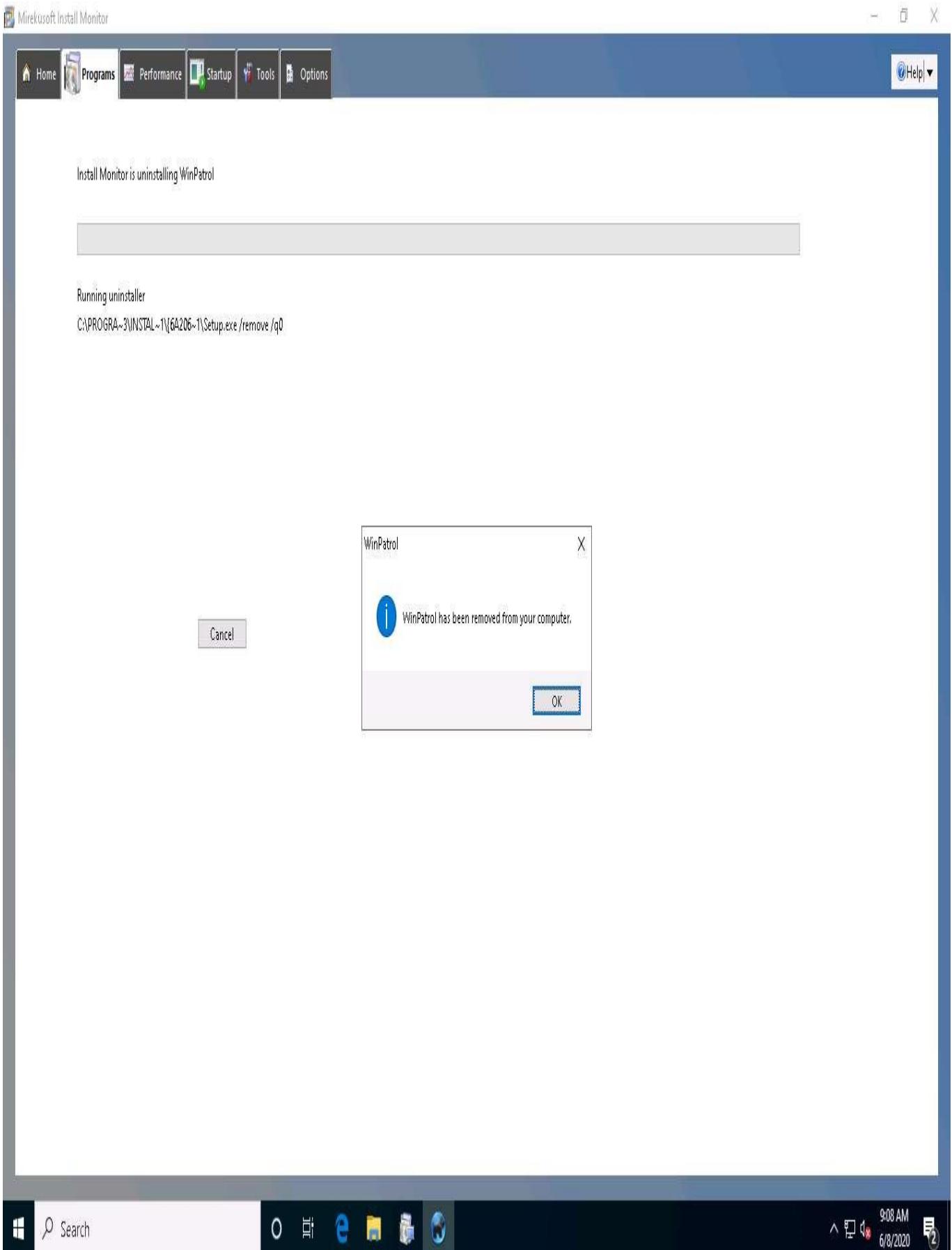
Search

9:05 AM
6/8/2020

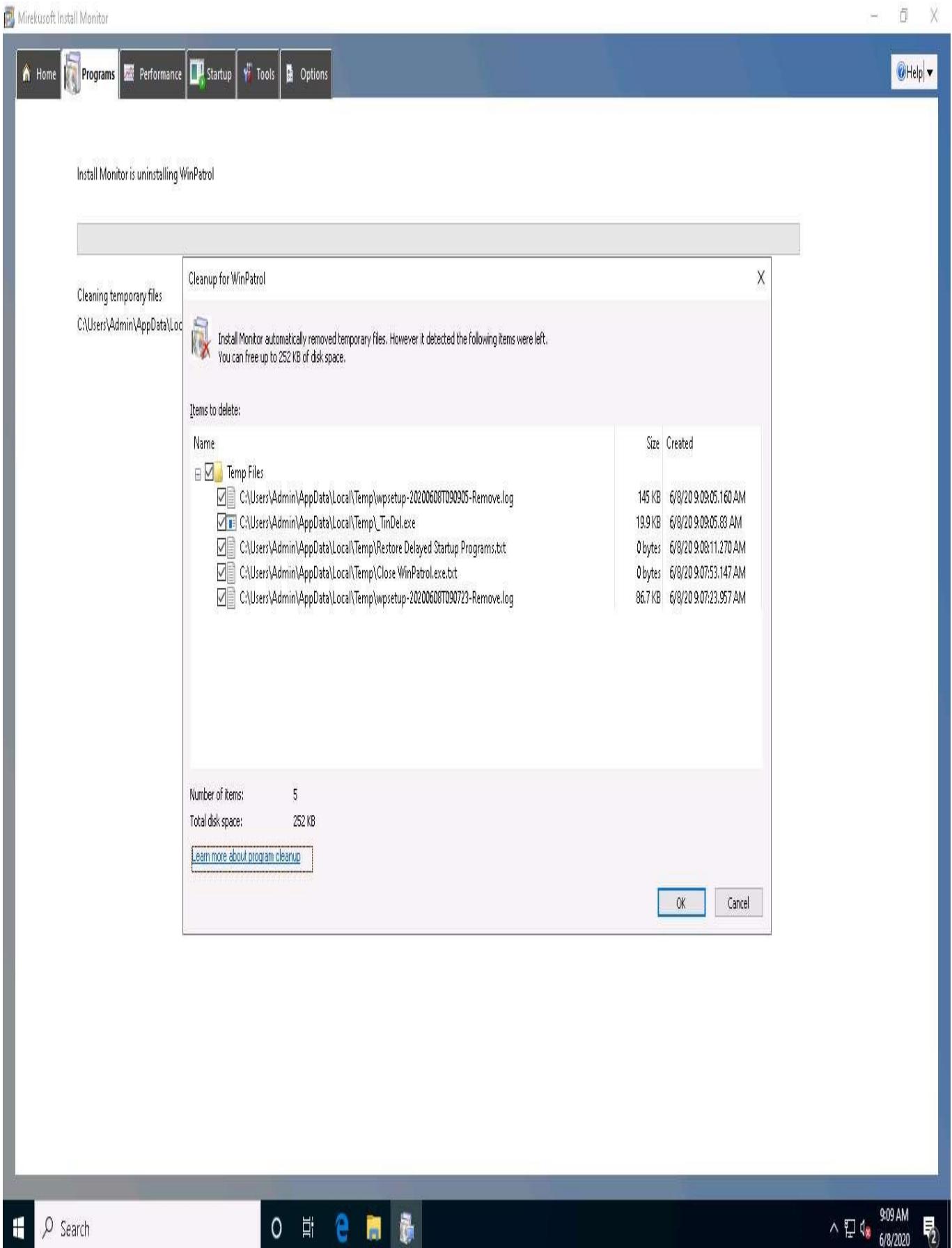
7. While uninstalling the application, a selected program pop-up appears, click **Yes** in all the **WinPatrol** pop-ups.



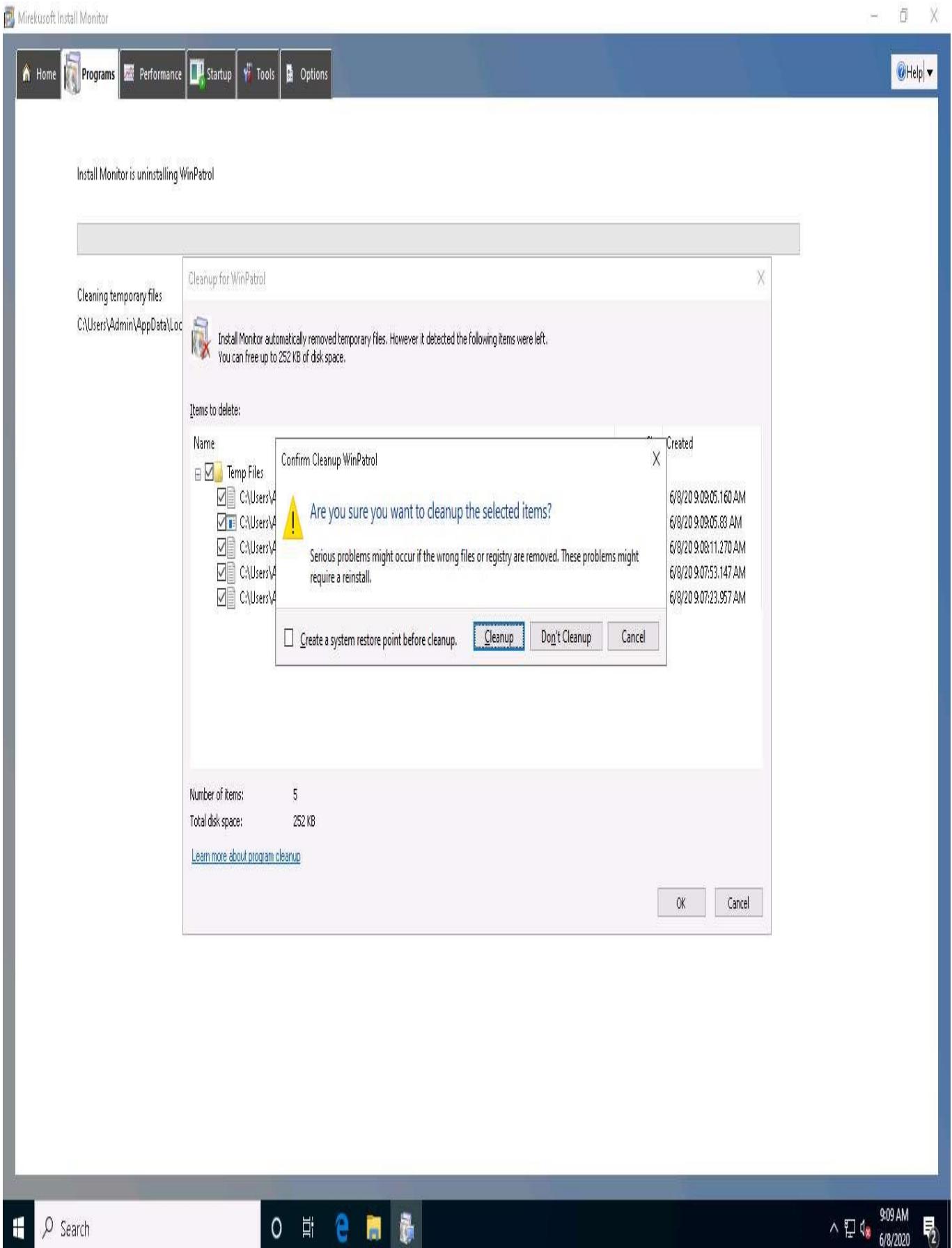
8. The **selected application is uninstalled from your computer** pop-up appears; click **OK**.



9. If a **Cleanup for Selected Program** window appears (here, **WinPatrol**), click **OK**.



10. The **Confirm Cleanup** pop-up appears; click **Cleanup**. This will delete all the supported files for the related application that you have uninstalled from your computer.



11. The selected application is uninstalled from your computer. Click the **Performance** tab to view and terminate currently running programs.
12. Here, you can select any program from the list and click **End Program** to terminate the program.
13. Click the **Startup** tab to view the programs that run automatically on Windows Startup.

14. In this lab, Mirekusoft Install Monitor has not detected startup programs. If the program does detect them, choose the application that you want to disable on startup, and click **Disable**.
15. You can restart the machine to detect the startup programs.

The screenshot shows the Mirekusoft Install Monitor application window. At the top, there is a menu bar with icons for Home, Programs, Performance, Startup (which is highlighted with a red box), Tools, Options, and Help. Below the menu is a section titled "Manage startup programs". A table with columns for Program, Publisher, Installed, Load time, and Status is displayed, but it is currently empty. At the bottom of the window, a message states "Startup Monitor might not have any monitoring data. It will monitor the next restart." To the right of this message are four buttons: Details, Apply, Enable all, and Disable all. The taskbar at the bottom of the screen shows the Windows Start button, a search bar, and several pinned icons for File Explorer, Edge, and File History. The system tray on the far right displays the date (6/8/2020), time (9:13 AM), battery status, signal strength, and a notification icon.

16. This is how to monitor a Windows machine using Mirekusoft Install Monitor. Close all applications.
 17. You can also use other installation monitoring tools such as **SysAnalyzer** (<https://www.aldeid.com>), **Advanced Uninstaller PRO** (<https://www.advanceduninstaller.com>), **REVO UNINSTALLER PRO** (<https://www.revouninstaller.com>), or **Comodo Programs Manager** (<https://www.comodo.com>) to perform installation monitoring.
-

Task 7: Perform Files and Folder Monitoring using PA File Sight

Malware can modify system files and folders to save information in them. You should be able to find the files and folders that malware creates and analyze them to collect any relevant stored information. These files and folders may also contain hidden program code or malicious strings that the malware plans to execute on a specific schedule.

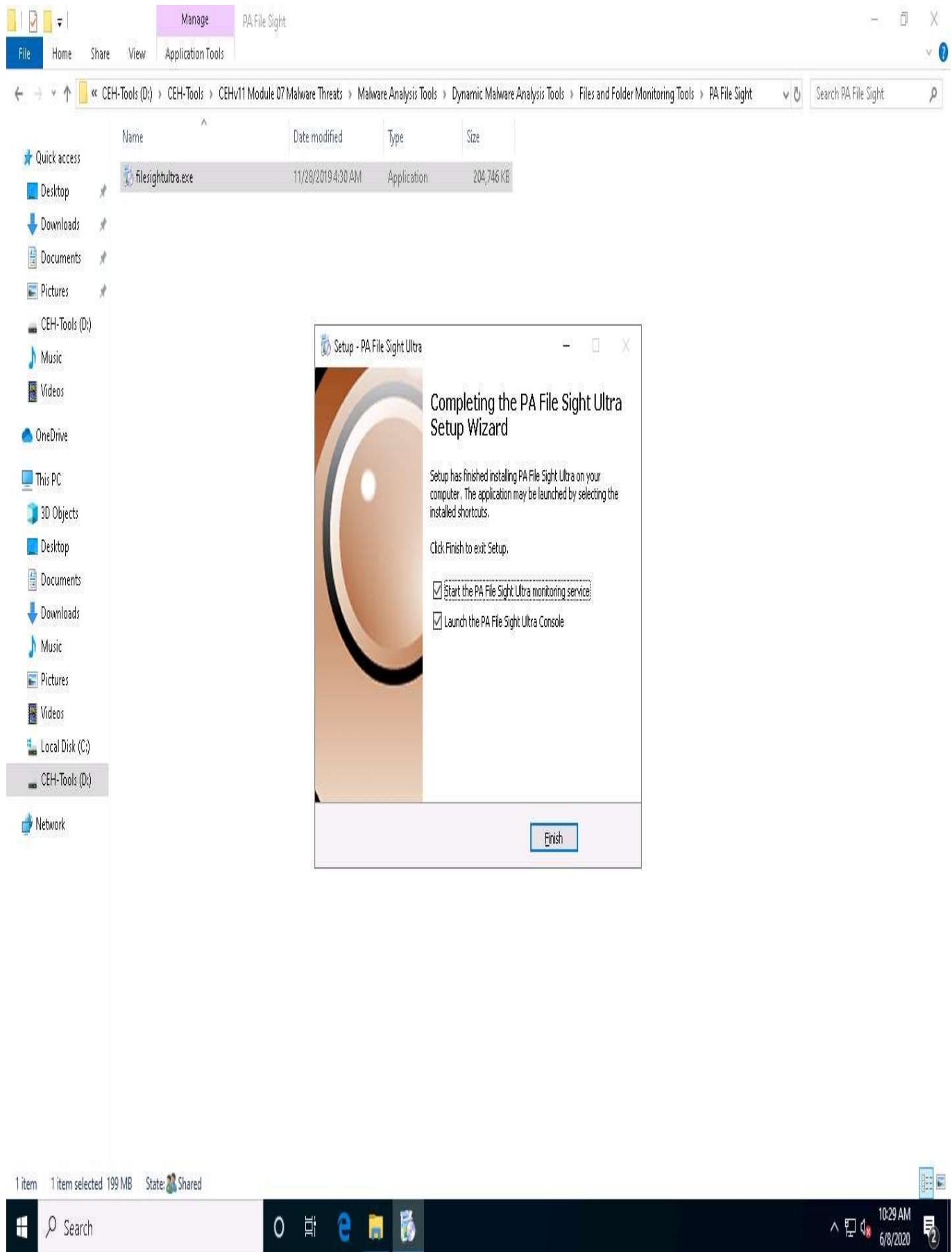
An ethical hacker or penetration tester must scan the system for suspicious files and folders using file and folder monitoring tools such as PA File Sight to detect any malware installed and any system file modifications. PA File Sight is a protection and auditing tool. It detects ransomware attacks coming from a network and stops them.

Features:

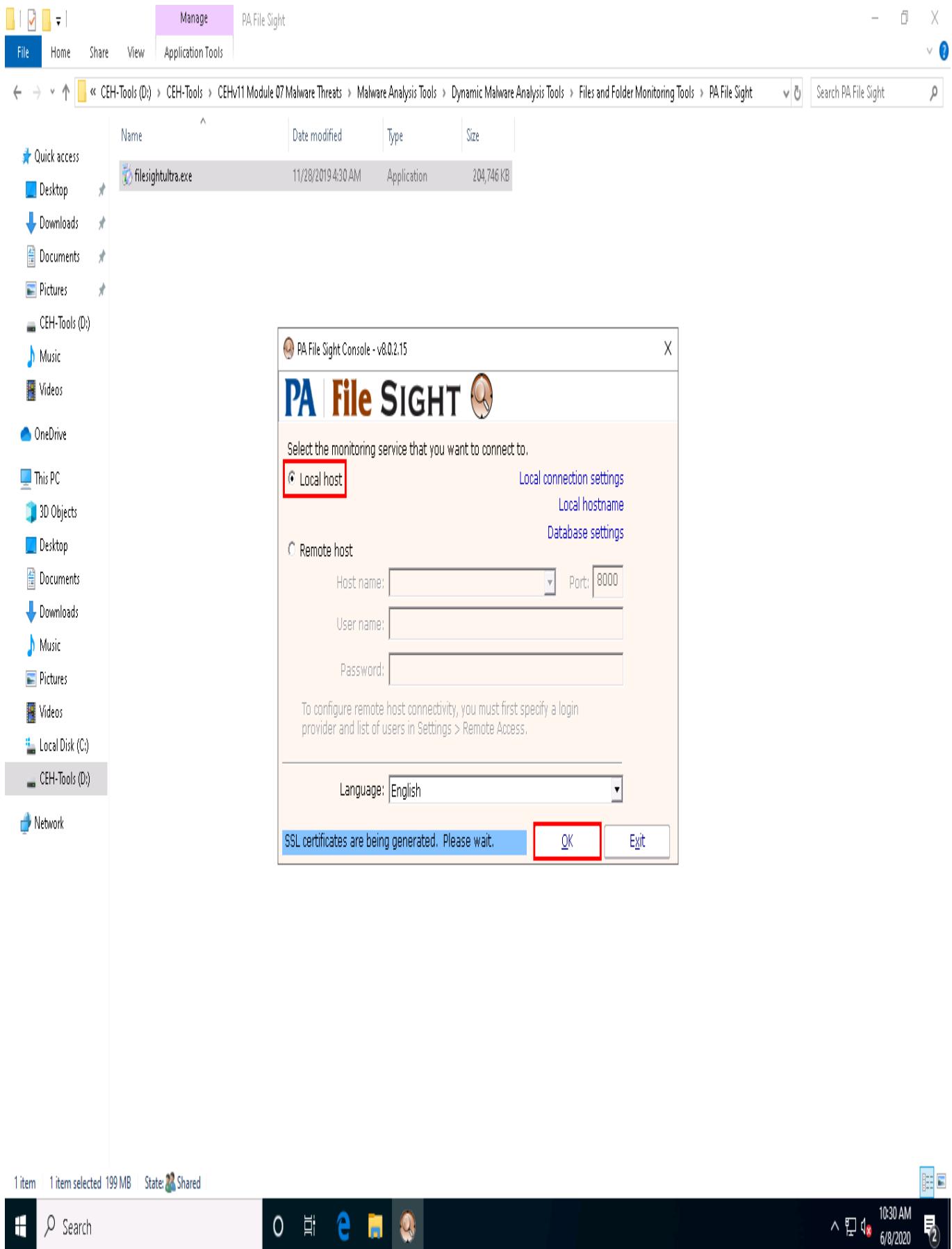
- Compromised computers are blocked from reaching files on other protected servers on the network
 - Detects users copying files and optionally blocks access
 - Real-time alerts allow the appropriate staff to investigate immediately
 - Audits who is deleting, moving, and reading files
1. On the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **filesightultra.exe**.

If a **User Account Control** window appears, click **Yes**.

2. The **Select Setup Language** pop-up appears; choose your preferred language, and then click **OK**.
3. Follow the default installation steps to install **PA File Sight**.
4. **Completing the PA File Sight Ultra Setup Wizard** appears; make sure that both the **Start the PA File Sight Ultra monitoring service** and the **Launch the PA File Sight Ultra Console** options are checked, and click **Finish**.
5. This will run the PA File Sight service and automatically launch the application.



6. The **PA File Sight Console** window appears. By default, the **Local host** radio button is selected; click **OK**.



7. The **PA File Sight Ultra Console** main window appears.

If a **Start Wizard** window appears, close it.



STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Servers

< Back

Open in Browser

Print

Servers/Devices

All Actions

Advanced Services

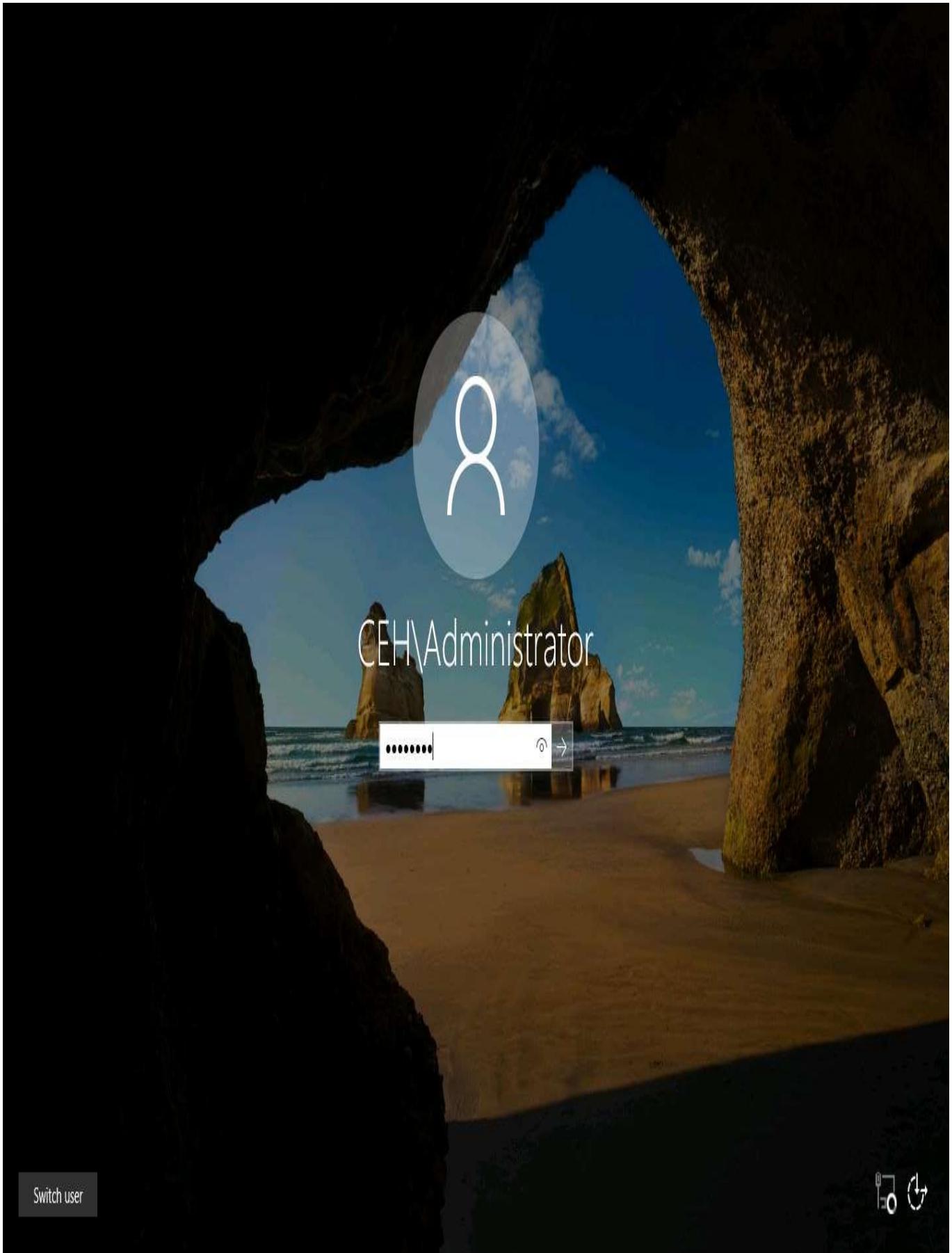
Endpoint Services

Updates

Reports

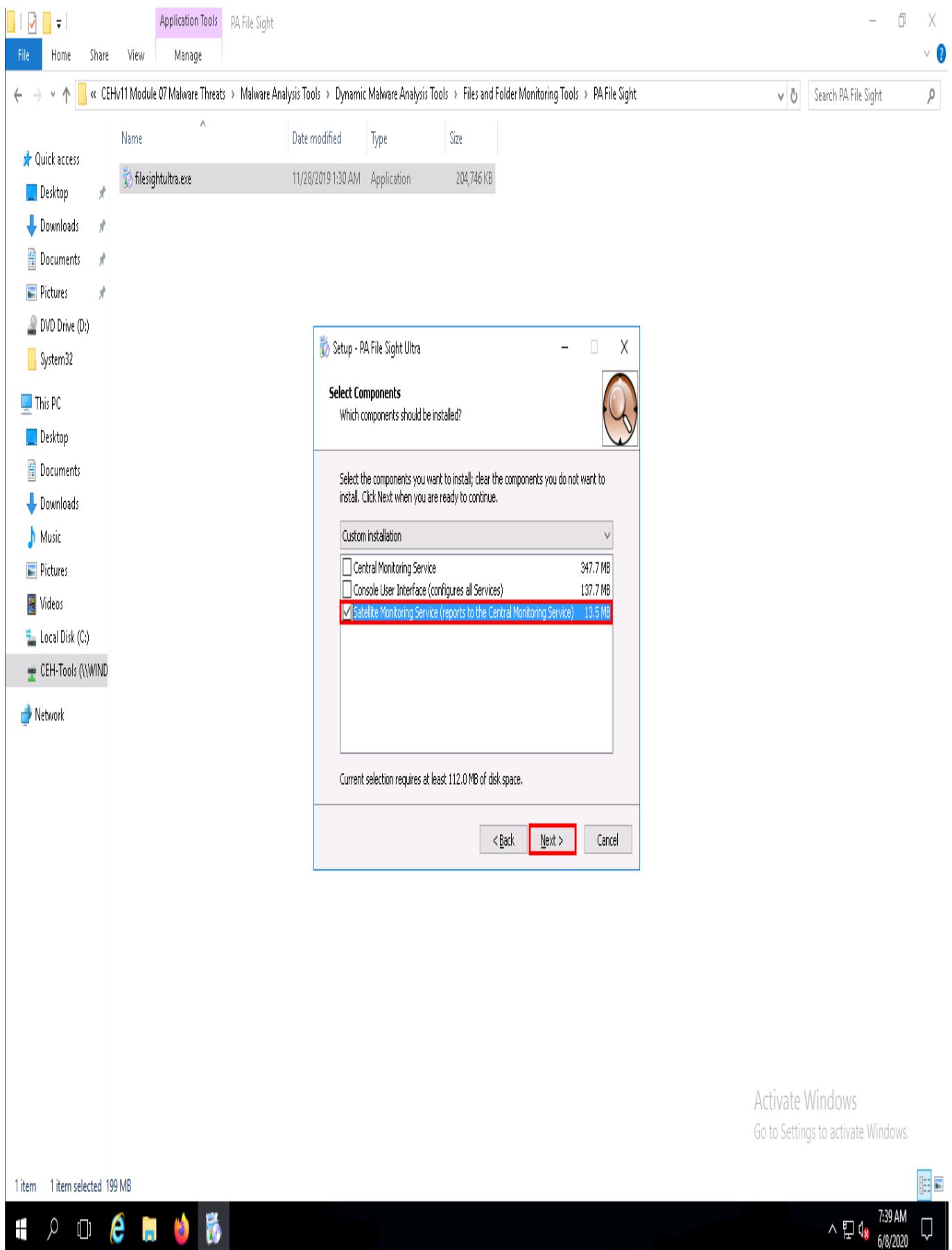

 10:33 AM
 6/8/2020

8. Click [Windows Server 2016](#) to switch to the **Windows Server 2016** machine Click [**Ctrl+Alt+Delete**](#) to activate the machine, by default, **CEH\Administrator** account is selected, click **Pa\$\$w0rd** to enter the password and press **Enter**.



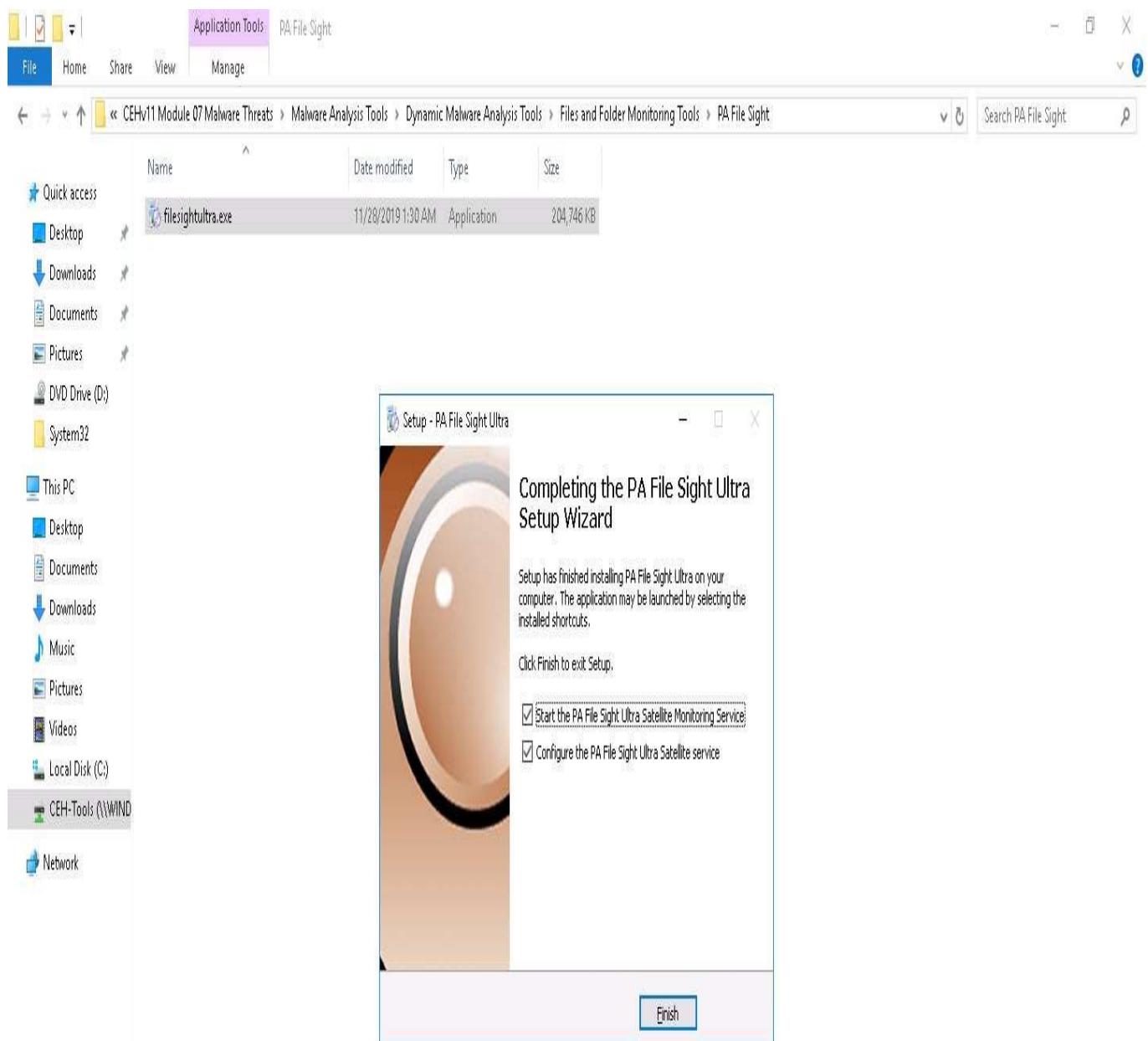
9. Navigate to Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight and double-click **filesightultra.exe**.
10. The **Select Setup Language** pop-up appears; choose your preferred language and click **OK**.
11. Click the **Next** button until you see the **Select Components** wizard.

12. In the **Select Components** wizard, uncheck the **Central Monitoring Service** and **Console User Interface (configure all Services)** options, and check the **Satellite Monitoring Service (reports to Central Monitoring Service)** option; then, click **Next**.



Activate Windows
Go to Settings to activate Windows.

13. Follow the wizard-driven installation steps to install the application.
14. In the final step of the installation, make sure that the **Start the PA File Sight Ultra Satellite Monitoring Service** and **Configure the PA File Sight Ultra Satellite service** options are checked; then, click **Finish**.

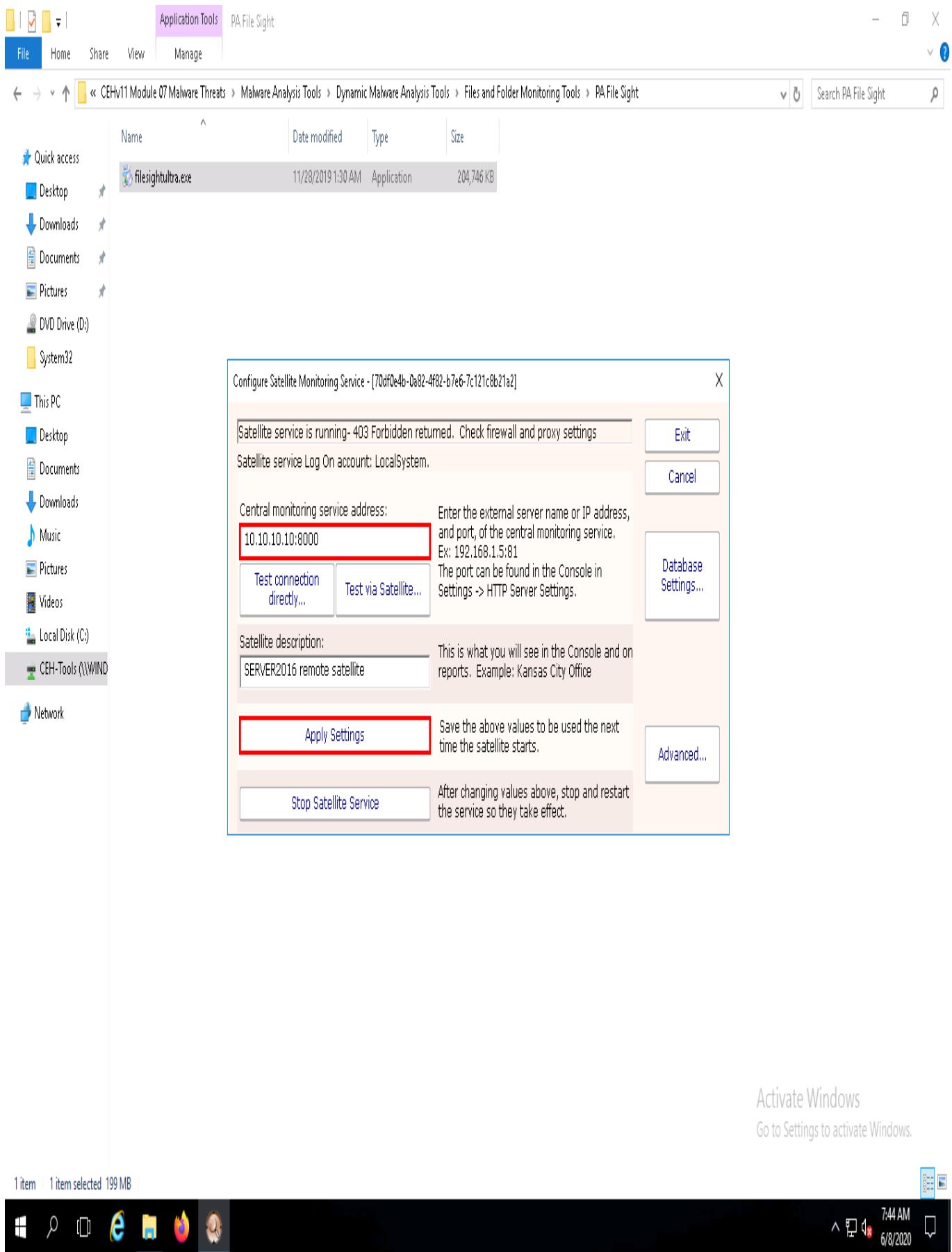


Activate Windows
Go to Settings to activate Windows.

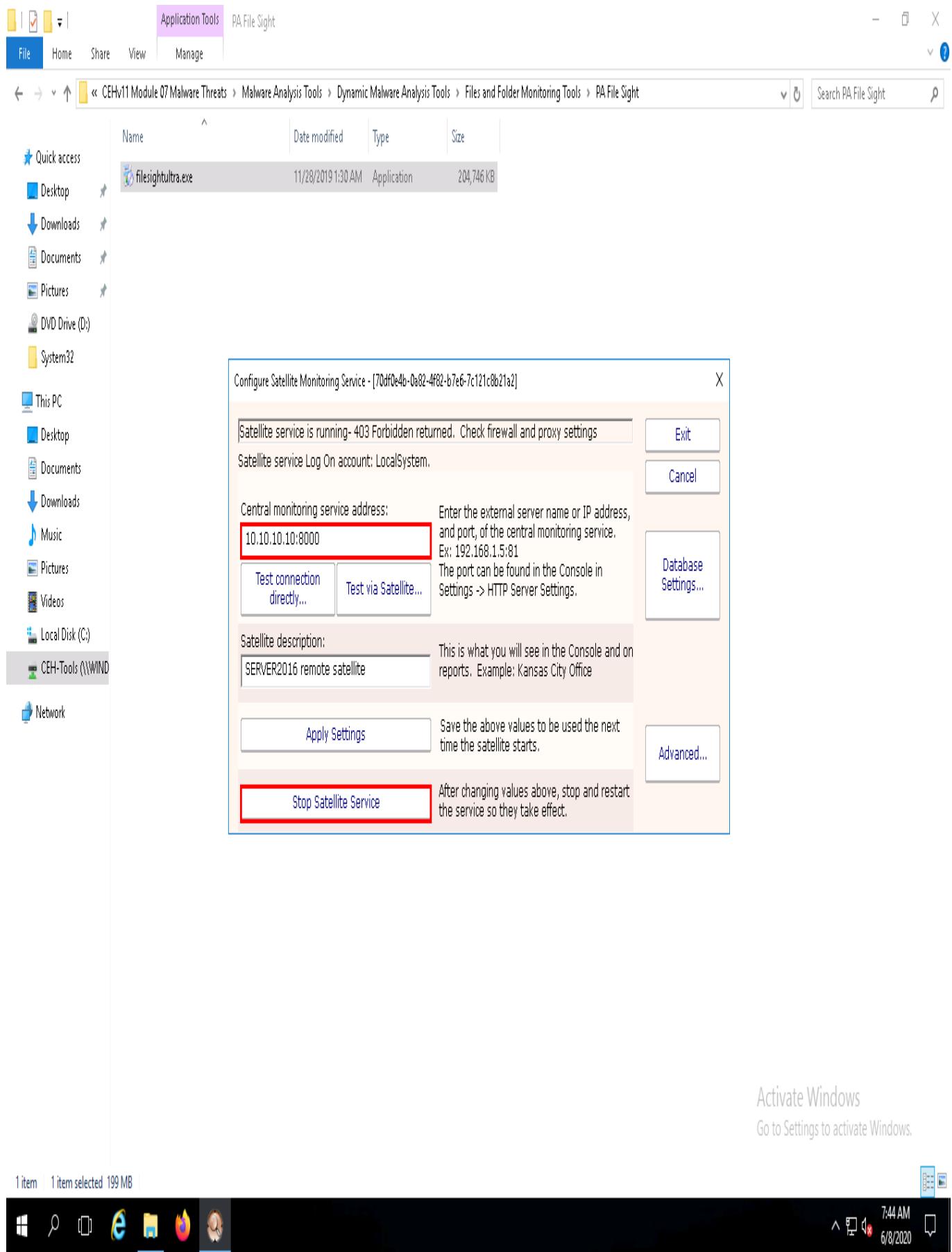


15.  The **Configure Satellite Monitoring Service** window appears; type the **Windows 10** IP address into the **Central monitoring service address** field along with port **8000**. Leave the other settings to default and click **Apply Settings**.

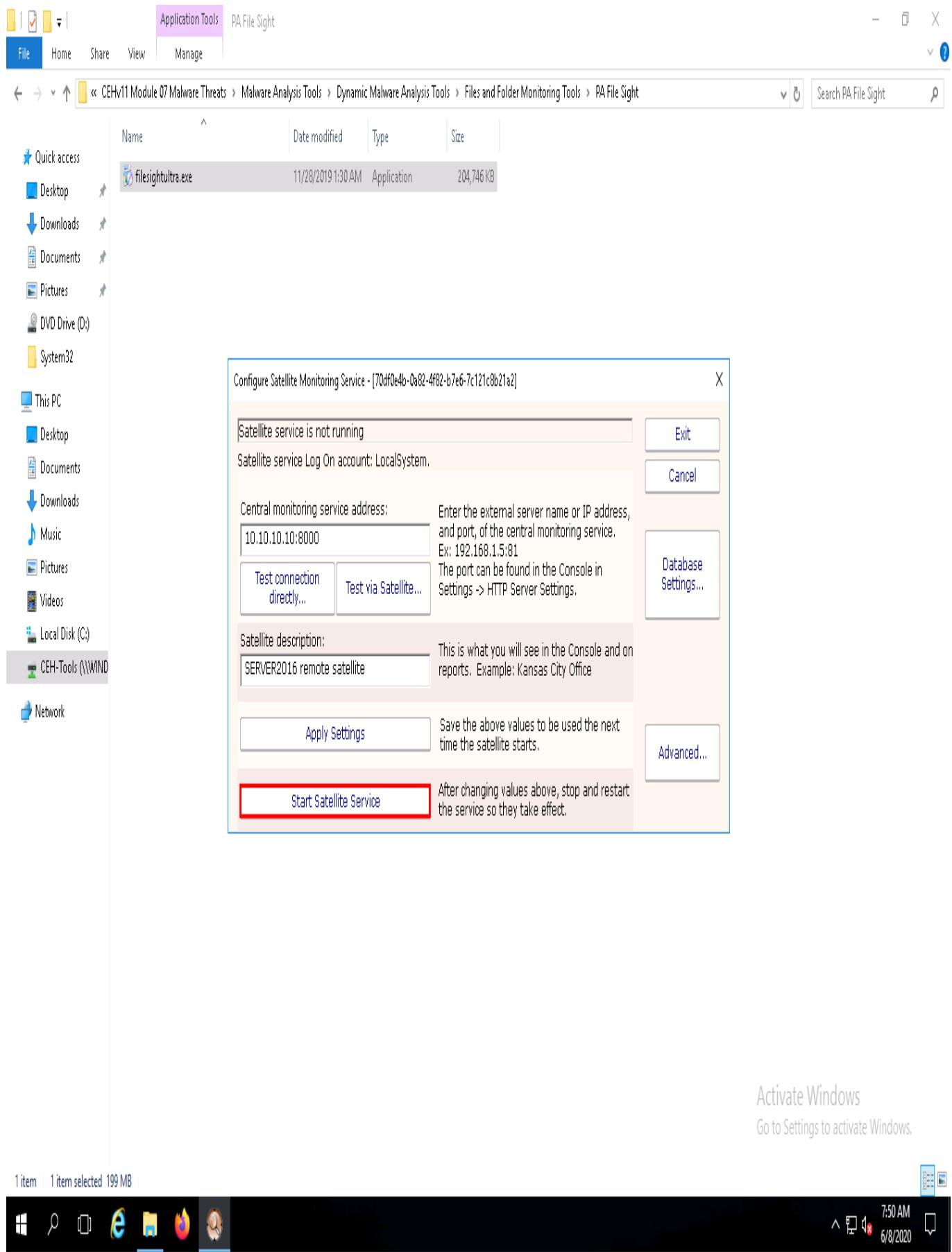
In this task, the IP address of the **Windows 10** machine is **10.10.10.10**. the IP address may vary in your lab environment.



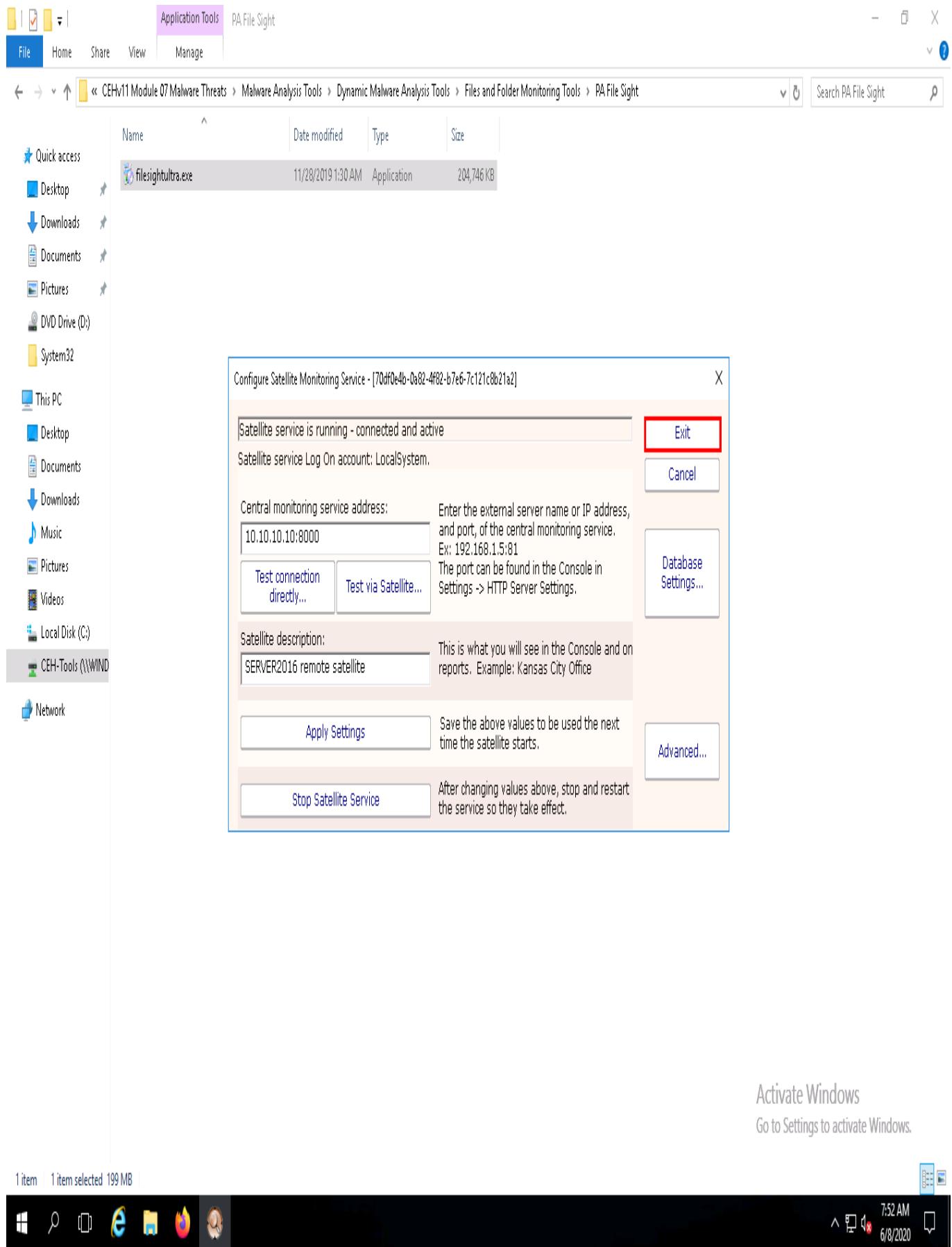
16. Click **Stop Satellite Service** to stop the satellite service.



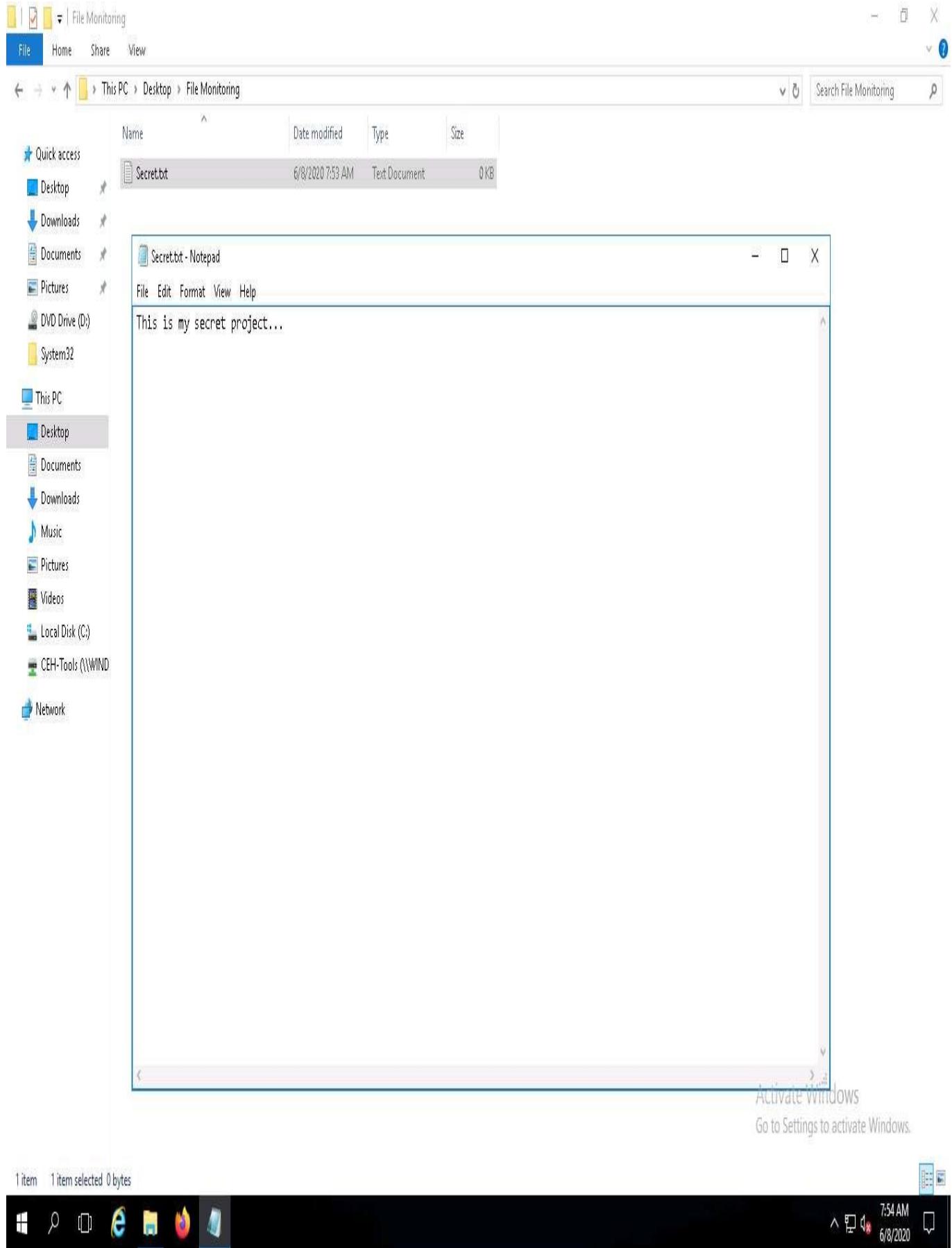
17. Once the service is stopped, click **Start Satellite Service**.



18. Once the service has started, click **Exit** to close the application.



19. Create a folder named **File Monitoring** on **Desktop** and open it. Create a new text document in the folder, name it **Secret.txt**, type some text content in the file, and save it. **Close** the notepad window.



20. Click [Windows 10](#) to switch back to the **Windows 10** machine, and observe that PA File Sight starts monitoring the **Windows Server 2016** machine.



STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Servers

< Back

Open in Browser

Print

[+] Servers/Devices
[+] SERVER2016

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 08 Jun 2020 10:53 AM

[All Reports](#) | [PDF Version](#)

Server Status Counts

0 OK	0 Alert	0 Error	1 Other
------	---------	---------	---------

Monitor Status Counts

0 OK	0 Alert	0 Error	1 Other
------	---------	---------	---------

Servers/Devices

SERVER2016

[+] Inventory Collector
 Probe methods: WMI, System
 Details program Scheduled

This status report will always be available at [https://Windows10:8000/STATUS_GROUP_\(0\)/index.html?CMD=REFRESH_REPORT&RTYPE=1&ROBJ=0](https://Windows10:8000/STATUS_GROUP_(0)/index.html?CMD=REFRESH_REPORT&RTYPE=1&ROBJ=0)
 Created in 0 ms

 Generated by PA File Sight
 v8.0.2

All Actions

Advanced Services

Endpoint Services

Updates

Reports



Search


 10:55 AM
 6/8/2020

21. Expand the **SERVER2016** node, select **Inventory Collector** in the left-hand pane, and click the **Apply** button from the right-hand pane.

File View Configuration Settings Licensing Help Quiet...

PA | File SIGHT

STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Licensed to:
PA File Sight v8 Ultra Trial License (30 days left)

Servers

- Servers/Devices
 - SERVER2016
 - Inventory Collector



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

All Actions

Advanced Services

Endpoint Services

Updates

Reports

Schedule...



Search

10:56 AM
6/8/2020

22. Now, right-click on **Inventory Collector** and click **Run Now!** from the context menu.



OK +1 monitors run

STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Servers

Servers/Devices

SERVER2016

Inventory Collector

Delete Inventory Collector

Run Now!

Disable Monitor

Immediate Maintenance: Pause Monitoring ...

Rename Monitor

Copy Monitor

Custom Properties ...

Template Operations >

Current Status: Scheduled

Collect simple System Details information

Probe methods: WMI, System Details program

Last Run: 08 Jun 2020 10:47:51 AM

Next Run: 08 Jun 2020 04:47:51 PM

Apply

Reset

Advanced Options...

All Actions

Advanced Services

Endpoint Services

Updates

Reports

Schedule...



Search

11:00 AM
6/8/2020

23. Select **SERVER2016** in the left pane and scroll down, and you can see the complete system information for the **Windows Server 2016** machine on the dashboard.



STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Servers



< Back

Open in Browser

Print

YOUR LOGO HERE

To change or remove this logo, go to:
Settings > Report Settings

SERVER2016

SERVER2016 remote satellite

Updated 08 Jun 2020 11:07:45 AM

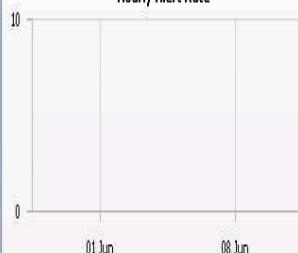
Group Reports

All Reports

PDF Version

System Information

Hourly Alert Rate



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.

System Details

Uptime
0 days, 7 hours, 54 minutes

Operating System
Microsoft Windows Server 2016
Standard 10.0.14393

CPU
Intel(R) Xeon(R) Gold 6230 CPU @
2.10GHz (64 bit, None)

CPU: Core Count
CPU0: 1

Memory
Physical: 4,095 MB

Model
Microsoft CorporationVirtual Machine

Monitor Status

Monitor

Last Status

Last Checked



11:08 AM
6/8/2020 2

24. Right-click on SERVER2016 and click the **Add New Monitor** option from the context menu.



STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Servers

< Back

Open in Browser

Print

Servers/Devices

SERVER2016

Inventory

YOUR LOGO HERE

To change or remove this logo, go to:
Settings > Report Settings

Updated 08 Jun 2020 11:07:45 AM

Group Reports

All Reports

PDF Version

- Add New Monitor ...
- Delete SERVER2016
- Set Server Alias ...
- Change Hostname / IP Address
- Move Device to Different Group

- Maintenance Period
- Disable monitoring of server/device

- Configuration
- Copy Computer
- Custom Properties ...
- Prevent Template Propagation
- Block Auto Configuration

- Report & Delivery Settings
- Operations
- Notes ...

- Monitored from: SERVER2016 remote satellite

Rate

08 Jun

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.

System Details

Uptime
0 days, 7 hours, 54 minutes

Operating System
Microsoft Windows Server 2016 Standard 10.0.14393

CPU
Intel(R) Xeon(R) Gold 6230 CPU @ 2.10GHz (64 bit, None)

CPU: Core Count
CPU: 1

Memory
Physical: 4,095 MB

Model
Microsoft CorporationVirtual Machine

Monitor Status

Monitor	Last Status	Last Checked

- All Actions
- Advanced Services
- Endpoint Services
- Updates
- Reports

Windows Search



11:08 AM
6/8/2020

25. The **Add New Monitor** window appears, select the **File Sight Monitor** icon, and then click **OK**.



STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Servers



< Back

Open in Browser

Print

YOUR LOGO HERE

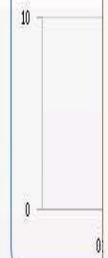
To change or remove this logo, go to:
[Settings](#) > [General Settings](#)

Add New Monitor

X

SERV
ERVER

System Info



Select the type of monitor for computer SERVER2016

OK

Cancel



Inventory Collector

Selected Monitor Description

Monitor files and be notified when someone reads from, writes to, renames or deletes the files. Notification includes file name, user account and IP address, and sometimes what application was being used.

Updated 08 Jun 2020 11:07:45 AM

[Group Reports](#) [All Reports](#) [PDF Version](#)

arithmetic Scale)

Total I/O

Reads

Writes

Deletes

show more

show less

All Actions
Advanced Services
Endpoint Services
Updates
Reports

System Details

Uptime
0 days, 7 hours, 54 minutes

Operating System
Microsoft Windows Server 2016 Standard 10.0.14393

CPU
Intel(R) Xeon(R) Gold 6230 CPU @ 2.10GHz (64 bit, None)

CPU: Core Count
CPU0: 1

Memory
Physical: 4,095 MB

Model
Microsoft CorporationVirtual Machine

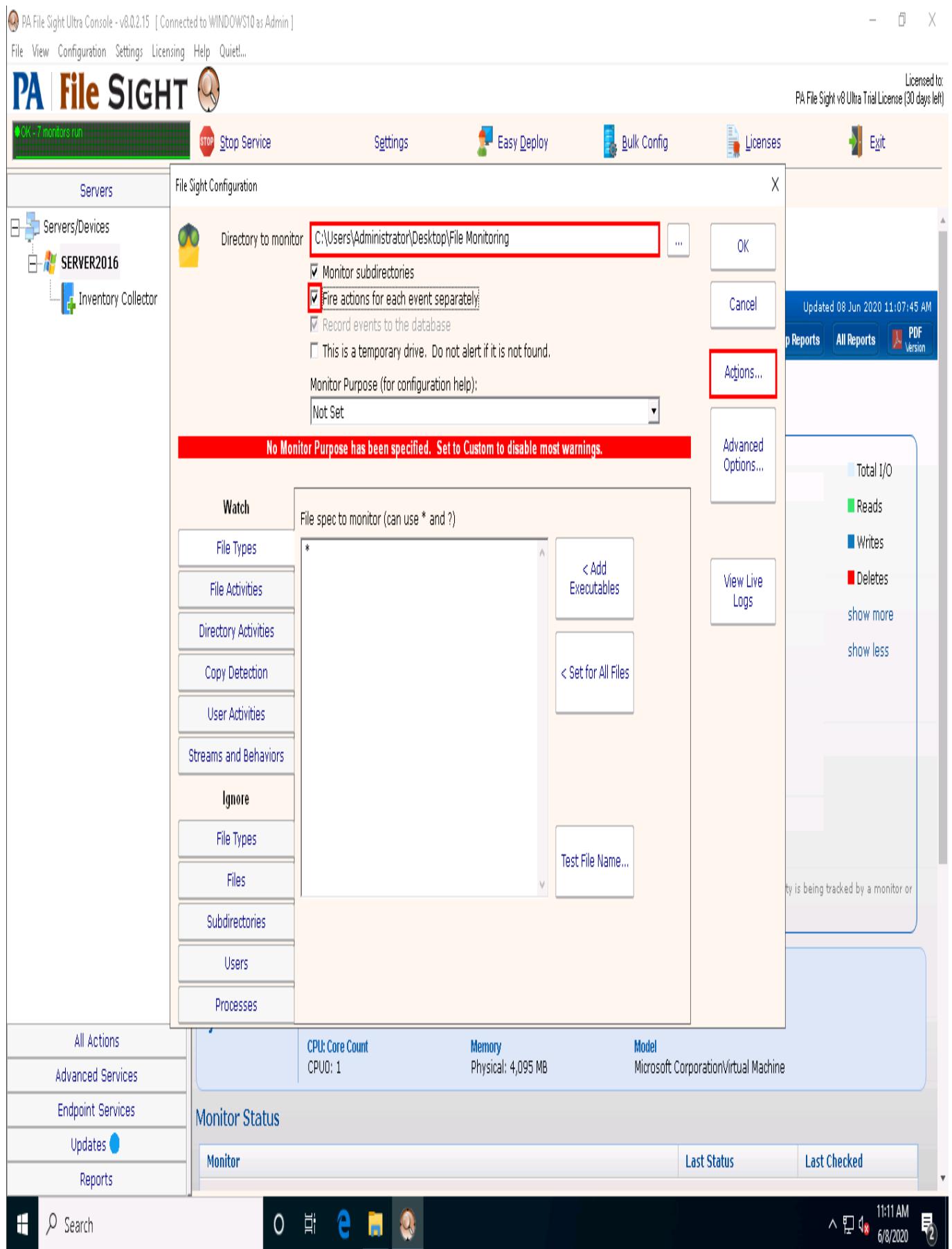
Monitor Status

Monitor	Last Status	Last Checked

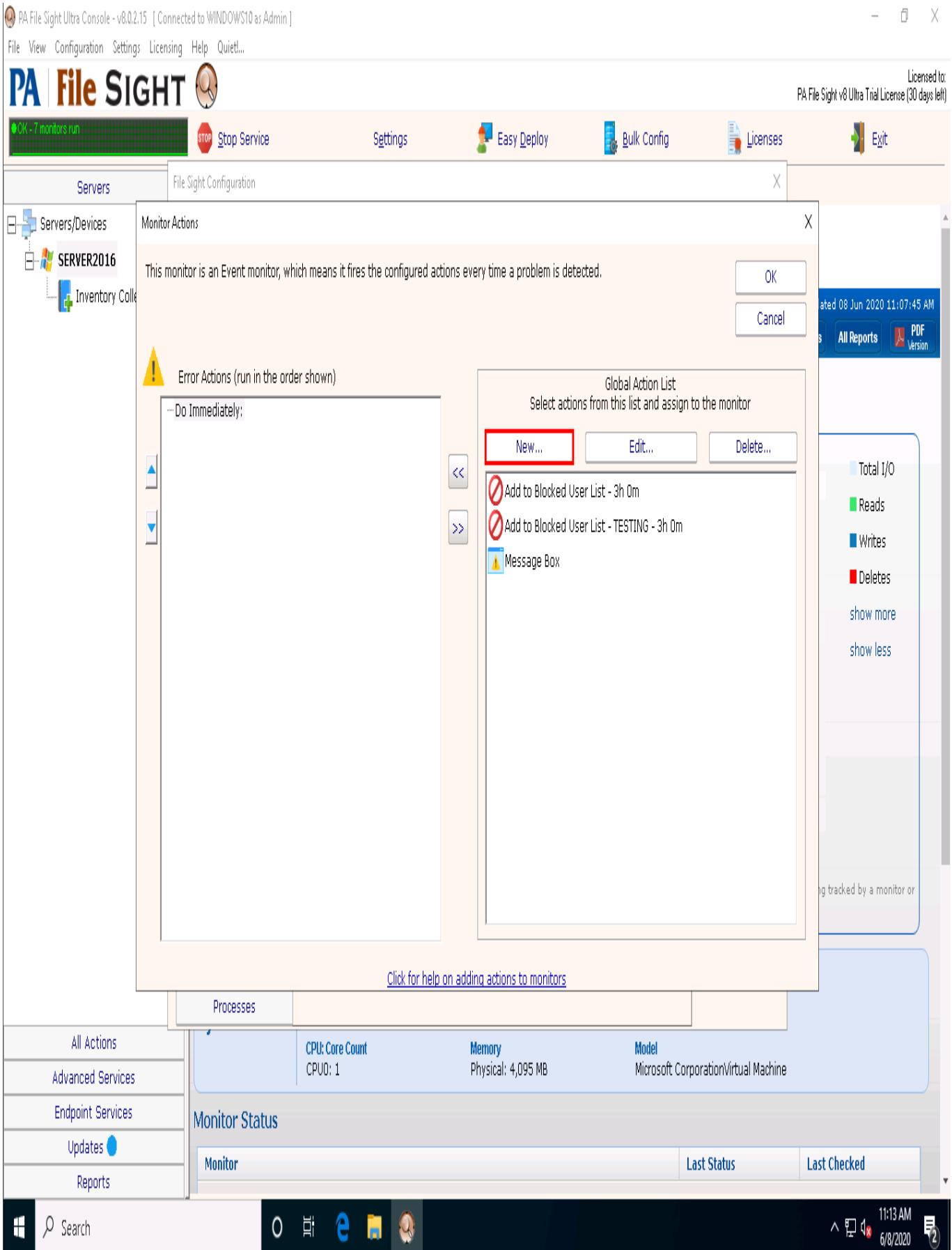


26. The **File Sight Configuration** window appears; click the **Browse** button to provide a path for directory monitoring for the **SERVER2016** machine (here, **C:\users\Administrator\Desktop\File Monitoring**) and tick the **Fire actions for each event separately** checkbox.

27. Choose **Audit file activity** from the **Monitor Purpose (for configuration help)** drop-down list, and then click **Actions**.



28. The **Monitor Actions** window appears; click **New** under **Global Action List**.



29. The **Add New Action** window appears. Select the **Action List** icon and click **OK**.

File View Configuration Settings Licensing Help Quiet...

Licensed to:
PA File Sight v8 Ultra Trial License (30 days left)

STOP Stop Service

Settings **Easy Deploy** **Bulk Config** **Licenses** **Exit**

Servers **File Sight Configuration**

Monitor Actions

This monitor is an Event monitor, which means it fires the configured actions every time a problem is detected.

Error Actions (run

Add New Action

Select an action from the list below

Available Action Types

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.

Processes

All Actions Advanced Services Endpoint Services Updates Reports

CPU: Core Count CPU: 1 Memory Physical: 4,095 MB Model Microsoft Corporation/Virtual Machine

Monitor Status

Monitor	Last Status	Last Checked
---------	-------------	--------------

Search

11:15 AM 6/8/2020

30. The **Action List** window appears. Type a description in the **Description** field and click **Add** to choose actions.



STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Servers

File Sight Configuration

X



Monitor Actions

This monitor is an Event monitor, which means it fires the configured actions every time a problem is detected.

OK

Cancel

OK

Cancel

Schedule...

Created 08 Jun 2020 11:07:45 AM

All Reports PDF Version

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

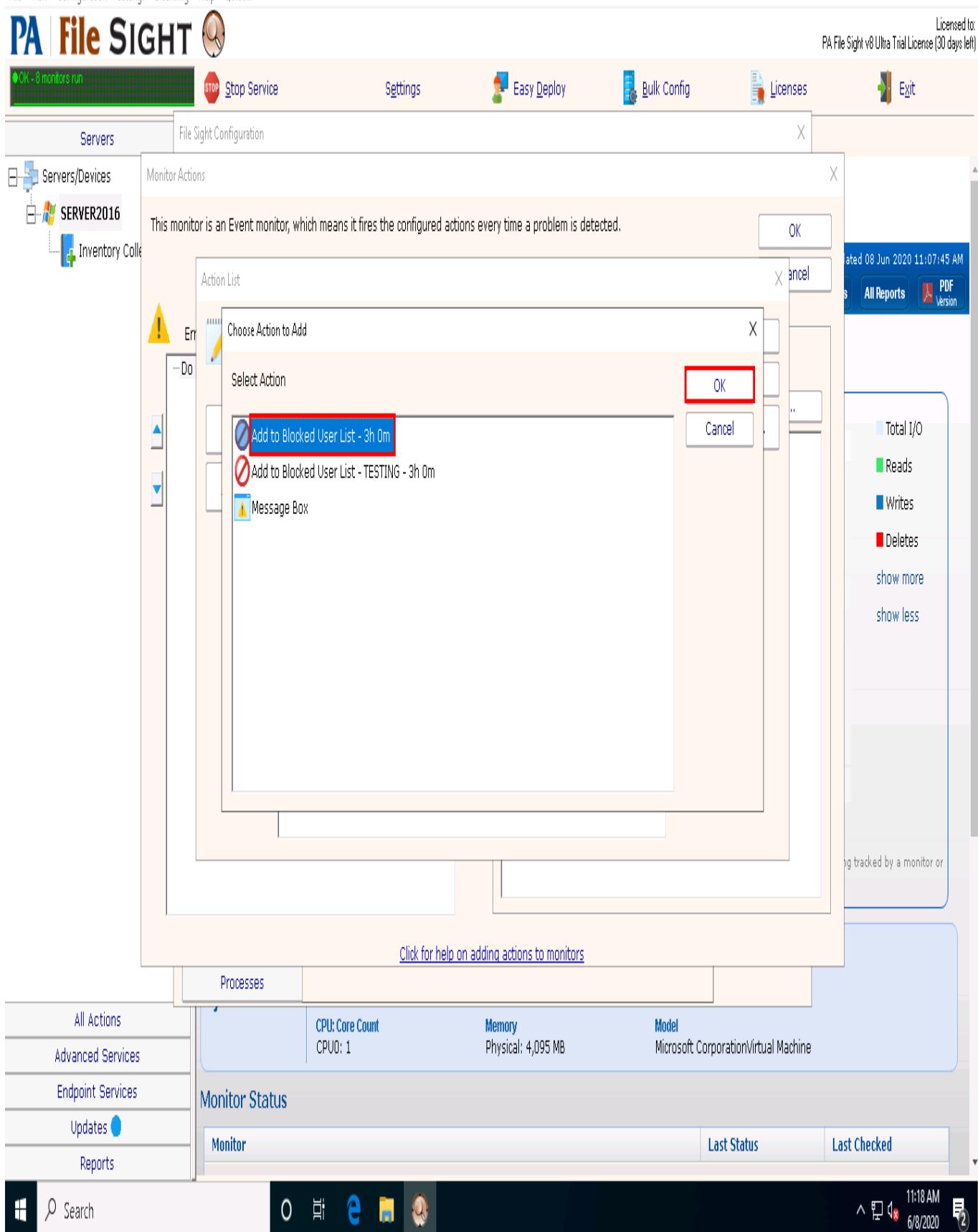
X

X

X

X

X



32. Click **OK** in the **Action List** window.
33. The **Monitor Actions** window appears; choose the newly created action (here, **Monitoring File**); and then click the << icon to add the action.



STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Servers

File Sight Configuration

X



Monitor Actions

This monitor is an Event monitor, which means it fires the configured actions every time a problem is detected.

OK

Cancel



Error Actions (run in the order shown)

Do Immediately:

Global Action List
Select actions from this list and assign to the monitor

New...

Edit...

Delete...

- Add to Blocked User List - 3h 0m
- Add to Blocked User List - TESTING - 3h 0m
- Message Box
- Monitoring File

Total I/O

Reads

Writes

Deletes

show more

show less

Click for help on adding actions to monitors

Processes

CPU: Core Count

CPU: 1

Memory

Physical: 4,095 MB

Model

Microsoft Corporation\Virtual Machine

Monitor Status

Monitor

Last Status

Last Checked

11:19 AM
6/8/2020

34. Once the action is added to the **Monitor Actions** window, click **OK**.



STOP Stop Service Settings Easy Deploy Bulk Config Licenses Exit

Servers File Sight Configuration

Monitors

This monitor is an Event monitor, which means it fires the configured actions every time a problem is detected.

Error Actions (run in the order shown)

- Do Immediately:
 - Monitoring File

Global Action List
Select actions from this list and assign to the monitor

New... Edit... Delete...

Add to Blocked User List - 3h 0m
Add to Blocked User List - TESTING - 3h 0m
Message Box
Monitoring File

Click for help on adding actions to monitors

Processes

All Actions	CPU: Core Count	Memory	Model
Advanced Services	CPU: 1	Physical: 4,095 MB	Microsoft Corporation\Virtual Machine

Monitor Status

Monitor	Last Status	Last Checked

Windows Start Search Task View Internet Explorer File Explorer File Sight

11:21 AM 6/8/2020

Total I/O
Reads
Writes
Deletes
show more
show less

35. In the **File Sight Configuration** window, click the **File Activities** tab and check the **Existing file is written to** and **Ignore file appends (this is useful for monitoring log file integrity)** options. Leave the other settings to default and click **OK**.



STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Servers

Servers/Devices
 SERVER2016
 Inventory Collector

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): Not Set

No Monitor Purpose has been specified. Set to Custom to disable most warnings.

Watch

File Types
 File Activities (highlighted with red box)
 Directory Activities
 Copy Detection
 User Activities
 Streams and Behaviors
 Ignore

File Activities (highlighted with red box):

- 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 renamed
- Existing file is written to
 - Ignore file appends (this is useful for monitoring log file integrity)
- File is moved
- File is renamed
 - For all checked actions, watch:
 - Just successful actions
 - Just failed actions
 - Both successful and failed
- File owner changed
- File access permissions changed
- File audit settings changed

Fire actions if the above file activities occur

All Actions
 Advanced Services
 Endpoint Services
 Updates
 Reports

CPU: Core Count: CPU0: 1
Memory: Physical: 4,095 MB
Model: Microsoft Corporation\Virtual Machine

Monitor Status

Monitor	Last Status	Last Checked

Windows Start Search Task View Home e File Sight 11:23 AM 6/8/2020

36. Under the **SERVER2016** node, File Sight Directory Monitoring will be added, as shown in the screenshot. Click **Apply**, and then right-click on the **File Monitoring** node and click **Run Now!** from the context menu.



STOP Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

Servers

- Servers/Devices
- SERVER2016**
- Watch C:\Users\Adminis
- Inventory Coll...

Directory to monitor: C:\Users\Administrator\Desktop\File Monitoring\

Monitor subdirectories
 Fire actions for each event separately
 Record events to the database

Run Now! Please specify. Set to Custom to disable most warnings.

Disable Monitor
Immediate Maintenance: Pause Monitoring ...
Rename Monitor
Copy Monitor
Custom Properties ...
Template Operations
Run Ad Hoc Report

Current Status: Scheduled
Last Run: Never/Reset
Next Run: 08 Jun 2020 11:26:15 AM

Copy Detection

- User Activities
- Streams and Behaviors
- Ignore
- File Types
- Files
- Subdirectories
- Users
- Processes

< Add Executables
< Set for All Files
Test File Name...

All Actions
Advanced Services
Endpoint Services
Updates
Reports

Search

11:26 AM
6/8/2020

37. Click the **SERVER2016** node to view the dashboard. Scroll down in the dashboard; observe that the File Monitoring directory is being monitored.



Servers

OK - 15 monitors run

Stop Service

Settings

Easy Deploy

Bulk Config

Licenses

Exit

< Back Open in Browser Print

NT AUTHORITY\SYSTEM [fe80::e564:31cb:49c5:7bc7]

2.5 5

This chart is showing real-time file activity counts for all monitored drives, whether the activity is being tracked by a monitor or not.

System Details

Uptime 0 days, 7 hours, 55 minutes	Operating System Microsoft Windows Server 2016 Standard 10.0.14393	CPU Intel(R) Xeon(R) Gold 6230 CPU @ 2.10GHz (64 bit, None)
CPU: Core Count CPU: 1	Memory Physical: 4,095 MB	Model Microsoft CorporationVirtual Machine

Monitor Status

Monitor	Last Status	Last Checked
Inventory Collector Probe methods: WMI	OK	6/8/2020 11:07:44 AM
Watch C:\Users\Administrator\Desktop\File Monitoring\	OK	6/8/2020 11:27:57 AM

Recent Alerts

Full History: 1 day | 5 days | 15 days | 30 days | 60 days

No recent alerts to display

Acknowledge: All for Computer/Device | All Shown Above | Refresh

All Actions

Advanced Services

Endpoint Services

Updates

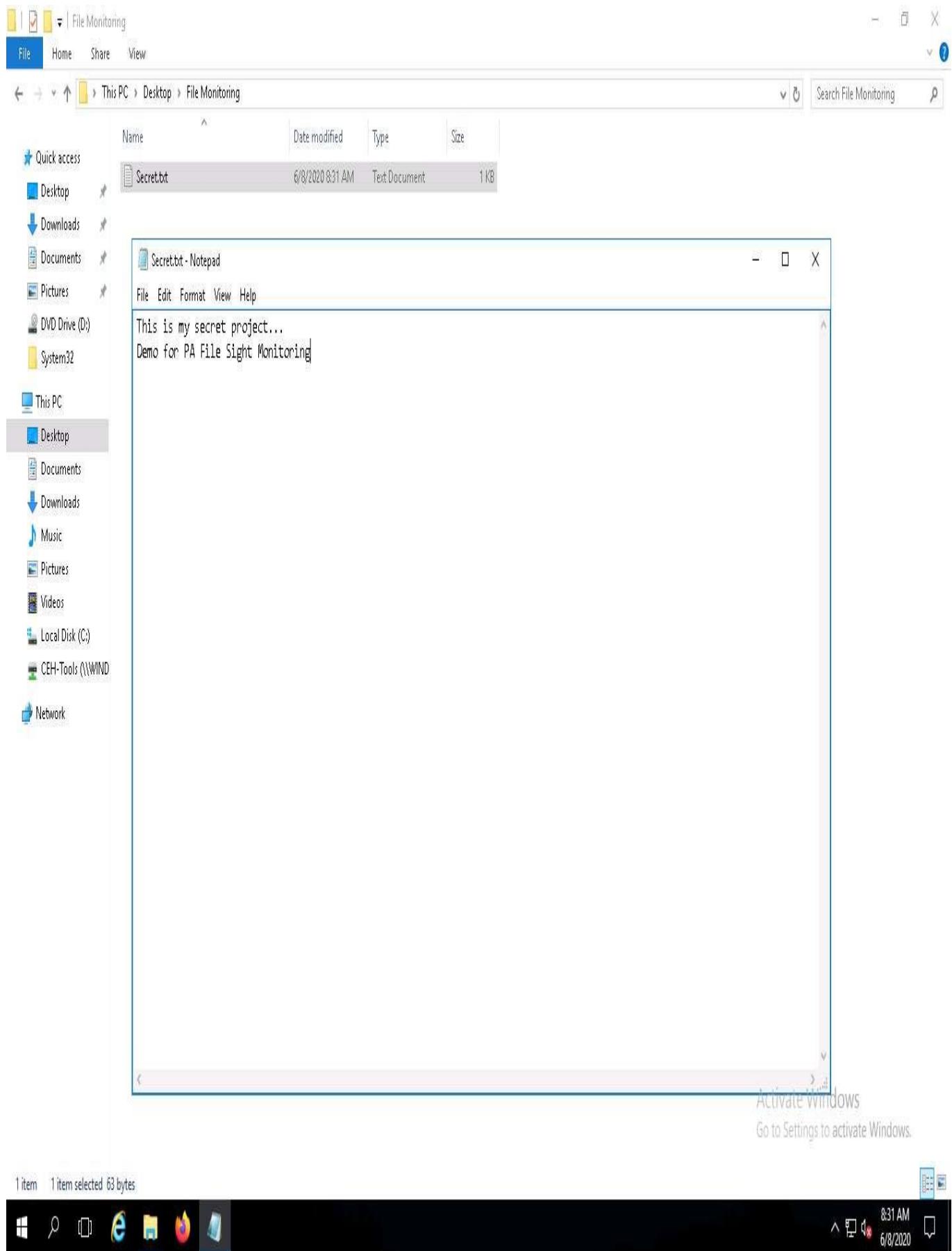
Reports

This status report will always be available at [https://Windows10:8000/STATUS_DEVICE_\(2\)/index.htm?PROJ=2](https://Windows10:8000/STATUS_DEVICE_(2)/index.htm?PROJ=2)
Created in 2 ms

Generated by PA File Sight v8.0.2

Search 11:28 AM 6/8/2020

38. Click [Windows Server 2016](#) to switch to the **Windows Server 2016** machine Click [Ctrl+Alt+Delete](#) to activate the machine, by default, **CEH\Administrator** account is selected, click **Pa\$\$w0rd** to enter the password and press **Enter**. Open **Secret.txt** in the **File Directory** on **Desktop**, modify some of the text in the file, and then **Save** and close the file.



39. Click [Windows 10](#) to switch back to the **Windows 10** machine and observe that PA File Sight has recorded some activity in the notepad file, as shown in the screenshot.
 40. The software even shows the File Accessed/min in the graphical method, as shown in the screenshot.
 41. Click on the **notepad.exe** link to view the activities done by the user.



OK - 179 monitors run

Stop Service **Settings** **Easy Deploy** **Bulk Config** **Licenses** **Exit**

Servers

< Back Open in Browser Print

YOUR LOGO HERE

To change or remove this logo, go to:
Settings > Report Settings

Updated 08 Jun 2020 11:27:56 AM

SERVER2016 SERVER2016 remote satellite

Group Reports All Reports PDF Version

System Information

Hourly Alert Rate

01 Jun 08 Jun

Bytes Written (MB)/min

0.001MB 0.000MB

11:26 AM 11:27 AM 11:28 AM 11:29 AM
08 Jun 08 Jun 08 Jun 08 Jun

Bytes Read (MB)/min

0.001MB 0.000MB

11:26 AM 11:27 AM 11:28 AM 11:29 AM
08 Jun 08 Jun 08 Jun 08 Jun

Files Accessed/min

5 0

11:26 AM 11:27 AM 11:28 AM 11:29 AM
08 Jun 08 Jun 08 Jun 08 Jun

15 Minute Total I/O Operations (Logarithmic Scale)

User Process	Total I/O
CEH\Administrator [explorer.exe]	~100
NT AUTHORITY\SYSTEM [LogonUI.exe]	~100
NT AUTHORITY\SYSTEM [svchost.exe]	~80
CEH\Administrator [svchost.exe]	~70
CEH\Administrator [notepad.exe]	~70
NT AUTHORITY\LOCAL SERVICE [svchost.exe]	~60
NT AUTHORITY\SYSTEM [taskhostw.exe]	~60
NT AUTHORITY\SYSTEM [PAAPIProxy32.exe]	~60
CEH\Administrator [taskhostw.exe]	~40
NT AUTHORITY\SYSTEM [dfsrs.exe]	~30

Reads Writes Deletes

show more show less

Activate Windows

This chart is showing real-time file activity counts for all monitored drives, whether the activity is being tracked by a monitor or not.

All Actions Advanced Services Endpoint Services Updates Reports

Search

11:32 AM 6/8/2020

42. The **CEH\Administrator notepad.exe** window appears. If it shows a blank window, then click [Windows Server 2016](#) to switch to the **Windows Server 2016** machine, type some content into the **Secret.txt** file, save the file, and then immediately click [Windows 10](#) to switch back to the **Windows 10** machine to view the activity.

43. If you have added some text in the Secret.txt file, you can view that in the activity window.

PA File Sight Ultra Console - v8.0.2.15 [Connected to WINDOWS10 as Admin]

File View Configuration Settings Licensing Help Quiet...

PA File SIGHT

OK - 179 monitors run

STOP Stop Service Settings Easy Deploy Bulk Config Licenses Exit

Servers < Back Open in Browser Print

To change or remove this logo, go to: Settings > Report Settings

YOUR LOGO HERE

Updated 08 Jun 2020 11:27:56 AM

Group Reports All Reports PDF Version

SERVER2016 SERVER2016 remote satellite

System Information CEH\Administrator [notepad.exe] Close

Time Operation File

11:34:56 AM Written C:\Users\Administrator\Desktop\File Monitoring\Secret.txt

Hourly

01 Jun

Files A

11:26 AM 08 Jun 11:27 AM 08 Jun

Total I/O

Reads Writes Deletes

show more show less

All Actions Advanced Services Endpoint Services Updates Reports

Activate Windows

This chart is showing real-time file activity counts for all monitored drives, whether the activity is being tracked by a monitor or not.

1 100

11:35 AM 6/8/2020

Windows Search Task View Edge File Explorer File Sight 11:35 AM 6/8/2020

The screenshot shows the PA File Sight Ultra Console interface. The main window displays a 'System Information' panel for 'CEH\Administrator [notepad.exe]' with a log entry for a file write operation at 11:34:56 AM on June 8th. Below this are two charts: 'Hourly' and 'Files A'. The 'Hourly' chart shows no activity for the day of the log entry. The 'Files A' chart shows activity starting at 11:26 AM, with a peak at 11:27 AM. A legend on the right indicates 'Total I/O' with 'Reads' (green), 'Writes' (blue), and 'Deletes' (red). A sidebar on the left lists navigation options: All Actions, Advanced Services, Endpoint Services, Updates (highlighted with a blue dot), and Reports. The status bar at the bottom shows the date and time as 6/8/2020 and 11:35 AM respectively.

44. Click [Windows Server 2016](#) to switch back to the **Windows Server 2016** machine and delete the **Secret.txt** file, then click [Windows 10](#) to switch back to the **Windows 10** machine and scroll down to view the **Recent Alerts** section; you will find that the file has been deleted.
45. You can see all the actions performed on that file.

If you do not see the alerts, then click **Refresh** button to update alerts.



User Account added to Blocked User List.

Stop Service **Settings** **Easy Deploy** **Bulk Config** **Licenses** **Exit**

Servers	Open in Browser	Print									
Servers/Devices <ul style="list-style-type: none"> SERVER2016 <ul style="list-style-type: none"> Watch C:\Users\Administr... Inventory Collector 	0 days, 7 hours, 30 minutes System Details Microsoft Windows Server 2016 Standard 10.0.14393 CPU: Core Count 1 CPU0: 1 Monitor Status <table border="1"> <thead> <tr> <th>Monitor</th> <th>Last Status</th> <th>Last Checked</th> </tr> </thead> <tbody> <tr> <td>Inventory Collector Probe methods: WMI</td> <td>OK</td> <td>6/8/2020 11:07:44 AM</td> </tr> <tr> <td>Watch C:\Users\Administrator\Desktop\file Monitoring\ The following activities have occurred: Op: Deleted File: C:\Users\Administrator\Desktop\file Monitoring\Secret.txt User: CEH\Administrator Source: fonts [127.0.0.1] App: explorer.exe [More...]</td> <td>Alert</td> <td>6/8/2020 11:40:44 AM</td> </tr> </tbody> </table> Recent Alerts Full History: 1 day 5 days 15 days 30 days 60 days Acknowledge: All for Computer/Device All Shown Above Refresh	Monitor	Last Status	Last Checked	Inventory Collector Probe methods: WMI	OK	6/8/2020 11:07:44 AM	Watch C:\Users\Administrator\Desktop\file Monitoring\ The following activities have occurred: Op: Deleted File: C:\Users\Administrator\Desktop\file Monitoring\Secret.txt User: CEH\Administrator Source: fonts [127.0.0.1] App: explorer.exe [More...]	Alert	6/8/2020 11:40:44 AM	Intel(R) Xeon(R) Gold 6230 CPU @ 2.10GHz (64 bit, None) Model Microsoft CorporationVirtual Machine
Monitor	Last Status	Last Checked									
Inventory Collector Probe methods: WMI	OK	6/8/2020 11:07:44 AM									
Watch C:\Users\Administrator\Desktop\file Monitoring\ The following activities have occurred: Op: Deleted File: C:\Users\Administrator\Desktop\file Monitoring\Secret.txt User: CEH\Administrator Source: fonts [127.0.0.1] App: explorer.exe [More...]	Alert	6/8/2020 11:40:44 AM									

All Actions

Advanced Services

Endpoint Services

Updates

Reports

Search

11:43 AM 6/8/2020

46. This is how to monitor the file integrity using PA File Sight.
47. Close all open windows.
48. You can also use other file and folder integrity checking tools such as **Tripwire File Integrity and Change Manager** (<https://www.tripwire.com>), **Netwrix**

Auditor (<https://www.netwrix.com>), **Verisys** (<https://www.ionx.co.uk>), or **CSP File Integrity Checker** (<https://www.cspsecurity.com>) to perform file and folder monitoring.

Task 8: Perform Device Driver Monitoring using DriverView and Driver Reviver

When the user downloads infected drivers from untrusted sources, the system installs malware along with the device drivers; malware uses these drivers as a shield to avoid detection. One can scan for suspicious device drivers using tools such as DriverView and Driver Reviver that verify if they are genuine and downloaded from the publisher's original site.

DriverView The DriverView utility displays a list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as the load address of the driver, description, version, product name, and developer.

Driver Reviver Without proper drivers, computers start to misbehave. Sometimes updating the drivers using conventional methods can be a daunting task. Outdated drivers are more vulnerable to hacking and can lead to a breach in the system. Driver Reviver provides an effective way of scanning your PC to identify out of date drivers. Driver Reviver can quickly and easily update these drivers to restore optimum performance to your PC and its hardware and extend its life.

An ethical hacker and penetration tester must scan the system for suspicious device drivers and make sure that the systems runs smoothly by ensuring that all outdated drivers are updated and that the system processes optimized to keep the performance of the system at its peak.

1. On the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\DriverView** and double-click **DriverView.exe** to launch the application.



2. The **DriverView** main window appears with a list of the installed drivers on your system, as shown in the screenshot.



File Edit View Options Help

- X



Driver Name	Address	End Address	Size	Load Count	Index	File Type	Description	Version	Company	Product Name	Modified Date	Cr.
3ware.sys	0x457D0000	0x457EE000	0x0001e000	1	61	System Driver	LSI 3ware SCSI Storport Driver	5.1.0.51	LSI	LSI 3ware RAID Controller	N/A	N/
ACPI.sys	0x44800000	0x4499C000	0x0001c000	1	24	System Driver	ACPI Driver for NT	10.0.18362.329	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
acpiex.sys	0x44830000	0x44B55000	0x00025000	1	21	Dynamic Link Li...	ACPIEx Driver	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
ADP8000.SYS	0x45E30000	0x4608C000	0x0025c000	1	89	System Driver	PMC-Sierra Storport Driver For SPC&...	1.3.0.10769	PMC-Sierra	PMC-Sierra HBA Controller	N/A	N/
afd.sys	0x478F0000	0x47997000	0x000a7000	1	144	System Driver	Ancillary Function Driver for WinSock	10.0.18362.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
afunix.sys	0x47800000	0x478E3000	0x00013000	1	143	System Driver	AF_UNIX socket provider	10.0.18362.693	Microsoft Corpora...	Microsoft® Windows® Oper...	4/14/2020 5:11:52 ...	4/1
ahcache.sys	0x47CF0000	0x47D3F000	0x0004f000	1	158	System Driver	Application Compatibility Cache	10.0.18362.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
amdsata.sys	0x457F0000	0x4580F000	0x0001f000	1	62	System Driver	AHCI 1.3 Device Driver	1.1.3.277	Advanced Micro D...	AHCI 1.3 Device Driver	N/A	N/
amdsbs.sys	0x45820000	0x45887000	0x00067000	1	64	System Driver	AMD Technology AHCI Compatible C...	3.7.1540.43	AMD Technologies...	AMD Technology AHCI Comp...	N/A	N/
amdkata.sys	0x45810000	0x4581C000	0x0000c000	1	63	System Driver	Storage Filter Driver	1.1.3.277	Advanced Micro D...	Storage Filter Driver	N/A	N/
arcgas.sys	0x45890000	0x458B5000	0x00025000	1	65	System Driver	Adaptec SAS RAID WS03 Driver	7.5.0.32048	PMC-Sierra, Inc.	Adaptec RAID Controller	N/A	N/
atapi.sys	0x45D80000	0x45D8D000	0x0000d000	1	85	System Driver	ATAPI IDE Miniport Driver	10.0.18362.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
ataport.SYS	0x45D90000	0x45DCB000	0x0003b000	1	86	System Driver	ATAPI Driver Extension	10.0.18362.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
bam.sys	0x47CD0000	0x47CE6000	0x00016000	1	157	System Driver	BAM Kernel Driver	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
BasicDisplay.sys	0x477A0000	0x477B6000	0x00016000	1	136	Display Driver	Microsoft Basic Display Driver	10.0.18362.329	Microsoft Corpora...	Microsoft® Windows® Oper...	4/14/2020 5:10:17 ...	4/1
BasicRender.sys	0x477C0000	0x477D1000	0x00011000	1	137	Display Driver	Microsoft Basic Render Driver	10.0.18362.329	Microsoft Corpora...	Microsoft® Windows® Oper...	4/14/2020 5:10:18 ...	4/1
Beep.SYS	0x481B0000	0x481BA000	0x0000a000	1	133	System Driver	BEEP Driver	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
BOOTVID.dll	0x443A0000	0x443AB000	0x0000b000	1	10	Display Driver	VGA Boot Driver	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	3/19/2019 12:45:20...	3/1
bowser.sys	0x484F0000	0x48B15000	0x00025000	1	203	System Driver	NT Lan Manager Datagram Receiver ...	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
bttfilt.sys	0x46BE0000	0x46BEF000	0x0000f000	1	113	System Driver	VHD BTTF Filter Driver	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
bxbvda.sys	0x45460000	0x454E9000	0x00089000	1	53	Network Driver	QLogic Gigabit Ethernet VBD	7.12.31.105	QLogic Corporation	QLogic Gigabit Ethernet	N/A	N/
cdd.dll	0x63260000	0x632A8000	0x00048000	1	194	Display Driver	Canonical Display Driver	10.0.18362.719	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
cdrom.sys	0x48130000	0x48160000	0x00030000	1	129	System Driver	SCSI CD-ROM Driver	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
CEA.sys	0x44BC0000	0x44BD9000	0x00019000	3	36	Dynamic Link Li...	Event Aggregation Kernel Mode Library	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
cht4sx64.sys	0x45C00000	0x45C5B000	0x0005b000	1	83	System Driver	Chelsio iSCSI Miniport Driver	6.9.12.400	Chelsio Communi...	Chelsio Communications iSC...	N/A	N/
Cl.dll	0x44560000	0x4463D000	0x000dd000	2	15	System Driver	Code Integrity Module	10.0.18362.628	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
CLASSPNP.SYS	0x45520000	0x455B8000	0x0006b000	2	55	System Driver	SCSI Class System Dll	10.0.18362.628	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
cldfilt.sys	0x48A20000	0x48A97000	0x00077000	1	200	System Driver	Cloud Files Mini Filter Driver	10.0.18362.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
CLFSS.SYS	0x44310000	0x44378000	0x00068000	4	7	System Driver	Common Log File System Driver	10.0.18362.657	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
clipsp.sys	0x443B0000	0x444B5000	0x00105000	2	12	System Driver	CLIP Service	10.0.18362.387	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
cmimcext.sys	0x44540000	0x4454E000	0x0000e000	1	13	System Driver	Kernel Configuration Manager Initial ...	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
cng.sys	0x44640000	0x446FC000	0x000bc000	15	16	System Driver	Kernel Cryptography, Next Generation	10.0.18362.295	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
CompositeBus.sys	0x47DF0000	0x47E01000	0x00011000	1	161	Dynamic Link Li...	Multi-Transport Composite Bus Enum...	10.0.18362.329	Microsoft Corpora...	Microsoft® Windows® Oper...	4/14/2020 5:10:16 ...	4/1
condrv.sys	0x48700000	0x48713000	0x00013000	1	221	System Driver	Console Driver	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
crashdump.sys	0x48090000	0x480AD000	0x0001d000	1	128	System Driver	Crash Dump Driver	10.0.18362.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
csc.sys	0x47AB0000	0x47B44000	0x00094000	1	150	System Driver	Windows Client Side Caching Driver	10.0.18362.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
dfsc.sys	0x47C80000	0x47CA0000	0x0002c000	1	156	System Driver	DPS Namespace Client Driver	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/
disk.sys	0x46EB0000	0x46ECC000	0x0001c000	1	127	System Driver	PnP Disk Driver	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N/

223 item(s), 1 Selected



Type here to search

12:31 AM
6/9/2020

3. Right-click on any driver from the list and click **Properties** to view the complete details of the driver.



File Edit View Options Help

- X

Driver Name	Address	End Address	Size	Load Count	Index	File Type	Description	Version	Company	Product Name	Modified Date	Cr.
3ware.sys	0x457D0000	0x457EE000	0x0001e000	1	61	System Driver	LSI 3ware SCSI Storport Driver	5.1.0.51	LSI	LSI 3ware RAID Controller	N/A	N.
ACPI.sys	0x44800000	0x4499C000	0x000c000	1	24	System Driver	ACPI Driver for NT	10.0.18962.329	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
acpiex.sys	0x44830000	0x44B55000	0x00025000	1	21	Dynamic Link Li...	ACPIEx Driver	10.0.18962.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
ADP8000.SYS	0x45E30000	0x4608C000	0x0025c000	1	89	System Driver	PMC-Sierra Storport Driver For SPC&...	1.3.0.10769	PMC-Sierra	PMC-Sierra HBA Controller	N/A	N.
afd.sys	0x478F0000	0x47997000	0x000a7000	1	144	System Driver	Ancillary Function Driver for WinSock	10.0.18962.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
afunix.sys	0x47998000	0x479FC000	0x00064000	1	143	System Driver	AF_UNIX socket provider	10.0.18962.693	Microsoft Corpora...	Microsoft® Windows® Oper...	4/14/2020 5:11:52 ...	4/1
Save Selected Items												
Ctrl+S												
Copy Selected Items												
Ctrl+C												
HTML Report - All Items												
HTML Report - Selected Items												
Choose Columns												
Auto Size Columns												
Ctrl+Plus												
File Properties												
F8												
Properties												
Alt+Enter												
Google Search												
Refresh												
F5												
Beep.SYS												
BOOTVID.dll												
bowserv.sys												
bttflt.sys	0x46BE0000	0x46BEF000	0x0000f000	1	113	System Driver	VHD BTTF Filter Driver	10.0.18962.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
bxbvda.sys	0x45460000	0x454E9000	0x00089000	1	53	Network Driver	QLogic Gigabit Ethernet VBD	7.12.31.105	QLogic Corporation	QLogic Gigabit Ethernet	N/A	N.
cdd.dll	0x63260000	0x632A8000	0x00048000	1	194	Display Driver	Canonical Display Driver	10.0.18962.719	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
cdrom.sys	0x48130000	0x48160000	0x00030000	1	129	System Driver	SCSI CD-ROM Driver	10.0.18962.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
CEA.sys	0x44BC0000	0x44BD9000	0x00019000	3	36	Dynamic Link Li...	Event Aggregation Kernel Mode Library	10.0.18962.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
cht4sx64.sys	0x45C00000	0x45C5B000	0x0005b000	1	83	System Driver	Chelsio iSCSI Miniport Driver	6.9.12.400	Chelsio Communi...	Chelsio Communications iSC...	N/A	N.
Cl.dll	0x44560000	0x4463D000	0x000dd000	2	15	System Driver	Code Integrity Module	10.0.18962.628	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
CLASSPNP.SYS	0x45520000	0x455B8000	0x00068000	2	55	System Driver	SCSI Class System Dll	10.0.18962.628	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
cldflt.sys	0x48A20000	0x48A97000	0x00077000	1	200	System Driver	Cloud Files Mini Filter Driver	10.0.18962.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
CLFSS.SYS	0x44310000	0x44378000	0x00068000	4	7	System Driver	Common Log File System Driver	10.0.18962.657	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
clipsp.sys	0x443B0000	0x444B5000	0x00105000	2	12	System Driver	CLIP Service	10.0.18962.387	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
cmimcext.sys	0x44540000	0x4454E000	0x0000e000	1	13	System Driver	Kernel Configuration Manager Initiali...	10.0.18962.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
cng.sys	0x44640000	0x446FC000	0x000bc000	15	16	System Driver	Kernel Cryptography, Next Generation	10.0.18962.295	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
CompositeBus.sys	0x47D0F000	0x47E01000	0x00011000	1	161	Dynamic Link Li...	Multi-Transport Composite Bus Enum...	10.0.18962.329	Microsoft Corpora...	Microsoft® Windows® Oper...	4/14/2020 5:10:16 ...	4/1
condrv.sys	0x48700000	0x48713000	0x00013000	1	221	System Driver	Console Driver	10.0.18962.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
crashdump.sys	0x48090000	0x480AD000	0x0001d000	1	128	System Driver	Crash Dump Driver	10.0.18962.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
csc.sys	0x47AB0000	0x47B44000	0x00094000	1	150	System Driver	Windows Client Side Caching Driver	10.0.18962.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
dfsc.sys	0x47C80000	0x47CA0000	0x0002c000	1	156	System Driver	DPS Namespace Client Driver	10.0.18962.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
disk.sys	0x46EB0000	0x46ECC000	0x0001c000	1	127	System Driver	PnP Disk Driver	10.0.18962.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.

223 item(s), 1 Selected



4. The **Properties** window appears with the complete details of the installed driver, as shown in the screenshot. Once the analysis is done, click **OK**.



File Edit View Options Help

- □ X

Driver Name	Address	End Address	Size	Load Count	Index	File Type	Description	Version	Company	Product Name	Modified Date	Cr.	
3ware.sys	0x457D0000	0x457EE000	0x0001e000	1	61	System Driver	LSI 3ware SCSI Storport Driver	5.1.0.51	LSI	LSI 3ware RAID Controller	N/A	N.	
ACPI.sys	0x44800000	0x4499C000	0x000c000	1	24	System Driver	ACPI Driver for NT	10.0.18362.329	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.	
acpiex.sys	0x44830000	0x44B55000	0x00025000	1	21	Dynamic Link Li...	ACPIEx Driver	10.0.18362.1	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.	
ADP8000.SYS	0x45E30000	0x4608C000	0x0025c000	1	89	System Driver	PMC-Sierra Storport Driver For SPC&...	1.3.0.10769	PMC-Sierra	PMC-Sierra HBA Controller	N/A	N.	
afd.sys	0x478F0000	0x47997000	0x000a7000	1	144	System Driver	Ancillary Function Driver for WinSock	10.0.18362.693	Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.	
afunix.sys	0x478D0000	0x478E3000	0x00013000	1	Properties	Driver Name: afunix.sys Address: 0x478D0000 End Address: 0x478E3000 Size: 0x00013000 Load Count: 1 Index: 143 File Type: System Driver Description: AF_UNIX socket provider Version: 10.0.18362.693 Company: Microsoft Corporation Product Name: Microsoft® Windows® Operating System Modified Date: 4/14/2020 5:11:52 AM Created Date: 4/14/2020 5:11:52 AM Filename: C:\WINDOWS\system32\drivers\afunix.sys File Attributes: A Service Name: afunix Service Display Name: afunix Digital Signature: OK	Properties	X	Microsoft Corpora...	Microsoft® Windows® Oper...	4/14/2020 5:11:52 ...	4/1	
ahcache.sys	0x47CF0000	0x47D3F000	0x0004f000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
amdsata.sys	0x457F0000	0x4580F000	0x0001f000	1						Advanced Micro D...	AHCI 1.3 Device Driver	N/A	N.
amdsbs.sys	0x45820000	0x45887000	0x00067000	1						AMD Technologies...	AMD Technology AHCI Comp...	N/A	N.
amdkata.sys	0x45810000	0x4581C000	0x0000c000	1						Advanced Micro D...	Storage Filter Driver	N/A	N.
arcgas.sys	0x45890000	0x45885000	0x00025000	1						PMC-Sierra, Inc.	Adaptec RAID Controller	N/A	N.
atapi.sys	0x45D80000	0x45D8D000	0x000d000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
ataport.SYS	0x45D90000	0x45DCB000	0x0003b000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
barn.sys	0x47CD0000	0x47CE6000	0x00016000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
BasicDisplay.sys	0x477A0000	0x477B6000	0x00016000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	4/14/2020 5:10:17 ...	4/1
BasicRender.sys	0x477C0000	0x477D1000	0x00011000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	4/14/2020 5:10:18 ...	4/1
Beep.SYS	0x481B0000	0x481BA000	0x0000a000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
BOOTVID.dll	0x443A0000	0x443AB000	0x0000b000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	3/19/2019 12:45:20...	3/1
bowser.sys	0x484F0000	0x48B15000	0x00025000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
bttflt.sys	0x46BE0000	0x46BEF000	0x0000f000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
bxbvda.sys	0x45460000	0x454E9000	0x00089000	1						QLogic Corporation	QLogic Gigabit Ethernet	N/A	N.
cdd.dll	0x63260000	0x632A8000	0x00048000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
cdrom.sys	0x48130000	0x48160000	0x00030000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
CEA.sys	0x44BC0000	0x44BD9000	0x00019000	3						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
cht4sx64.sys	0x45C00000	0x45C5B000	0x0005b000	1						Chelsio Communi...	Chelsio Communications iSC...	N/A	N.
Cl.dll	0x44560000	0x4463D000	0x000dd000	2						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
CLASSPNP.SYS	0x45520000	0x455B8000	0x0006b000	2						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
cldflt.sys	0x48A20000	0x48A97000	0x00077000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
CLFS.SYS	0x44310000	0x44378000	0x00068000	4						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
clipsp.sys	0x443B0000	0x444B5000	0x00105000	2						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
cmimcext.sys	0x44540000	0x4454E000	0x0000e000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
cng.sys	0x44640000	0x446FC000	0x000bc000	15						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
CompositeBus.sys	0x47DF0000	0x47E01000	0x00011000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	4/14/2020 5:10:16 ...	4/1
condrv.sys	0x48700000	0x48713000	0x00013000	1						Microsoft Corpora...	Microsoft® Windows® Oper...	N/A	N.
crashdump.sys	0x48090000	0x480AD000	0x0001d000	1						Microsoft Corpora...	Crash Dump Driver	10.0.18362.693	N/A
csc.sys	0x47AB0000	0x47B44000	0x00094000	1						Microsoft Corpora...	Windows Client Side Caching Driver	10.0.18362.693	N/A
dfsc.sys	0x47C80000	0x47CA0000	0x0002c000	1						Microsoft Corpora...	DFS Namespace Client Driver	10.0.18362.1	N/A
disk.sys	0x46EB0000	0x46ECC000	0x0001c000	1						Microsoft Corpora...	PnP Disk Driver	10.0.18362.1	N/A

223 item(s), 1 Selected

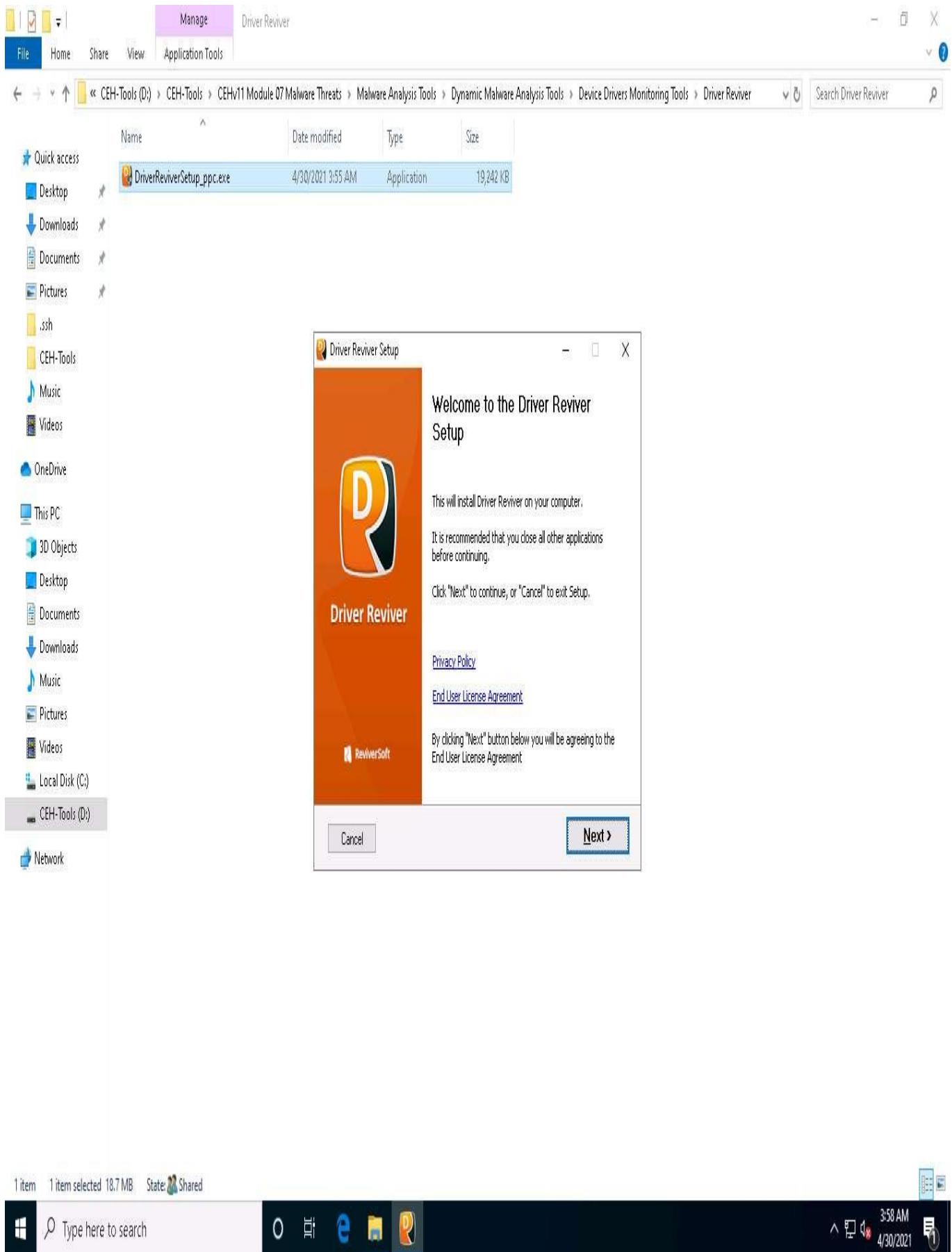


Type here to search

12:33 AM
6/9/2020

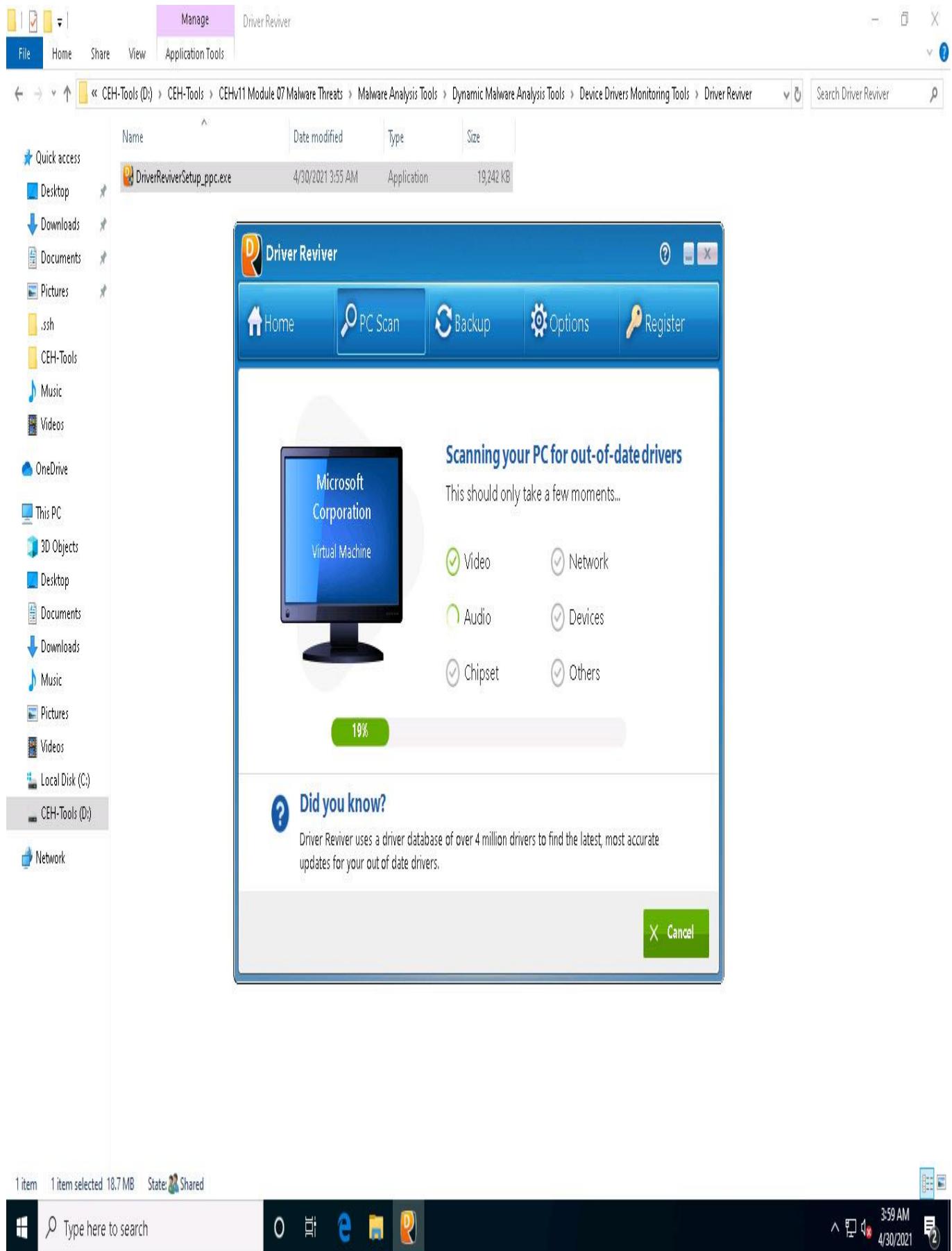
5. This is how to monitor the drivers installed on a machine. Close the **DriverView** window.
6. Now, we will see how to update system drivers and optimize the PC performance using Driver Reviver.

7. On **Windows 10**, navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Reviver**. Double-click **DriverReviverSetup.exe** to launch the setup.
8. If a **User Account Control** window appears, click **Yes**.
9. **Driver Reviver Setup** window appears, click **Next** to install the tool.

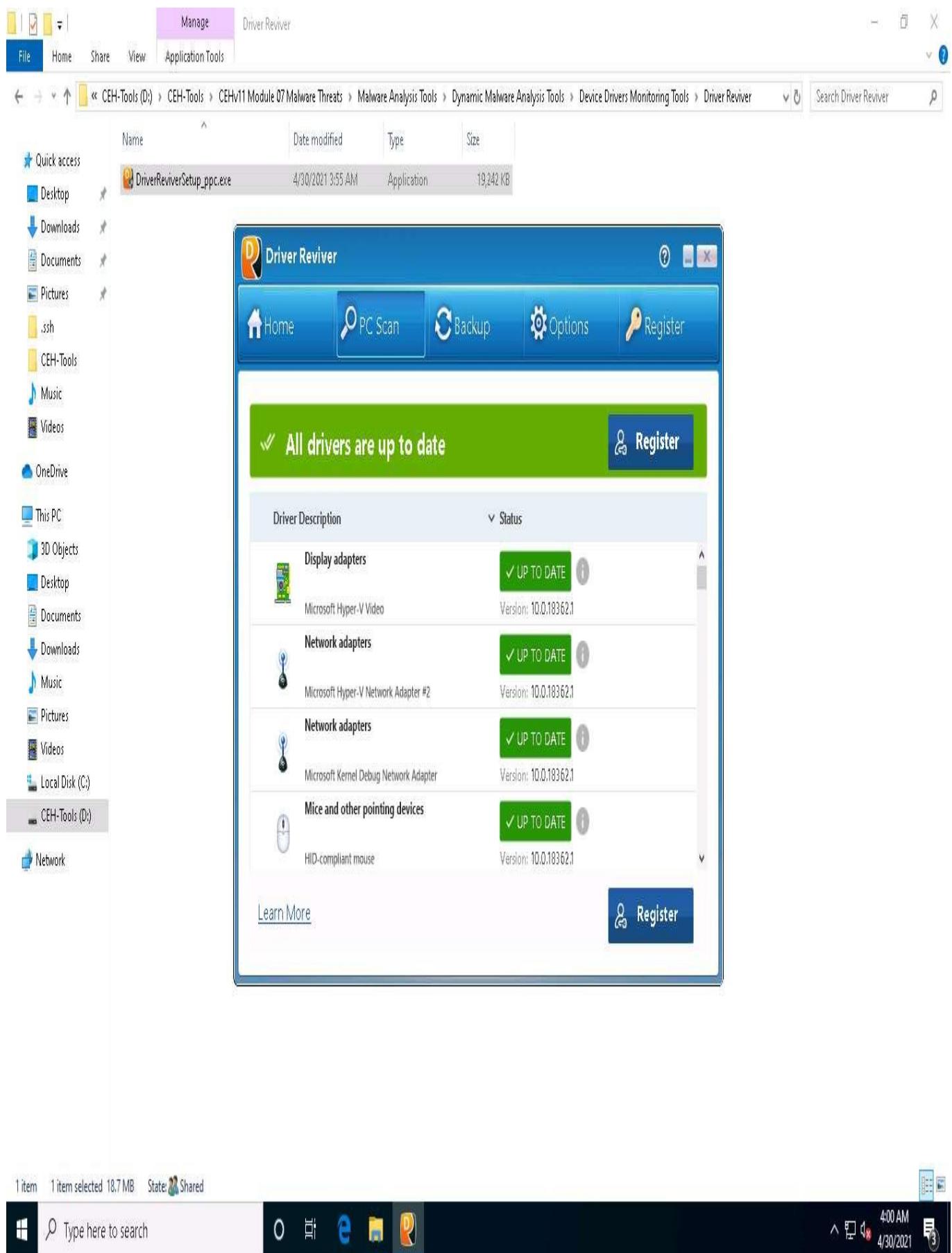


10. Installation window appears and after the completion of installation, Driver Reviver initializes the scan for drivers, as shown in the screenshot.

If a browser window opens automatically close the browser.

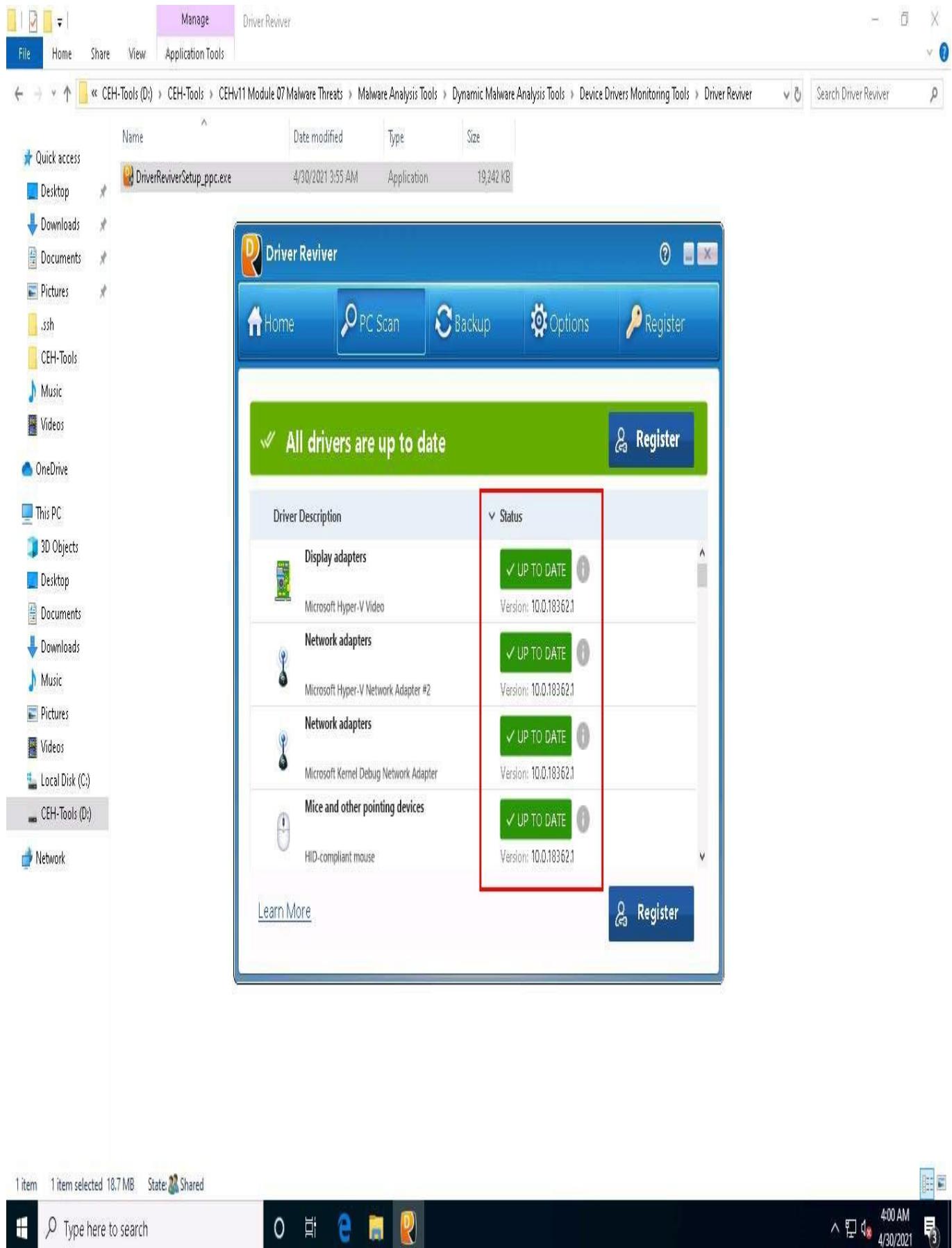


11. After the scan finishes, a list of system drivers are displayed.

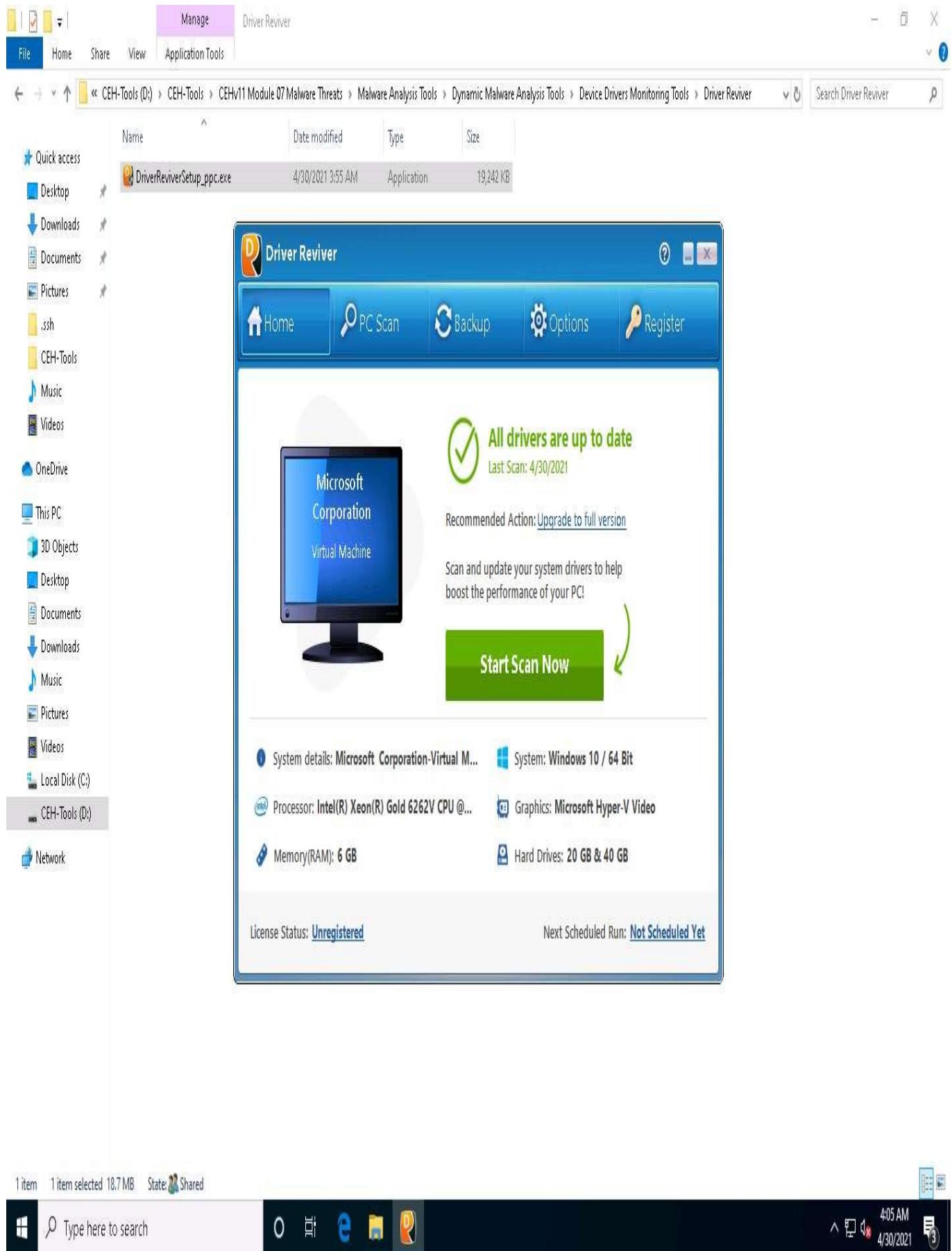


12. Along with the list of drivers you can see their **Status** as **OUTDATED** or **UP TO DATE**.

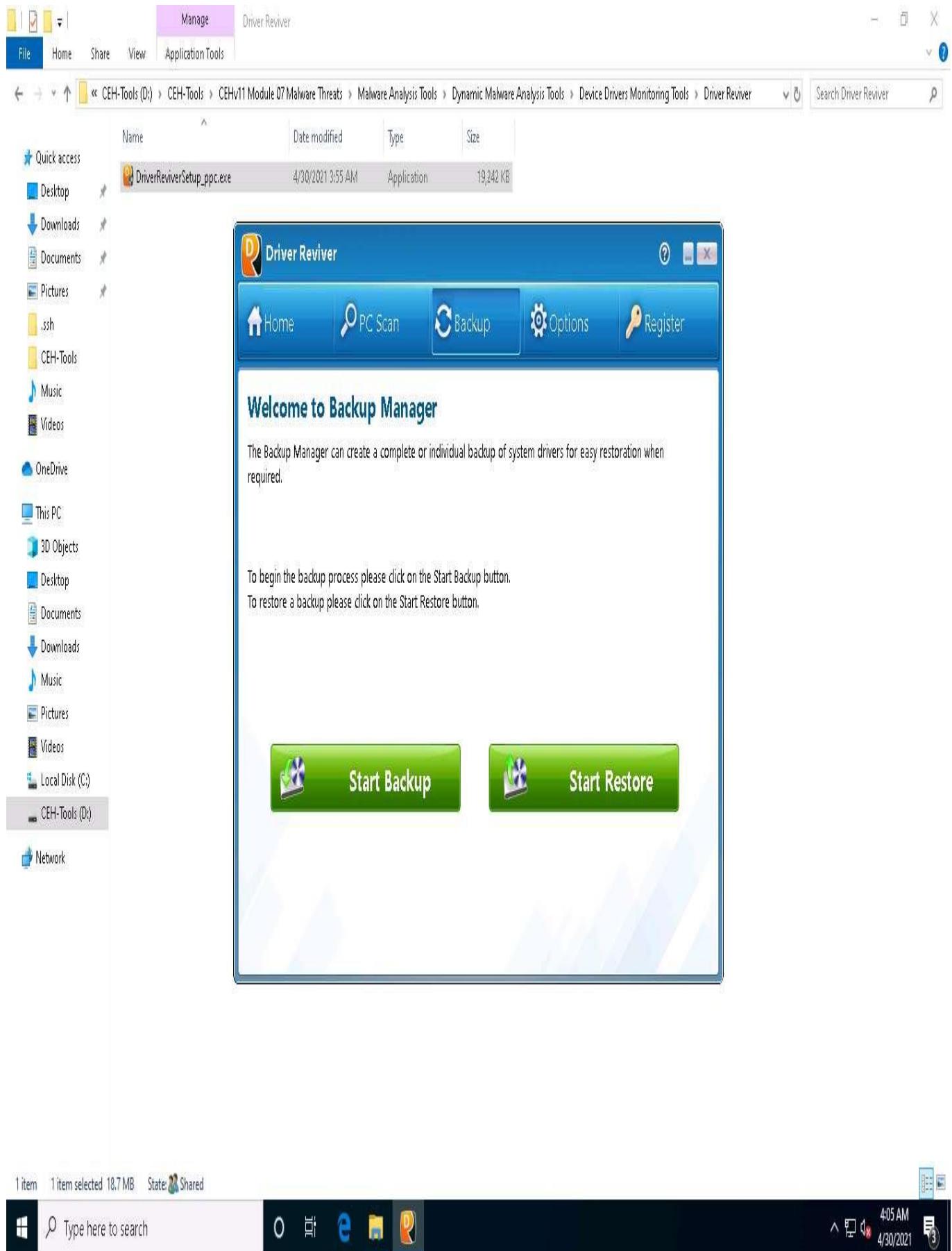
Here, all the drivers are already up to date.
The result might vary in your lab environment



13. If the drivers are outdated then you can click **Update All** button to update all the drivers.
14. Now, navigate to the **Home** tab, here you can view information such as **System details, System, Processor, Graphics, Memory(RAM) and Hard Drives**, as shown in the screenshot,



15. Navigate to the **Backup** tab, here you can create Backup or Restore the system drivers.



16. Uninstall the **Driver Reviver** software by navigating to **Control Panel** --> **Programs** --> **Uninstall a program**.

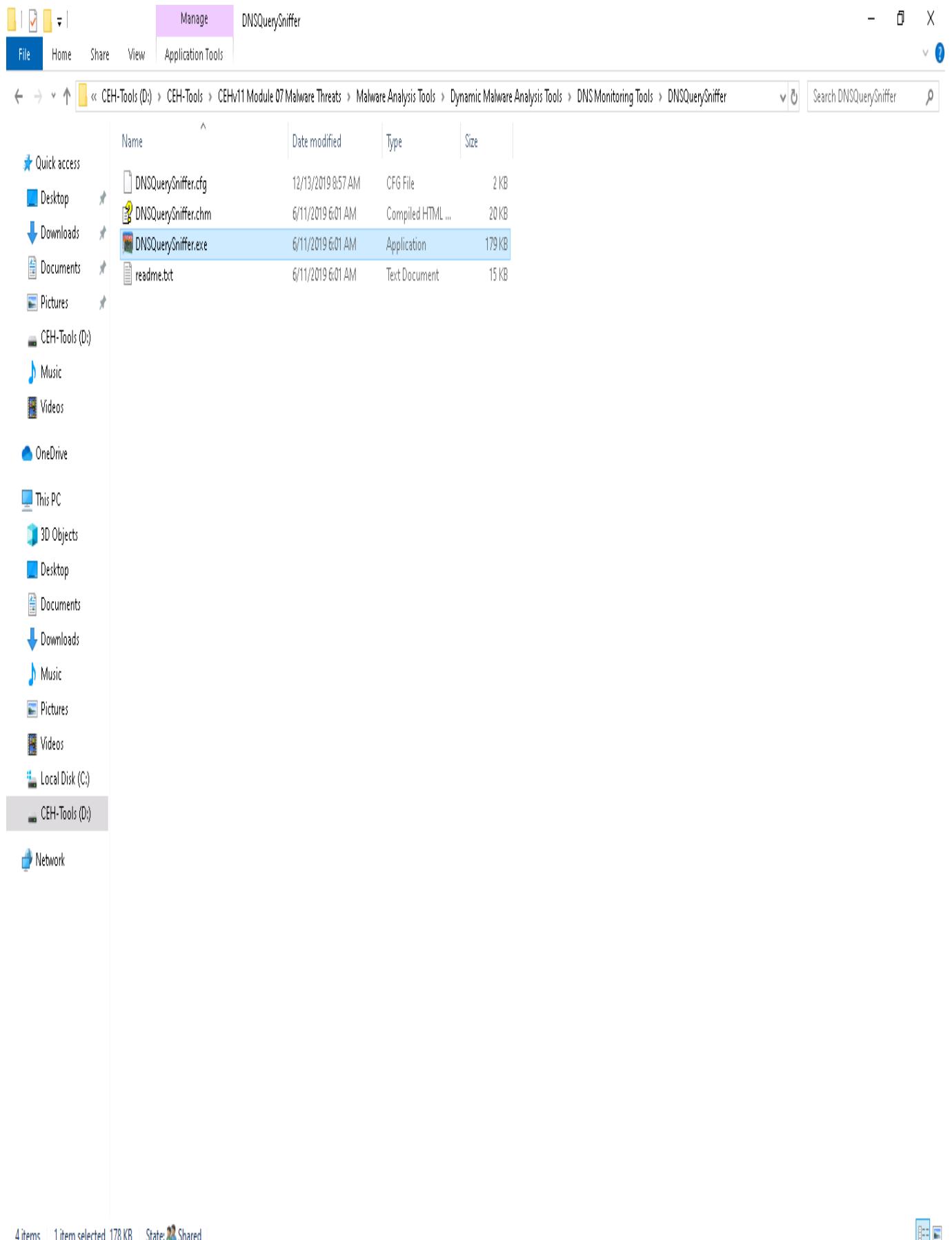
While uninstalling, remove all the files of tools from the system.

17. Close all open windows.
 18. You can also use other device driver monitoring tools such as **Driver Booster** (<https://www.iobit.com>), **Driver Easy** (<https://www.drivereeasy.com>), **Driver Fusion** (<https://treexy.com>), or **Driver Genius** (<http://www.driver-soft.com>) to perform device driver monitoring.
-

Task 9: Perform DNS Monitoring using DNSQuerySniffer

DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: Host Name, Port Number, Query ID, Request Type (A, AAAA, NS, MX, and other types), Request Time, Response Time, Duration, Response Code, Number of records, and the content of the returned DNS records. You can easily export the DNS query information to a CSV, tab-delimited, XML, or HTML file, or copy the DNS queries to the clipboard and then paste them into Excel or another spreadsheet application.

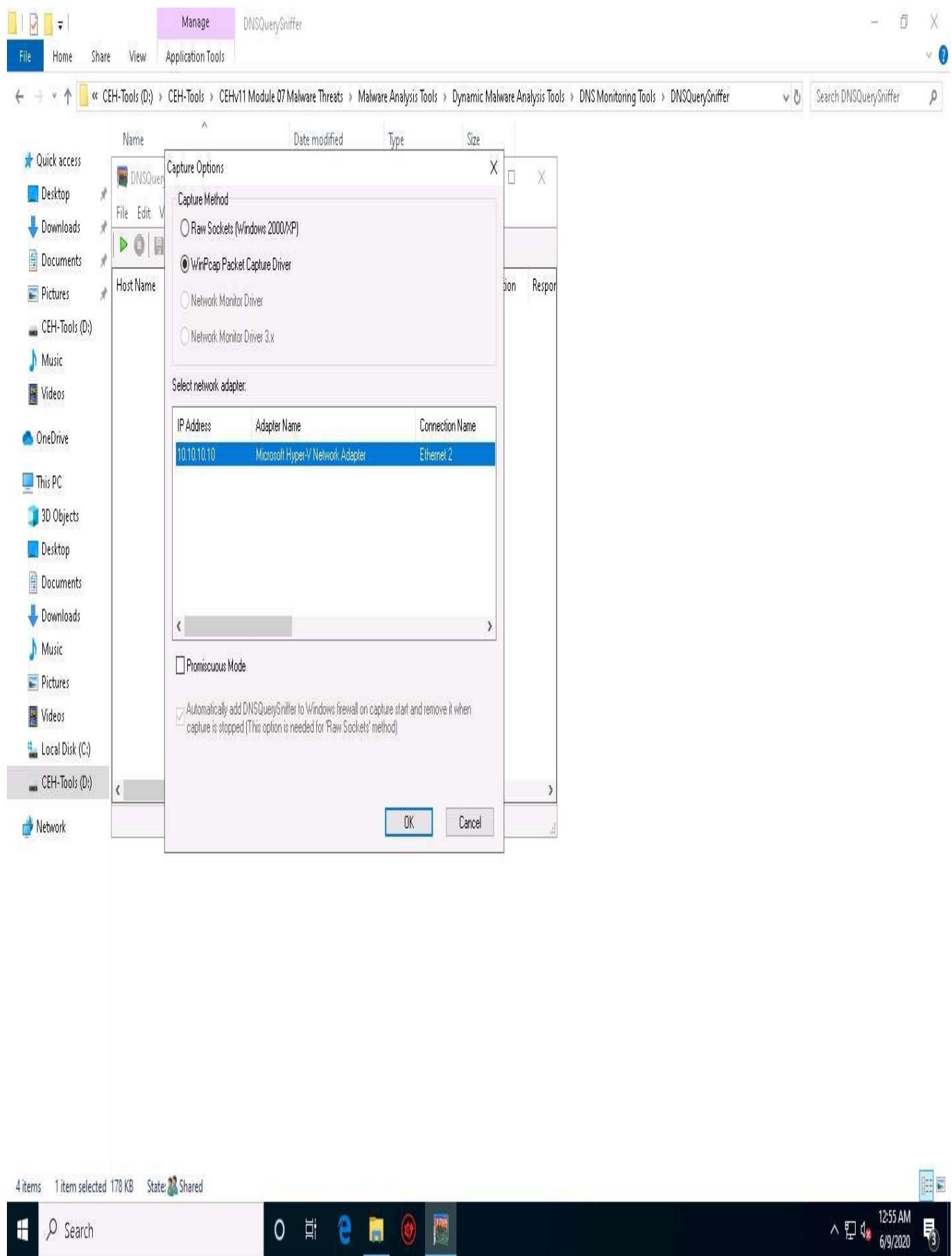
1. On the **Windows 10** machine, navigate to **D\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**, and then double-click **DNSQuerySniffer.exe**.



2. The main window of **DNSQuerySniffer** appears, along with the **Capture Options** window.

If the **Capture Options** window does not appear, then navigate to the **Options** menu and select **Capture Options**.

3. In the **Capture Options** window, ensure that the **WinPcap Packet Capture Driver** option is selected under the **Capture Method** field.
4. In the Select network adapter section, select the **Windows 10** network adapter (here, **Ethernet2**).
5. Click **OK** to start sniffing.



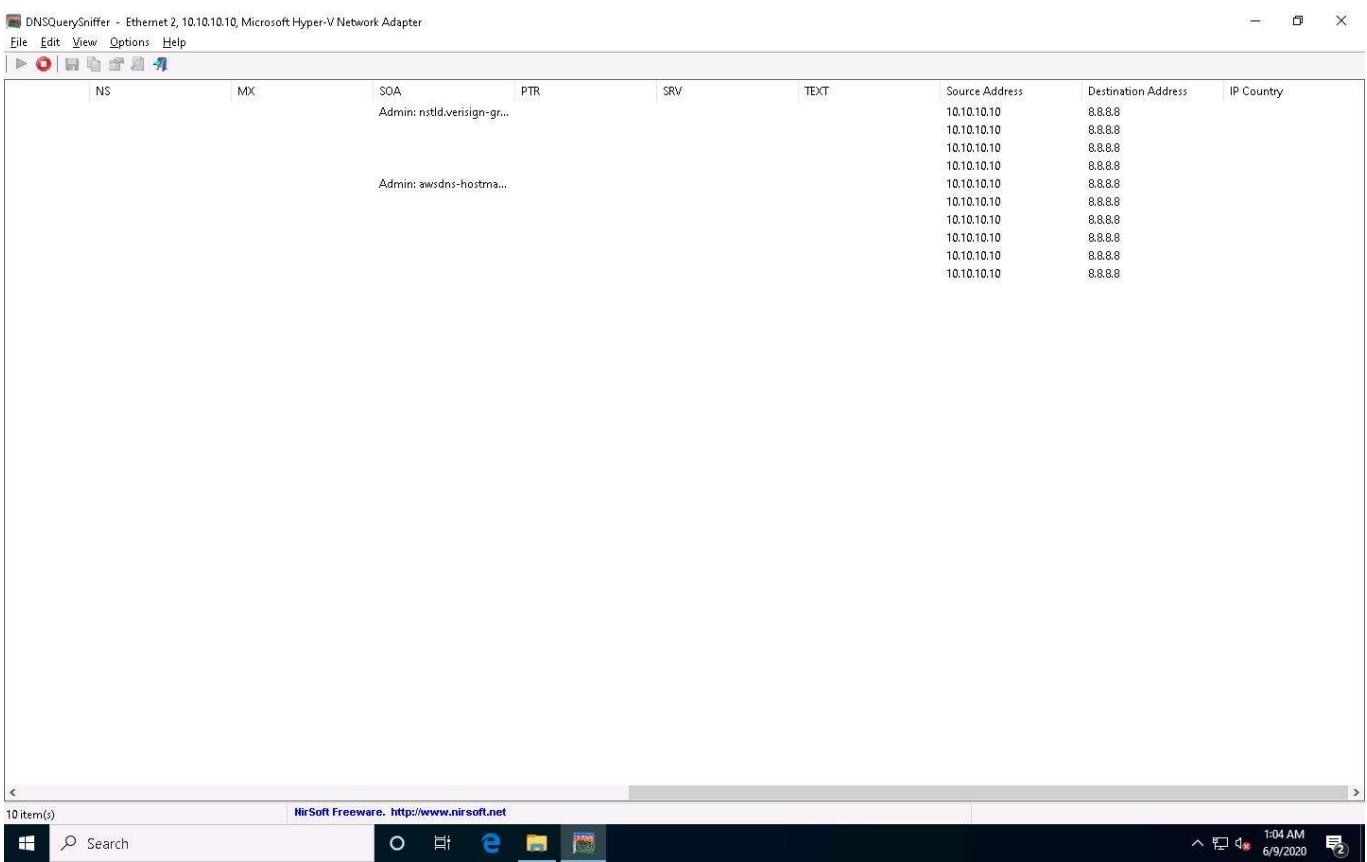
6. The DNSQuerySniffer starts monitoring the network traffic and takes some time to capture the traffic. Leave the window intact. It shows the DNS queries sent on your system along with its complete information such as host name, port number, request time, response time, duration, source address, and destination address, as shown in the screenshot.

To view the **Source Address** and **Destination Address** columns, scroll to the right side of the window.

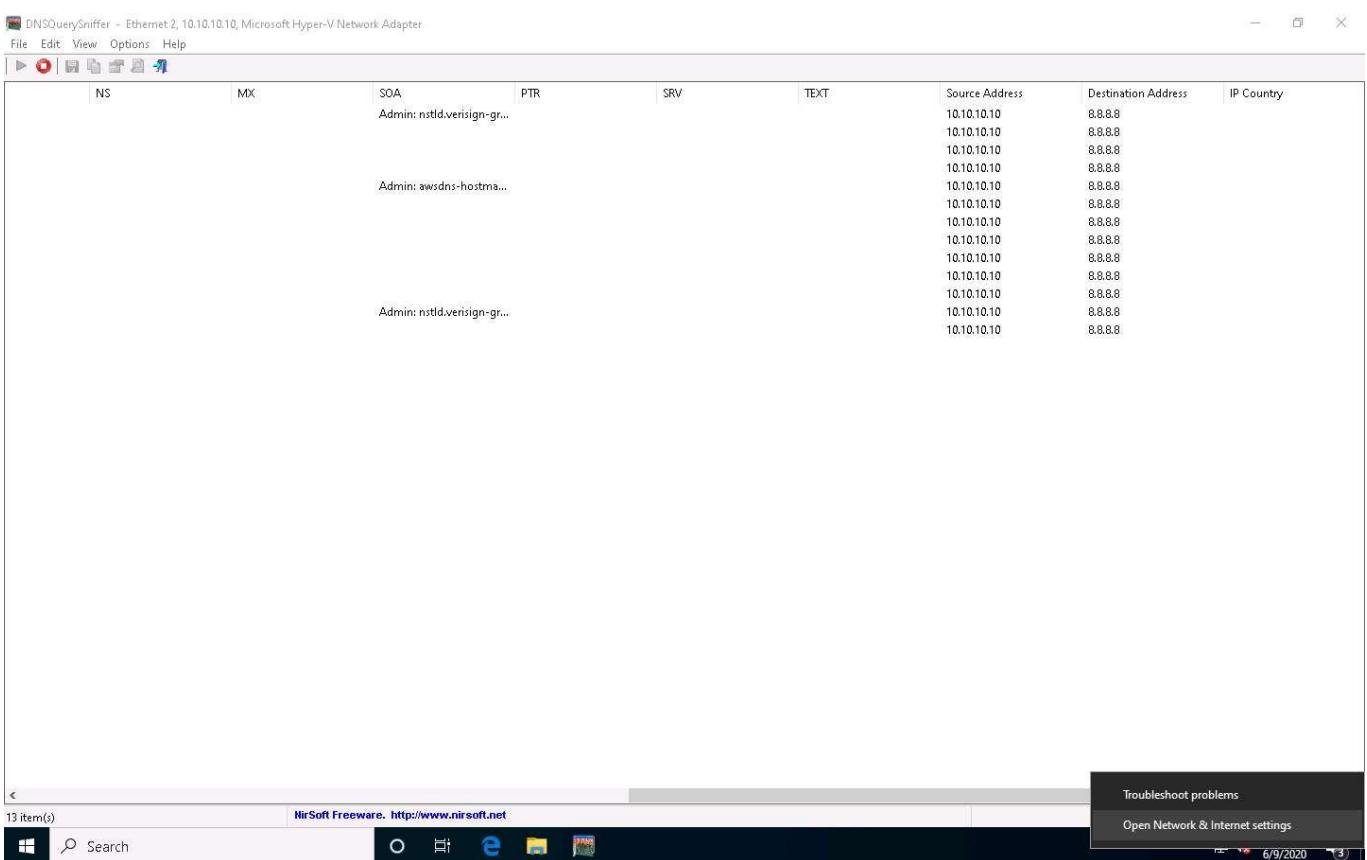
File Edit View Options Help

Host Name	Port Number	Query ID	Request Type	Request Time	Response Time	Duration	Response Code	Records Count	A	CNAME	AAAA	NS
wpad.localdo...	58270	35D6	A	6/9/2020 1:01...	6/9/2020 1:01:31 A...	8 ms	Name Error	1				
cdn.content.pr...	61006	5823	A	6/9/2020 1:02...	6/9/2020 1:02:12 A...	34 ms	Ok	3	184.28.89.214	cdn.content.prod.cms...		
assets.msn.com	65483	55C7	A	6/9/2020 1:02...	6/9/2020 1:02:12 A...	35 ms	Ok	4	23.34.58.2 23.34.58.254	assets.msn.com.edgeke...		
plugins.nessus...	52980	DF81	A	6/9/2020 1:02...	6/9/2020 1:02:15 A...	48 ms	Ok	3	18.211.211.204	pds-geo.lb.tenablesecur...		
plugins.nessus...	62050	DB8D	AAAA	6/9/2020 1:02...	6/9/2020 1:02:15 A...	21 ms	Ok	3		pds-geo.lb.tenablesecur...		
clientwncs.win...	62926	1409	A	6/9/2020 1:02...	6/9/2020 1:02:28 A...	152 ms	Ok	4	52.179.224.121	wns.notify.windows.co...		
pti.store.micro...	53947	462A	A	6/9/2020 1:02...	6/9/2020 1:02:28 A...	20 ms	Ok	5	13.107.246.10	sfd-production.azurefd...		
v10.events.dat...	56371	3D7D	A	6/9/2020 1:02...	6/9/2020 1:02:40 A...	8 ms	Ok	3	52.114.74.45	global.asimov.events.da...		
settings-win.d...	51364	42D0	A	6/9/2020 1:02...	6/9/2020 1:02:49 A...	39 ms	Ok	2	52.167.249.196	settings.sfd-geo.trafficma...		
www.bing.com	57587	3108	A	6/9/2020 1:03...	6/9/2020 1:03:07 A...	39 ms	Ok	4	204.79.197.200 13.107.21...	a-0001.a-afdbnby.net.tr...		

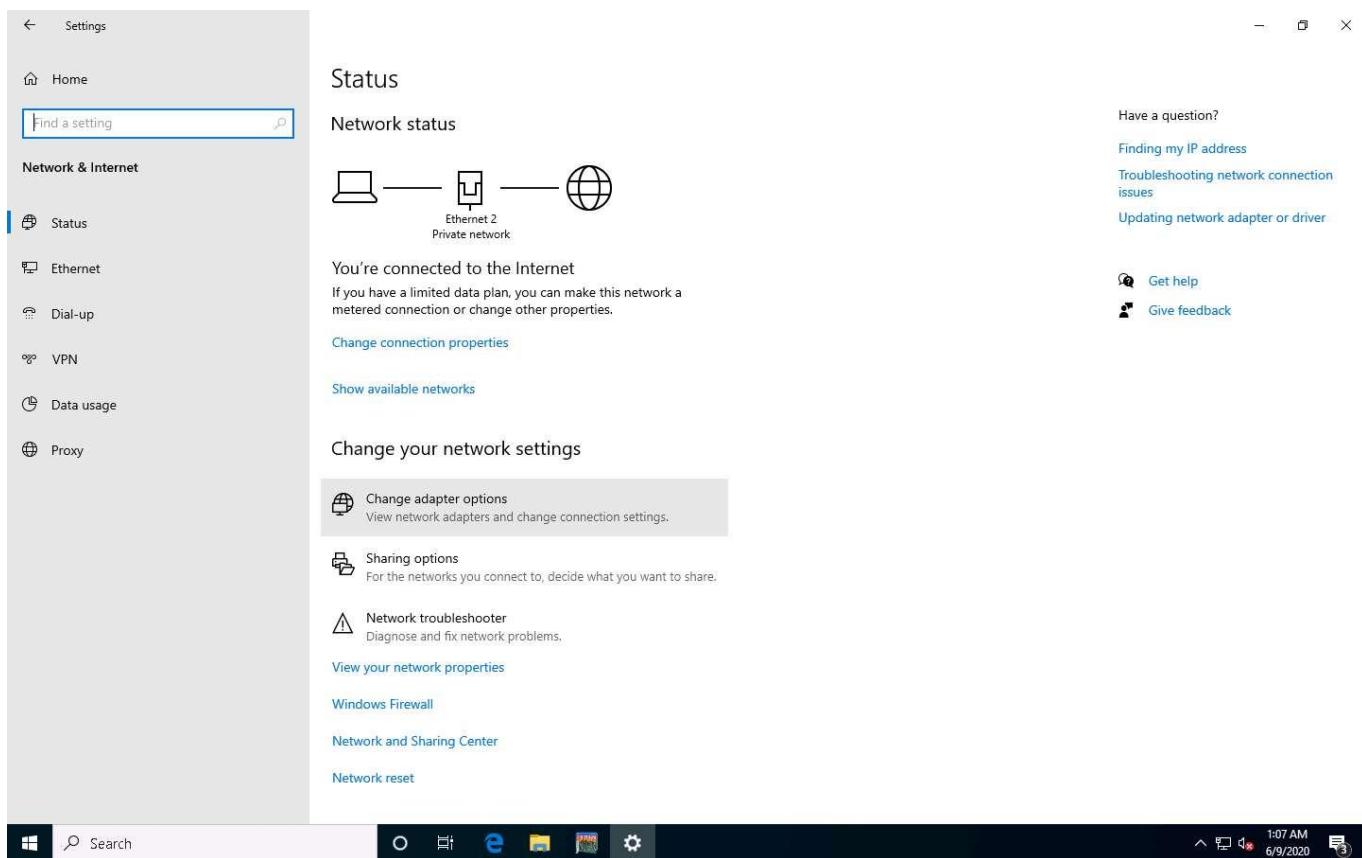




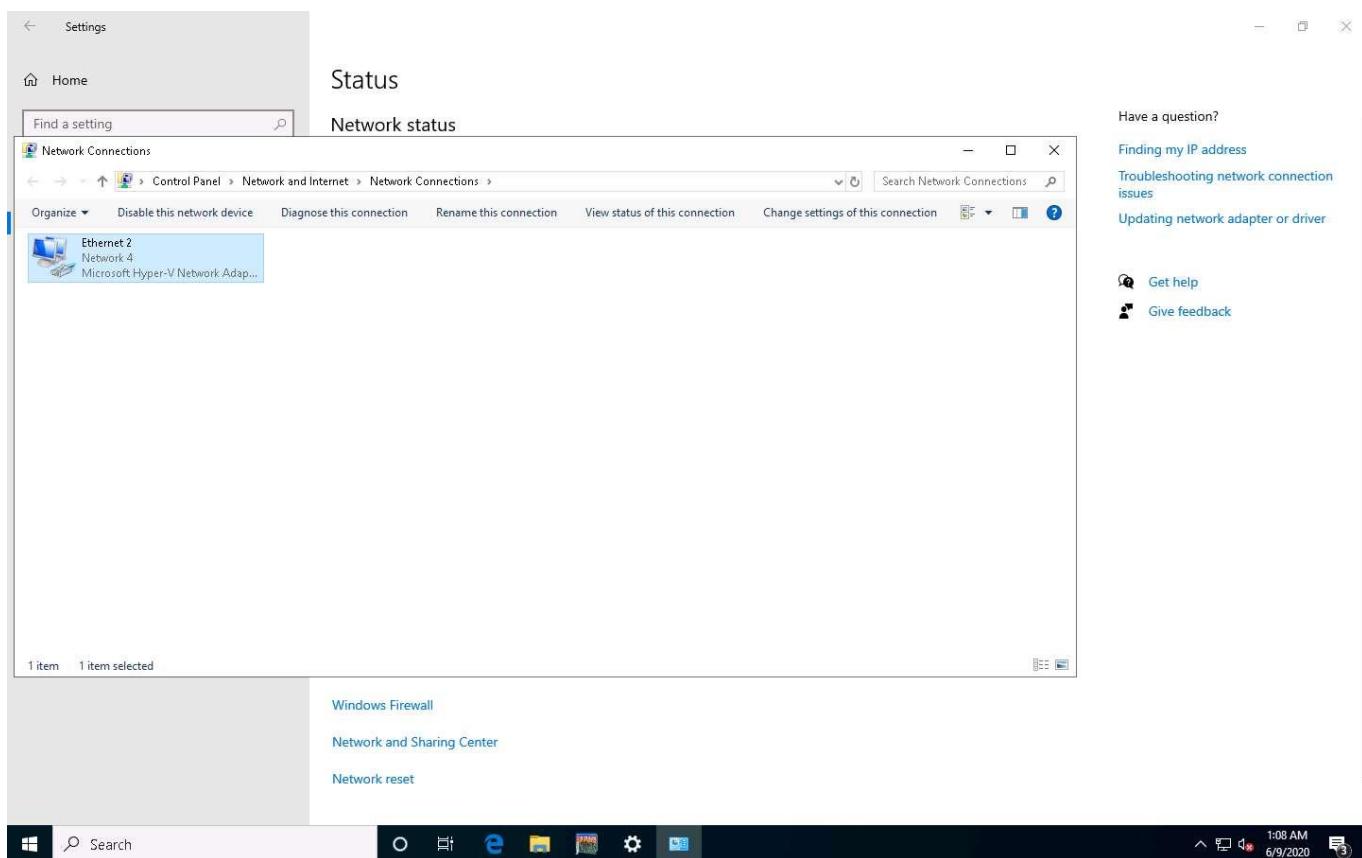
7. As you can see in the above screenshot, the DNS address is **8.8.8.8**.
8. In real-time, attackers will use malicious applications like DNSChanger to change the DNS of the target machine. For demonstration purposes, we are changing the DNS of the **Windows 10** machine in the **Network & Internet settings**.
9. Right-click on the **Network** icon in the lower-right corner of Desktop and click **Open Network & Internet settings**.



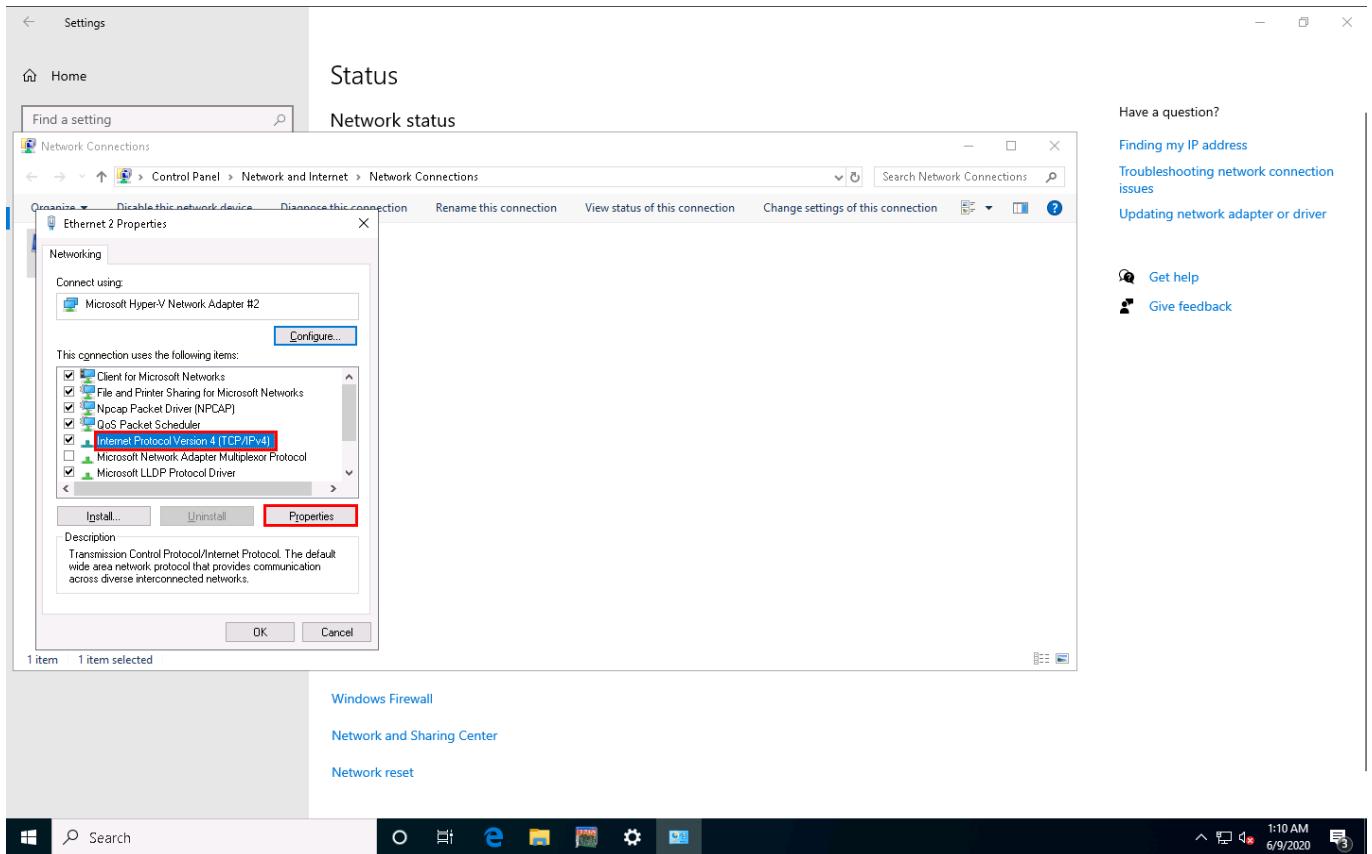
10. The Network Status window appears. Click **Change adapter options** under **Change your network settings**.



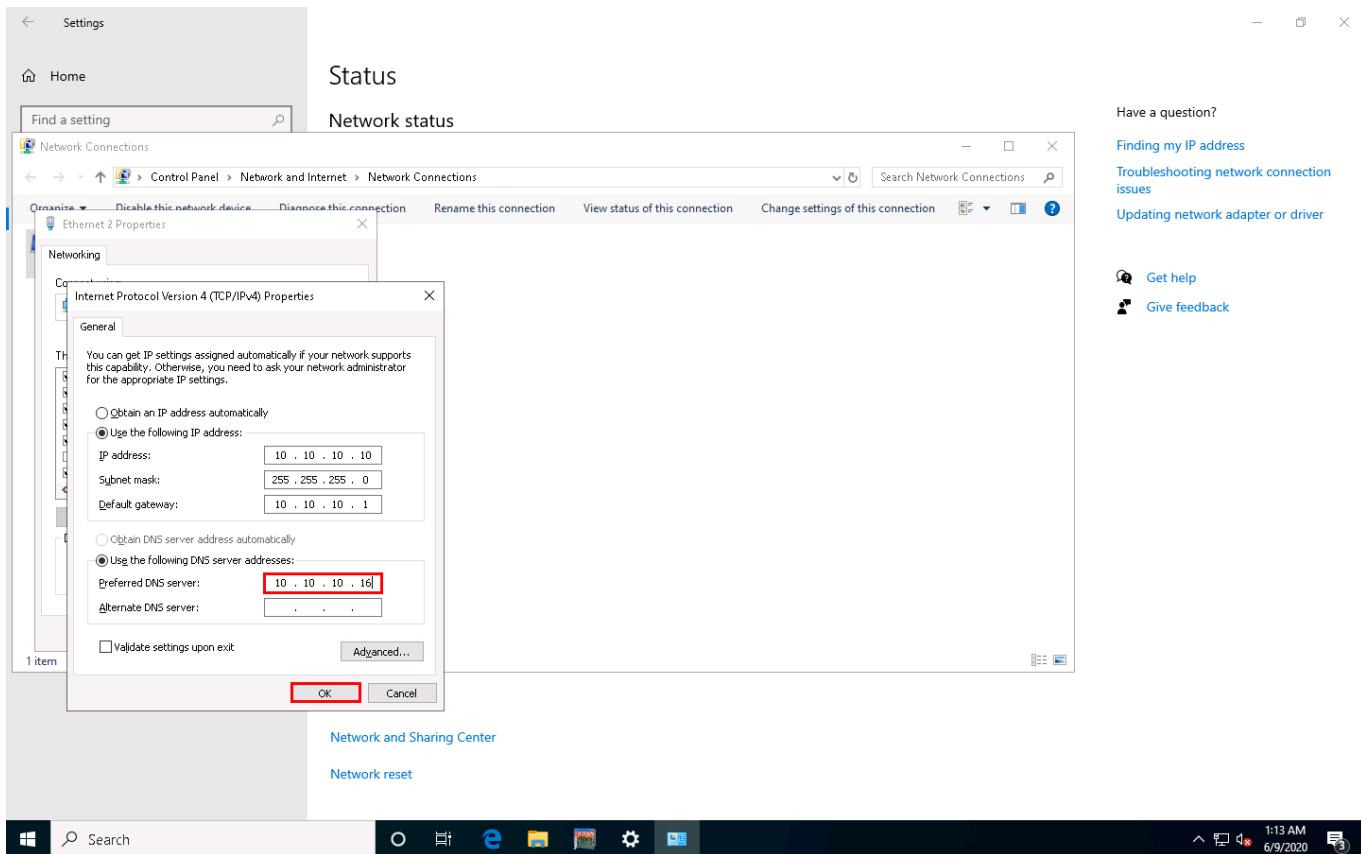
11. Right-click on the network adapter (here, **Ethernet2**) and click **Properties**.



12. The **Adapter Properties** window appears. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



13. The **Internet Protocol Version 4(TCP/IPv4) Properties** window appears. Change the **Preferred DNS server** with the **Windows Server 2016** IP address and click **OK**. In this task, the **Windows Server 2016** IP address is **10.10.10.16**. This may vary in your lab environment.
14. Click **OK**, and then **Close** the Adapter Properties window.



15. Switch to the **DNSQuerySniffer** window; observe the few recorded logs. Right-click on the log for which DNS has changed and select **Properties** from the context menu.

Host Name	Port Number	Query ID	Request Type	Request Time	Response Time	Duration	Response Code	Records Count	A	CNAME	AAAA	NS	
wpad.localdo...	58270	35D6	A	6/9/2020 1:01...	6/9/2020 1:01:31 A...	8ms	Name Error	1					
cdn.content.p...r...	61006	5B23	A	6/9/2020 1:02...	6/9/2020 1:02:12 A...	34 ms	Ok	3	184.28.89.214	cdn.content.prod.cms....			
assets.msn.com	65483	55C7	A	6/9/2020 1:02...	6/9/2020 1:02:12 A...	35 ms	Ok	4	23.34.58.2 23.34.58.254	assets.msn.com.edgekey...			
plugins.nessus...	52980	DF81	A	6/9/2020 1:02...	6/9/2020 1:02:15 A...	49 ms	Ok	3	18.211.211.204	pds-geo.lb.tenablesecu...			
plugins.nessus...	62050	DB80	AAAA	6/9/2020 1:02...	6/9/2020 1:02:15 A...	21 ms	Ok	3		pds-geo.lb.tenablesecu...			
client.wms.win...	62926	1409	A	6/9/2020 1:02...	6/9/2020 1:02:28 A...	152 ms	Ok	4	52.179.224.121	wms.notify.windows.co...			
pti.store.micro...	53947	462A	A	6/9/2020 1:02...	6/9/2020 1:02:28 A...	20 ms	Ok	5	13.107.246.10	sfd-production.azurefd...			
✓ v10.events.dat...	56371	3070	A	6/9/2020 1:02...	6/9/2020 1:02:40 A...	8 ms	Ok	3	52.114.74.45	global.asimov.events.da...			
✓ settings-wind...			Save Selected Items	Ctrl+S	0 1:02...	6/9/2020 1:02:49 A...	39 ms	Ok	2	52.167.249.196	settings-sfd-geo.trafficm...		
✓ www.bing.cor...			Copy Selected Items	Ctrl+C	0 1:03...	6/9/2020 1:03:07 A...	39 ms	Ok	4	204.79.197.200	13.107.21...	a-0001-a-afidentry.net.tr...	
✓ javadl-esd-sec...			HTML Report - All Items		0 1:05...	6/9/2020 1:05:09 A...	72 ms	Ok	3	104.112.175.40	javadl-esd-secure.oracle...		
✓ wpad.localdo...			HTML Report - Selected Items		0 1:05...	6/9/2020 1:05:09 A...	8 ms	Name Error	1				
✓ ocnex-live.azu...			Choose Columns		0 1:07...	6/9/2020 1:07:18 A...	46 ms	Ok	3	72.21.81.200	onecs-live.ec.azureedge...		
✓ www.bing.cor...			Auto Size Columns	Ctrl+Plus	0 1:09...	6/9/2020 1:09:38 A...	61 ms	Ok	4	204.79.197.200	13.107.21...	a-0001-a-afidentry.net.tr...	
✓ fe2cr.update...			Properties	Alt+Enter	0 1:09...	6/9/2020 1:09:38 A...	35 ms	Ok	4	20.36.252.130	fe2cr.update.microsoft.c...		
✓ downloadwin...			IPNetInfo - A Record	Ctrl+I	0 1:09...	6/9/2020 1:09:39 A...	8 ms	Ok	3	52.114.74.43	global.asimov.events.da...		
✓ fe3cr.delivery...			Refresh		0 1:09...	6/9/2020 1:09:40 A...	8 ms	Ok	3	65.52.108.90	fe3.delivery.mp.microso...		
✓ geover.prod.d...			F5		0 1:09...	6/9/2020 1:09:41 A...	23 ms	Ok	4	69.192.178.15	geover.prod.dodsp.mp...		
✓ geo.prod.do...	64947	7B22	A	6/9/2020 1:09...	6/9/2020 1:09:42 A...	8 ms	Ok	4	13.78.177.144	geo-prod.do.dodsp.mp.mi...			
✓ kv601.prod.do...	54526	8FCD	A	6/9/2020 1:09...	6/9/2020 1:09:42 A...	20 ms	Ok	4	104.77.69.193	kv601.prod.dodsp.mp.m...			
✓ cp601.prod.do...	56648	A5A3	A	6/9/2020 1:09...	6/9/2020 1:09:42 A...	34 ms	Ok	4	104.77.69.193	cp601.prod.dodsp.mp....			
✓ disc601.prod.d...	55772	6F80	A	6/9/2020 1:09...	6/9/2020 1:09:43 A...	35 ms	Ok	4	104.77.69.193	disc601.prod.dodsp.mp...			
✓ au.download...	60989	60DE	A	6/9/2020 1:09...	6/9/2020 1:09:44 A...	36 ms	Ok	4	184.26.143.114	audownload.windowsu...			
✓ v10.events.dat...	50509	0D90	A	6/9/2020 1:09...	6/9/2020 1:09:50 A...	8 ms	Ok	3	52.114.75.149	global.asimov.events.da...			
✓ v10.events.dat...	50926	AFD3	A	6/9/2020 1:10...	6/9/2020 1:10:15 A...	8 ms	Ok	3	138.91.140.216	global.asimov.events.da...			
✓ wpad.localdo...	61398	C5E3	A	6/9/2020 1:11...	6/9/2020 1:11:31 A...	8 ms	Name Error	1					
✓ armmfa.adobe...	56371	8BD8	A	6/9/2020 1:11...	6/9/2020 1:11:45 A...	35 ms	Ok	3	104.116.98.66	ssl.adobe.com.edgekey...			
✓ ardownload.ad...	62435	5981	A	6/9/2020 1:11...	6/9/2020 1:11:51 A...	34 ms	Ok	4	23.55.62.138	ardownload.adobe.com...			

16. In the **Properties** window, observe that there is a change in DNS.

DNSQuerySniffer - Ethernet 2, 10.10.10.10, Microsoft Hyper-V Network Adapter

Host Name	Port Number	Query ID	Request Type	Request Time	Response Time	Duration	Response Code	Records Count	A	CNAME	AAAA	NS
wpad.localdo...	58270	35D6	A	6/9/2020 1:01...	6/9/2020 1:01:31 A...	8 ms	Name Error	1		cdn.content.prod.cms...		
cdn.content.pri...	61006	5B23	A	6/9/2020 1:02...	6/9/2020 1:02:12 A...	34 ms	Ok	3	184.28.89.214			
assets.msn.com...	65483	55C7	A	6/9/2020 1:02...	6/9/2020 1:02:12 A...	34 ms				assets.msn.com.edgeke...		
plugins.nessus...	52980	DF81	A	6/9/2020 1:02...	6/9/2020 1:02:12 A...	34 ms				pds-geo.lb.tenablesecu...		
client.ows.win...	62926	1409	A	6/9/2020 1:02...	6/9/2020 1:02:12 A...	34 ms				pds-geo.lb.tenablesecu...		
pti.store.micro...	53947	462A	A	6/9/2020 1:02...	6/9/2020 1:02:12 A...	34 ms				wns.notify.windows.com...		
v10.events.dat...	56371	3D7D	A	6/9/2020 1:02...	6/9/2020 1:02:40 AM...	649 ms				sfd-production.azuref...		
settings.win.d...	51364	420D	A	6/9/2020 1:02...	6/9/2020 1:02:40 AM...	649 ms				global.asimov.events.da...		
www.bing.com...	57587	3108	A	6/9/2020 1:03...	6/9/2020 1:03:01 A...	1 ms				settingfd-geo.trafficm...		
javatl-esd-sec...	62745	D04A	A	6/9/2020 1:05...	6/9/2020 1:05:01 A...	1 ms				a-0001-a-afidentry.net...		
wpad.localdo...	62261	289F	A	6/9/2020 1:05...	6/9/2020 1:05:01 A...	1 ms				javatl-esd-secure.oracle...		
ocsp.digicert...	57513	1333	A	6/9/2020 1:05...	6/9/2020 1:05:01 A...	1 ms				cs9.wac.phicdn.net		
onics-live.azure...	56965	A03A	A	6/9/2020 1:05...	6/9/2020 1:05:01 A...	1 ms				onics-live.ee.azureedge...		
www.bing.com...	51423	CB20	A	6/9/2020 1:07...	6/9/2020 1:07:01 A...	1 ms				a-0001-a-afidentry.net...		
fe2cr.update....	57239	601B	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				fe2cr.update.microsoft.c...		
download.win...	65466	D2D1	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				185.2...		
v10.events.dat...	55907	B3C8	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				2-01-3cf7-0009.cdx.cede...		
fe3cr.delivery...	50280	2AF3	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				global.asimov.events.da...		
geover.prod.d...	61559	BAF2	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				fe3.delivery.mp.microso...		
geo.prod.do.d...	64947	7B22	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				geover.prod.dodisp.mp...		
lv601.prod.do...	54526	8FC0	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				lv601.prod.dodisp.mp.m...		
cp601.prod.d...	56648	A5A3	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				cp601.prod.dodisp.mp...		
disc601.prod.d...	55772	6F80	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				disc601.prod.dodisp.mp...		
au.download...	60989	60DE	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				audownload.windowsu...		
v10.events.dat...	50509	009D	A	6/9/2020 1:09...	6/9/2020 1:09:01 A...	1 ms				global.asimov.events.da...		
v10.events.dat...	50936	AFD3	A	6/9/2020 1:10...	6/9/2020 1:10:01 A...	1 ms				global.asimov.events.da...		
wpad.localdo...	61398	C5E3	A	6/9/2020 1:11...	6/9/2020 1:11:01 A...	1 ms				ssl.adobe.com.edgekey...		
armmf.adobe...	56371	8BD8	A	6/9/2020 1:11...	6/9/2020 1:11:01 A...	1 ms				ardownload.adobe.com...		
ardownload.ad...	62435	5981	A	6/9/2020 1:11...	6/9/2020 1:11:01 A...	1 ms						

Properties

Host Name: v10.events.data.microsoft.com
 Port Number: 56371
 Query ID: 3D7D
 Request Type: A
 Request Time: 6/9/2020 1:02:40 AM.649
 Response Time: 6/9/2020 1:02:40 AM.658
 Duration: 8 ms
 Response Code: Ok
 Records Count: 3
 A: 52.114.74.45
 CNAME: global.asimov.events.data.trafficmanager.net.s
 AAAA:
 NS:
 MX:
 SOA:
 PTR:
 SRV:
 TEXT:
 Source Address: 10.10.10.10
 Destination Address: 10.10.10.16
 IP Country:

OK

30 item(s), 1 Selected

NirSoft Freeware, http://www.nirsoft.net

Windows Search

1:17 AM 6/9/2020

17. After completion of the task, go to the network settings, change DNS **8.8.8.8** in the **Windows 10** machine, and close all applications.

DNSQuerySniffer - Ethernet 2, 10.10.10.10, Microsoft Hyper-V Network Adapter

Host Name	Port Number	Query ID	Request Type	Request Time	Response Time	Duration	Response Code	Records Count	A	CNAME	AAAA	NS
wpad.localdo...	58270	35D6	A	6/9/2020 1:01...	6/9/2020 1:01:31 A...	8 ms	Name Error	1		cdn.content.prod.cms...		
cdn.content.pri...	61006	5B23	A	6/9/2020 1:02...	6/9/2020 1:02:12 A...	34 ms	Ok	3	184.28.89.214			
Network Connections												
Control Panel > Network and Internet > Network Connections												
Ethernet 2 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.												
<input type="radio"/> Obtain an IP address automatically												
<input checked="" type="radio"/> Use the following IP address:												
IP address:	10 . 10 . 10 . 10											
Subnet mask:	255 . 255 . 255 . 0											
Default gateway:	10 . 10 . 10 . 1											
<input type="radio"/> Obtain DNS server address automatically												
<input checked="" type="radio"/> Use the following DNS server addresses:												
Preferred DNS server:	8 . 8 . 8 . 8											
Alternate DNS server:	.	.	.									
<input type="checkbox"/> Validate settings upon exit												
Advanced...												
1 item												
OK	Cancel											
3/2020 1:20:14 A...	49 ms	Ok	2	13.83.151.160	fe2cr.update.microsoft.c...							
3/2020 1:20:15 A...	73 ms	Ok	7	72.21.81.240	2-01-3cf7-0009.cdx.cede...							
6/9/2020 1:20:15 A...	9 ms	Ok	3	138.91.140.216	global.asimov.events.da...							
6/9/2020 1:20:16 A...	9 ms	Ok	3	191.232.139.2	fe3.delivery.mp.micro...							
6/9/2020 1:20:17 A...	0 ms	Ok	3	138.91.140.216	global.asimov.events.da...							
6/9/2020 1:20:18 A...	22 ms	Ok	3	138.91.140.216	global.asimov.events.da...							
40 item(s), 1 Selected												
NirSoft Freeware, http://www.nirsoft.net												
Windows Search												
1:21 AM 6/9/2020												

18. Close all open windows.

19. You can also use other DNS monitoring/resolution tools such as **DNSstuff** (<https://www.dnsstuff.com>), **DNS Lookup Tool** (<https://www.ultratools.com>), or **Sonar Lite** (<https://constellix.com>) to perform DNS monitoring.