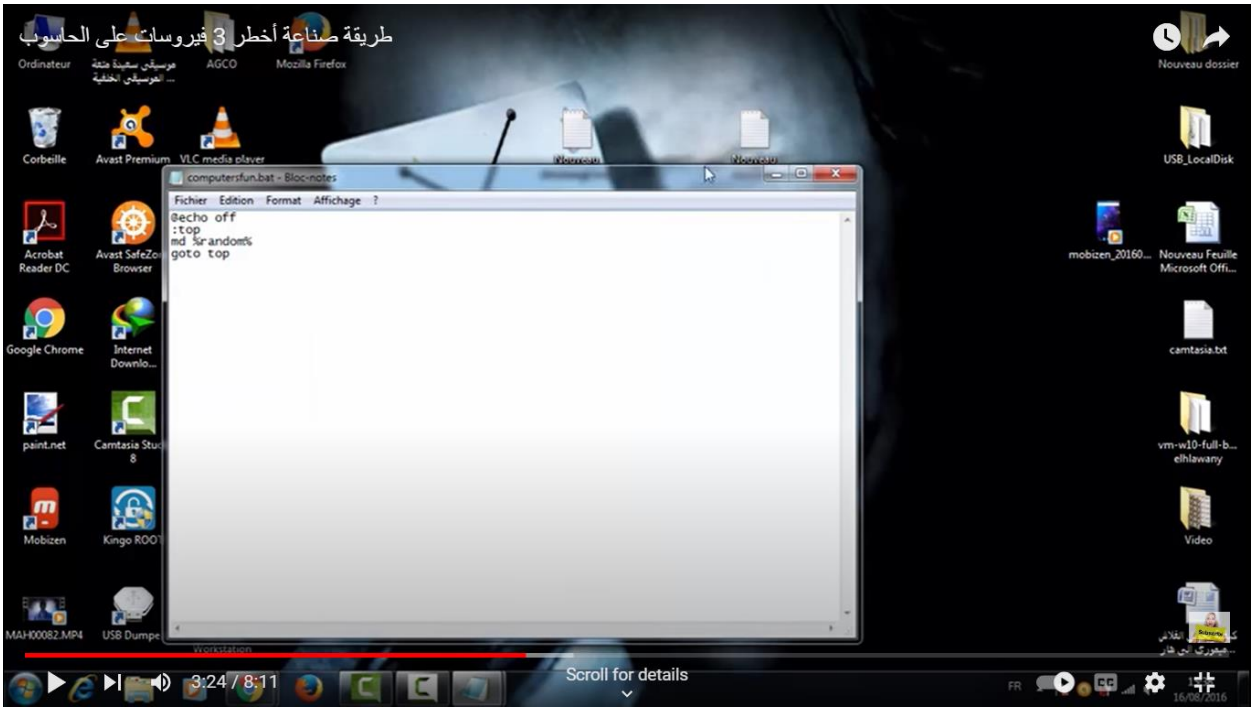
THE THIRD LECTURE

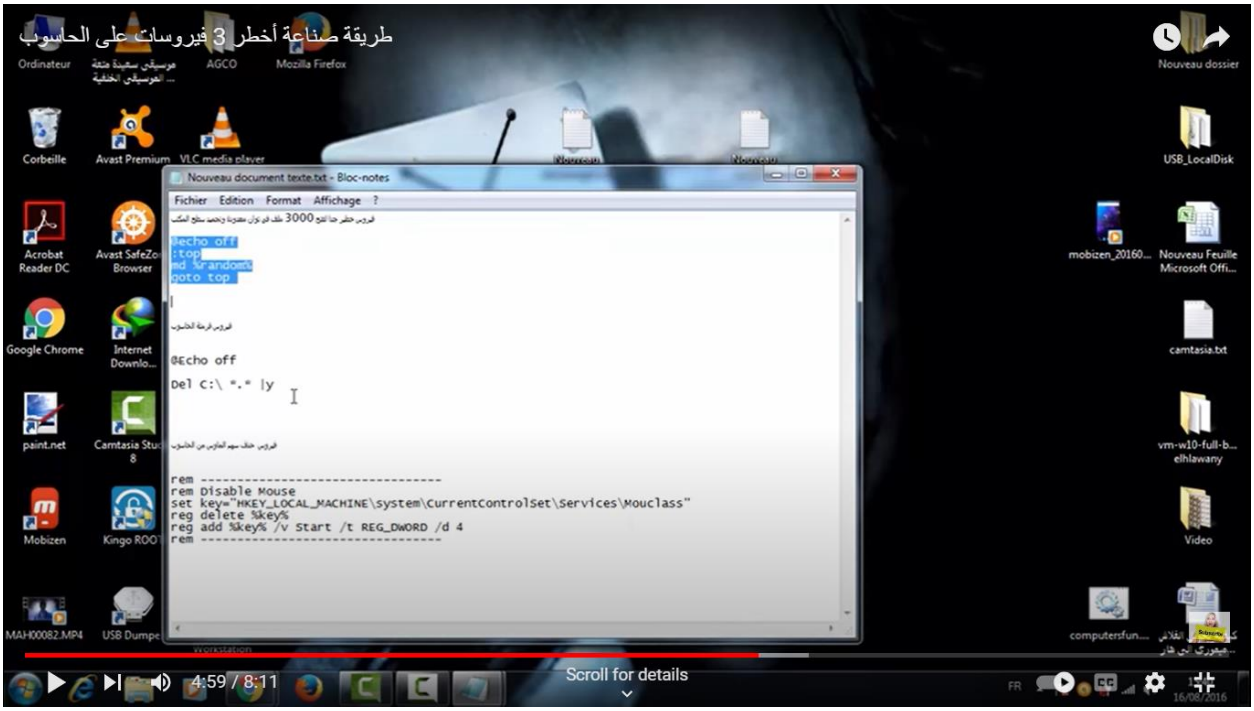
MALICIOUS CODES

How to use TCPVIEW and AUTORUN program

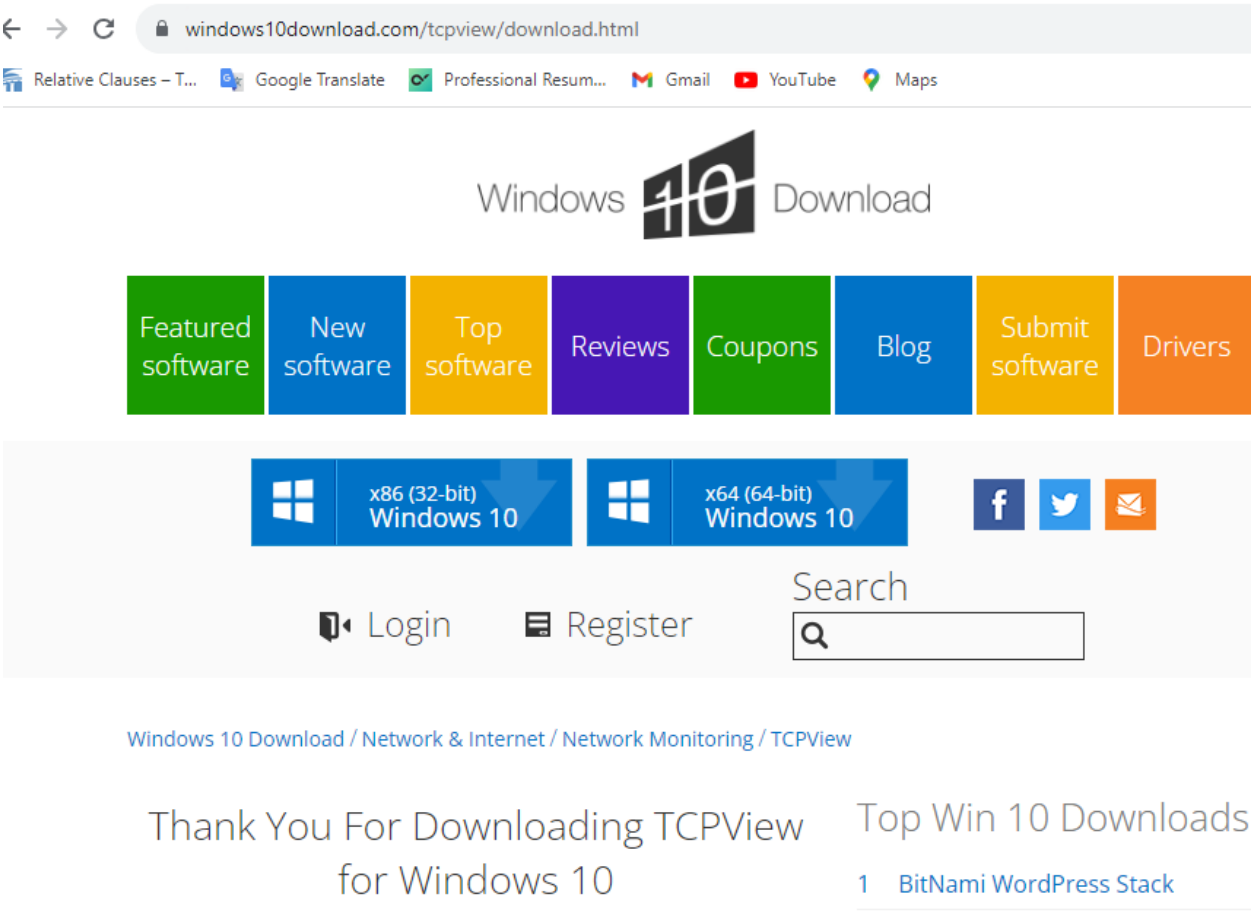
A.P MOHANAD ALI METTEAB

HOW TO MAKE SIMPLE VIRUSES





Download TCPVIEW from (https://www.windows10download.com/tcpview/download.html) and then setup it



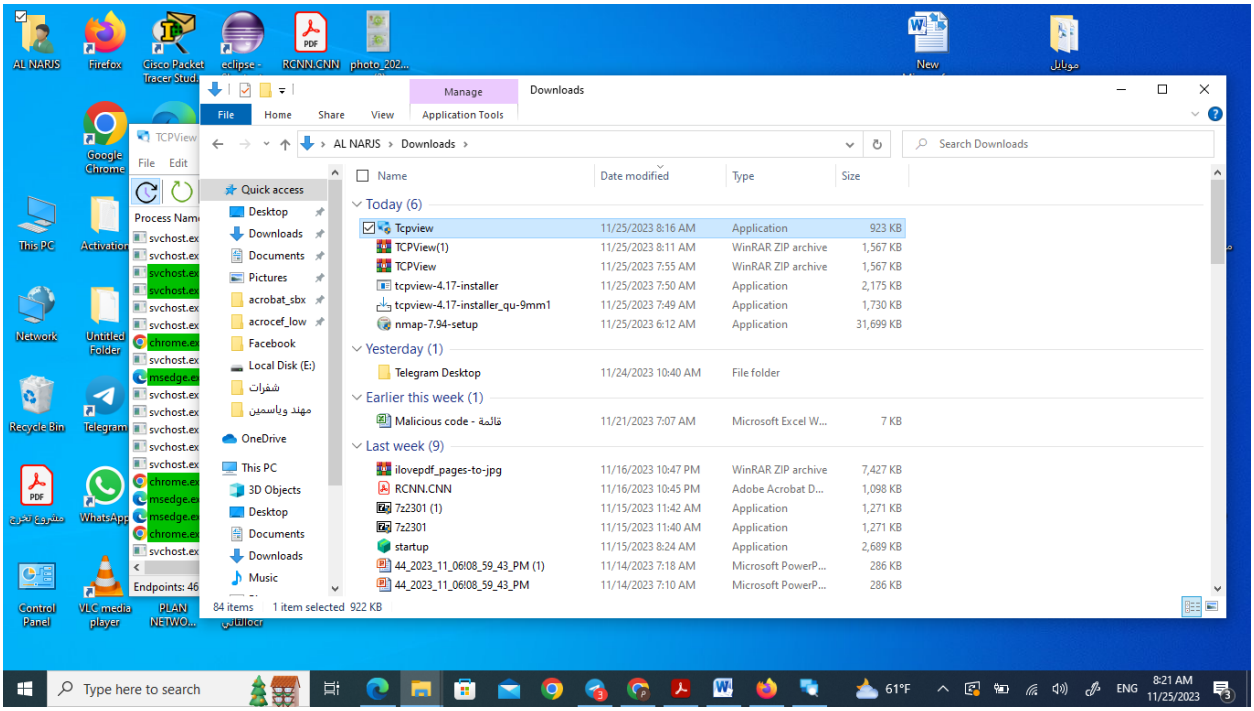
Using TCPView

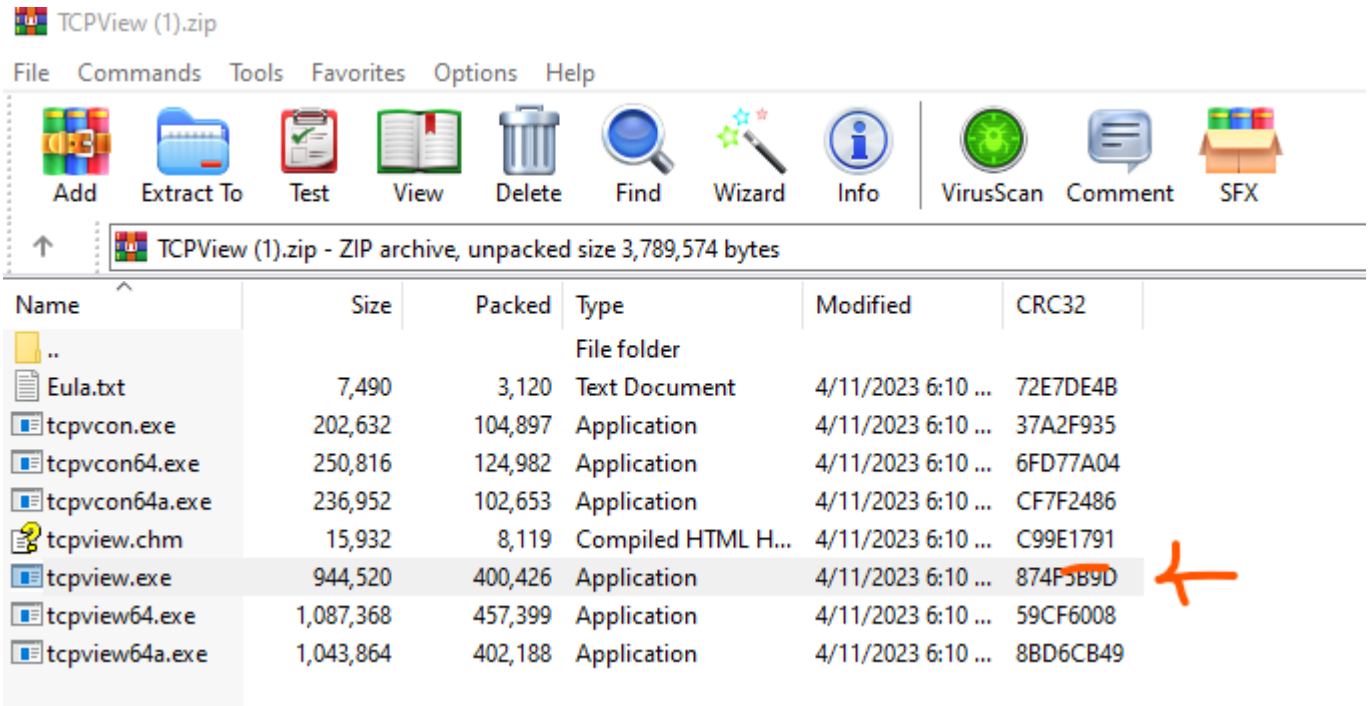
When you start TCPView it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. You can use a toolbar button or menu item to toggle the display of resolved names. TCPView shows the name of the process that owns each endpoint, including the service name (if any).

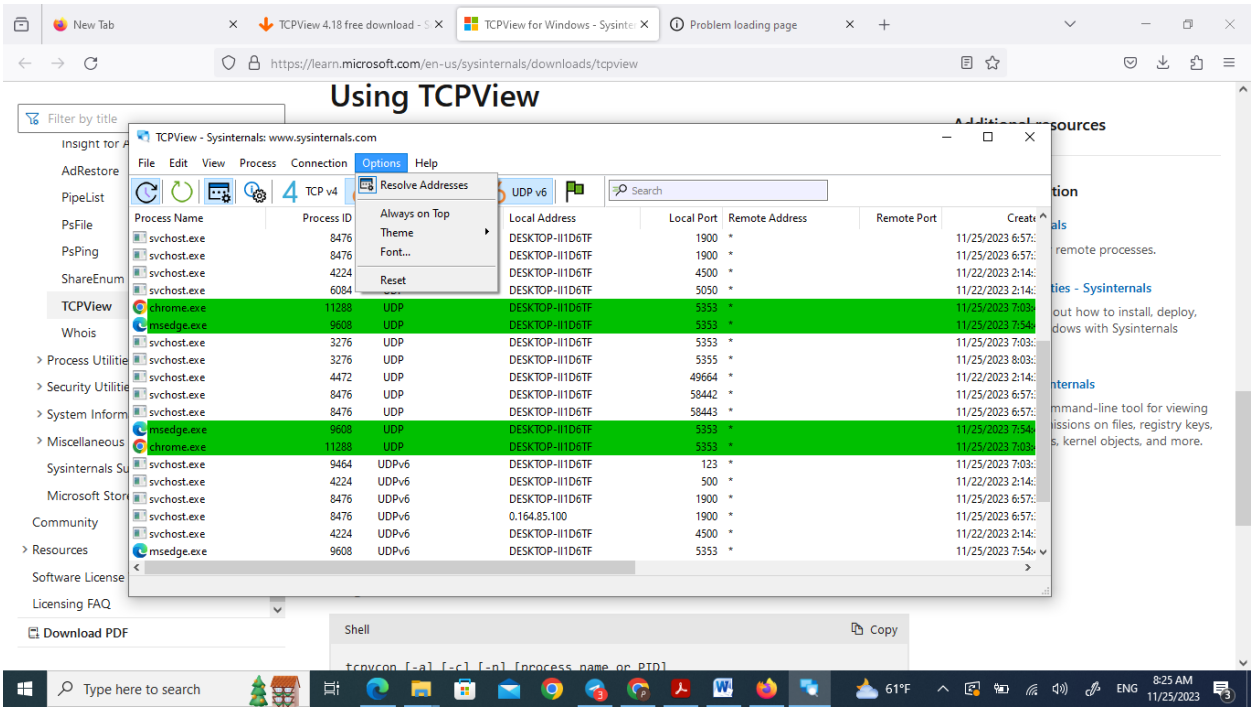
By default, TCPView updates every second, but you can use the Options|Refresh Rate menu item to change the rate. Endpoints that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new endpoints are shown in green.

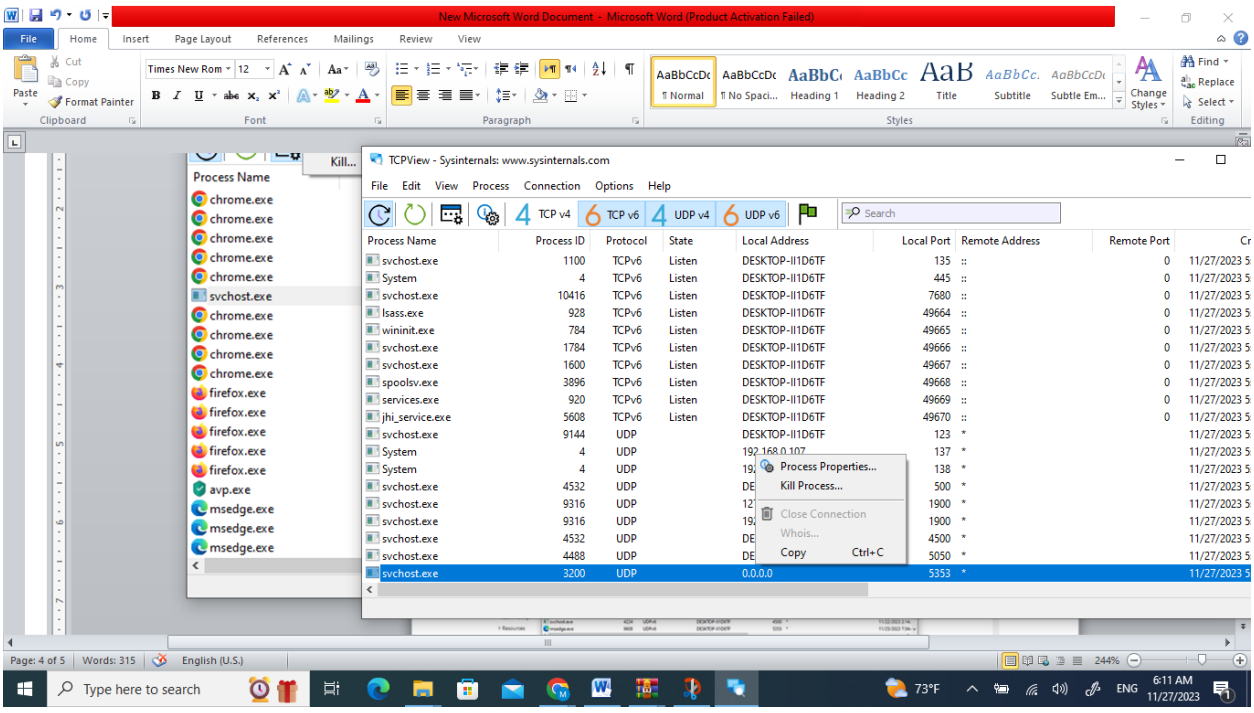
You can close established TCP/IP connections (those labeled with a state of ESTABLISHED) by selecting File|Close Connections, or by right-clicking on a connection and choosing Close Connections from the resulting context menu.

You can save TCPView's output window to a file using the Save menu item.


Downloads
Manage
File
Home
Share
View
Application Tools
AL NARJS › Downloads ›
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
acrobat_sbx
acrocef_low
Facebook
Local Disk (E:)
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Name
Date modified
Type
Size
Today (6)
Tcpview 11/25/2023 8:16 AM Application 923 KB
TCPView(1) 11/25/2023 8:11 AM WinRAR ZIP archive 1,567 KB
TCPView 11/25/2023 7:55 AM WinRAR ZIP archive 1,567 KB
tcpview-4.17-installer 11/25/2023 7:50 AM Application 2,175 KB
tcpview-4.17-installer_qu-9mm1 11/25/2023 7:49 AM Application 1,730 KB
nmap-7.94-setup 11/25/2023 6:12 AM Application 31,699 KB
Yesterday (1)
Telegram Desktop 11/24/2023 10:40 AM File folder
Earlier this week (1)
Malicious code - قائمة 11/21/2023 7:07 AM Microsoft Excel W... 7 KB
Last week (9)
ilovepdf_pages-to-jpg 11/16/2023 10:47 PM WinRAR ZIP archive 7,427 KB
RCNN.CNN 11/16/2023 10:45 PM Adobe Acrobat D... 1,098 KB
7z2301 (1) 11/15/2023 11:42 AM Application 1,271 KB
7z2301 11/15/2023 11:40 AM Application 1,271 KB
startup 11/15/2023 8:24 AM Application 2,689 KB
44_2023_11_06l08_59_43_PM (1) 11/14/2023 7:18 AM Microsoft PowerP... 286 KB
44_2023_11_06l08_59_43_PM 11/14/2023 7:10 AM Microsoft PowerP... 286 KB
84 items
1 item selected 922 KB
Type here to search
61°F
ENG
8:21 AM
11/25/2023


TCPView (1).zip
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
Info
VirusScan
Comment
SFX
TCPView (1).zip - ZIP archive, unpacked size 3,789,574 bytes
Name Size Packed Type Modified CRC32
.. File folder
Eula.txt 7,490 3,120 Text Document 4/11/2023 6:10 ... 72E7DE4B
tcpvcon.exe 202,632 104,897 Application 4/11/2023 6:10 ... 37A2F935
tcpvcon64.exe 250,816 124,982 Application 4/11/2023 6:10 ... 6FD77A04
tcpvcon64a.exe 236,952 102,653 Application 4/11/2023 6:10 ... CF7F2486
tcpview.chm 15,932 8,119 Compiled HTML H... 4/11/2023 6:10 ... C99E1791
tcpview.exe 944,520 400,426 Application 4/11/2023 6:10 ... 874F5B9D
tcpview64.exe 1,087,368 457,399 Application 4/11/2023 6:10 ... 59CF6008
tcpview64a.exe 1,043,864 402,188 Application 4/11/2023 6:10 ... 8BD6CB49





Autorun program free download from (https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns)

Usage

Simply run Autoruns and it shows you the currently configured auto-start applications as well as the full list of Registry and file system locations available for auto-start configuration. Autostart locations displayed by Autoruns include logon entries, Explorer add-ons, Internet Explorer add-ons including Browser Helper Objects (BHOs), Appinit DLLs, image hijacks, boot execute images, Winlogon notification DLLs, Windows Services and Winsock Layered Service Providers, media codecs, and more. Switch tabs to view autostarts from different categories.

To view the properties of an executable configured to run automatically, select it and use the Properties menu item or toolbar button. If Process Explorer is running and there is an active process executing the selected executable then the Process Explorer menu item in the Entry menu will open the process properties dialog box for the process executing the selected image.

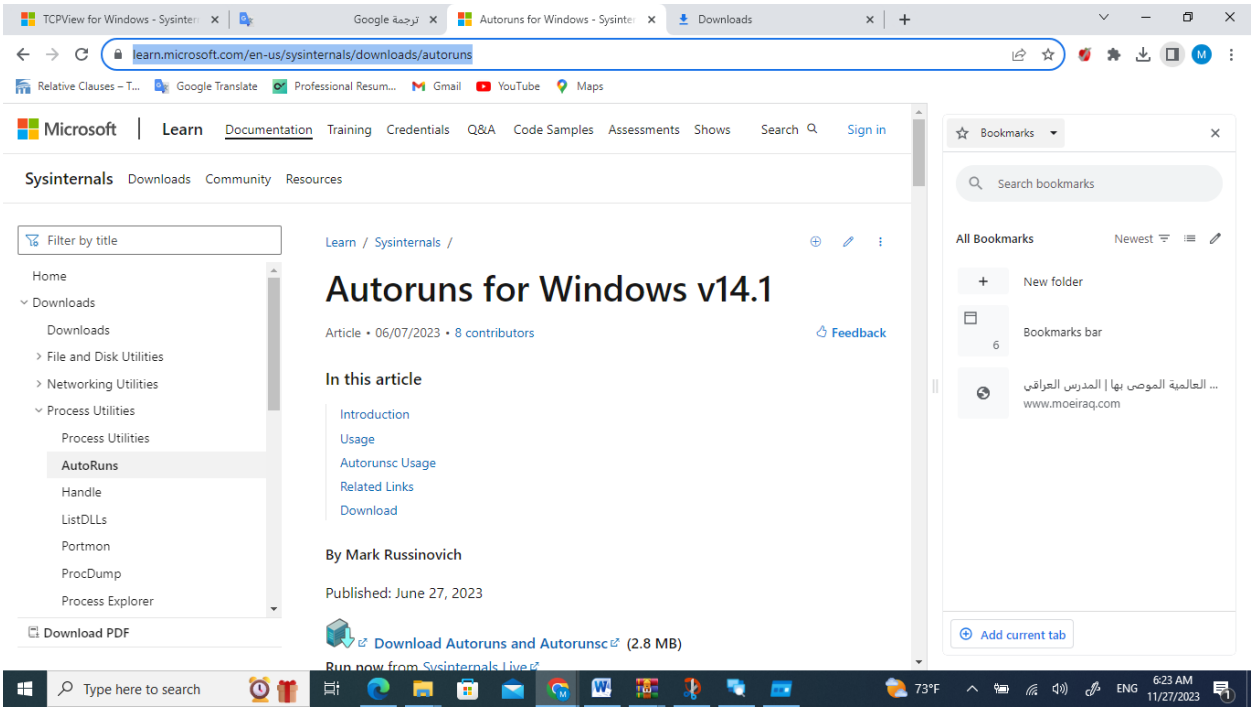
Navigate to the Registry or file system location displayed or the configuration of an auto-start item by selecting the item and using the Jump to Entry menu item or toolbar button, and navigate to the location of an autostart image.

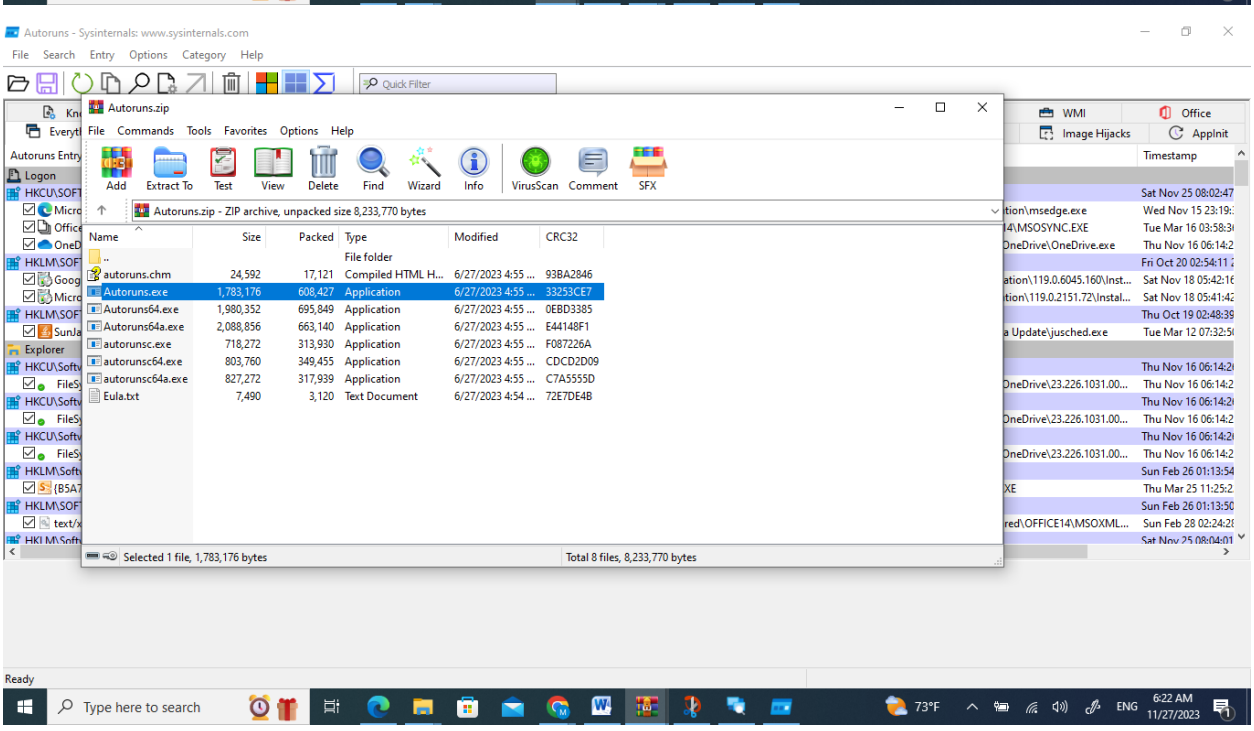
To disable an auto-start entry uncheck its check box. To delete an auto-start configuration entry use the Delete menu item or toolbar button.

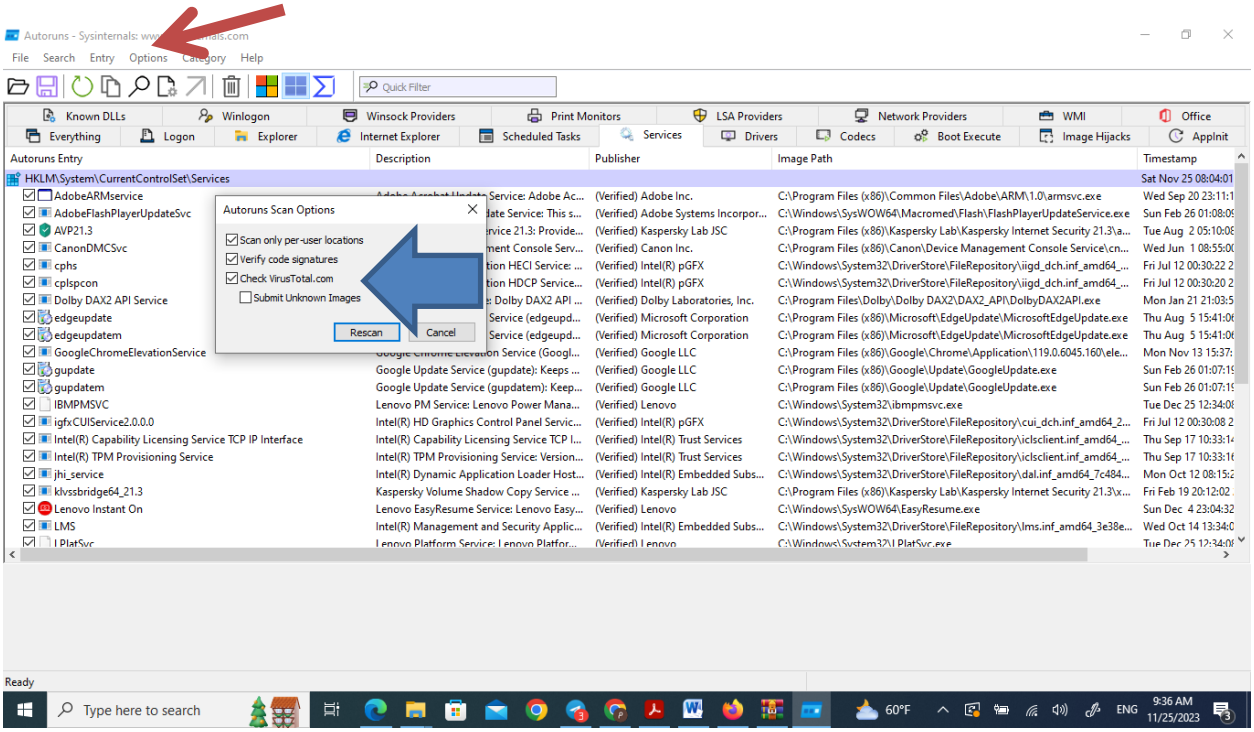
The Options menu includes several display filtering options, such as only showing non-Windows entries, as well as access to a scan options dialog from where you can enable signature verification and Virus Total hash and file submission.

Select entries in the User menu to view auto-starting images for different user accounts.

More information on display options and additional information is available in the on-line help.


TCPView for Windows - Sysinter
Google ترجمة
Autoruns for Windows - Sysinte
Downloads
learn.microsoft.com/en-us/sysinternals/downloads/autoruns
Relative Clauses – T...
Google Translate
Professional Resum...
Gmail
YouTube
Maps
Microsoft | Learn
Documentation
Training
Credentials
Q&A
Code Samples
Assessments
Shows
Search
Sign in
Sysinternals
Downloads
Community
Resources
Filter by title
Home
Downloads
Downloads
File and Disk Utilities
Networking Utilities
Process Utilities
Process Utilities
AutoRuns
Handle
ListDLLs
Portmon
ProcDump
Process Explorer
Download PDF
Learn / Sysinternals /
Autoruns for Windows v14.1
Article • 06/07/2023 • 8 contributors
Feedback
In this article
Introduction
Usage
Autorunsc Usage
Related Links
Download
By Mark Russinovich
Published: June 27, 2023
Download Autoruns and Autorunsc (2.8 MB)
Run now from Sysinternals Live
Bookmarks
Search bookmarks
All Bookmarks
Newest
New folder
Bookmarks bar
6
العالمية الموصى بها | المدرس العراقي ...
www.moeiraq.com
Add current tab
Type here to search
73°F
ENG
6:23 AM
11/27/2023


Autoruns - Sysinternals: www.sysinternals.com
File Search Entry Options Category Help
Quick Filter
Autoruns.zip
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX
Autoruns.zip - ZIP archive, unpacked size 8,233,770 bytes
Name Size Packed Type Modified CRC32
File folder
autoruns.chm 24,592 17,121 Compiled HTML H... 6/27/2023 4:55 ... 93BA2846
Autoruns.exe 1,783,176 608,427 Application 6/27/2023 4:55 ... 33253CE7
Autoruns64.exe 1,980,352 695,849 Application 6/27/2023 4:55 ... 0EBD3385
Autoruns64a.exe 2,088,856 663,140 Application 6/27/2023 4:55 ... E44148F1
autorunsc.exe 718,272 313,930 Application 6/27/2023 4:55 ... F087226A
autorunsc64.exe 803,760 349,455 Application 6/27/2023 4:55 ... CDCD2D09
autorunsc64a.exe 827,272 317,939 Application 6/27/2023 4:55 ... C7A5555D
Eula.txt 7,490 3,120 Text Document 6/27/2023 4:54 ... 72E7DE4B
Selected 1 file, 1,783,176 bytes
Total 8 files, 8,233,770 bytes
WMI
Office
Image Hijacks
AppInit
Timestamp
Logon
Explorer
Ready
Type here to search
73°F
ENG
6:22 AM
11/27/2023


Autoruns - Sysinternals: www.sysinternals.com
File Search Entry Options Category Help
Quick Filter
Known DLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit
Autoruns Entry Description Publisher Image Path Timestamp
HKLM\System\CurrentControlSet\Services Sat Nov 25 08:04:01
AdobeARMservice (Verified) Adobe Inc. C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe Wed Sep 20 23:11:1
AdobeFlashPlayerUpdateSvc (Verified) Adobe Systems Incorpor... C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe Sun Feb 26 01:08:0
AVP21.3 (Verified) Kaspersky Lab JSC C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3\a... Tue Aug 2 05:10:0
CanonDMCSvc (Verified) Canon Inc. C:\Program Files (x86)\Canon\Device Management Console Service\cn... Wed Jun 1 08:55:0
cphs (Verified) Intel(R) pGFX C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_... Fri Jul 12 00:30:22 2
cplspcon (Verified) Intel(R) pGFX C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_... Fri Jul 12 00:30:20 2
Dolby DAX2 API Service (Verified) Dolby Laboratories, Inc. C:\Program Files\Dolby\Dolby DAX2\DAX2_API\DolbyDAX2API.exe Mon Jan 21 21:03:5
edgeupdate (Verified) Microsoft Corporation C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe Thu Aug 5 15:41:0
edgeupdatem (Verified) Microsoft Corporation C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe Thu Aug 5 15:41:0
GoogleChromeElevationService (Verified) Google LLC C:\Program Files (x86)\Google\Chrome\Application\119.0.6045.160\ele... Mon Nov 13 15:37:
gupdate Google Update Service (gupdate): Keeps ... (Verified) Google LLC C:\Program Files (x86)\Google\Update\GoogleUpdate.exe Sun Feb 26 01:07:1
gupdatem Google Update Service (gupdatem): Keep... (Verified) Google LLC C:\Program Files (x86)\Google\Update\GoogleUpdate.exe Sun Feb 26 01:07:1
IBMPMSVC Lenovo PM Service: Lenovo Power Mana... (Verified) Lenovo C:\Windows\System32\ibmpmsvc.exe Tue Dec 25 12:34:0
igfxCUIService2.0.0.0 Intel(R) HD Graphics Control Panel Servic... (Verified) Intel(R) pGFX C:\Windows\System32\DriverStore\FileRepository\cui_dch.inf_amd64_2... Fri Jul 12 00:30:08 2
Intel(R) Capability Licensing Service TCP IP Interface Intel(R) Capability Licensing Service TCP I... (Verified) Intel(R) Trust Services C:\Windows\System32\DriverStore\FileRepository\iclsclient.inf_amd64_... Thu Sep 17 10:33:1
Intel(R) TPM Provisioning Service Intel(R) TPM Provisioning Service: Version... (Verified) Intel(R) Trust Services C:\Windows\System32\DriverStore\FileRepository\iclsclient.inf_amd64_... Thu Sep 17 10:33:1
jhi_service Intel(R) Dynamic Application Loader Host... (Verified) Intel(R) Embedded Subs... C:\Windows\System32\DriverStore\FileRepository\dal.inf_amd64_7c484... Mon Oct 12 08:15:2
klvssbridge64_21.3 Kaspersky Volume Shadow Copy Service ... (Verified) Kaspersky Lab JSC C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3\x... Fri Feb 19 20:12:02
Lenovo Instant On Lenovo EasyResume Service: Lenovo Easy... (Verified) Lenovo C:\Windows\SysWOW64\EasyResume.exe Sun Dec 4 23:04:32
LMS Intel(R) Management and Security Applic... (Verified) Intel(R) Embedded Subs... C:\Windows\System32\DriverStore\FileRepository\lms.inf_amd64_3e38e... Wed Oct 14 13:34:0
Autoruns Scan Options
Scan only per-user locations
Verify code signatures
Check VirusTotal.com
Submit Unknown Images
Rescan
Cancel
Ready
Type here to search
60°F
ENG
9:36 AM
11/25/2023