Internet Processes Viewer

View TCP & UDP connections on your computer along with details of each connection's starting executable, process owner, and loaded modules

InetProcs.exe version 3.8.5.0

SHA-256 = 814fa4d55277e46a81ca07c110977191f521499989acbee2bff7e41d0b2d1c28

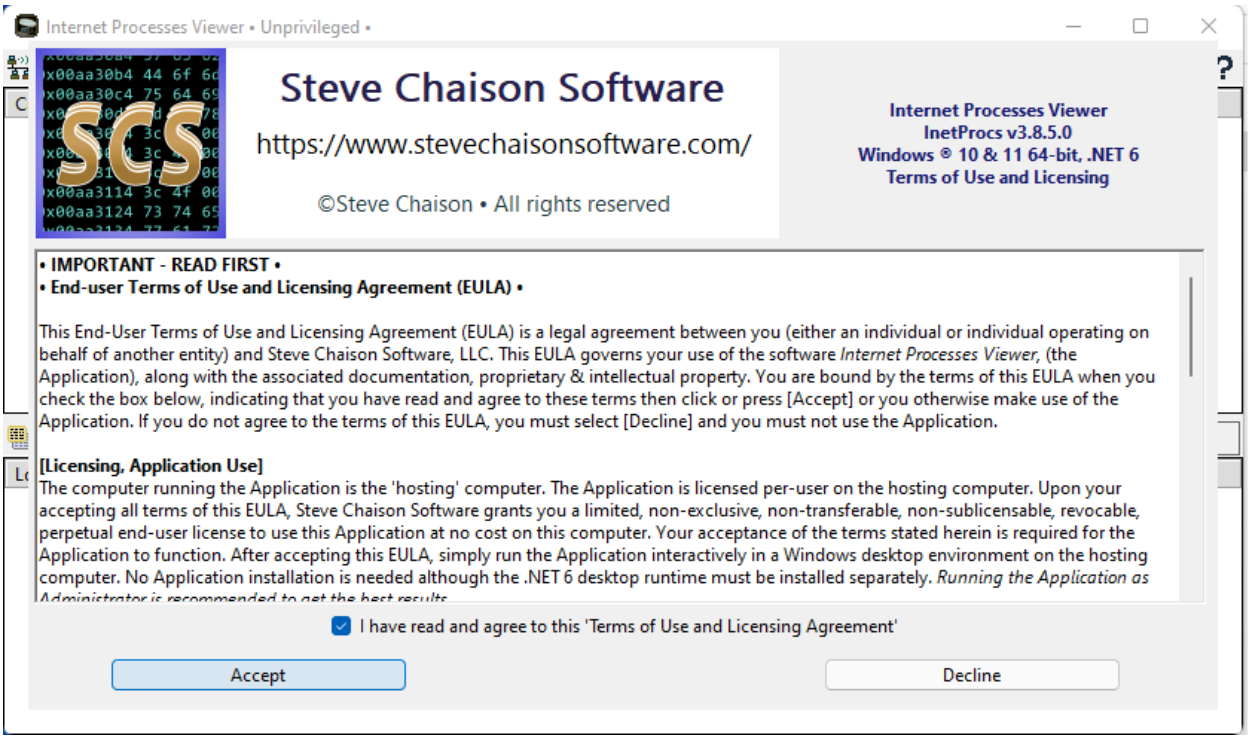
User's Guide

System Requirements:

- Operating system = Windows 10.0.19041.0 or better, or Windows 11
- CPU architecture = 64-bit
- Microsoft .NET 6 Desktop runtime
- Disk space = 30MB for use by the Application
- At least one active TCP/IP-enabled network interface

Application Distribution and Usage License:

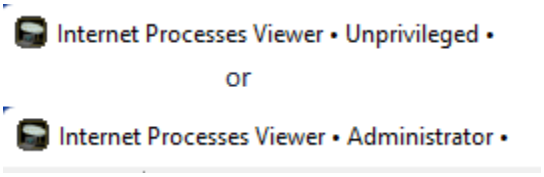
Internet Processes Viewer retrieves a detailed snapshot of your computer's active TCP & UDP network connections each time you run it. It is simple to use and gives quick results with a level of detail helpful when analyzing Cybersecurity incidents and monitoring or troubleshooting network applications. Authorized copies of this application along with this User's Guide can be found in the *InetProcs.zip* archive available on https://www.stevechaisonsoftware.com/. The *End-User Terms of Use and License Agreement* (EULA) is displayed when the application is first launched. Please read the EULA completely as your agreement is required before using this software. After you agree to the EULA, you may use this application at no cost on the computer. This application provides a brief sample of technologies covered by custom applications which may result from engagements you can optionally initiate with *Steve Chaison Software, LLC*. The following image shows the EULA screen that the application displays when first run.



- A reference copy of this license is available through the application's help **[?]** button after you begin using the application.

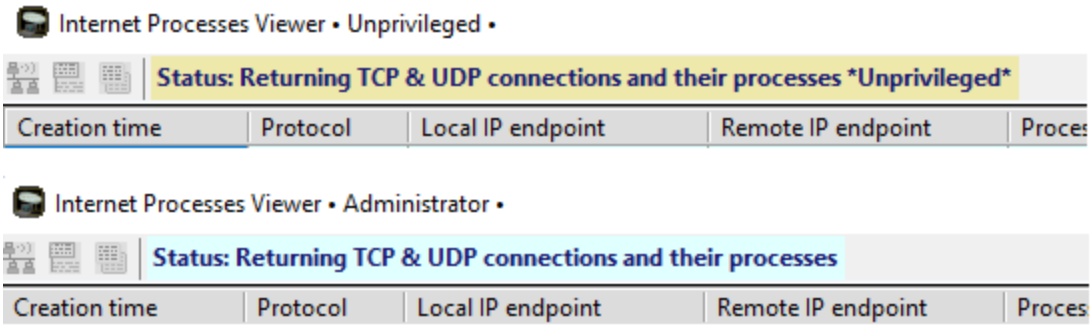
Running the Application:

No installation is needed. If your computer meets the System Requirements shown above, you can get started quickly. To start the application, simply run the InetProcs.exe executable file. **Running the Application as Administrator is recommended to get the best results**. The Windows operating system will reveal details of certain protected system-level network connections and processes only to the Administrator or an account with equivalent elevated privileges. The application title bar displays the privilege level used when you launched InetProcs.exe.



Usage Steps:

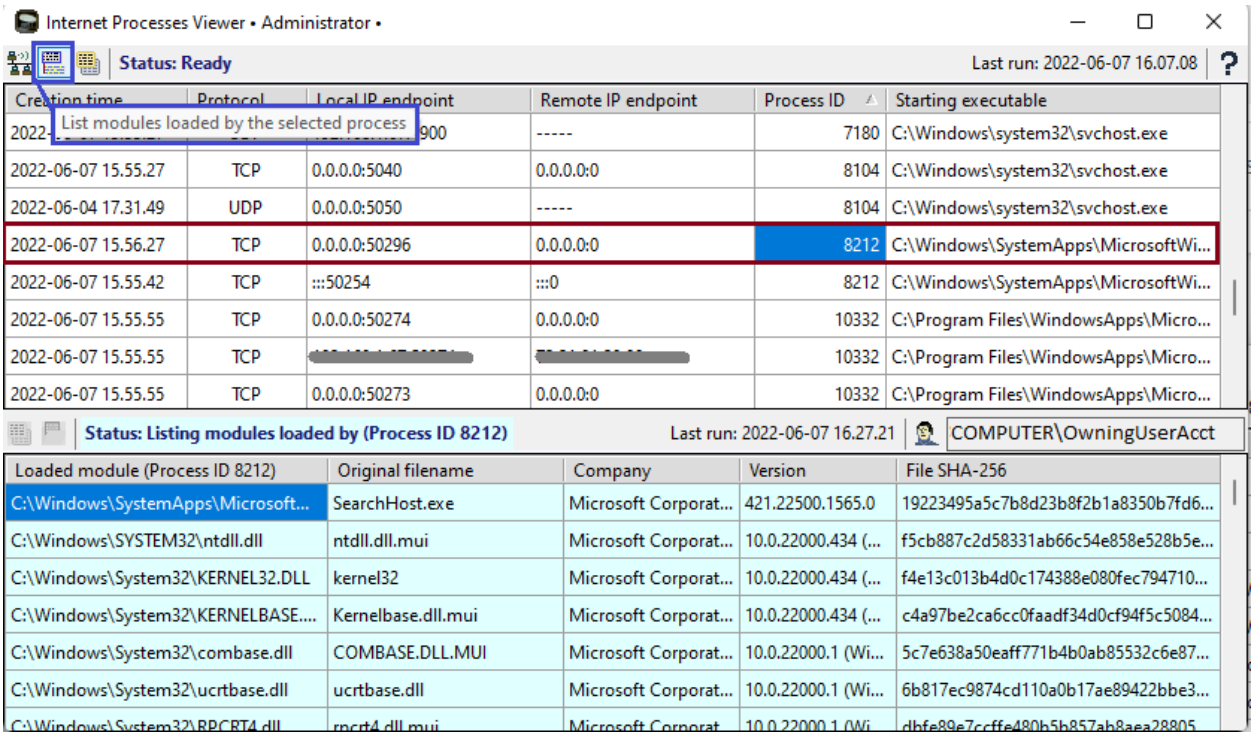
[1] Begin by clicking the 'View TCP & UDP connections' button at the top left of the user interface (UI). This will take a snapshot of currently active (and accessible) TCP & UDP - IP network connections and the executable that started each connection. The application highlights the working status messages in different colors to let you know, at-a-glance, whether you are running in unprivileged (user-level) mode or privileged (administrator-level) mode. Yellow-tan color indicates unprivileged, light cyan indicates running privileged.



The background color of an output area will always be light-cyan while information is being collected and returned to the output area. Upon completion, the background color of an output area returns to 'white' along with a corresponding 'Status: Ready' message. The UI manages the availability of certain application functions during runtime. When in a 'Ready' status, all functions are available, and the application is again ready for your input. During a view operation, properties retrieved that contain no data or properties whose values are inaccessible will return a placeholder value "-----".

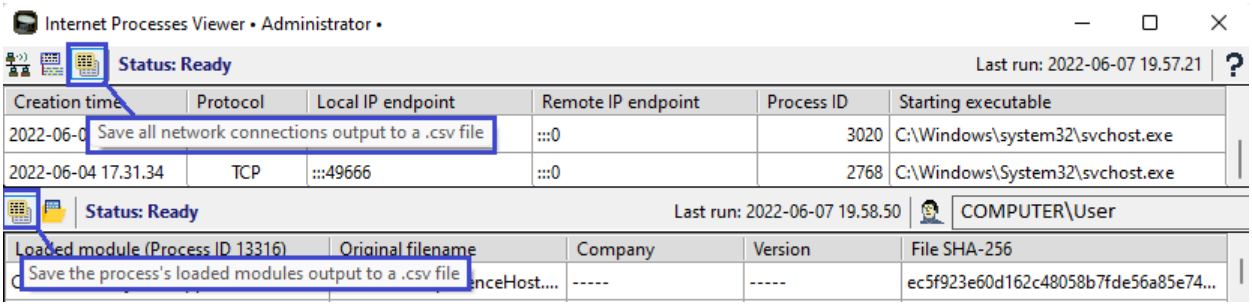
When a viewing operation is complete, you can sort the output ascending or descending by clicking on the column header by which you sort the output. Use this built-in sorting feature when you wish to group or more easily find data of interest.

[2] Next, view the process main module that starts a particular network connection along with all the executable modules the process loads at runtime to build and maintain the network connection. Select any cell within the same row corresponding to a connection or process then click the 'list modules' button to return the process's loaded modules and the process owner to the bottom output view in the UI. (example)

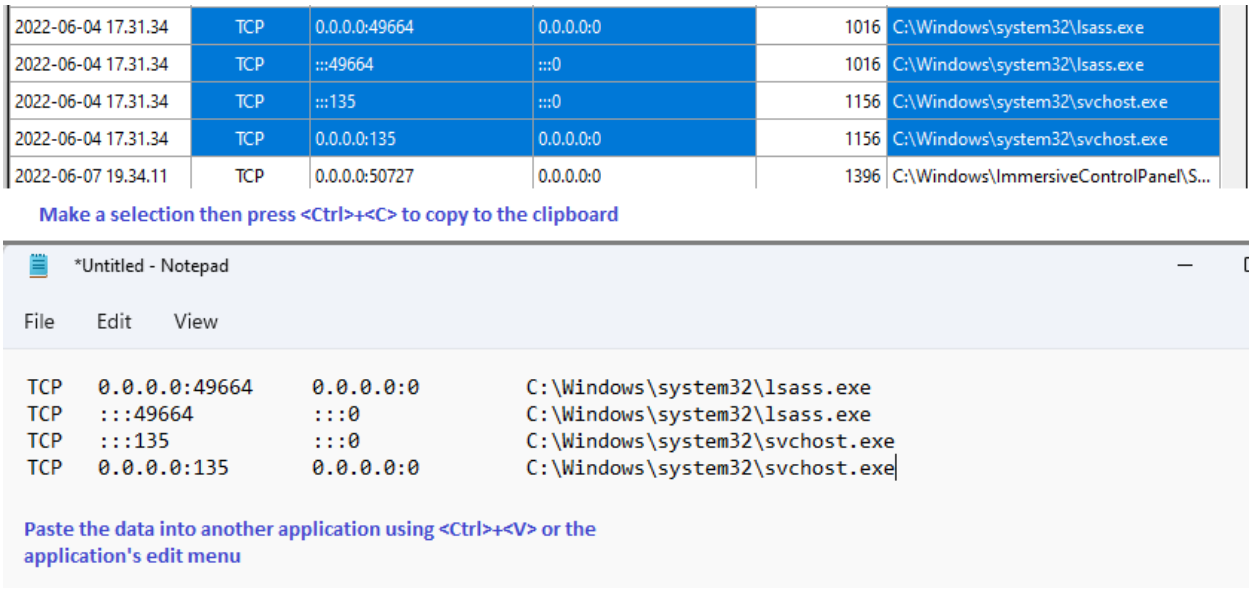


In the above example, by selecting any cell in the indicated row, you can return modules loaded by the process indicated in that row – (Process ID 8212 in this example).

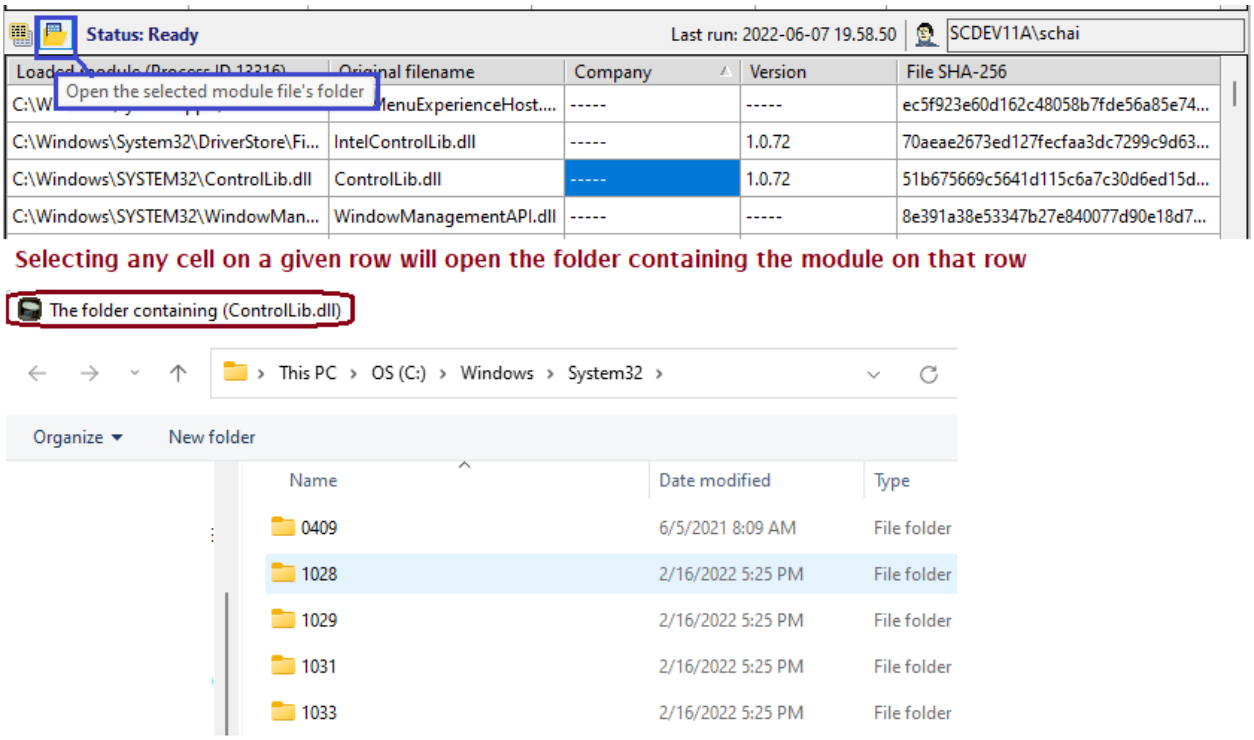
[3] Saving output from either the network connections view or loaded modules view can be done using the 'save' button associated with an output area on either view's toolstrip. The output is saved in .csv format to a storage location you choose in the folder selection window that is presented on save.



Alternatively, simple copying of cell contents can be done by selecting a cell or cells then using the standard keyboard shortcut keys (<Ctrl>+<C>) to copy data to the clipboard. The following example illustrates copying selected data from cells then pasting this into another application using this technique.



[4] The process's loaded modules view in the bottom output area of the UI shows data that uniquely identifies each module file loaded into process memory at runtime. If you need further information or want to quickly navigate to a module file's location on disk, simply use the button to open the selected module file's folder. Selecting any single cell on a row in the loaded modules view output area will open a standard Windows Explorer-style window to the folder that contains the module entry for that row. You can then easily use any Explorer contextmenu options already enabled on your computer when the folder view is opened. (example)



Internet Processes Viewer can be used to collect valuable IP network process information that can provide insights to activity on your personal computer or work computer. This application makes no system changes, is secure, and will not affect the operation of other applications on your hosting computer. If you are using it with authorization on a company computer, consider saving the output collected by the application to share with your IT or InfoSec support teams. Often the data this application provides can augment and be used in conjunction with company SIEM systems to help expedite identification of networked unsafe or malicious processes during all phases of incident response. Your company support teams can use this application as part of an incident response program and incrporate the .csv logs it produces into incident reports.
