Recently Created or Modified Executables Search

Uniquely identify executable modules, file artifacts, deposited by System processes and unsafe user activity during a Cybersecurity incident time. Helps associate modules with unsafe or risky applications.

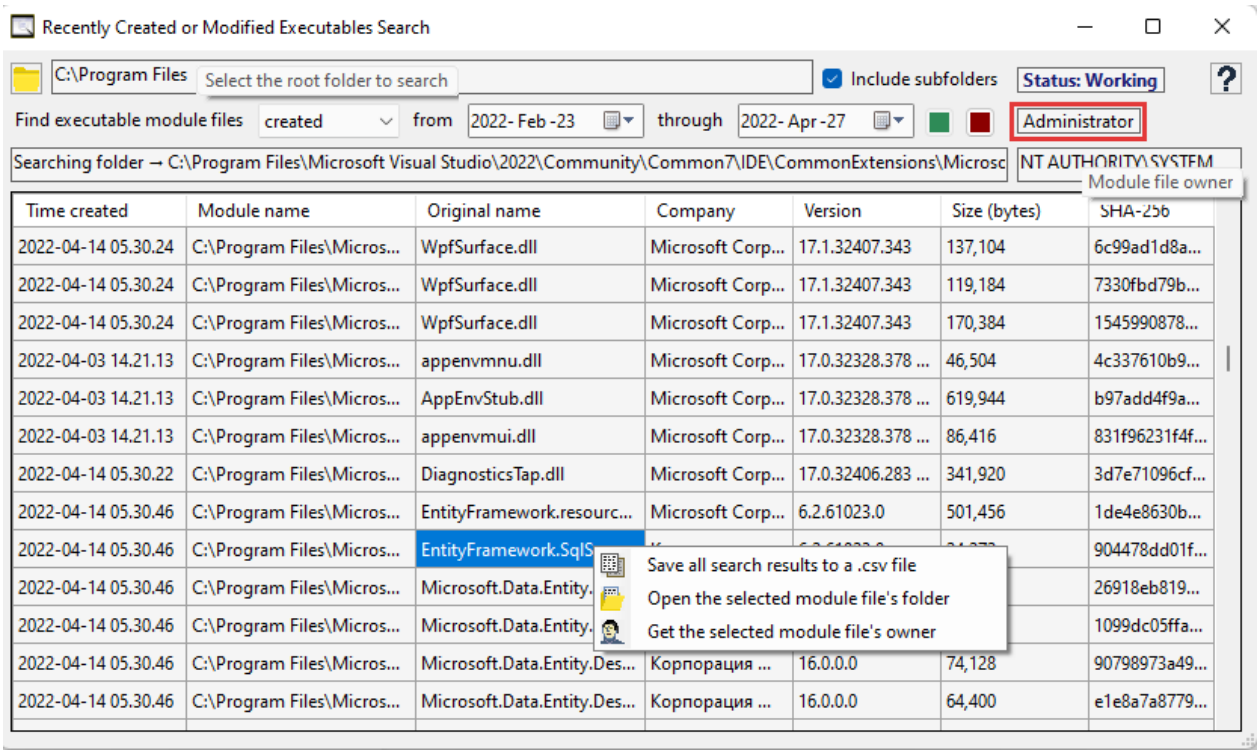
RESearch.exe version 2.1.0.2

User's Guide

System Requirements:

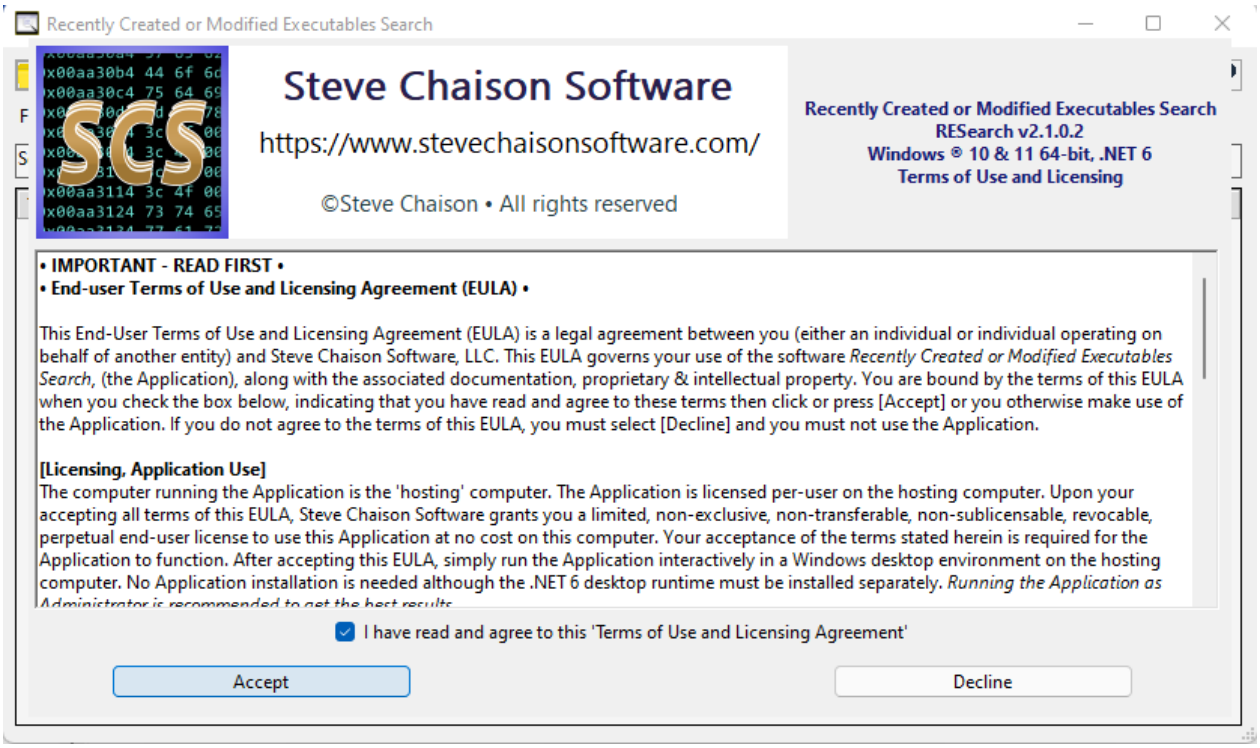
- Operating system = Windows 10.0.20348.0 or better, or Windows 11
- CPU architecture = 64-bit
- Microsoft .NET 6 Desktop runtime
- Disk space = 30MB for use by the Application, create & write rights to HKCU registry

Usage:



Running the Application:

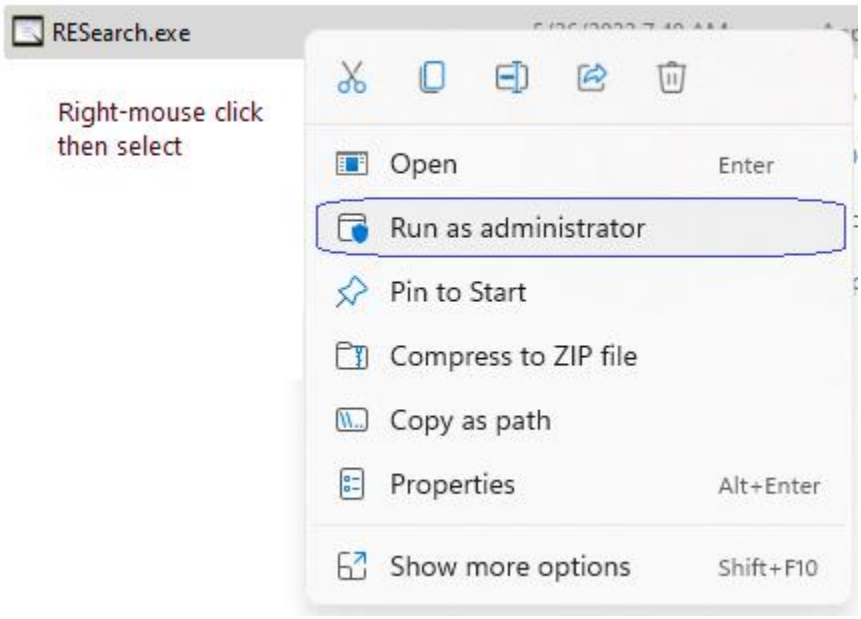
Recently Created or Modified Executables Search is simple to use. Authorized copies of this application can be found in the *RESearch.zip* archive available on https://www.stevechaisonsoftware.com/. The .zip archive also contains an updated *User's Guide* (this document). This document covers general usage and recommendations to help you get the best results from this application. No installation is needed so if your computer meets the System Requirements shown above, you can get started quickly. To start the application, simply run the RESearch.exe executable file. The first time you run the application, the End User Terms of Use and License Agreement (EULA) is displayed. Please read the EULA completely as your agreement is required before using this software. Once you agree to the EULA on a given computer, an acceptance key gets written to HKEY_CURRENT_USER\Software\SteveChaisonSoftware on your computer. Your acceptance of the EULA permits you to use this Application at no cost on the computer. Each unique user running this Application must accept the EULA terms before using it. 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.

The Application, version 2.1.0.2, is a fully functional version. It identifies executable module files using binary analysis. This makes RESearch.exe helpful when identifying module files even if the file name or extension is not typical of executables or the file name or extension given attempts to mislead or misrepresent the content of the file. Malicious programs and sometimes users may misrepresent the content of a file by changing the file's extension. **Running this Application as 'Administrator' is recommended** as it will generally give you greater access to the computer's filesystem (see the 'Run As'

image below). The Application displays the privilege level you are using to run the present instance just under the 'Status' message in the top-right area of the Application UI.

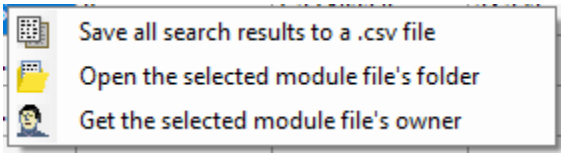


Begin by defining your search filter

Just identify the root folder from which to start your search, choose whether to collect matches based on each file's 'creation' time or 'last modified' time. You may choose one of these options in the drop-down filter selector. Check the box to 'include subfolders' in your search. Leaving this box unchecked will search only the root folder you supply. Select the inclusive 'start' and 'end' dates that the filter will match to the file timestamp of interest – 'created' or 'modified'. You can set the start and end dates to the same date if you'd like to search for files created or modified on that single day.

Next Start searching

After you've set up your search filter, simply click the 'start searching' button. The search will run to completion using the filter values you provided. You may cancel the search at any time while it is running by clicking the 'stop searching' button. While the application is running, the status indicator at the top right of the application UI will show 'working'. After your search completes or is stopped, you may perform additional tasks using the right-click context menu.



The owner of a module file you select in the output is displayed in the top right area of the UI under the Application's running privilege level. In addition to the file version and hash value uniquely identifying each module file, getting the file owner can help you determine if the file was initially written to disk by a system process or similar automation, or if a user copied or created a particular module file.

The combination of these file properties quickly revealed by *Recently Created or Modified Executables Search*, RESearch.exe can safely help you in your forensic examination of executables during a cybersecurity malware incident or similar incident involving unsafe or suspicious executable modules.

Cautionary note when 'opening a selected module file's folder'. The Application context menu enables you to open a 'Windows Explorer-type' view to the folder where a module file is found. Since it is an Explorer interface, you can use related features specific to your computer right from the Application. Be careful not to unintentionally execute or run a suspicious or unsafe module when it is being viewed through this Explorer folder view.