Web Link Communications Security Inspector

Safely inspect and analyze suspicious web links from your email or web searches

before opening them in your web browser

WebLinkCSI.exe version 1.3.2.0

SHA-256 = 2186f8898e92517f1838a3d1bc10c81a96be35d2bc052ee5023be26d3423df19

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 with create & write rights to the Application's folder
- At least one active TCP/IP-enabled network interface

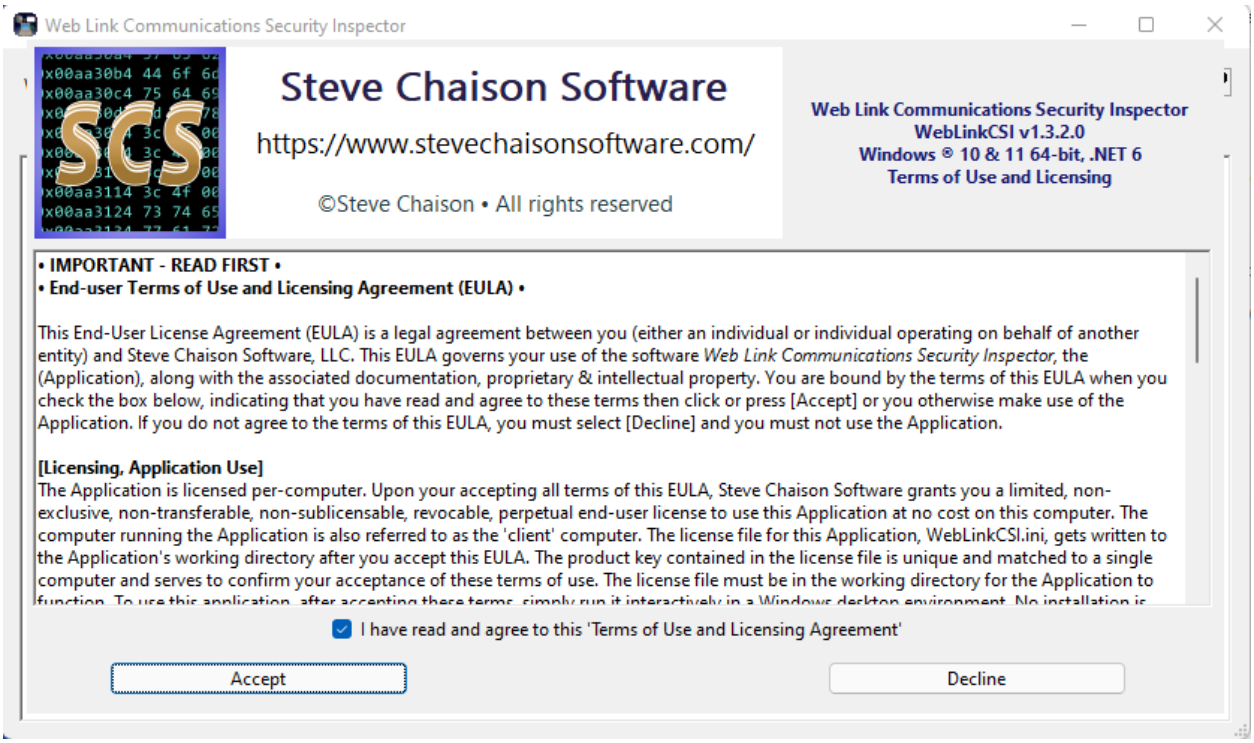
Output:

Output color conventions used:

Target host name & name-identity properties
Potential security risk, weak protocol

Application Distribution and Usage License:

Web Link Communications Security Inspector is simple to use. Authorized copies of this application along with this User's Guide can be found in the *WebLinkCSI.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. Once you agree to the EULA on a given computer, a license file – WebLinkCSI.ini – gets written to the folder in which the application was started. This license file must remain in the application's working directory on the computer. Your acceptance of the EULA permits you to use a fully functional instance of this application on the computer at no cost. The 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 WebLinkCSI.exe executable file. The first time you run the application, the End-user Terms of Use and License Agreement (EULA) is displayed. After you read and accept the EULA you can begin inspecting each URI element of web links you supply. The application analyzes both http and https elements found in the web link. The link you provide, in standard format, can be either simple or complex. It may contain a single target (remote) host, or it may contain multiple separate URI elements, multiple hosts, to which standard web link arguments or queries are passed. The links found in emails, for example, are often complex, passing more than one URI element in the web link. This application ideally suited to help you safely and privately inspect communications security in each URI element. The output from the inspection follows the following format:

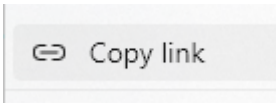
- The original web link you type or paste into the input box is unescaped, if necessary, and translated into that format at the top of the output.
- The application inspects the unescaped web link and any user or password strings found are highlighted in the unescaped link in the output area and noted as a finding.

Each URI element found in the web link you supply is inspected, and the analysis output is sectioned off between a set of horizontal lines in the output. The analysis output format of each section is:

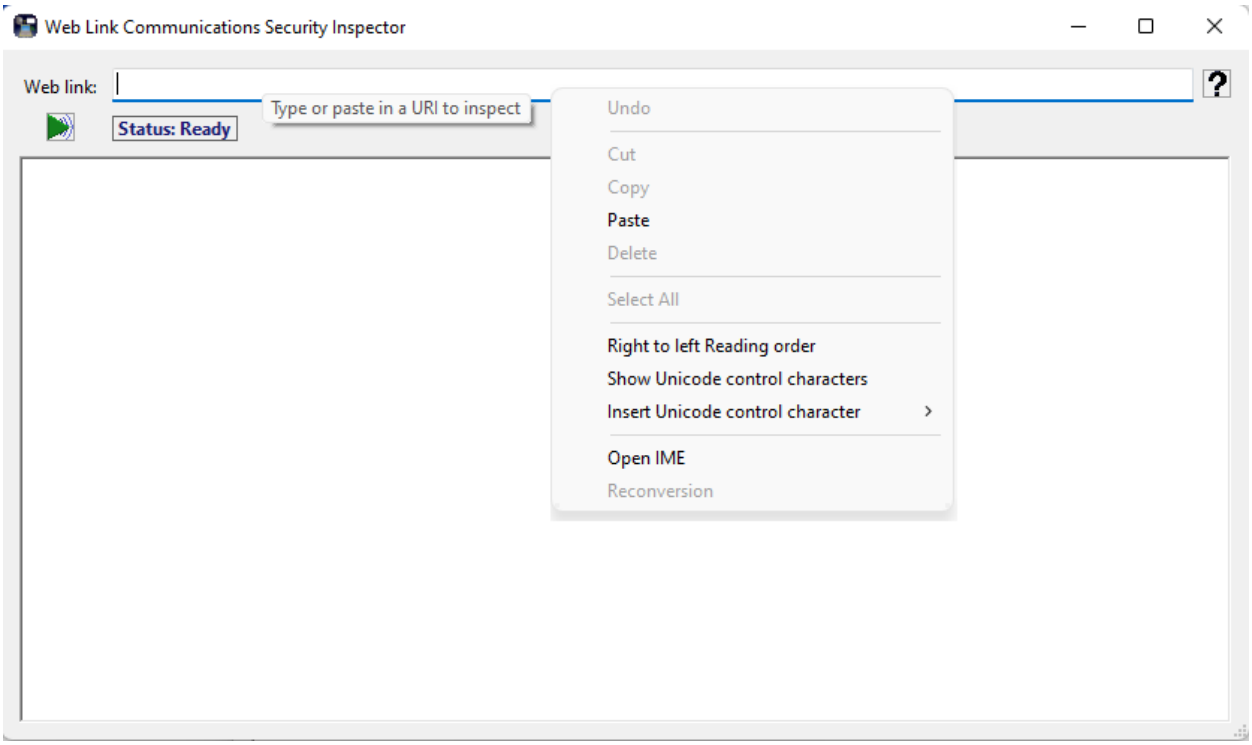
- The target host (name or IP address) with which the URI element tries to communicate
- The IP addresses of the target host, if the target is identified as a name in the link
- The web protocol, either http or https, and port number on the target host. Http connections are displayed in yellow highlight to give attention that this URI element communicates using the unsecure protocol
- The result of a simple connection test to the target host over the TCP port indicated in the web link. If the target replies, the replying IP address from the target and the receiving IP address on your client computer are returned
- On successful reply where a communication element uses 'https', a standard anonymous client-server protocol negotiation is conducted then the analysis further provides:
    - The session encryption handshake protocol used to set up communication. Where the agreed upon encryption protocol is considered weak, the weak protocol used will be highlighted in yellow.
    - The MAC hashing algorithm used to preserve integrity in the communication stream through qualities of messaging secrecy
    - The datastream cipher used to encrypt the payload data being transmitted between you and the target host
- The public certificate data from the target host is returned under '•Target host certificate identity information:'. All values returned here are useful in assessing security but the subject and issuing entity properties can provide a quick look at the target's identity to see if this is an organization (or country) you expect or trust. The elements in the certificate authority chain are also returned so that you can inspect each element and assess trust of the certificate chain.

Entering a Web Link (URI) to inspect into the input box:

The web link input supports http and https protocols, or schemes. You may type or paste an http:// URI or https:// URI in a standard format into the *Web link* box at the top of the application. One way to capture web links to inspect in this application is to use your browser's '**copy link**' feature typically available with a right-mouse click when viewing a page in your browser.

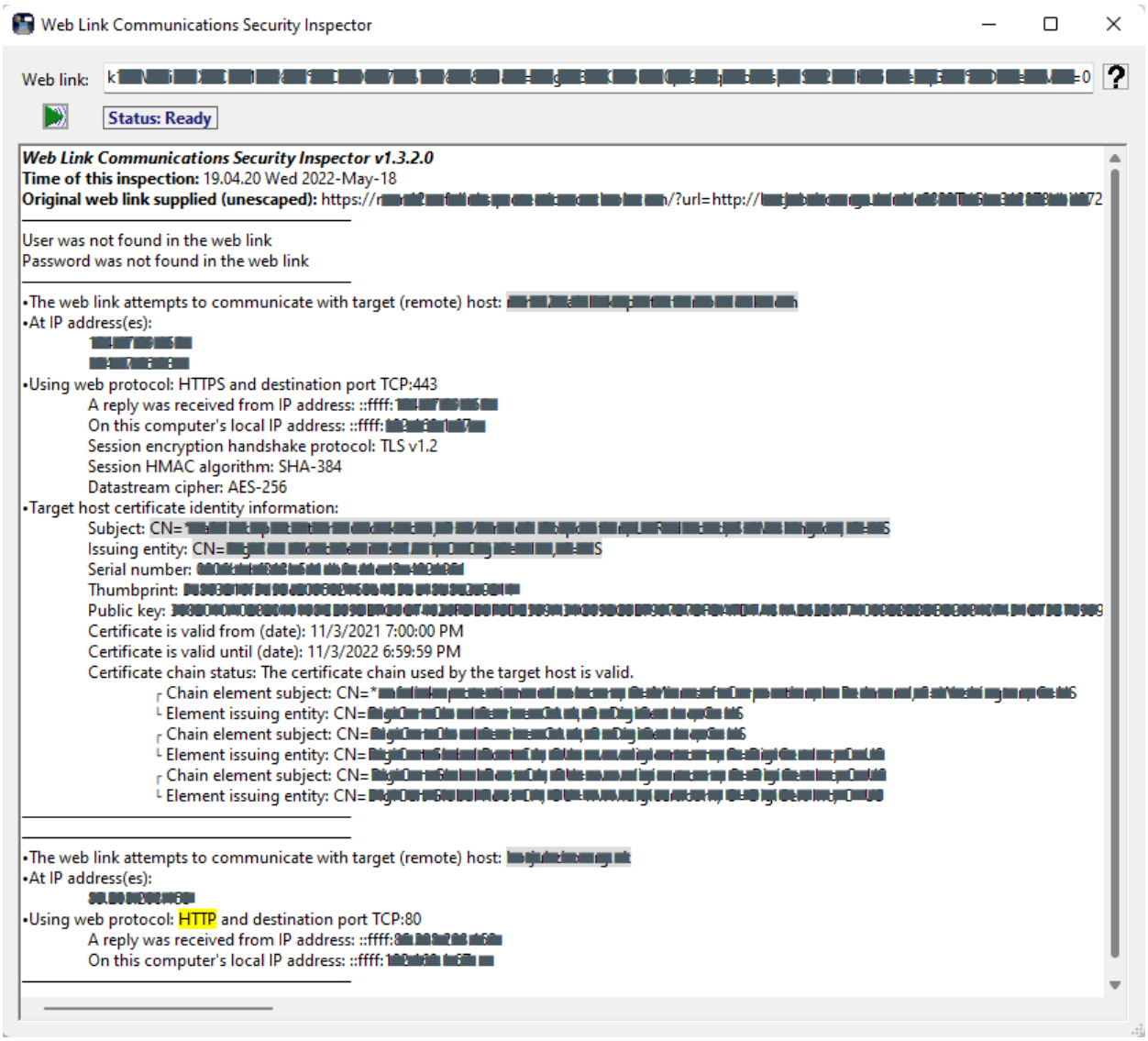


After you right click and choose 'copy link' in your browser, it will then be available for you to paste into this application. This application accepts key shortcuts, <Ctrl>+<V>, or the right-mouse click context menu paste operation.

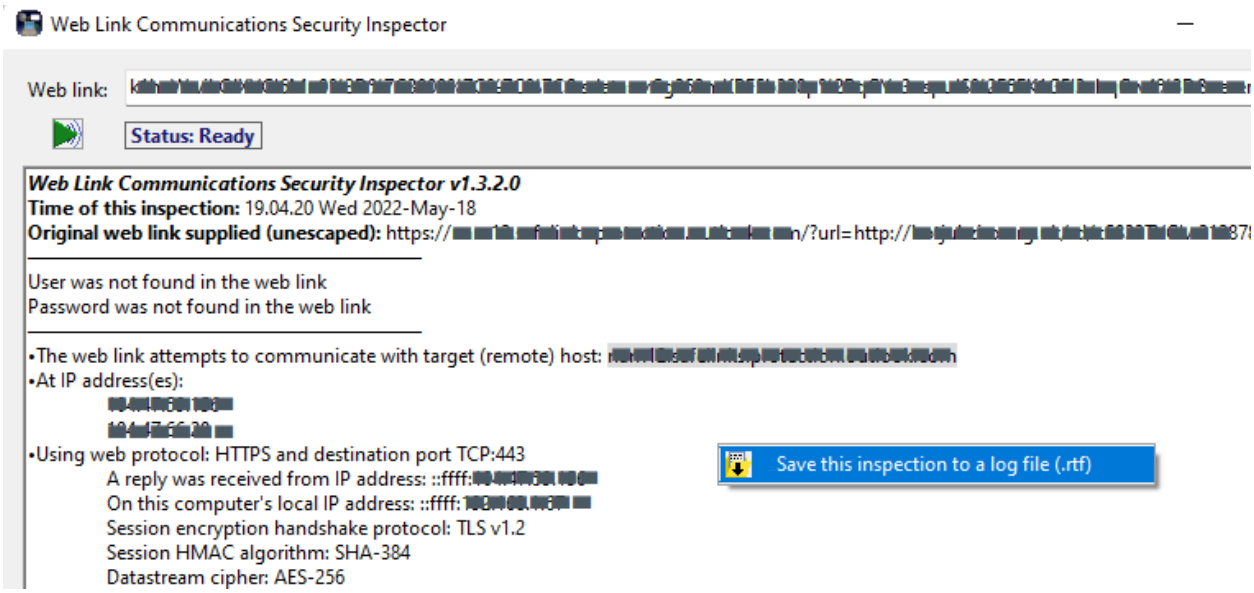


When you've pasted or typed a web link in the input area you are ready to run an inspection and get an analysis.

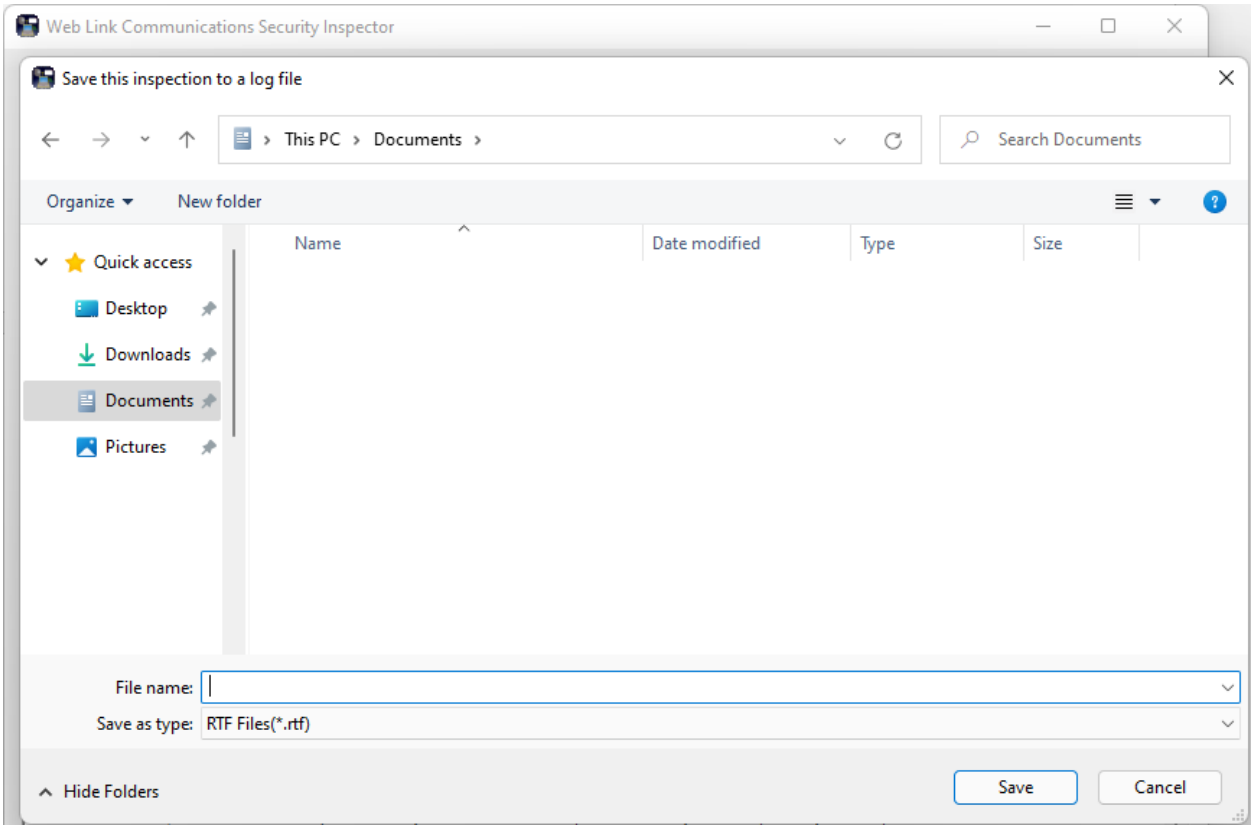
Click the buttons to run a safe inspection on the web link. The following image shows a sample of what is included in the output.



After you run an inspection, you can copy areas of the output that you select with your mouse, by using <Ctrl>+<C> to copy them to the Windows clipboard. If you would like to save the output to a report, a right-click of your mouse in the output area brings up the context menu. From the context menu you can save the inspection to a .rtf format log file. It is sometimes helpful to share such a report between members of support or cybersecurity incident response teams.



Simply enter the file name and location in the *save* dialog box to save your output.



Web Link Communications Security Inspector safely provides useful analytical information on web link communications whether you use it in a professional setting or personally from your own computer. In addition to analyzing suspicious web links from your email or other messaging system, you can also use this application to diagnose or validate communications with your company webservers or with your personal webserver before setting them up live on the Internet. This application may also be useful in security awareness training scenarios, to illustrate how the security of protocols used often varies from link-to-link or when you place constraints on TLS negotiation.