# ctie Documentation

*Release 1.0*

**John Rasiko**

**Apr 10, 2017**

# Contents:

CHAPTER 1

# FAQ

## What is the purpose of *CTIE*?

*CTIE* is used to quickly extract Indicators of Compromise (IoC) from multiple documents and consolidate the results into a file that can be imported in network defense appliances or as appendices to reports.

## What type of indicators does *CTIE* look for?

- MD5, SHA1 and SHA256 hashes;
- IPv4 and IPv6 addresses;
- URLs;
- Email addresses;
- Registry keys;

The unlimited version of *CTIE* can also extract:

- CARO-named malware names; and
- CVE references numbers.

And you can define your own extraction rules as well to get additional indicators.

## What kind of files can be read by *CTIE*?

*CTIE* can read the most common file formats used for reports, more precisely, *CTIE* can read the following files:

- Microsoft Word; .doc, .docx;
- Microsoft Excel; .xls, .xlsx;

- Microsoft PowerPoint; .ppt, .pptx;
- Portable Document Format; .pdf;
- Webpages; .htm, .html;
- Plain text files; .txt
- Rich Text Format; .rtf
- Comma-Separated Values (CSV) format; .csv

---

**Note:** *CTIE* should be able to read and extract indicators from any text file, but may not be able to parse its structure. For example, *CTIE* will be able to read XML files, but not parse it. Just rename the file to a *.txt* file to import it in the application.

---

CHAPTER 2

# Introduction

Welcome to *CTIE*, the Cyber Threat Intelligence Extractor, a light-weight tool to quickly extract Indicators of Compromise (IoC) from multiple reports.

## What is *CTIE*?

*CTIE* is a light-weight .NET application to quickly extract indicators of compromise from reports and export them into convenient file formats for network administrators, network defenders and cyber intelligence analysts.

## Why do I need *CTIE*?

More and more reports are coming out everyday and can easily overwhelm any analyst or any administrator. You certainly do not have the time to go throught all of these reports to copy/paste and craft rules or reports from scratch. *CTIE* automates this process for you: it reads files from different formats, extracts the IoC you need and outputs them in a convenient file format.

## How does it work?

1. Select the documents you want to analyze
2. Select which kind of indicators you want to extract
3. Review the results and discards unneeded indicators
4. Save to a file format of your choosing!

Read more to learn all the features of *CTIE*!

CHAPTER 3

# Quick Tutorial

This quick tutorial will show you the 3 steps to start extracting indicators out of documents and get you started using CTIE in less than 2 minutes.

## Step 1: Select Sources and Indicators

### Step 1(a): Select the Documents

To collect indicators, you must tell the application where to get them. You can select both local files or documents hosted on remote web sites. *CTIE* supports the most common file formats for reports such as Microsoft Office® documents or Portable Document Format (PDF) files. You can also include hyperlinks. Use the **Add File(s)**, **Add Folder** or **Add Link(s)** buttons (1) on the main window to select files to extract indicators from.

### Step 1 (b): Select the Indicators

Once you have selected where you want *CTIE* to look, you will need to tell the program what to look for or in other words, what indicators are you looking for. This is done by selecting the various indicator categories in the **Indicators (2)** section of the main window.

At this point, you're all set! Click **Next (3)** to start the extraction process. Depending on the quantity of documents to analyze, this may take a while. Proceed to step 2 to review the results.

## Step 2: Review the Results

It's very difficult to catch the exact indicators from such a wide variety of reports and file formats that currently exists. As such, *CTIE* may return a number of irrelevant results, such as benign web addresses or local Internet Protocol (IP) addresses. While you can configure *CTIE* to better filter out these, you should always review the results to make sure they fit your needs and the results does not include benign indicators. After the extraction process is completed, the program will display all the indicators it found and display them in a table.

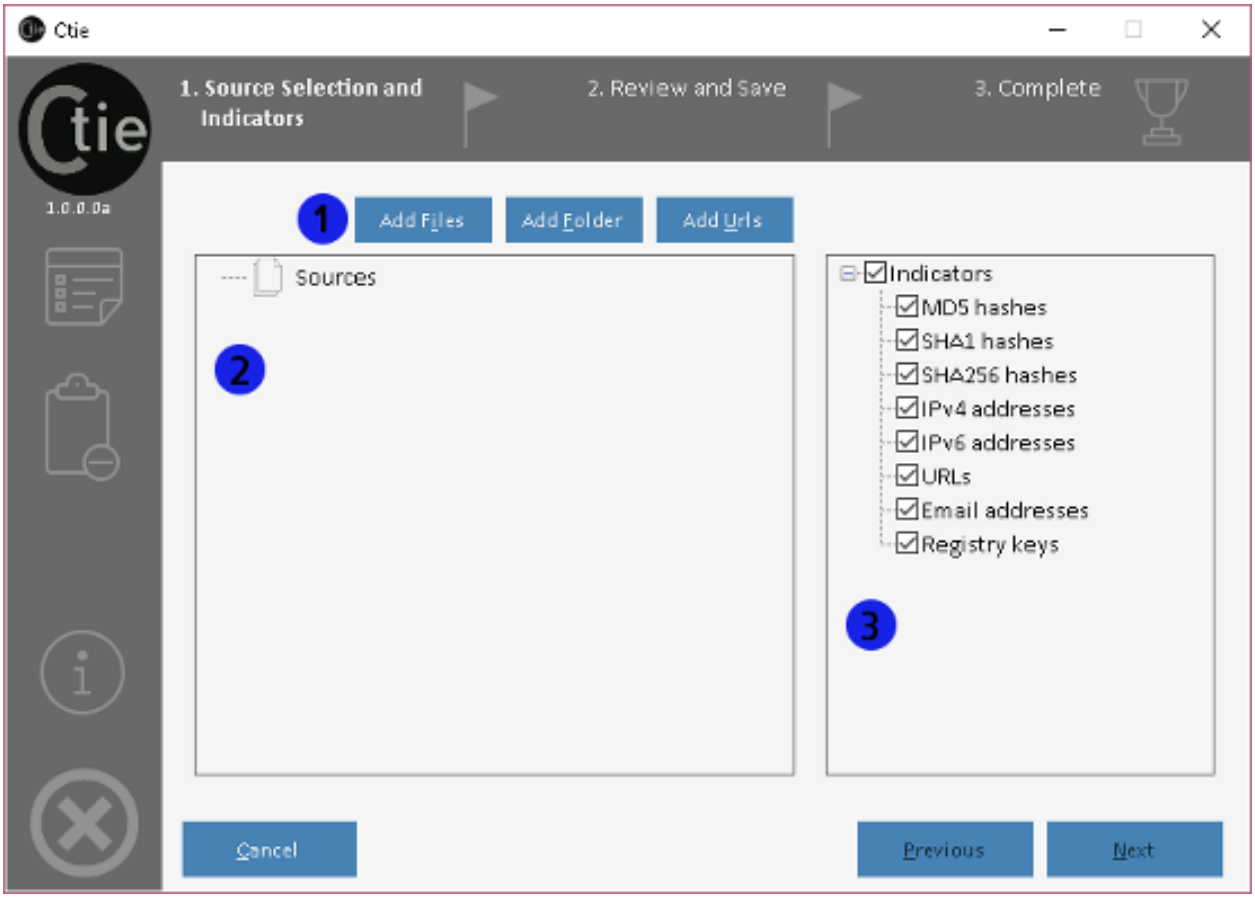


Fig. 3.1: Import **one or multiple sources (1)**. These sources will be displayed in the **Sources (2)** section and click **Next (3)** to start the extraction proces.

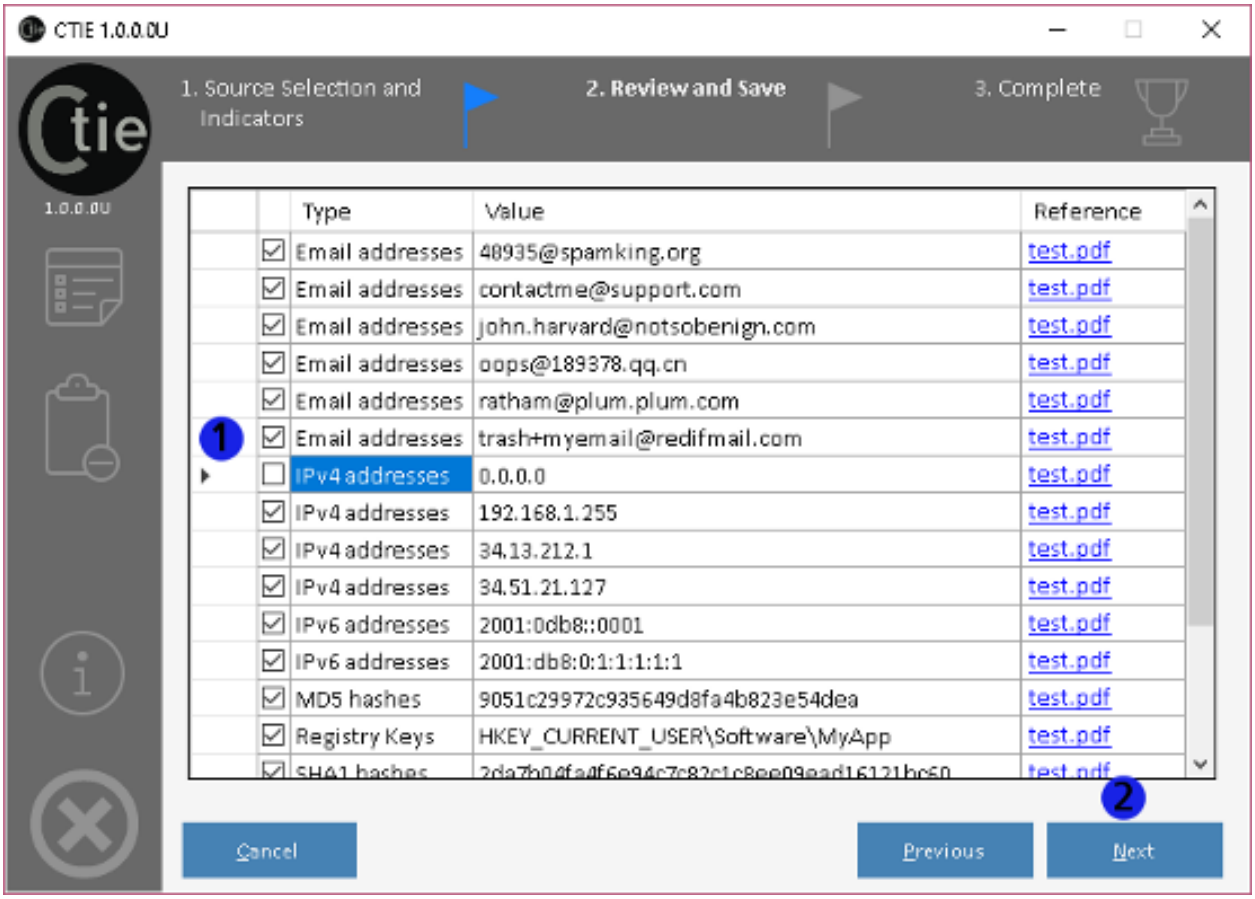


Fig. 3.2: **Unselect the undesired indicators (1)** and click **Next (2)** to export them into a file.

Simply unselect the indicators you do not wish to export by unchecking boxes (1). At any time, you can click "Previous" to modify the sources or indicators. Once you're satisfied with the results, click **Next (2)** to proceed to the last step.

## Step 3: Export to a File

Once you click **Next (2)**, you will be prompted to choose a location where to export the results and a file format. In the **Export As** dialog perform this steps:

1. Select a location on your computer (1);
2. Select a filename (2);
3. Select a file format (3); and
4. Click **OK** and you're done!

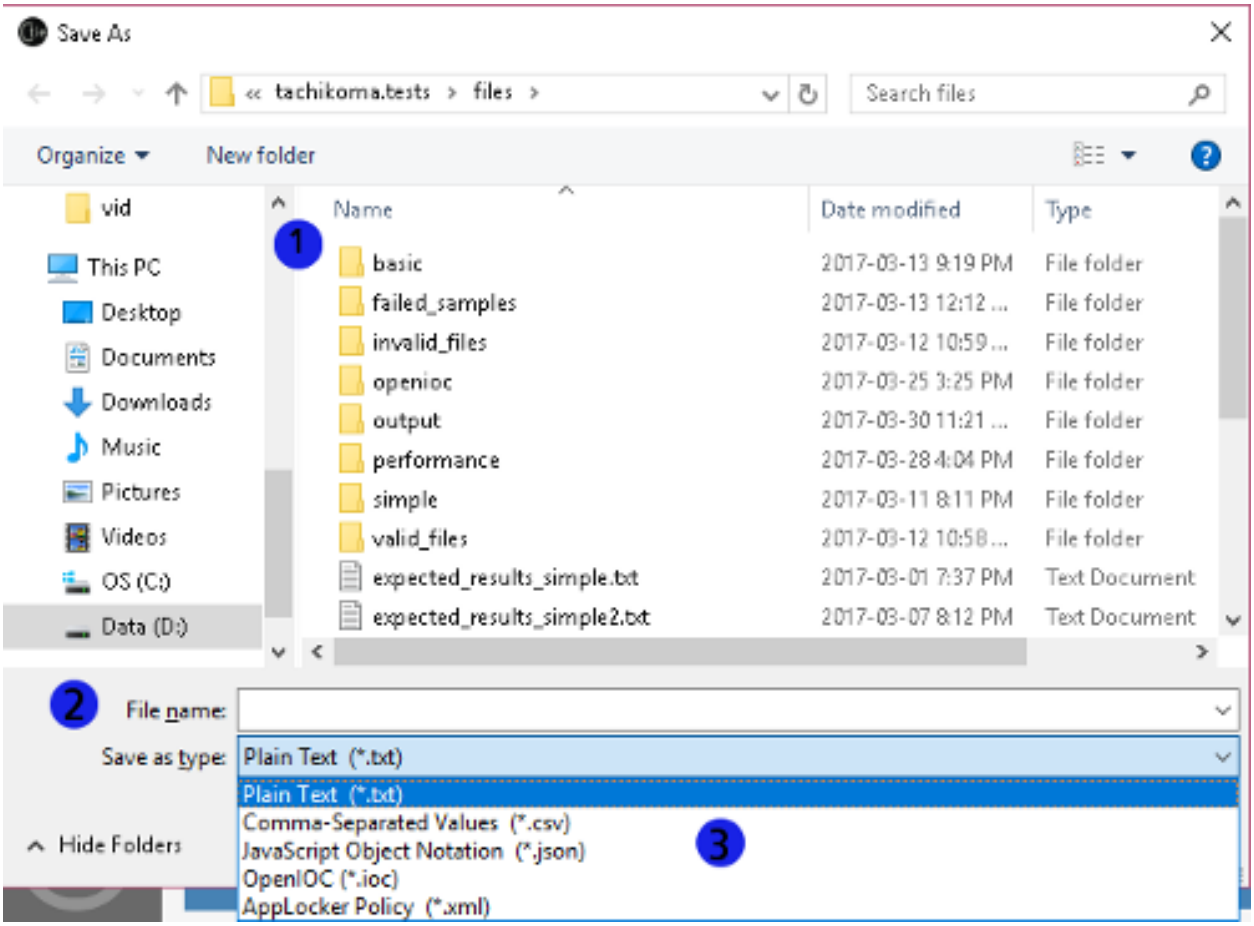


Fig. 3.3: **Select a location (1)** and **filename (2)**, **select a file format (3) and click **OK** to export the indicators into a file.

After clicking on **Save**, *CTIE* will create the file at the You can then review the output file by selecting **Open File** and/or start the extraction process again by clicking **Finish**.

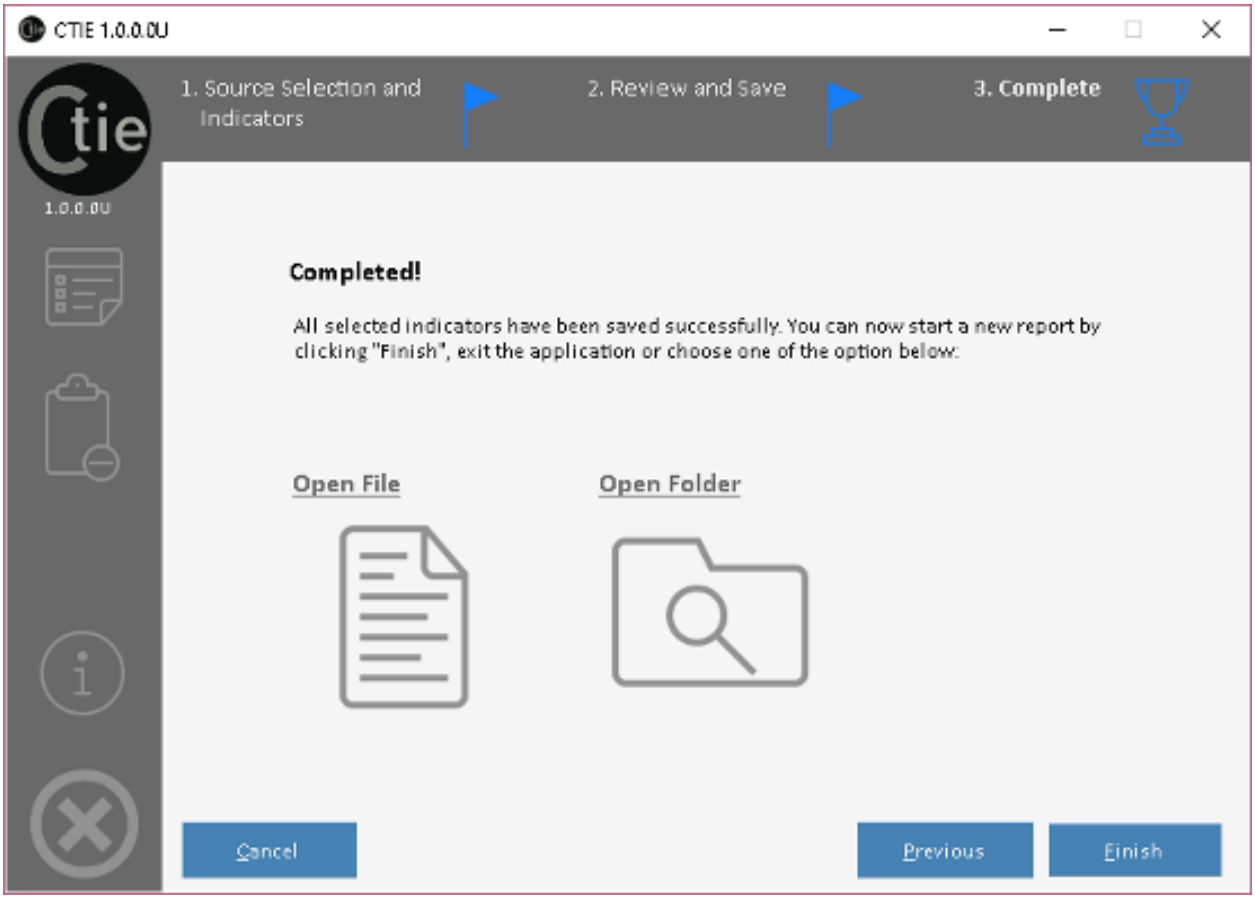


Fig. 3.4: Once the indicators has been saved, you can review the file or restart the process.

CHAPTER 4

# The User Interface

## The Main Window

### The Progression Bar

### The Settings Toolbar

### The Navigation Toolbar

## The Extraction Wizard

### The Source and Indicator Selection Panel

### The Indicators Review Panel

### The Conclusion Panel

## The Extraction Rules Editor

## The Exclusion Rules Editor

CHAPTER 5

# Selecting Sources and Indicators

The first step of the extraction process is to provide *CTIE* with documents to read. This is where the indicators will be extracted from. These documents can be offline or online as long as they are supported *CTIE* will be able to read their contents. You must also tell the application what do look for, i.e. hashes, emails or IP addresses.

## Import Files

Before the extraction process can occur, you must import documents into *CTIE*. To import files, follow the steps below:

1. Select the **Add Files (1)** button or press **Alt + i**. Doing so will open a **Open File** dialog
2. Using the **Open File** dialog, select one or multiple files (2). You can select multiple files from the same folder by pressing and holding the **Ctrl** key on your keyboard while clicking on the filenames. Once completed, click on **Open (3)**.
3. After clicking **Open (3)**, the dialog will close and the files selected will be added to the **Sources** section of the main window. Repeat this step as needed to add more files.

---

**Note:** *CTIE* should be able to read and extract indicators from any text file, but may not be able to parse its structure. For example, *CTIE* will be able to read XML files, but not parse it. Just rename the file to a *.txt* file to import text-based files in the application.

---

## Import Folders

In some cases, you may prefer to import all the files included in a folder rather than selecting files one by one. *CTIE* provides the ability to do so by using the **Add Folder (1)** button in the main window.

**Select the folder (2)** containing the files you wish to import into *CTIE* using the **Browse For Folder** dialog appearing. Click on **OK (3)** to start importing files.

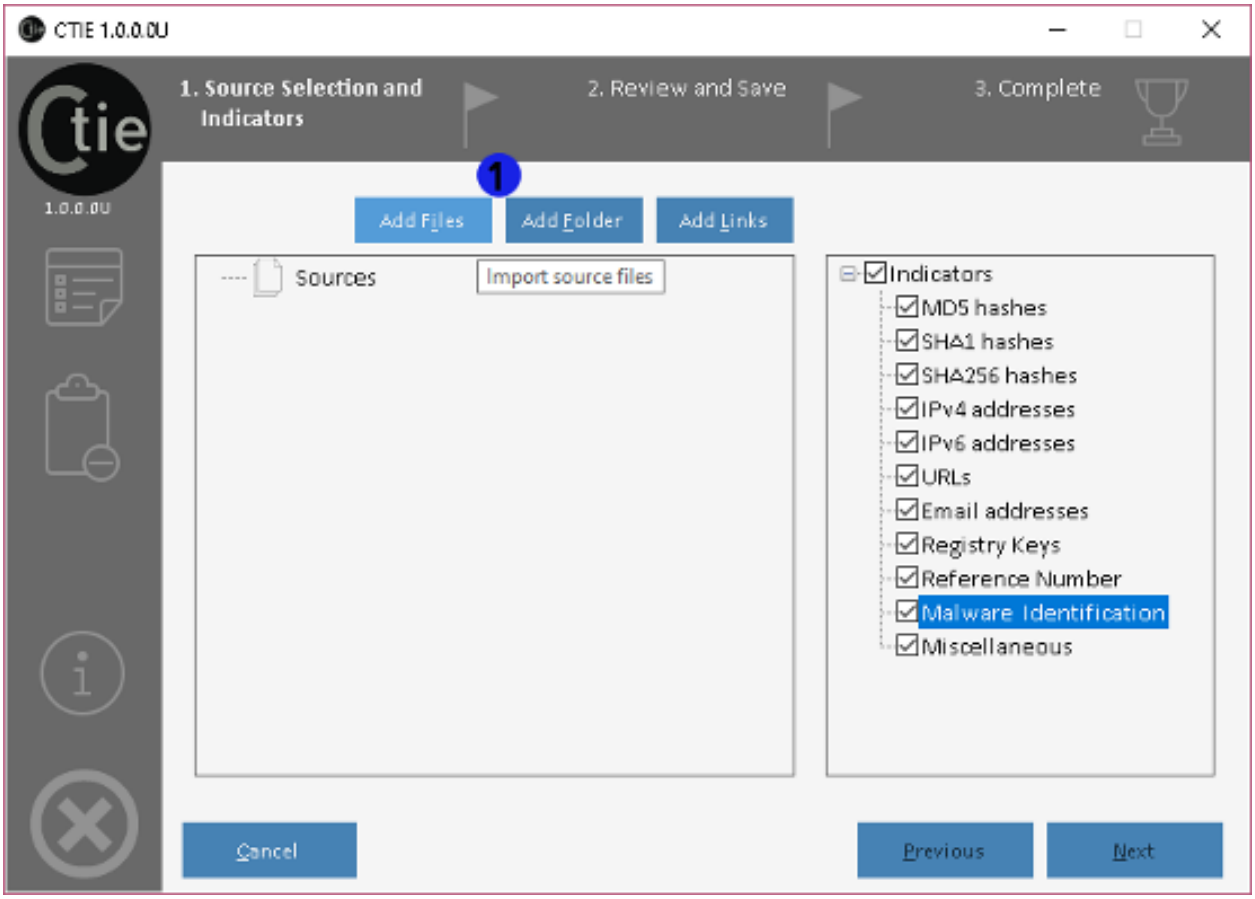


Fig. 5.1: Click the **Add Files (1)** button above the **Sources** section to show the **Open File** dialog.

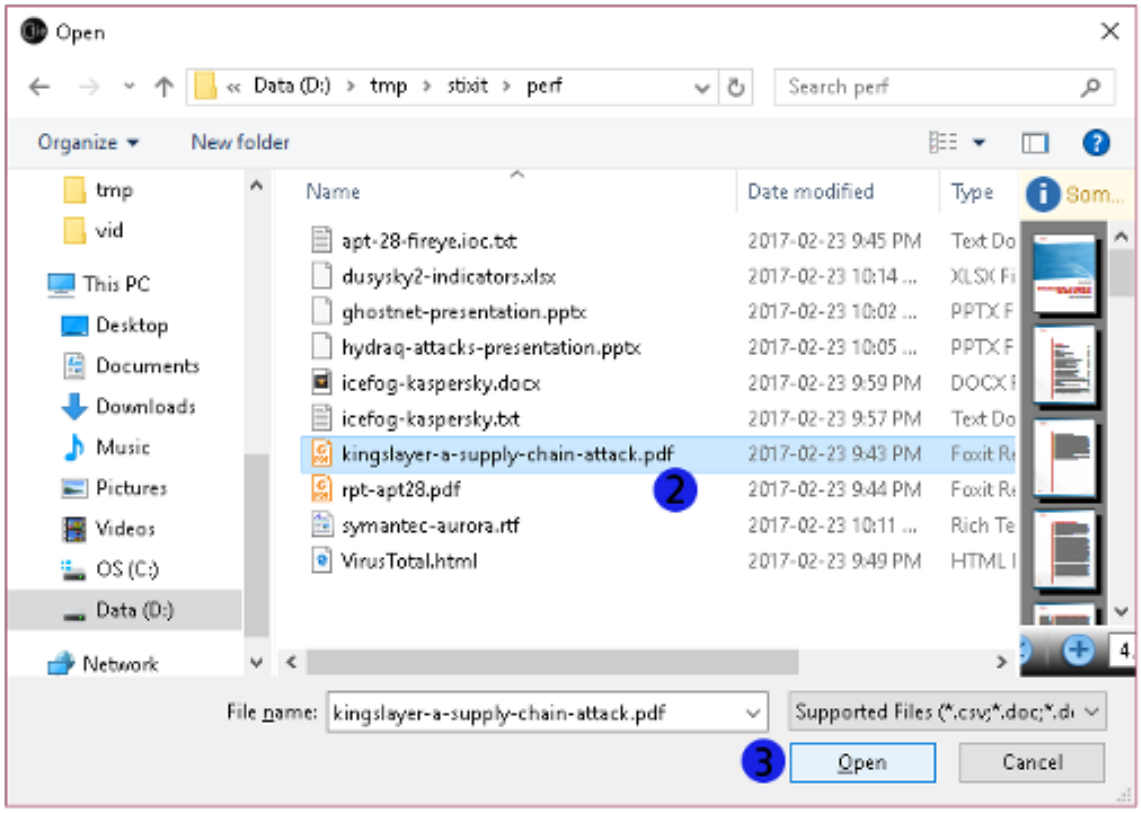


Fig. 5.2: Select **one or multiple files (2)** and click on **Open (3)** to add the selected files as sources.

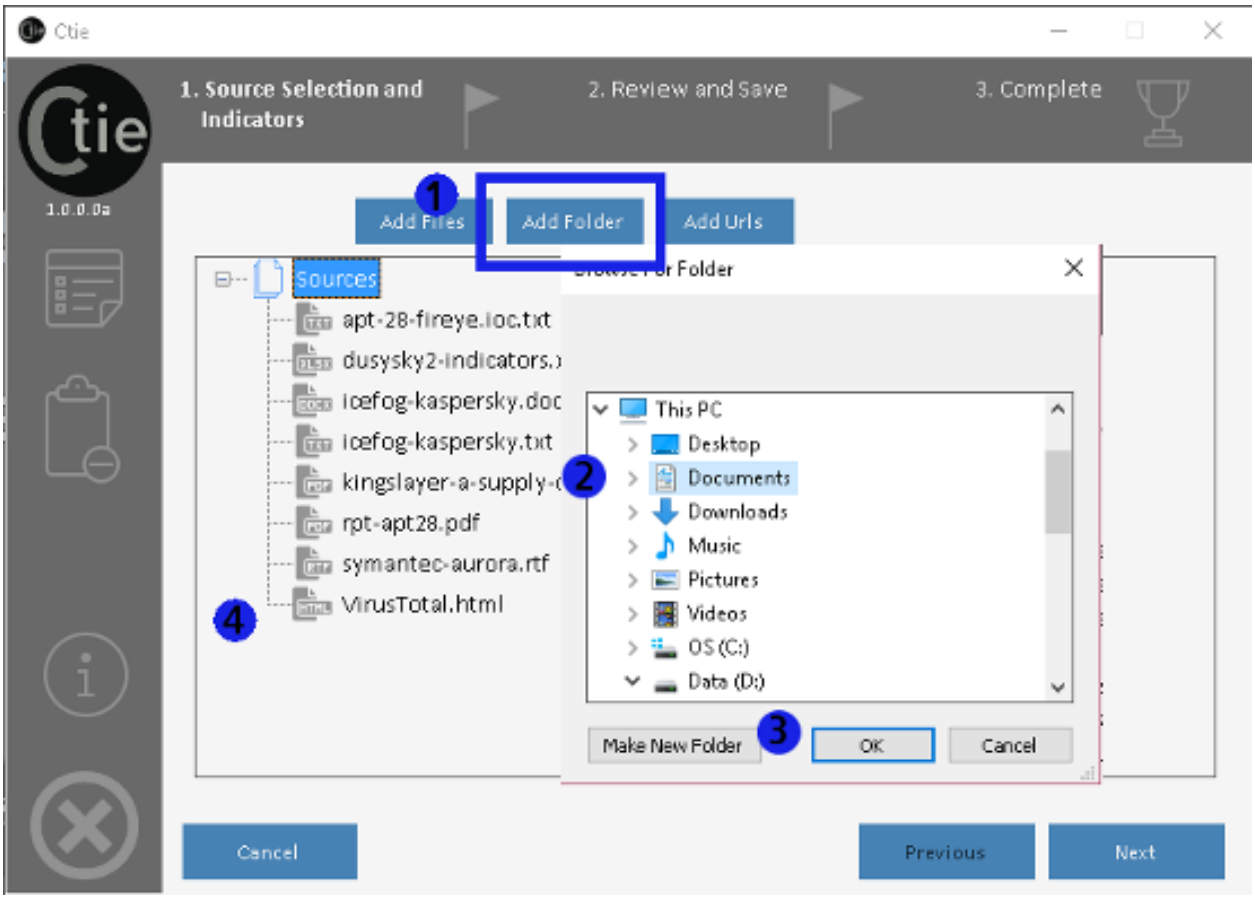


Fig. 5.3: Select the **Add Folder** button to show the **Browser for Folder** dialog to select a folder.

**Note:** Only files supported by the application will be imported. All files with unrecognized extensions will not be imported.

Once the program is finished, all files will be listed in the **Sources section (4)** of the main window.

## Import Links

*CTIE* allows you to read files directly from the web by specifying Uniform Resource Locators (URLs), e.g. web addresses. The program will read the given web pages and extract indicators from the visible text of its contents. To extract indicators from web pages, you will be required to be connected to the Internet and click on the **Add Links** button on the main page.

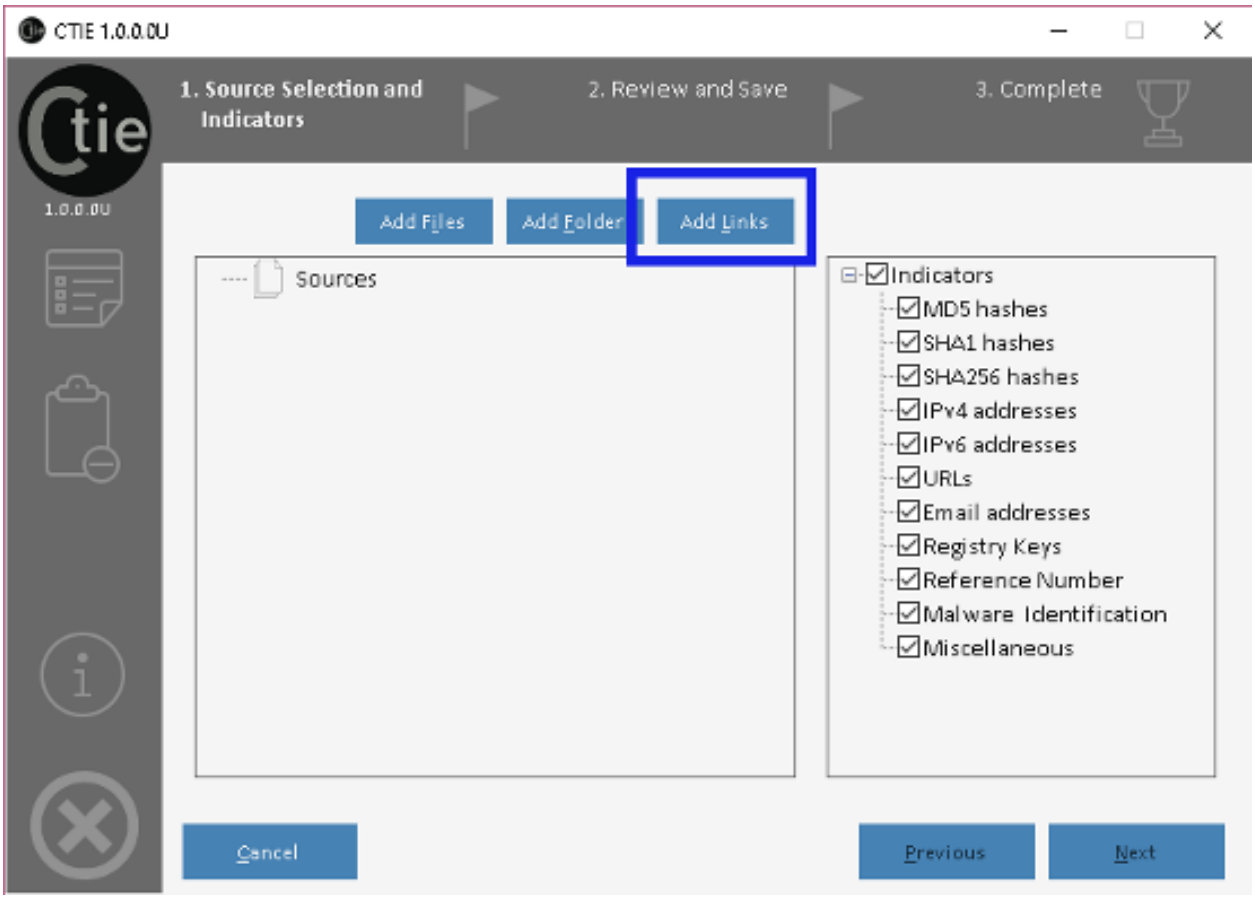


Fig. 5.4: Click on the **Add Links** on the **Source and Indicators Selection Panel** to include online documents.

Once clicked, a new window will appear into which you will be able to type or copy/paste multiple links to be imported. Each URL must be specified on an individual line. Note that the content hosted at any address must be a supported by CTIE, otherwise you will receive an error message during the extraction process. For example, an address to a binary file will fail.

Simply enter each address on a separate line and select **Add Links** to import the selected documents.

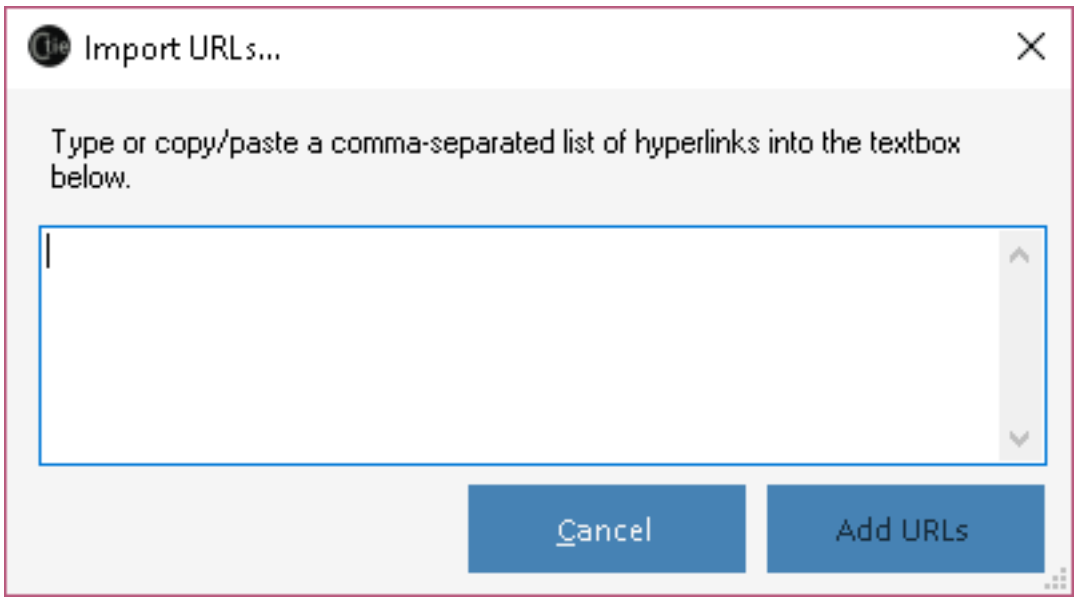


Fig. 5.5: After clicking **Add Links**, the **Import Links** dialog appears where you can specify one or more URLs.

> **Warning:** Each address must start with the **http** (or **https**) prefix, otherwise *CTIE* will not detect the document as an online file.

Web addresses specified must be to a supported document, otherwise *CTIE* will not be able to read its contents . At anytime, you can click **Cancel** to dismiss the dialog without importing the addresses entered.

After clicking **Add Links**, the dialog will close and links entered in the **Import Links** dialog will be added to the **Sources** section of the main window:

## Selecting and Removing Sources

If you want to remove one specific sources follow the instructions below:

1. Right-click on the document to remove in the **Sources** section to show the contextual menu;
2. Within the menu, select **Remove**. The selected file or URL will be removed from the list. You can also press the **Delete** key.

If you want to remove multiple sources, repeat steps 1 and 2 for each document. To remove all of the selected sources, select the **Remove All** option.

## Selecting Indicator Types

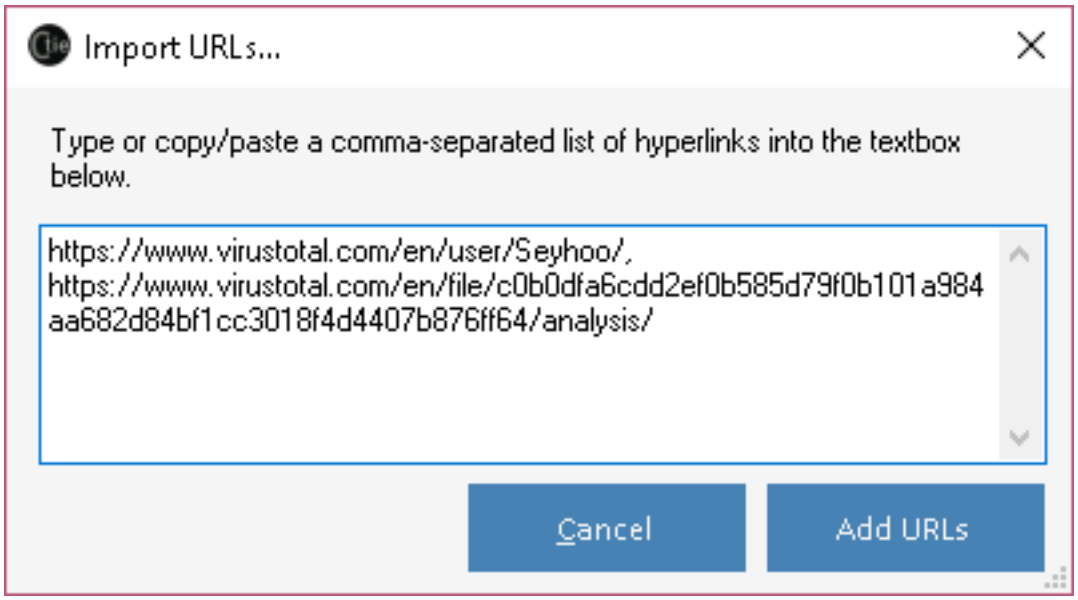


Fig. 5.6: Enter each URL on a separate line in the **Import Links** dialog and click **Add Links**.

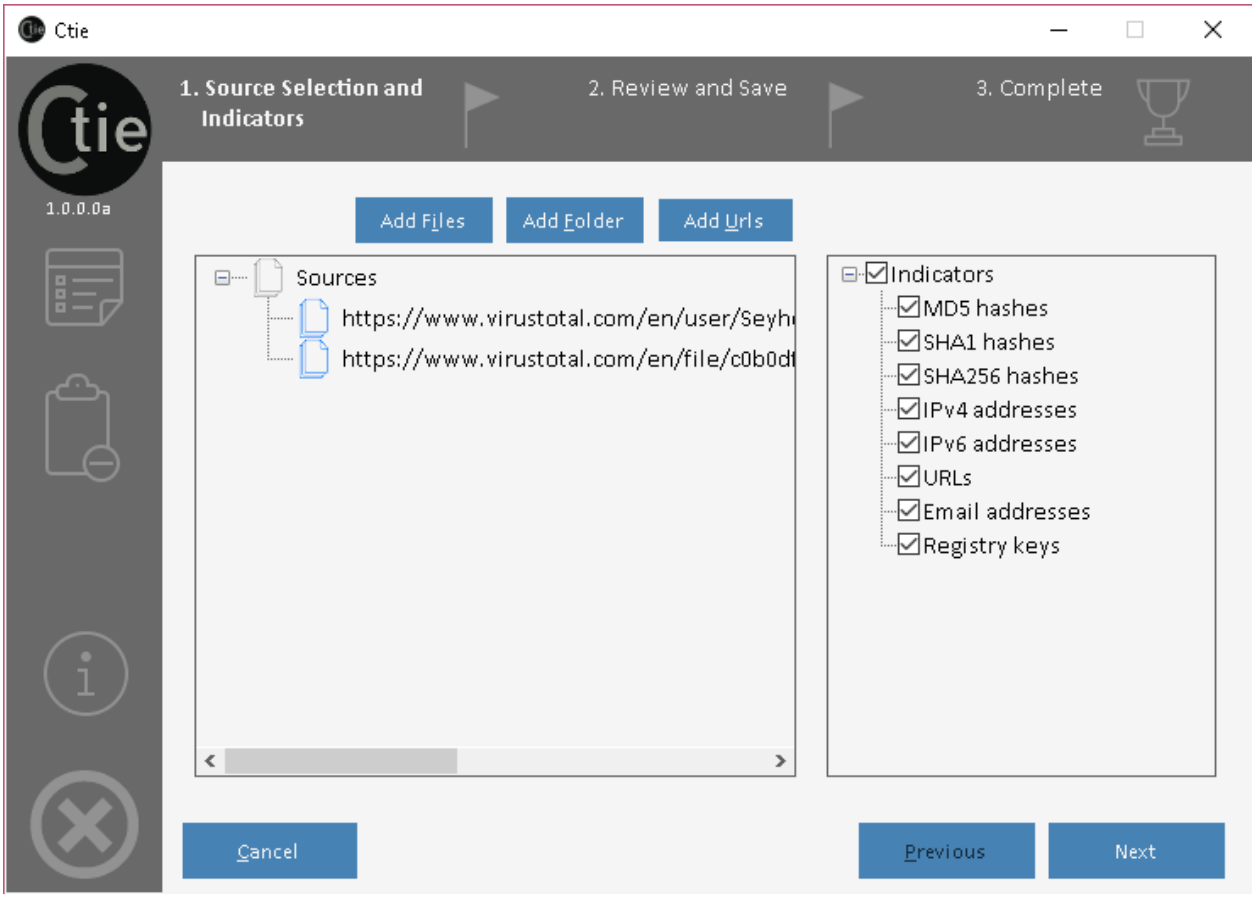


Fig. 5.7: The URLs are then added to the **Sources** section.

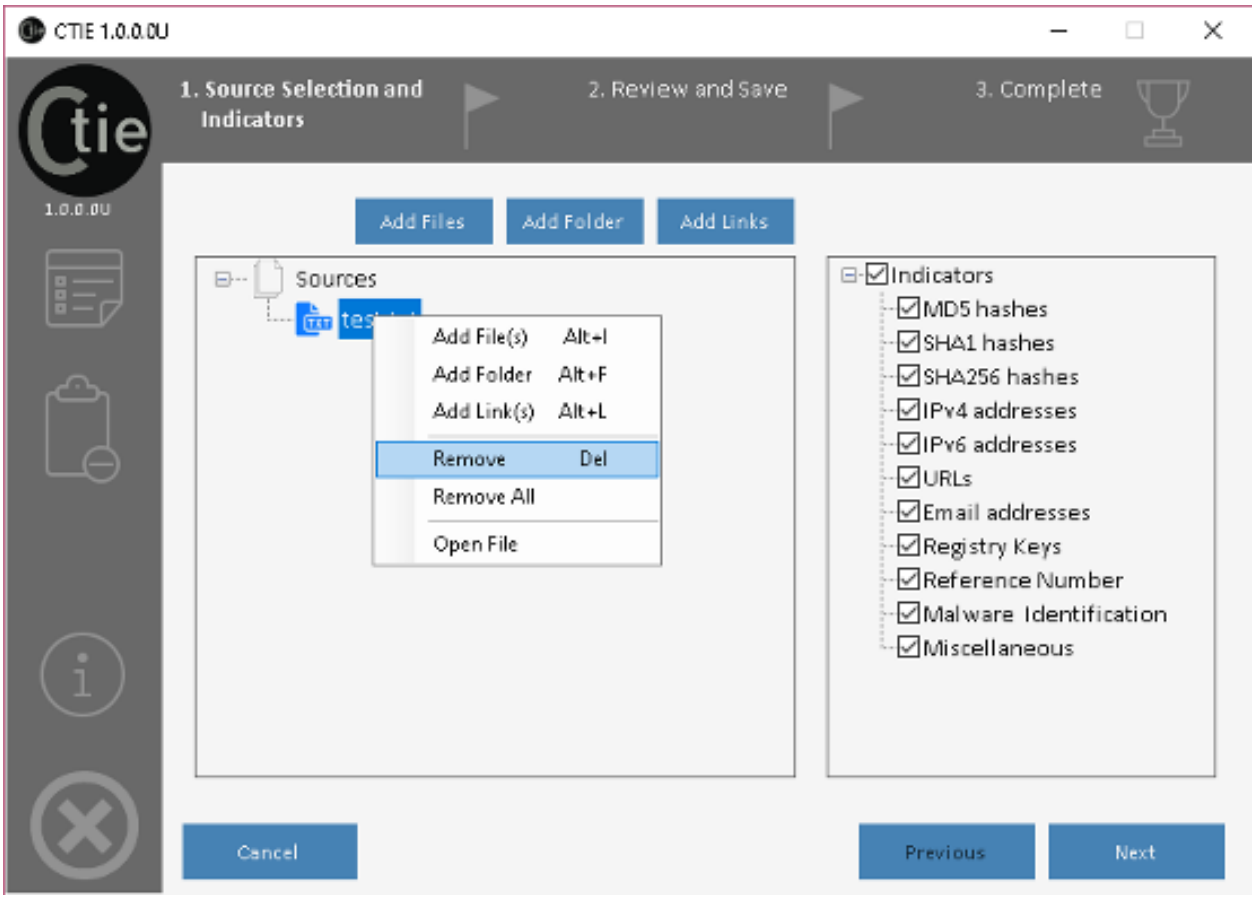


Fig. 5.8: Remove sources by choosing the appropriate option in the contextual menu on the **Sources** section.

CHAPTER 6

# Managing Extration Rules

## Adding or Updating Rules

## Deleting a Existing Rules

CHAPTER 7

# Managing Exclusion Rules

In many cases, you may want to filter out some of the results extracted by *CTIE*. For example, loopback IP addresses or valid URLs such as *google.com* should not be used as indicators.

## Adding and Updating Exclusion Rules

Exclusion rules allows you to discard indicators found during the extraction process which may not have any useful value to you. The rules are regular expressions that will be applied to the resulting indicators and be use to filter out false positive or garbage data, such as benign URLs or local IP addresses for example.

To add a new exclusion rule, first open the **Exclusion Rule Editor** by clicking on the **Exclusion List** icon on the main windows.

The **Exclusion Rules Editor** will appear and display the rules currently used by *CTIE*. To add a new rule, simply enter the following information in the last, empty row of the table;

1. A label uniquely identifying this rule.

> **Warning:** The label cannot be empty and must be unique.

2. The type of indicator to which this rule applies to. If a rule applies to multiple types, it will need to be entered multiple times.
3. The regular expression describing this rule.

> **Warning:** The regular expression cannot be empty and must be a valid C#-formatted regular expression. You can use an online regular expression tester such as RegexStorm

Once you are done adding new rules, click the **Save (5)** button. Rules will not be saved in the *CTIE* database until the **Save** button is clicked. To cancel all modifications since the last save, simply click **Close (4)**.

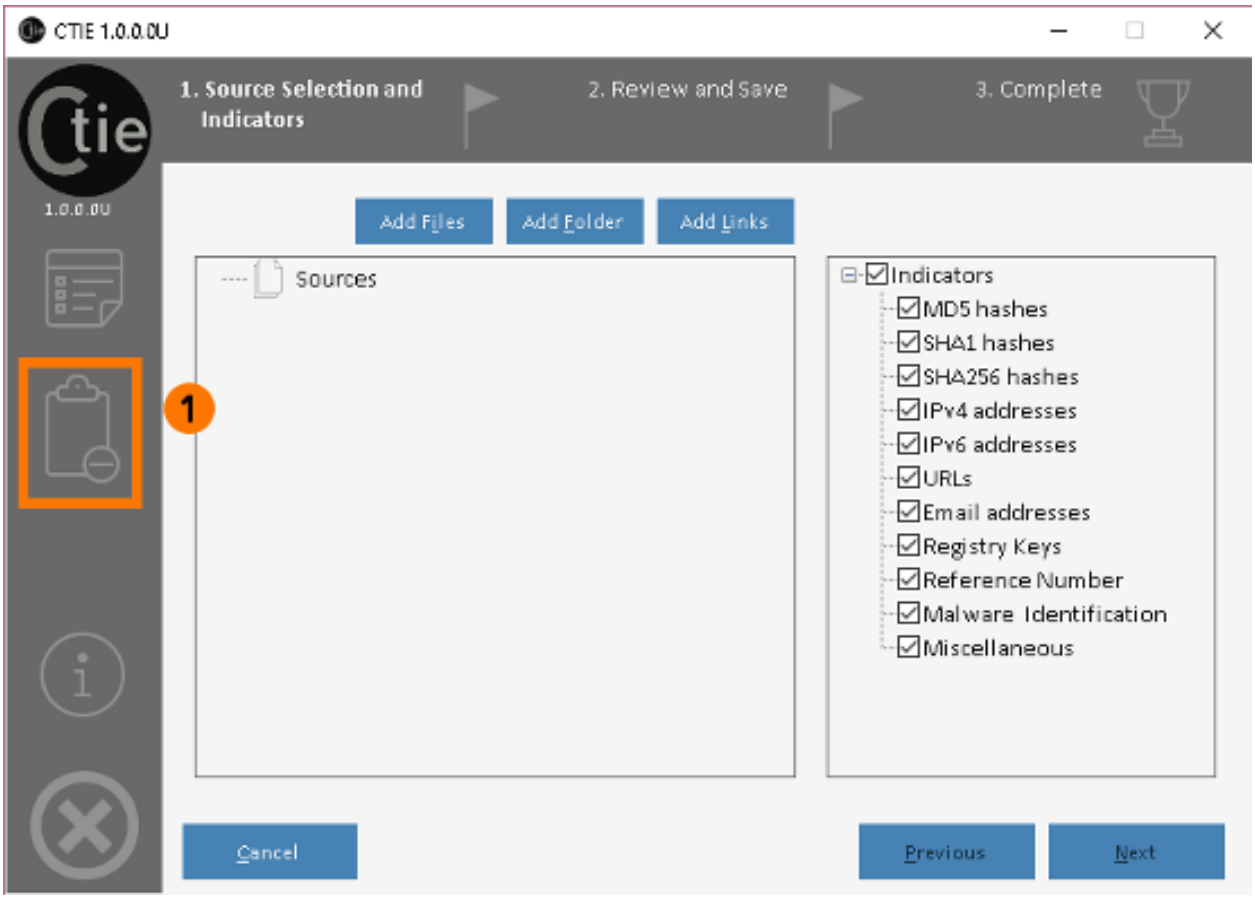


Fig. 7.1: Open the **Exclusion Rules Editor** by pressing the highlighted button (1) in the **Settings Bar**.

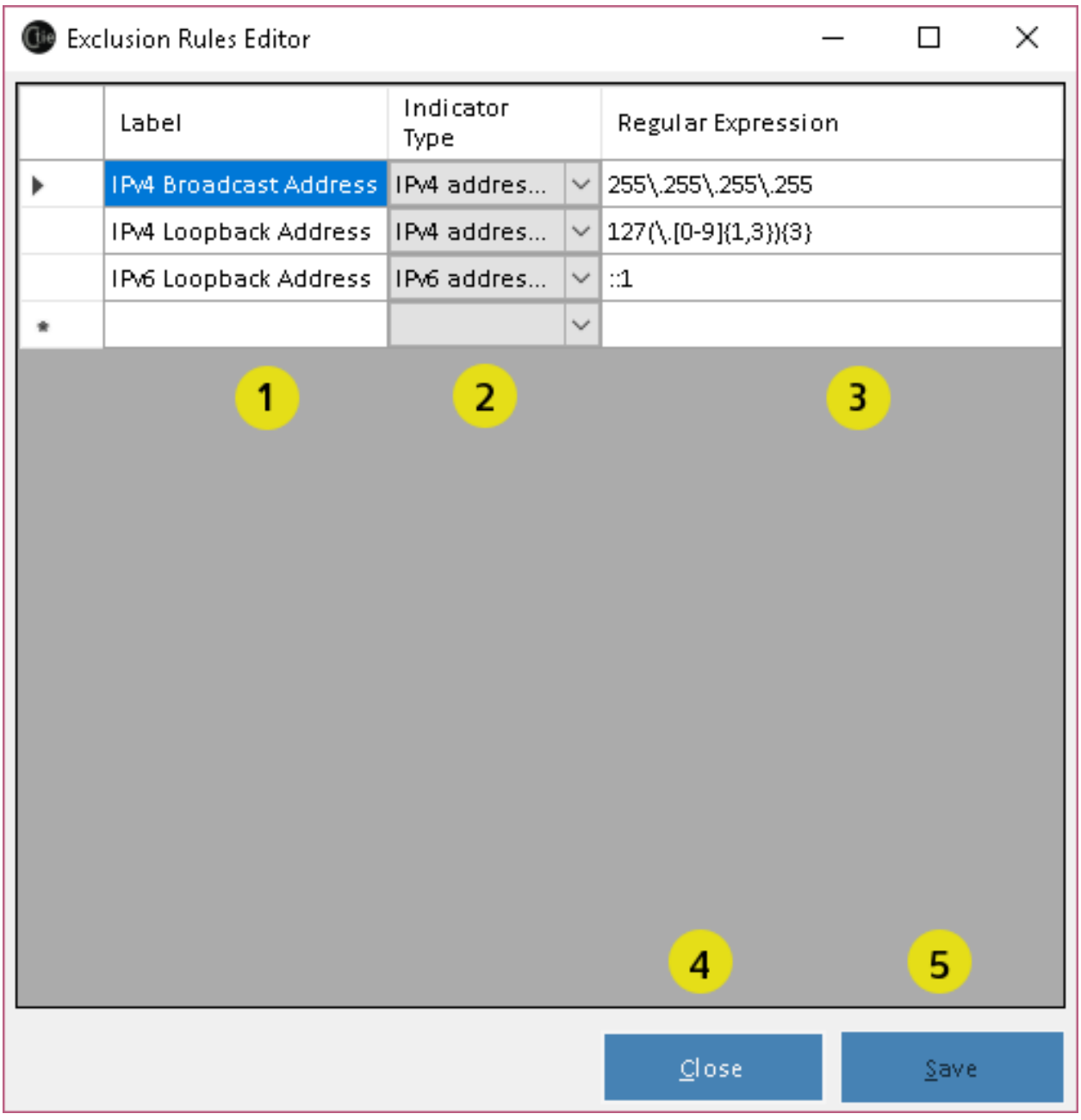


Fig. 7.2: The **Exclusion Rules Editor** user interface.

CHAPTER 8

# Reviewing the Extraction Results

CHAPTER 9

# Exporting to Files

## Exporting to the Plain Text Format

## Exporting to the CSV Format

## Exporting to the JSON Format

## Exporting to the OpenIOC Format

## Exporting as an AppLocker Policy

## Exporting to Snort Rules

CHAPTER 10

# Concluding the Process

## Reviewing the Resulting File

CHAPTER 11

# Indices and tables

- genindex
- modindex
- search