**UNDERSTANDING THE FUNCTIONS OF TOOL - 1**

Redline provides a variety of options for data collection, allowing you to gather essential information for analysis.

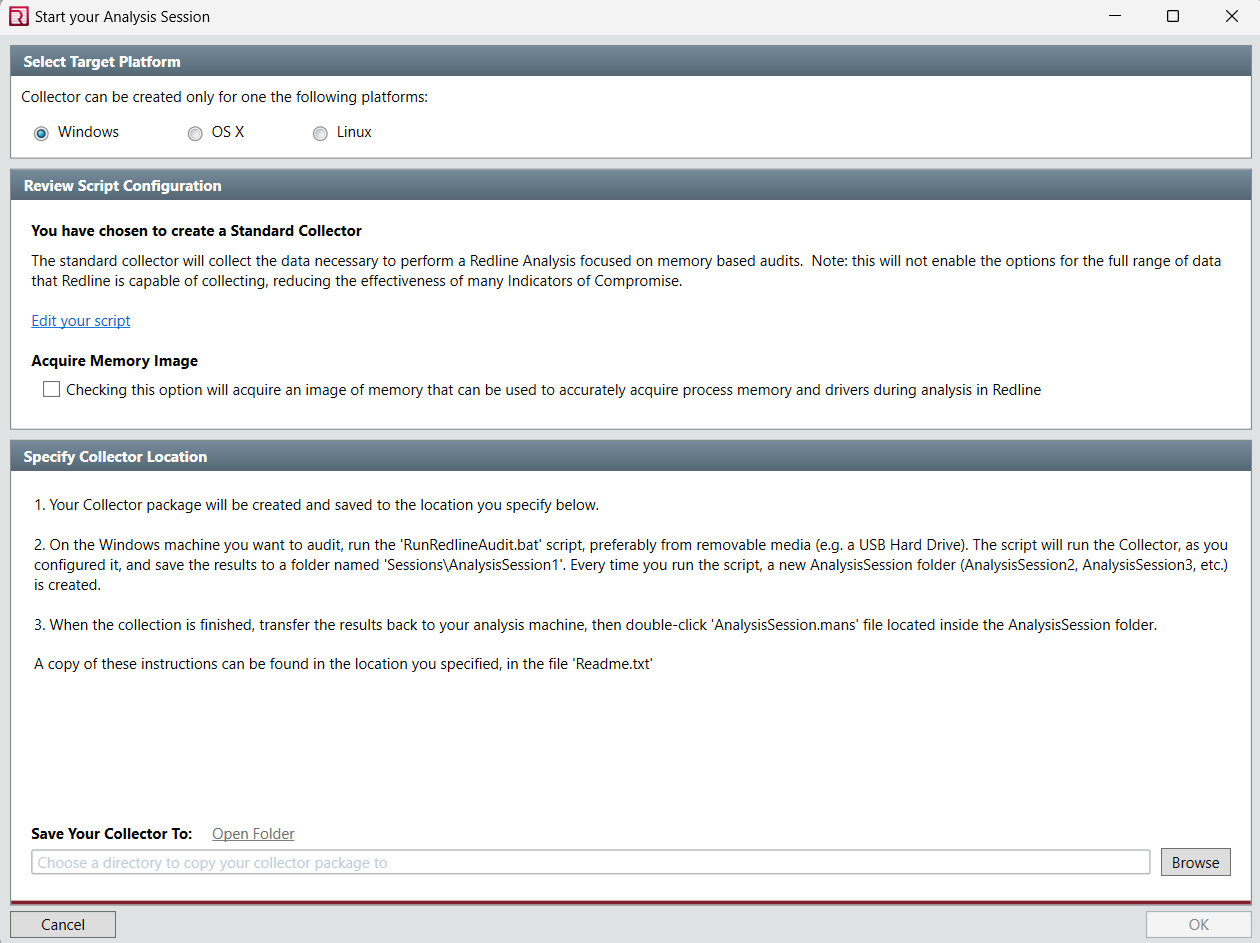
Following is the screenshot of how it looks when it is launched.

****

There are numerous options available to us. Let’s have a look on each:

**Under Collect Data:**

1. ***Create a Standard Collector:*** It configures a data collection package tailored to Redline’s assessment needs. It will collect all of the data needed by RedLine to score and assess a computer.



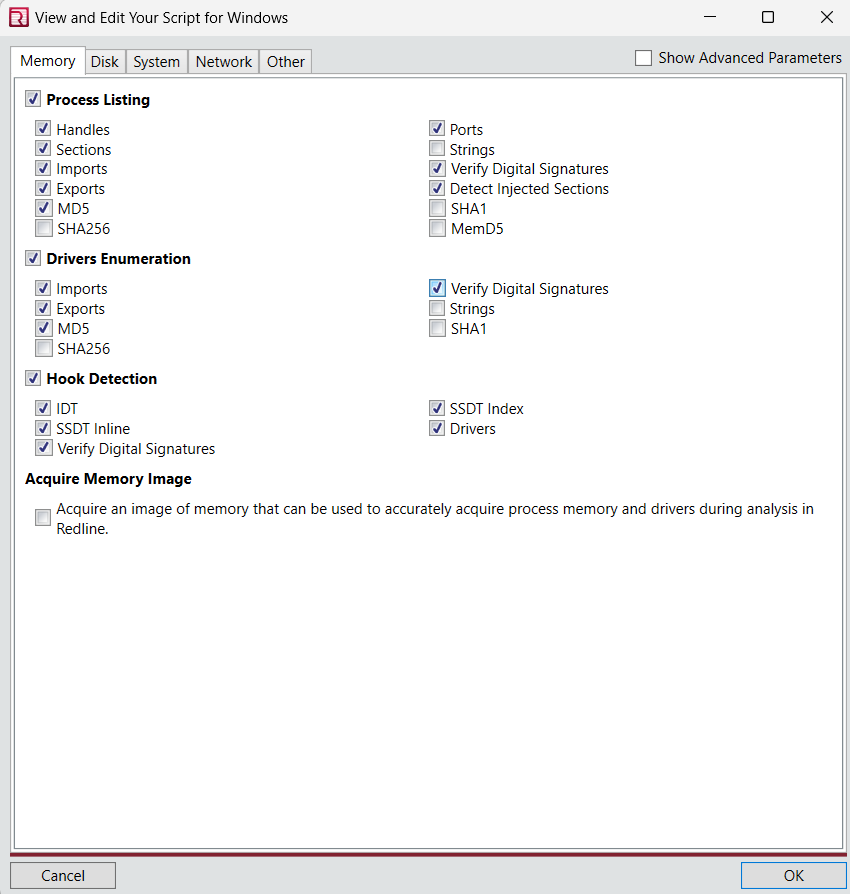
Now,

1. Select the target platform. (It could be Windows, Linux or OS X)

2. Click on edit your script to collect more data about the host.

3. When you click on Edit your script you will come across the following information and you can use it to acquire more data about the host, Memory, Disk, System and Network.

The screenshot for the same is attached below:

****

4. We can also acquire an image memory for the accuracy of process and drivers’ analysis by clicking on the checkbox present in the screenshot.



5. Click ok after browsing and selecting the destination folder and the first process will happen.

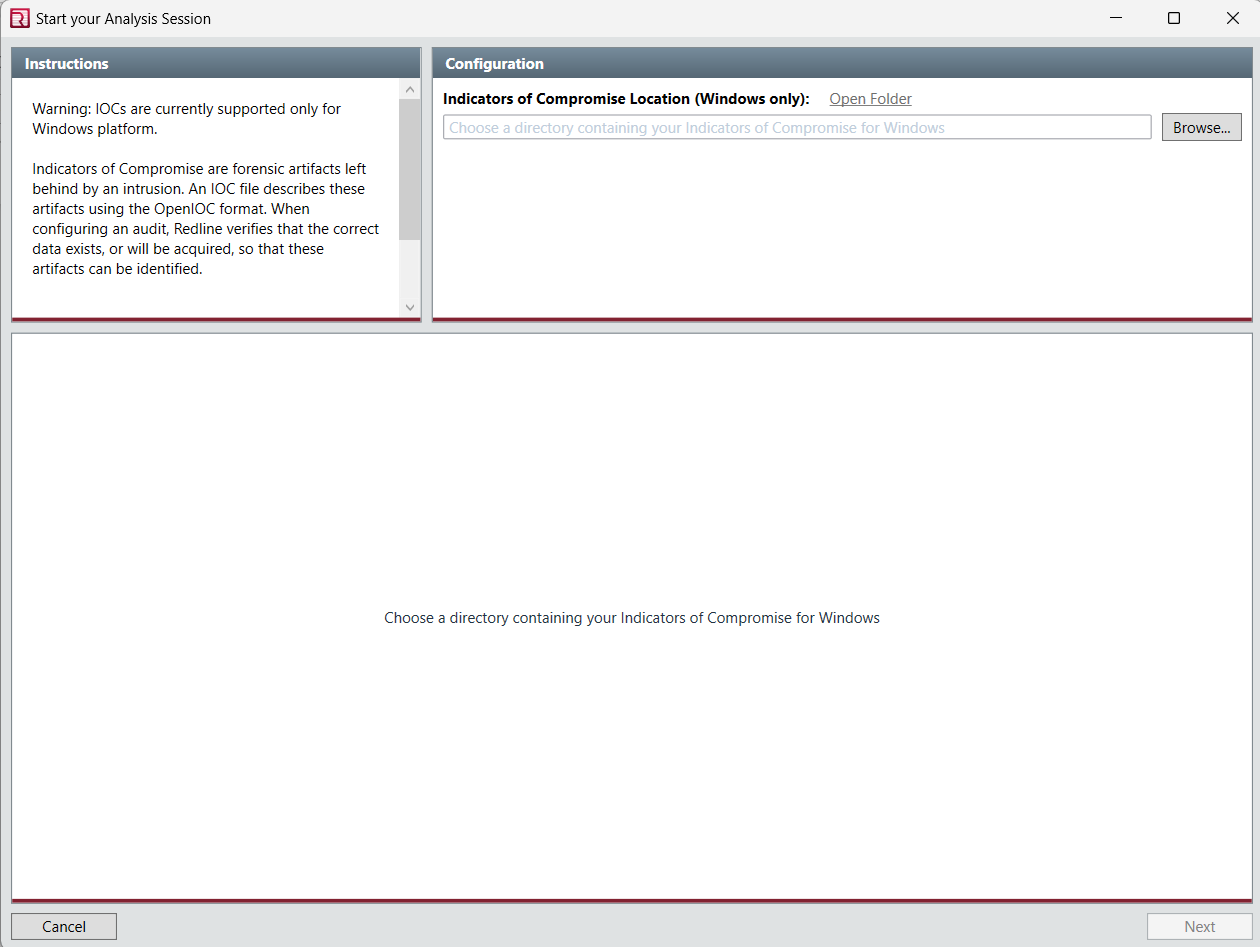
After following these steps your Collector package will be created and saved to the location you specified.

1. ***Create a Comprehensive Collector:*** It will configure a package which will collect all the data required by RedLine to assess and score a computer as well as additional data for Indicator of Compromise (IoC’s) searches.

The procedure for collecting is same as the previous one i.e. select target, edit script, acquire image(if needed), specify location and click on OK.

1. ***Create an IoC Search Collector:*** It will configure a package that will collect only the data needed to search for the Indicators of Compromise that you specify.

The following window appears when you select this option:



Here,

1. This functionality is supported for windows only, because the tool is windows based.

2. In the Configuration pane, choose the folder location in which you want RedLine store the resulting IoC’s.

3. IoCs are pieces of data, such as file hashes, IP addresses, domain names, or other artifacts, that indicate malicious activity or potential security breaches.

4. Once you've configured the settings, initiate the IoC search collector. Redline will then scan the specified system or network for the indicators of compromise based on your configurations.