**CREATION OF IOC REPORTS FOR THE IOC SEARCH COLLECTOR ANALYSIS**

Indicators of compromise (IOCs) are **digital evidence that suggests a system or network has been breached or attacked**. They can be used by information security professionals and system administrators to detect, diagnose, and respond to malicious activities. IOCs can take many forms, including:

* Unusual network traffic behavior
* Unexpected software installations
* User sign-ins from abnormal locations
* Large numbers of requests for the same file
* Virus signatures and IP addresses
* MD5 hashes of malware files
* URLs or domain names of botnet command and control servers

These are XML documents that help incident responders capture diverse information about threats including attributes of malicious files, characteristics of registry changes, artifacts in memory, and so on.

**INTRODUCING IOC EDITORS:**

We need an IOC Editor to create IOC reports. The IOC Editor is a tool that provides an interface for managing data and manipulating the logical structures of Indicators of Compromise (IOCs).

An IOC Editor can:

• Manipulate the logical structures that define the IOC

• Apply meta-information to IOCs including detailed descriptions or arbitrary labels

• Convert IOCs into XPath filters

• Manage lists of "Terms" that are used within IOCs

We can use any IOC editor for report creation, but here are some suggested ones:

1. **IOC EDITOR BY FIREEYE:** <https://fireeye.market/apps/S7cWpi9W>

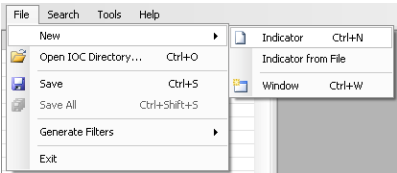
* Supported Operating Systems: Windows XP, Windows Vista, Windows 7 (32-bit and 64-bit)
* USER GUIDE: [https://fireeye.market/assets/apps/S7cWpi9W//9cb9857f/ug-ioc-editor.pdf](https://fireeye.market/assets/apps/S7cWpi9W/9cb9857f/ug-ioc-editor.pdf)

1. **OPENIOC 1.1 EDITOR:** <https://fireeye.market/apps/211404>

* Supported Operating Systems: Windows XP, Windows Vista, Windows 7 (32-bit and 64-bit), Windows 8.1 (32 and 64 bit), Windows 10 (32 and 64 bit)
* USER GUIDE: [https://fireeye.market/assets/apps/S7cWpi9W//9cb9857f/ug-ioc-editor.pdf](https://fireeye.market/assets/apps/S7cWpi9W/9cb9857f/ug-ioc-editor.pdf)

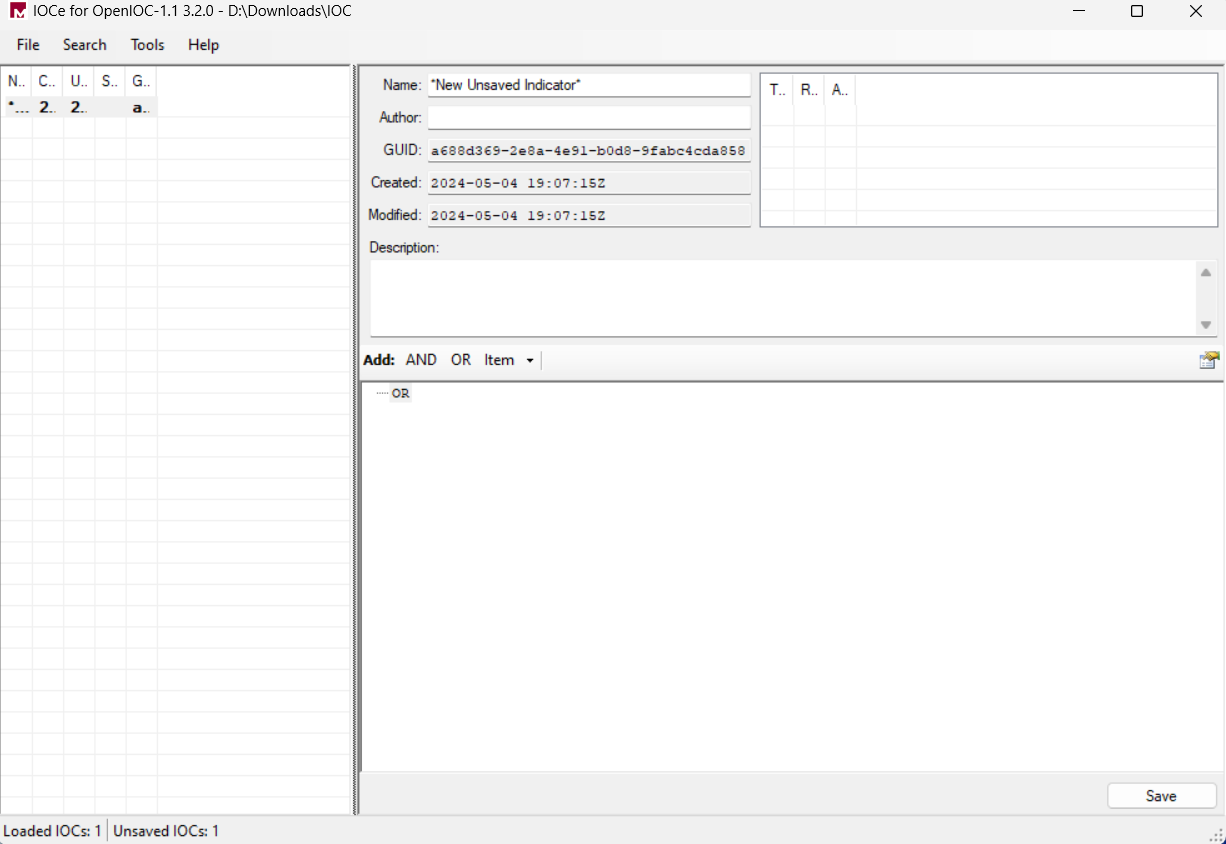
**USING IOC EDITORS TO CREATE IOC REPORTS:**

1. Launch the IOC Editor application and either open an empty directory or open a directory of existing IOCs. To open a directory, select File -> Open IOC Directory from the main menu bar.
2. To create a new IOC, select File -> New -> Indicator.



1. From here you can begin adding the meta information and expressions to the IOC.

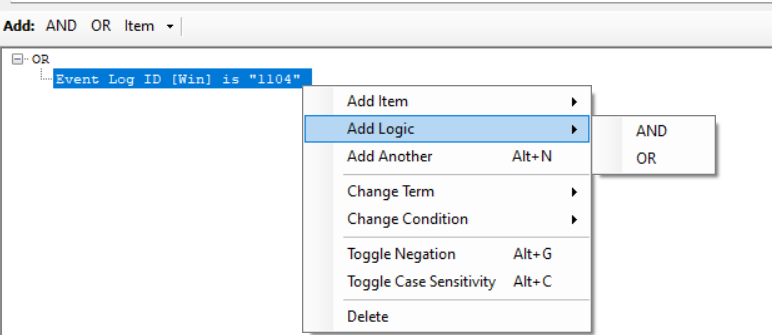
It displays three areas: a listing of all loaded IOCs(left), the meta information(top-right), and the definition(bottom-right).

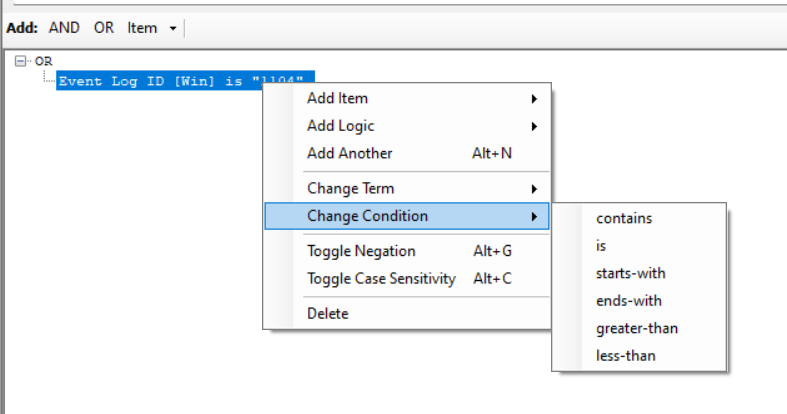


1. Name, Author, and Description are pretty self-explanatory.
2. The Definition area is where the expressions in an IOC are added. To add an expression under the top level OR, right-click in the Definition area and select Add Item. You will be presented with a menu of available Indicator terms.

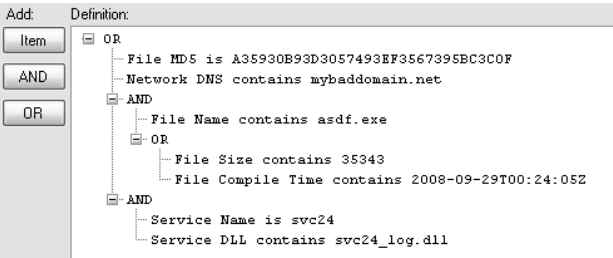
 

1. Here are some other functionalities you can use while creating a report:





1. The final report will somewhat look like this, (it’ll vary depending upon your logic):



1. Now just save it and you are goof to go!

Run IOC Search Collector on Redline tool and perform your analysis using the report you just made!

NOTE: IOC Search Collector will ignore the data that doesn't match an IOC you have gathered. Although, you can always choose to collect additional data. As the Redline User Guide states, the quality of the IOC analysis will depend on the data you have available in the analysis session.