

snorbert

snorbert is a [snort](#) data viewer, loosely based on [snorby](#). It is written in C# and uses .Net 4.5.

The aim of the application is to provide a fast, usable interface for accessing snort data. Depending on the snort deployment, the underlying data set can be extremely large, so care has been taken to optimise the data access. snorbert has various useful features:

Features

- Paged data access
- Configuration for multiple snort instances
- Signature based grouping of events
- User configurable searching
- Correlation of snort signatures to events for easy viewing of the signatures
- Query integration with NetWitness for quick session identification

Third party libraries

- [CsvHelper](#): CSV output
- [Be.HexEditor](#) : HEX view of packet data
- [IP Address Control](#) : Easy validation of IP addresses
- [SQL Server CE](#): SQL Server CE used for rule storage
- [MySql](#) : Access to snort MySQL databases
- [NPoco](#): Data access
- [ObjectListView](#) : Data viewing via lists
- [Utility](#) (woanware) : My helper library

Requirements

- Microsoft .NET Framework v4.5
- snort/barnyard database change (see below)

Database

snorbert requires a number of changes to the snort/barnyard database schema. The following files should be run to create new tables:

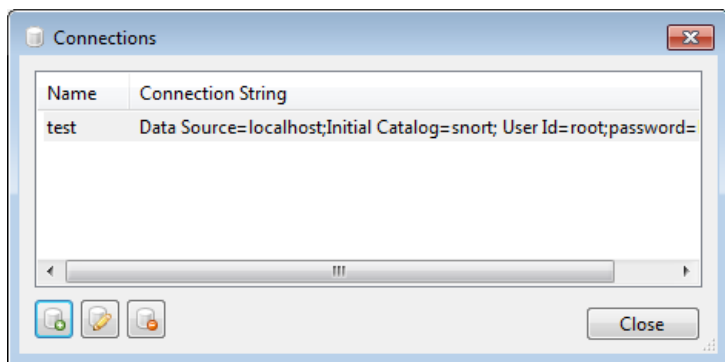
- Database\acknowledgment.sql
- Database\acknowledgment_class.sql
- Database\exclude.sql

Then the data population script (acknowledgment_class.data.sql) should be run to populate the **acknowledgment_class** table. The exclude table facilities the ability to exclude particular rules, IP addresses etc. The **acknowledgement** tables allow for better collaborative working so that one analyst can see that another analyst is already working on a particular rule.

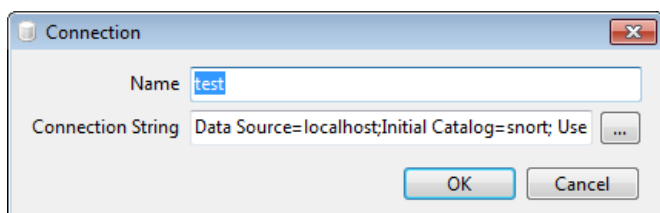
Usage

Connections

snorbert can connect to multiple snort instances. The database connections need to be defined for each snort instance. The database connections can be configured via the Tools->Connections menu. The Connections window will display all of the configured snort databases.



The Connections window allows the adding, editing and deleting of database connections. The Connection window is shown below:



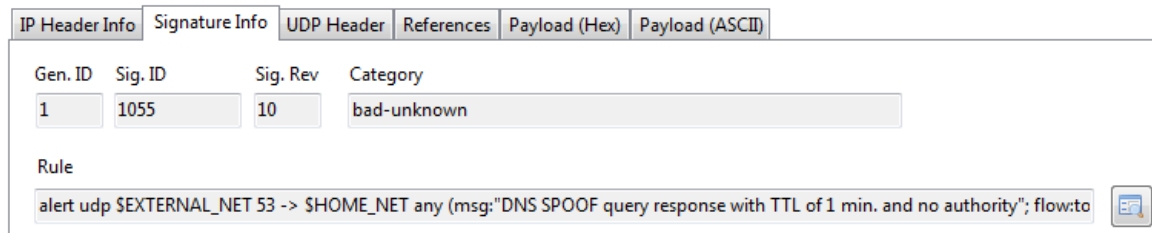
The ellipsis button will perform a connection test for the currently configured connection string. The connection string must be in the following format:

Data Source=#IP#;Initial Catalog=#Database#; User Id=#username#;password=#password#; default command timeout=60;

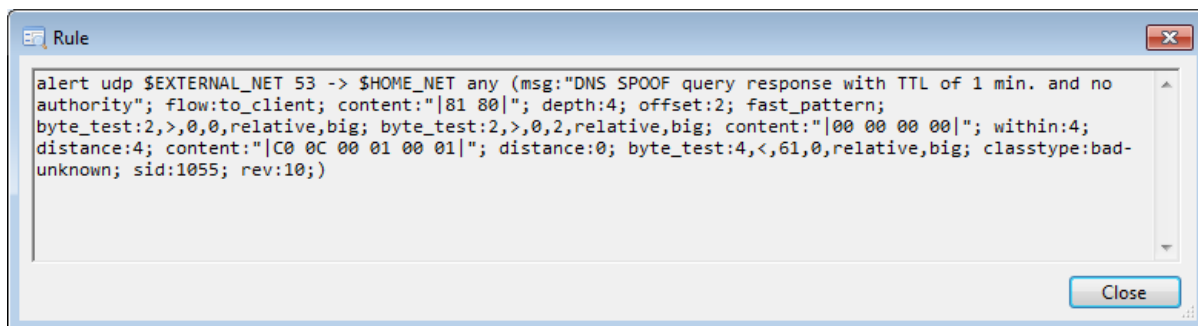
Note that the default command timeout can be configured for each instance, this allows for slow network connections, large datasets etc.

Rules/Signatures

The snort rule set can be imported into snorbert, this allows the signature/rule to be displayed that relates to a specific event. The screenshot below shows the signature details:



To view the full rule in a separate window, click the button next to the rule, the following window will be displayed:

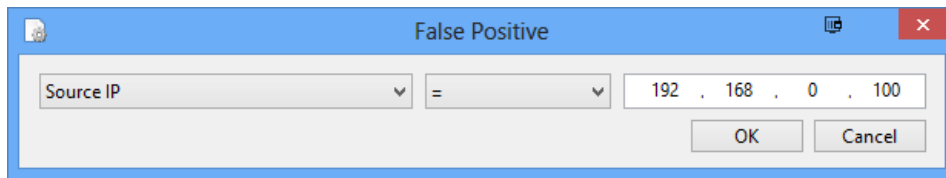


The rules can be imported manually via the Tools->Import Rules menu or they can be copied into the Rules directory located in the applications installation directory. The automated import will check the file names/timestamps and only import new or changed files.

False Positives

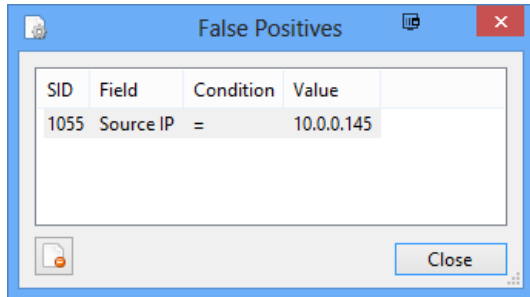
To help reduce the amount of “noise” returned by snort it is possible to add false positive filters to the data set. The false positive filters are only application to the Rules tab since they relate a filter to a specific snort rule.

To add a false positive filter, load the events for a rule, then right click on the Event line within the list. A context menu will be displayed, choose the Hide item. The following window will be displayed:



A dialog box titled "False Positive" with a blue header bar. It contains a form with a dropdown menu set to "Source IP", an equals sign operator, and a text field containing the IP address "192 . 168 . 0 . 100". At the bottom right are "OK" and "Cancel" buttons.

The values will be pre-populated using the event selected in the list; this is to speed up the process. To remove false positive filters, use the Tools->False Positive menu item, which will display the False Positives window.



A window titled "False Positives" with a blue header bar. It contains a table with the following data:

SID	Field	Condition	Value
1055	Source IP	=	10.0.0.145

At the bottom right is a "Close" button.

Select the false positive filter that you want to delete and use the delete button on the window or use the DEL key.