Raw Data Forensics

Raw Data files store flow records exported in a 5-minute interval.

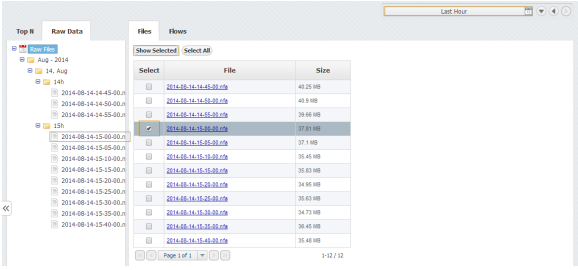
Raw Data Tree groups Raw Data files in folders according to the day/hour/minute. Selecting a node from the tree allows inspection of specific Raw Data files.

On this page:

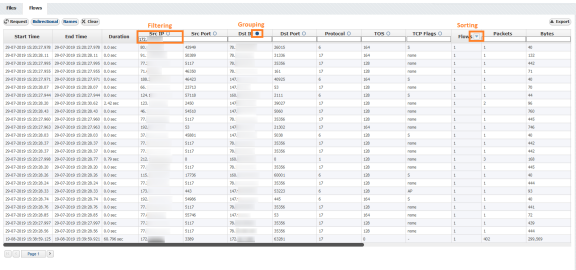
Inspecting Raw Data

To inspect Raw Data:

1. Go To **NetFlow > Raw Data > Files**
2. **Specify time period** in Time Window. The main panel and Raw Data Tree will show gathered files
3. **Select files** you want to inspect from the Main Panel (or alternatively, select a single file from Raw Data Tree)
4. Click **Show Selected**



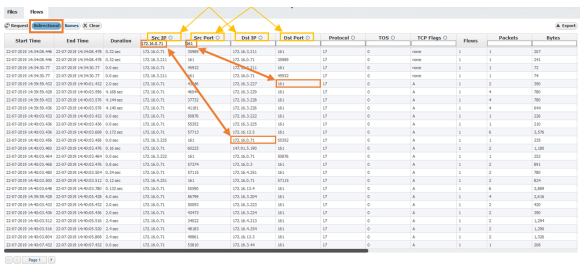
Raw Data table shows flow records from the selected Raw Data file(s). Data can be filtered, grouped and sorted by almost any field (source IP address, Bytes, Protocol etc.).



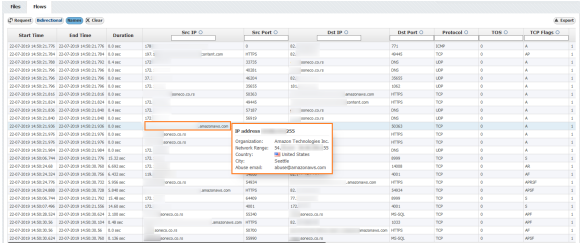
Clicking on **Bidirectional** button provides expanded filtering on two pairs of columns:

- Src IP and Dst IP
- Src Port and Dst Port

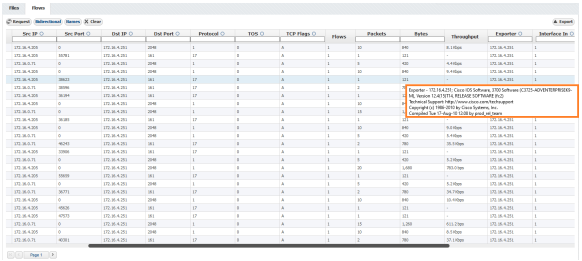
When you enable Bidirectional filtering, filter will be applied not only on filtered column, but also on bidirectional pair of that column. With this option enabled it is easier to find records for some IP address /port without knowledge if that IP address/port is source or destination. In example below, user is searching for one address and one port as source. With Bidirectional option enabled, result where that IP or port are destination will be also returned.



Clicking on **Names** button provides IP address resolution. If you move your mouse cursor over specific IP address you can see WhoIs information about that host.



If you want to see detailed description for fields in some columns all you need to do is to move mouse cursor over some IP address or port. Provided information is actually detailed description from Display Names section in Settings.

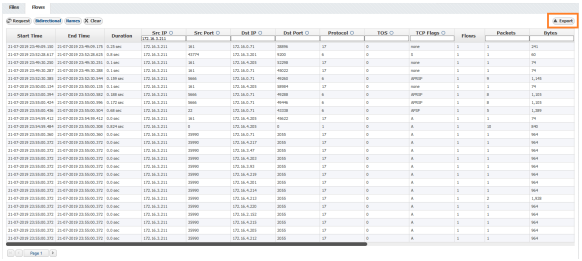


In order to enable IP address resolution, your NetVizura server should have local or remote commu nication with DNS server (for Hostname) and Internet access (for Whois information).

Exporting Raw Data

Raw Data table can be exported as a CSV file in order to present captured Netflow records as a report to a third party or for further analysis.

To export Raw Data, click on the the **Export** button in the upper right corner of the Raw Data Table.



Grouping, filtering and sorting the raw data table will affect the CSV as well. This will also make a CSV file much smaller.

Depending on the amount of data, export can last a couple of minutes

Depending on your browser settings, browser may ask you were to save the file or it will save the file to a default folder (usually **Downloads** folder). Some spreadsheet software may ask you which separator to use when opening the file - select **Comma**.