How To Use Wireshark With Nagios Network Analyzer 2026

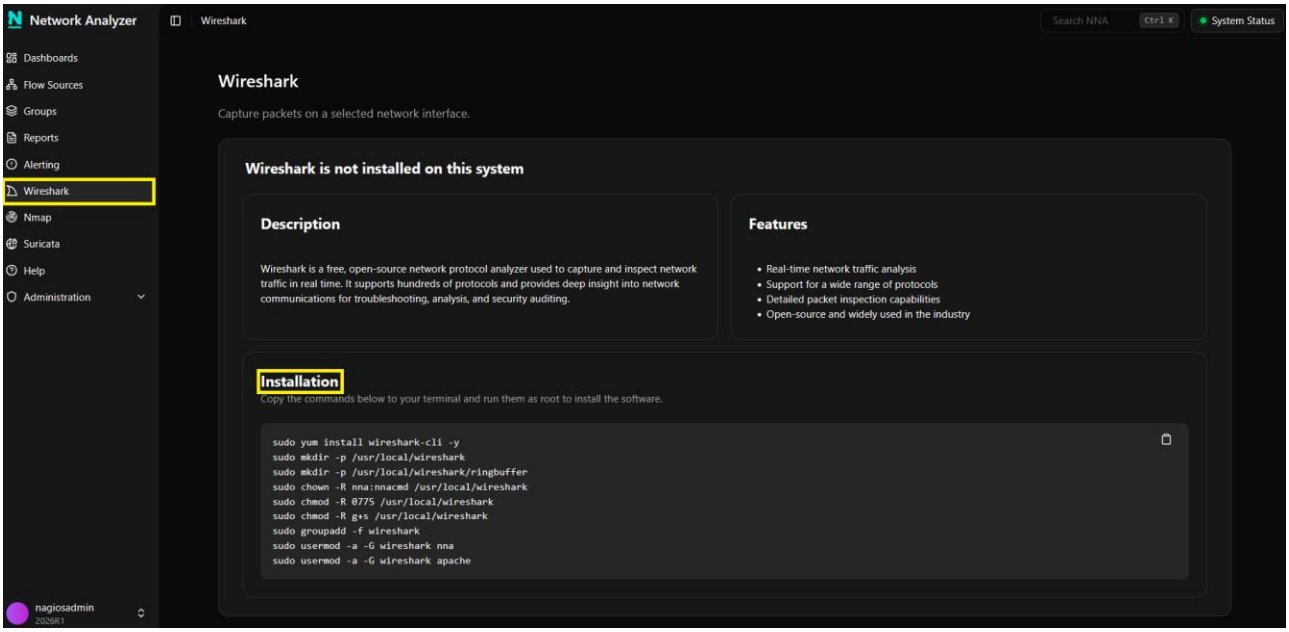
Purpose

This document describes how to leverage Wireshark with Nagios Network Analyzer 2026. This guide includes details on installing Wireshark on your Network Analyzer server, and on using the integrated tools to capture packets and manage live-generated and imported Pcap files.

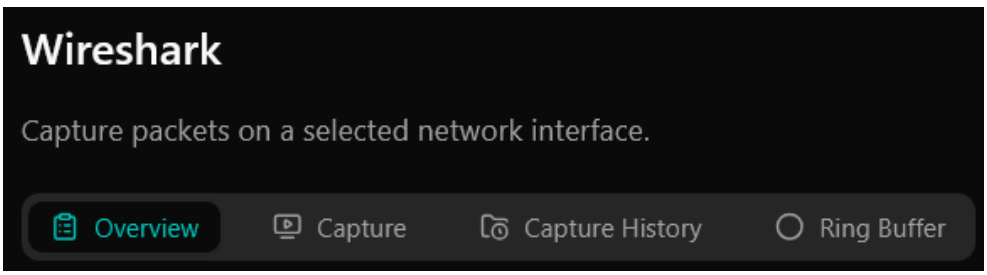
Initial Setup

To begin, navigate to the **Wireshark** section of the UI, and run the commands in the **Installation** section from the command line of your Network Analyzer server.

You can also find the commands in the Installation Commands section of this guide.

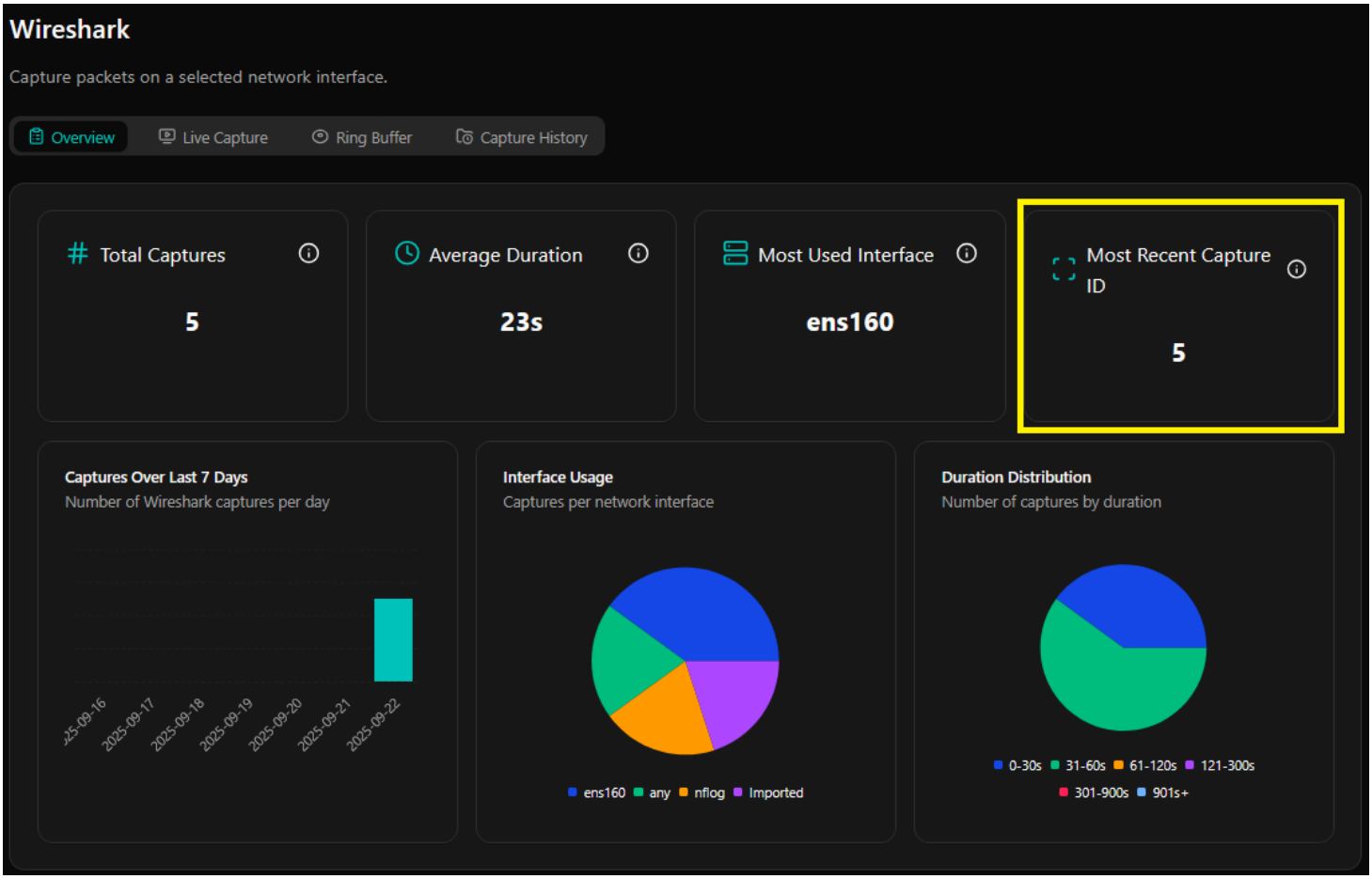


After the installation is completed, refresh the Wireshark page. You will now see several tabs of options:



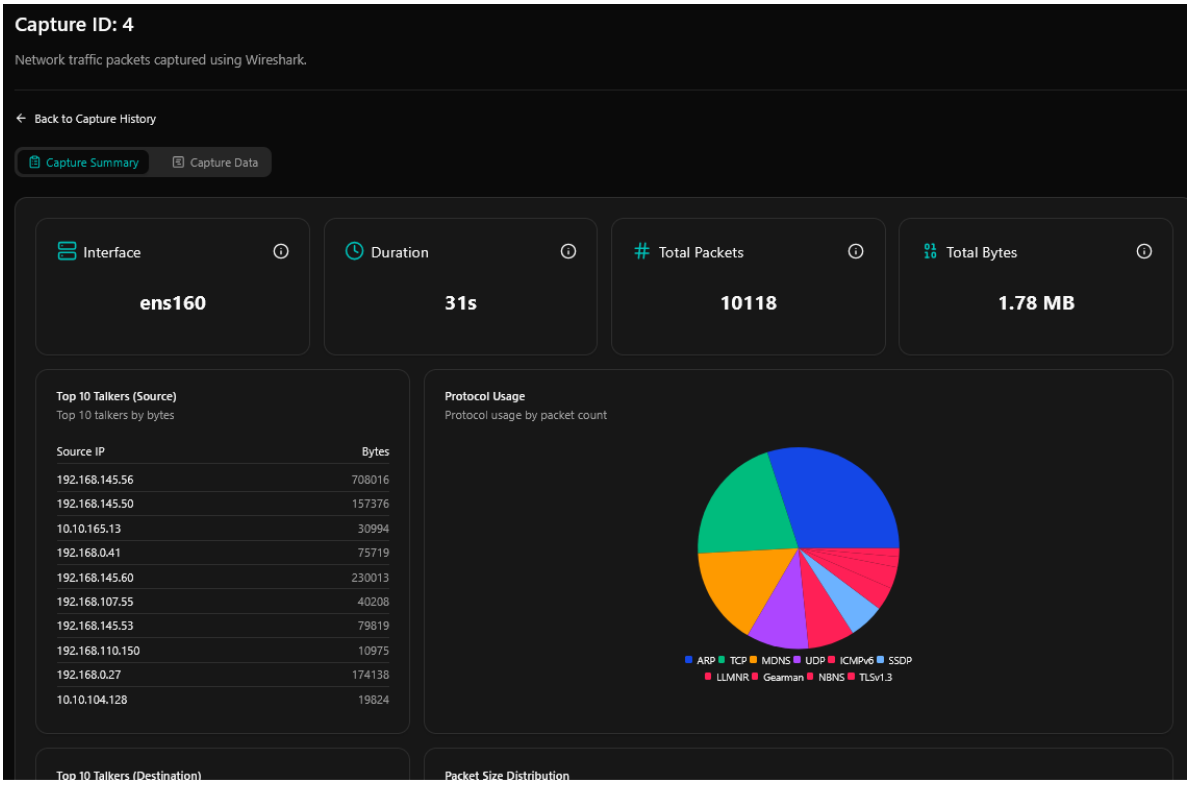
Overview Tab

In the **Overview** tab, you can view Total Captures, Average Duration, Most Used Interface, and Most Recent Capture Data, as well as a bar chart of Captures Over Last 7 Days, and pie charts of Interface Usage and Duration Distribution.

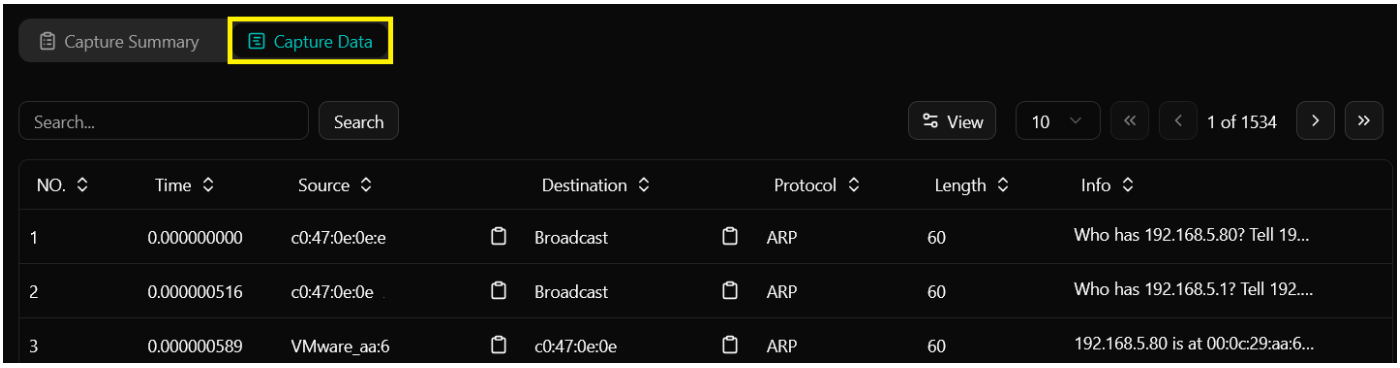


You can click anywhere in the Most Recent Capture ID panel to drill down to the **Capture Summary** page for the most recent capture.

On the **Capture Summary** page you can see details on the Interface, Total Packets, Total Bytes, and Duration, as well as lists of the Top 10 Talkers by source IP and Destination IP, and pie charts of Protocol Usage and Packet Size Distribution.

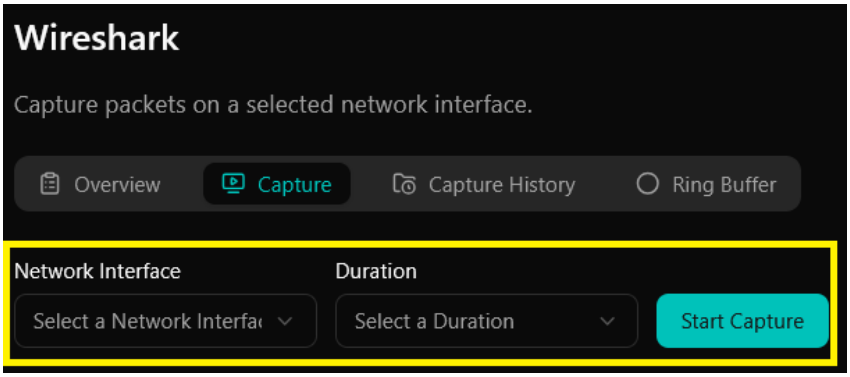


The **Capture Data** tab shows raw capture data from the scan:

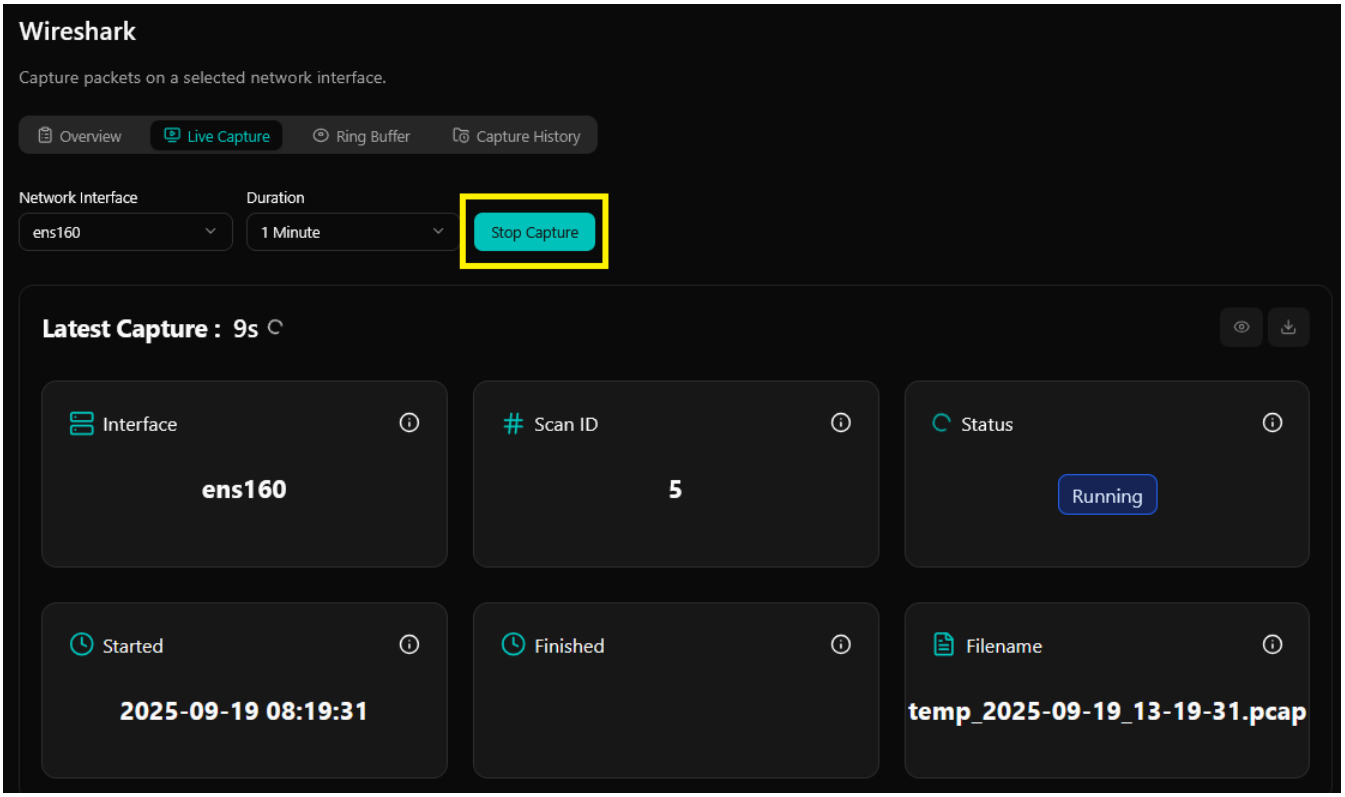


Capture Tab

To start a live capture of data from an interface on your Network Analyzer server, select a Network Interface and Duration from the drop-downs then click **Start Capture**.



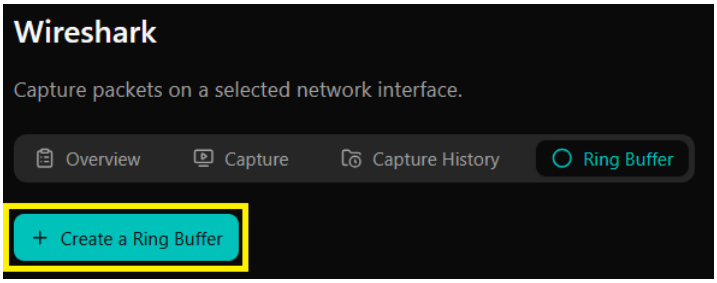
To stop the capture prior to the end of the chosen Duration, click **Stop Capture**. Once it stops, the capture will appear in **Capture History**, and be reflected in the **Overview** tab.



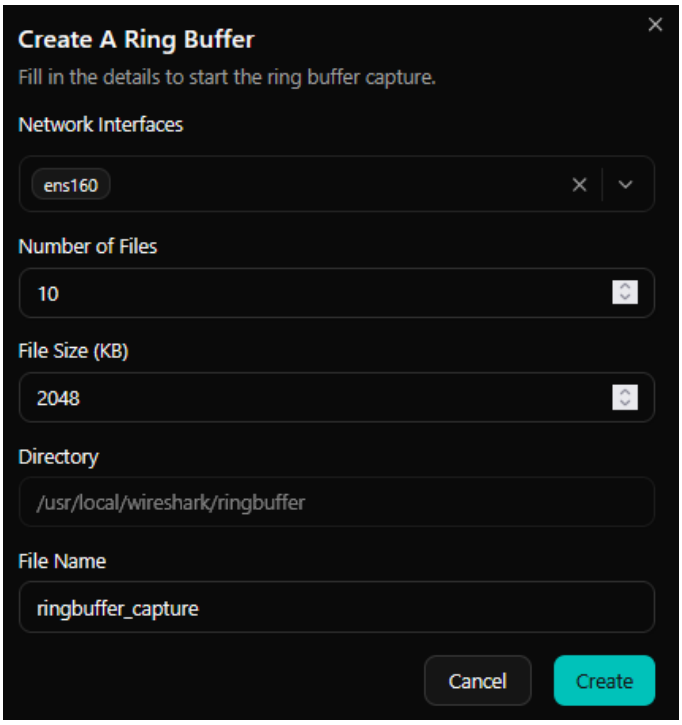
Ring Buffer Tab

Creating and Activating the Ring Buffer

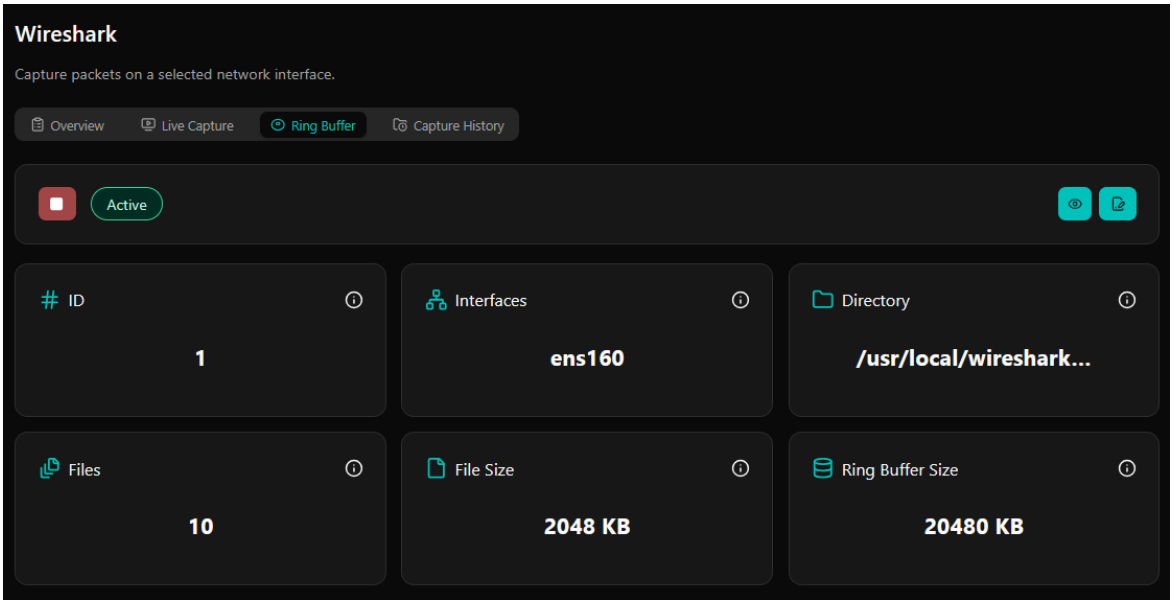
The Ring Buffer capability enables you to store Wireshark capture data across multiple smaller files, automatically overwriting the oldest capture file when either a maximum number of files or a specific file size is reached. This allows for long-term network monitoring without exhausting disk space. To enable Ring Buffer, click the **+ Create a Ring Buffer** button:



Next, configure the Ring Buffer settings, defining whether any or only certain **Network Interfaces** should employ it, the maximum **Number of Files** and maximum **File Size**, the storage **Directory** (should you wish to change it from the default), and a base **File Name**:



Once you click **Create**, the details of your ring buffer settings will populate to the **Ring Buffer** page, and the ring buffer will automatically activate.



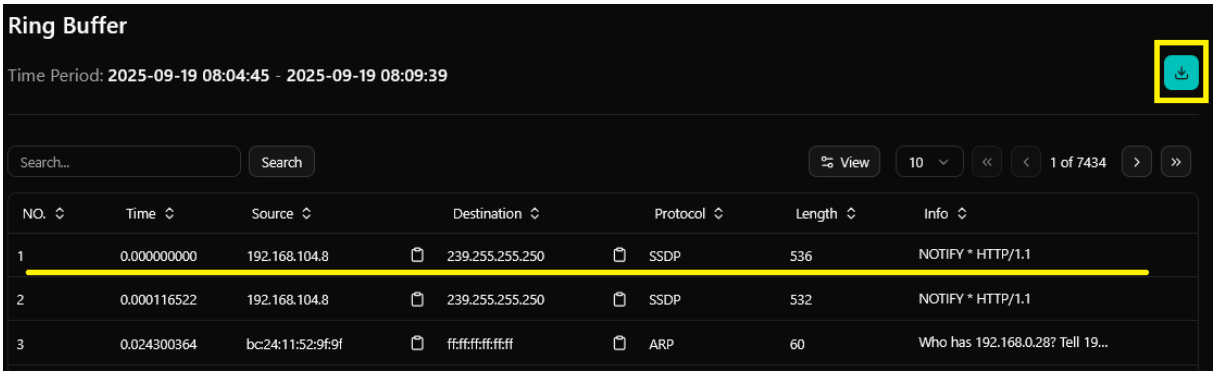
Editing Ring Buffer Settings

To adjust your ring buffer settings, click the edit icon on the upper right:

Viewing the Latest Time period

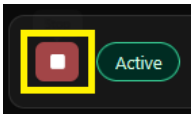
To view capture data from the latest time period, click the eye icon on the upper right:

You can then click through on each event in the table to view further details as a text summary or raw JSON, or download a PCAP with the Download button on the upper right.

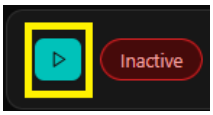


De-activating the Ring Buffer

To stop the ring buffer, click the **Stop** button on the upper left.



After de-activation, it will become **Start** button which you can click to re-activate it.



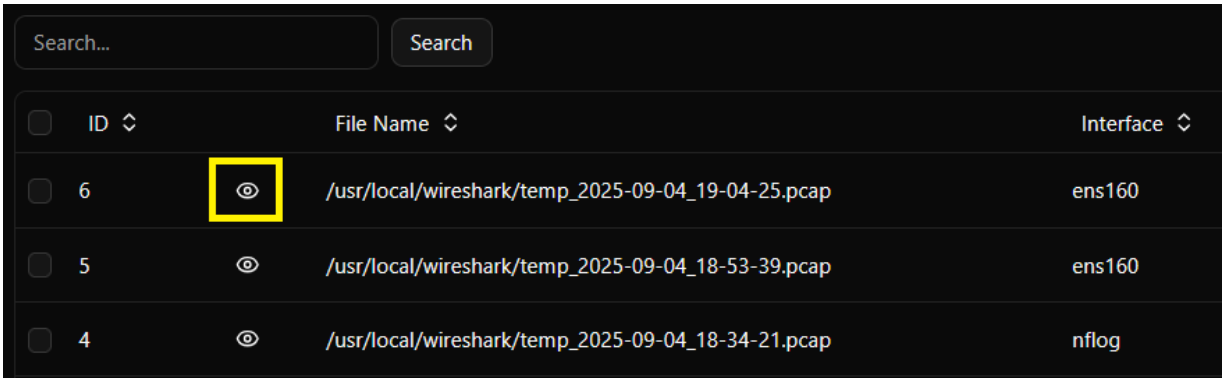
Important Note: If you stop, then re-activate the ring buffer, previous ring buffer file will be cleared and a new capture cycle will begin.

Capture History Tab

Here you can view and download pcap files of completed captures, scan completed captures with Suricata, and import pcap files for Wireshark analysis.

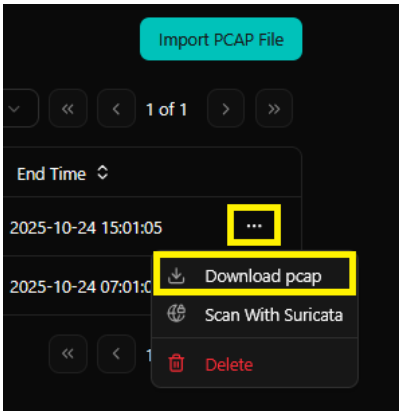
Viewing Capture Details

To view capture details, click the eye icon on the entry you wish to review to be brought to the Capture Summary page.



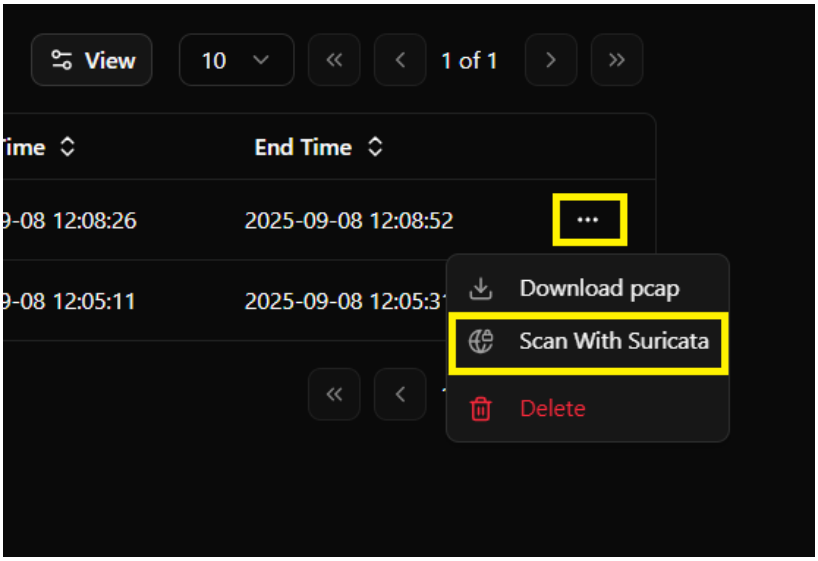
Downloading pcap Files

To download a pcap file of a capture, click the **Actions** icon on the far right, and select **Download pcap.**

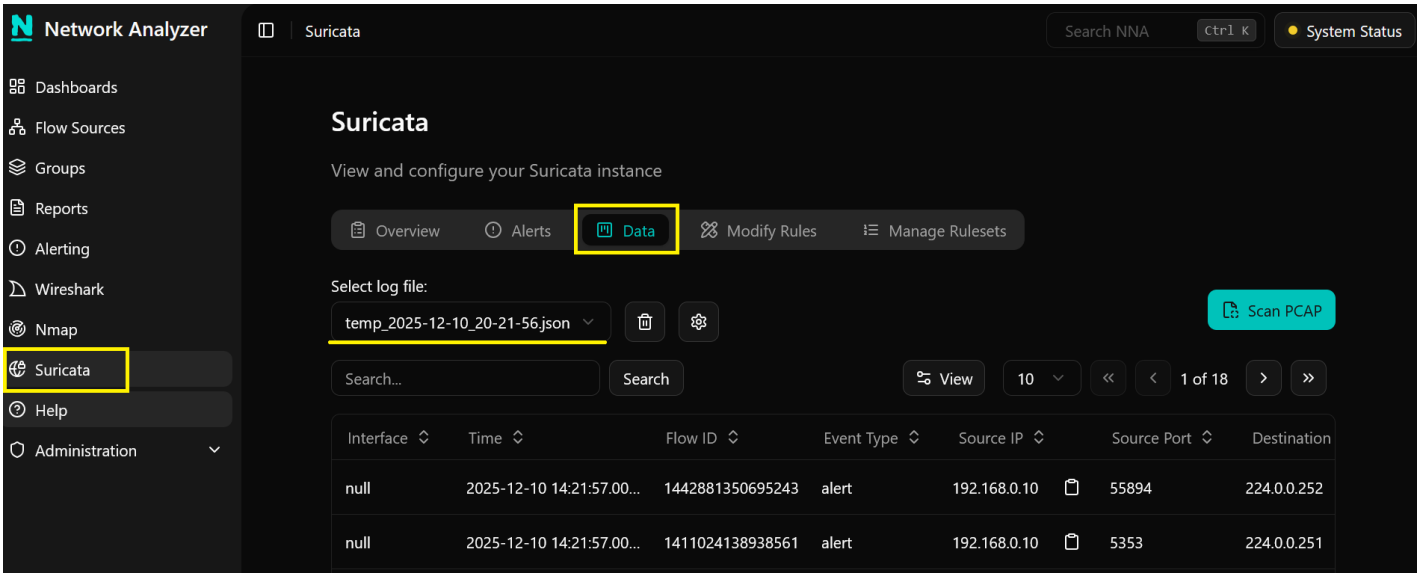


Scanning Pcap files with Suricata:

To scan a Wireshark-generated Pcap file in Suricata, click the **Actions** icon and select **Scan with Suricata**.

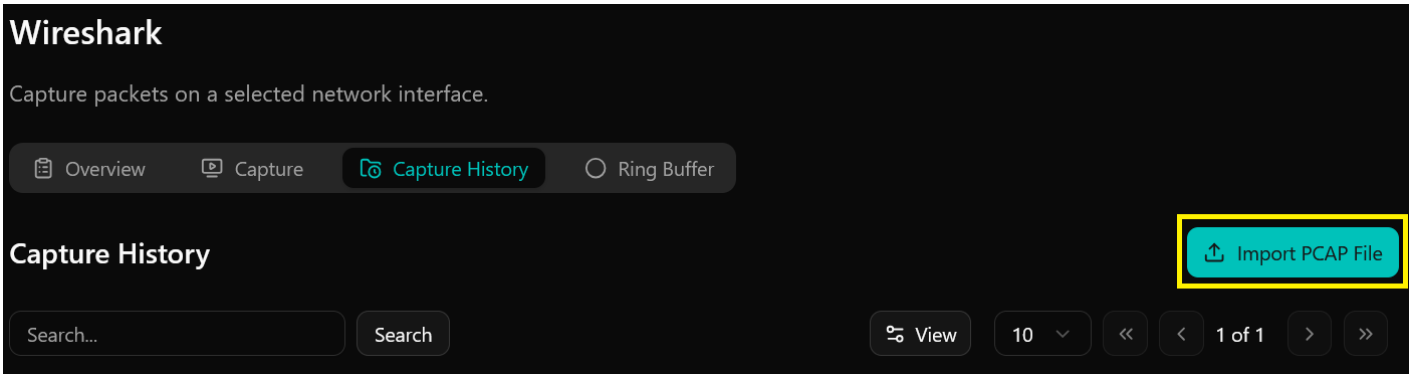


The results of the scan will be available for review in the **Data** tab of the Suricata section. Simply choose the migrated log file from the **Select Log File** dropdown to see the results:



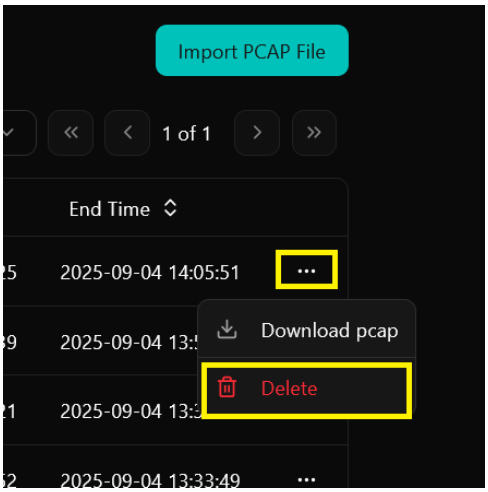
Importing pcap Files

To import pcap files for analysis in Wireshark, click the **Import PCAP File** button.



Deleting Captures

To delete an entry in your capture history, click the Actions icon on the far right of the entry and select Delete.



Installation Commands

Be sure to use the commands that match your Network Analyzer server OS (in the UI, the commands are automatically based on your OS). Note that some commands span multiple lines, and include a `\` (line continuation character). For best results, copy and paste the entire batch of commands at once into your terminal.

RHEL | CentOS | Oracle

```
sudo yum install wireshark-cli -y
sudo mkdir -p /usr/local/wireshark
sudo mkdir -p /usr/local/wireshark/ringbuffer
sudo chown -R nna:nnacmd /usr/local/wireshark
sudo chmod -R 0775 /usr/local/wireshark
sudo chmod -R g+s /usr/local/wireshark
sudo groupadd -f wireshark
sudo usermod -a -G wireshark nna
sudo usermod -a -G wireshark apache
```

Debian | Ubuntu

```
printf "wireshark-common wireshark-common/install-setuid boolean \
true" | sudo debconf-set-selections
sudo DEBIAN_FRONTEND=noninteractive apt-get install tshark -y
sudo mkdir -p /usr/local/wireshark
sudo mkdir -p /usr/local/wireshark/ringbuffer
sudo chown -R nna:nnacmd /usr/local/wireshark
sudo chmod -R 0775 /usr/local/wireshark
sudo chmod -R g+s /usr/local/wireshark
sudo groupadd -f wireshark
sudo usermod -a -G wireshark nna
sudo usermod -a -G wireshark www-data
```

Finishing Up

This completes the documentation on using Wireshark with Nagios Network Analyzer 2026. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library