

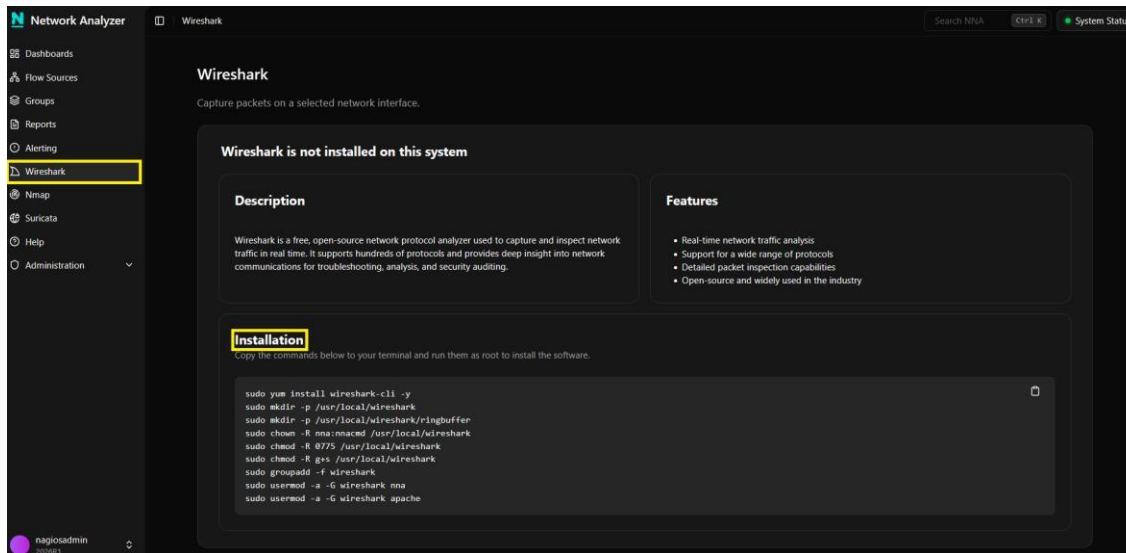
How To Use Wireshark With Nagios Network Analyzer 2026

Purpose

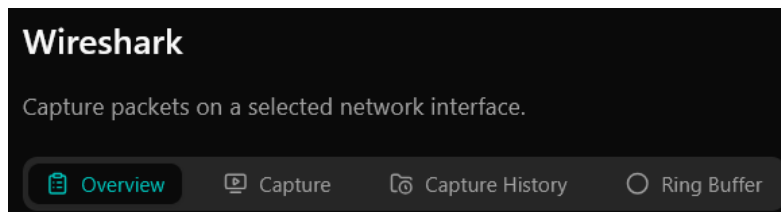
This document describes how to leverage Wireshark with Nagios Network Analyzer 2026. This guide includes details on installing Wireshark on your Network Analyzer server, and on using the integrated tools to capture packets and manage live-generated and imported Pcap files.

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.



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



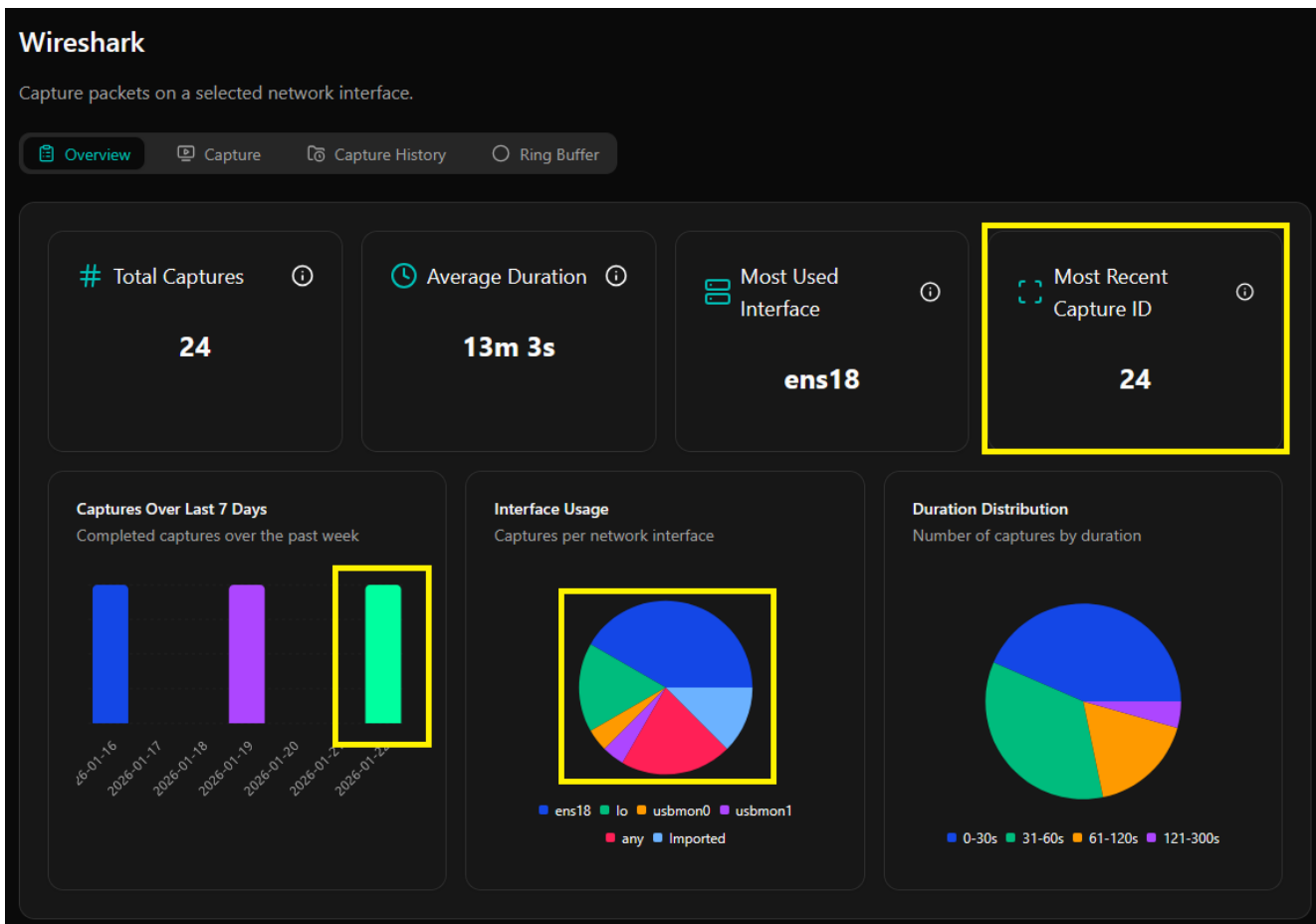
Note: after installation, you can click the **View Install Instructions** button on the upper right of the Wireshark menu to review the instructions.

How To Use Wireshark With Nagios Network Analyzer 2026

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.

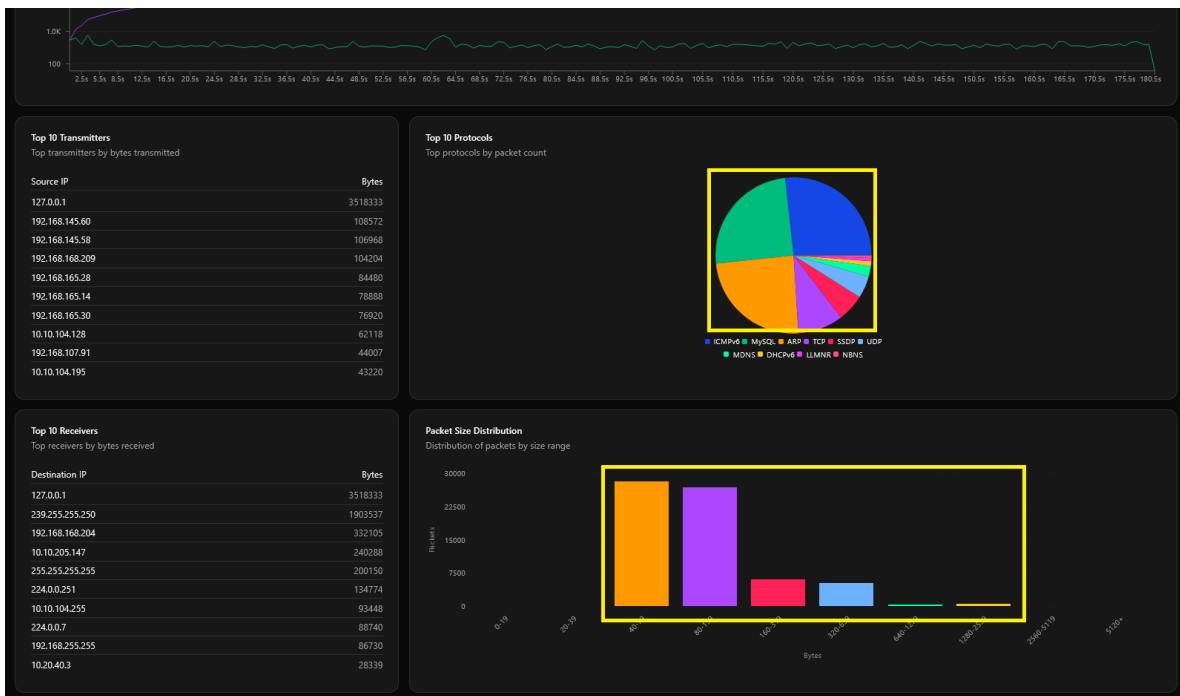
You can click anywhere in the Most Recent Capture ID panel to drill down to the Capture Summary page for the most recent capture, on any of the bars in the Captures Over Last 7 Days panel to see the Capture History for the day, or on any slice in the Interface Usage panel to view the Capture History for that interface.



How To Use Wireshark With Nagios Network Analyzer 2026

On the **Capture Summary** page you can see details on the Interface, Duration, Total Packets, and Total Bytes, 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.

You can also click any slice in the Top 10 Protocols panel to view Capture Data filtered for that protocol, or any of the bars in the Packet Size Distribution panel to see Capture Data filtered for that frame length.



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

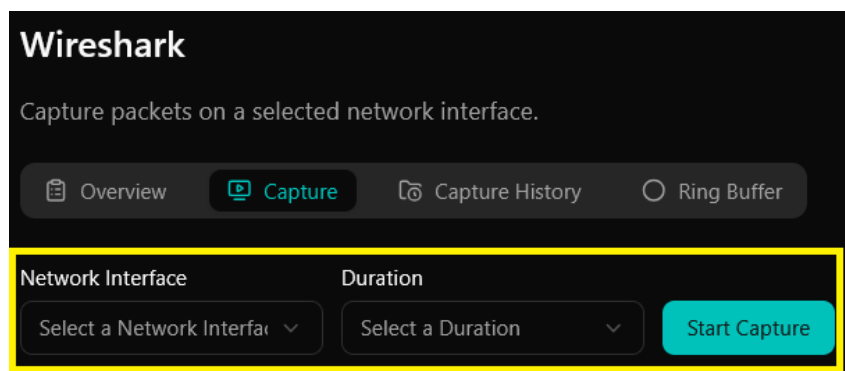
The screenshot shows the 'Capture Data' tab with a table of raw capture data. The table has columns for NO., Time, Source, Destination, Protocol, Length, and Info. The first three rows are highlighted.

| NO. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|---------------|-------------|----------|--------|-------------------------------------|
| 1 | 0.000000000 | c0:47:0e:0e:e | Broadcast | ARP | 60 | Who has 192.168.5.80? Tell 19... |
| 2 | 0.000000516 | c0:47:0e:0e | Broadcast | ARP | 60 | Who has 192.168.5.1? Tell 192... |
| 3 | 0.000000589 | VMware_aa:6 | c0:47:0e:0e | ARP | 60 | 192.168.5.80 is at 00:0c:29:aa:6... |

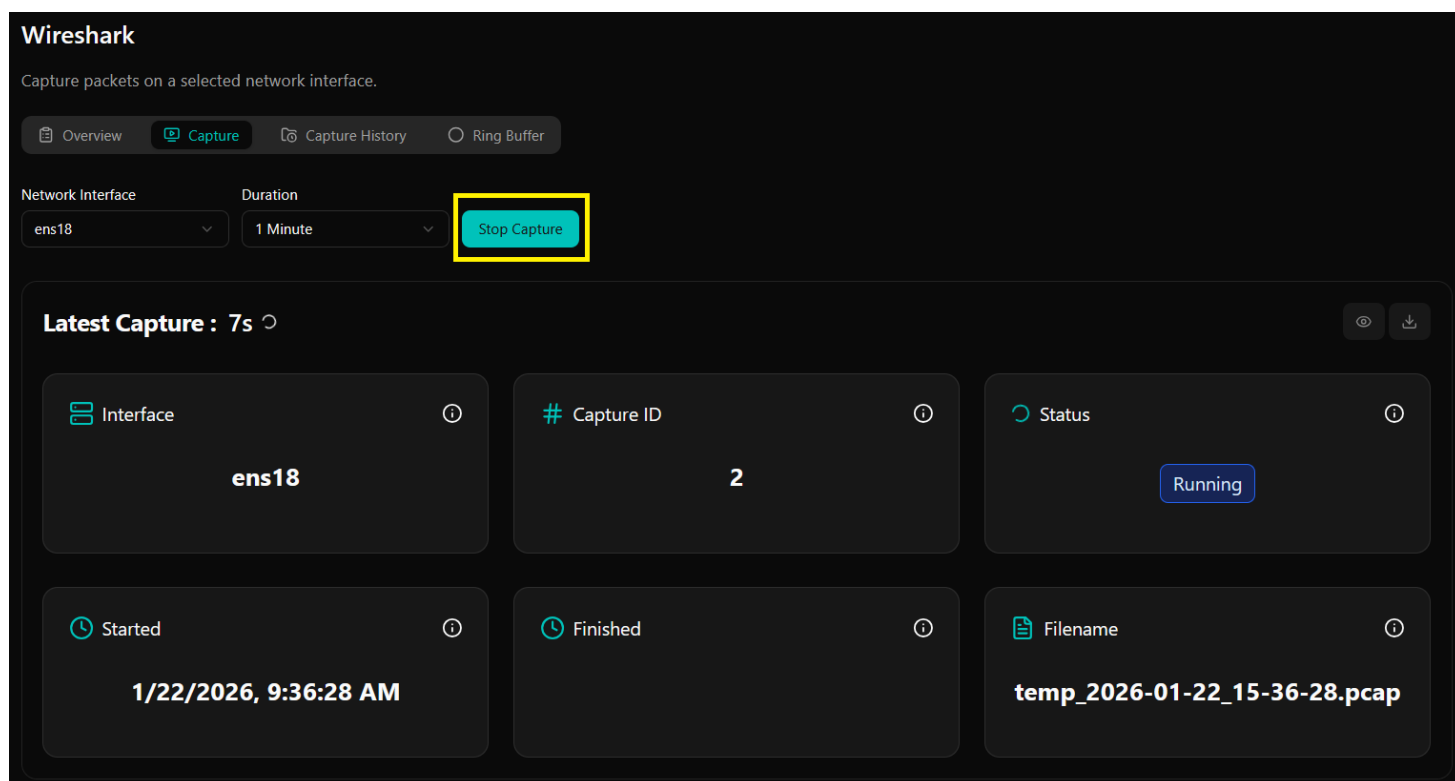
How To Use Wireshark With Nagios Network Analyzer 2026

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.

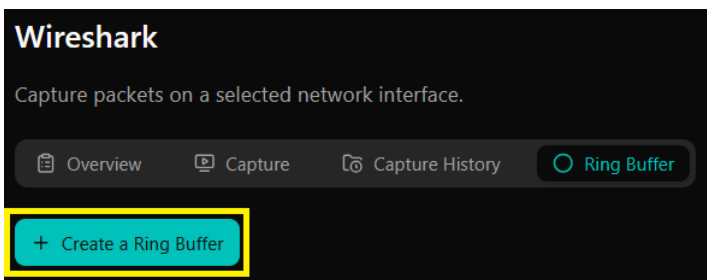


How To Use Wireshark With Nagios Network Analyzer 2026

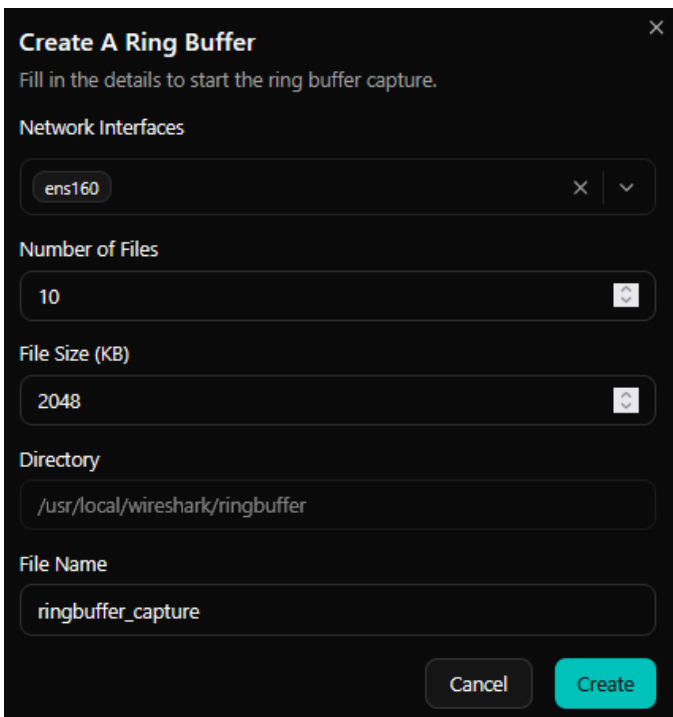
Ring Buffer Tab

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:

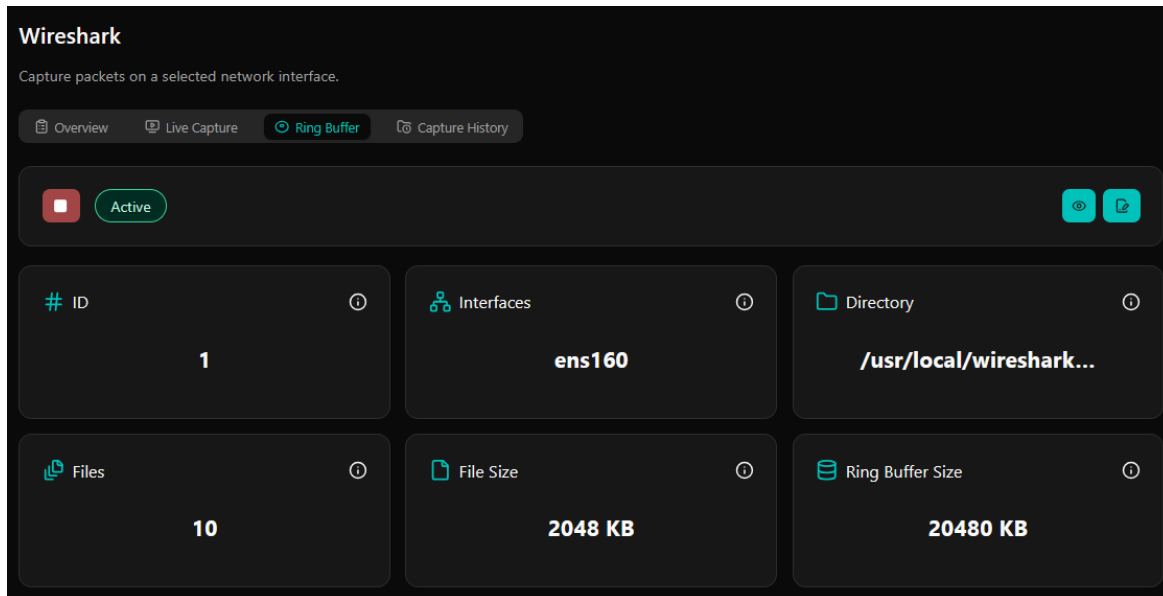


Next, configure the Ring Buffer settings, defining whether any or only certain **Network Interfaces** should employ it, the maximum **Number of Files** and maximum **File Size**, the storage **Directory** (should you wish to change it from the default), and a base **File Name**:



How To Use Wireshark With Nagios Network Analyzer 2026

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.

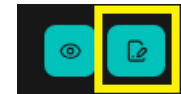


The screenshot shows the Wireshark interface with the Ring Buffer page active. The page displays a table with the following data:

| # | ID | Interfaces | Directory | Files | File Size | Ring Buffer Size |
|---|----|------------|-------------------------|-------|-----------|------------------|
| 1 | | ens160 | /usr/local/wireshark... | 10 | 2048 KB | 20480 KB |

Editing Ring Buffer Settings

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

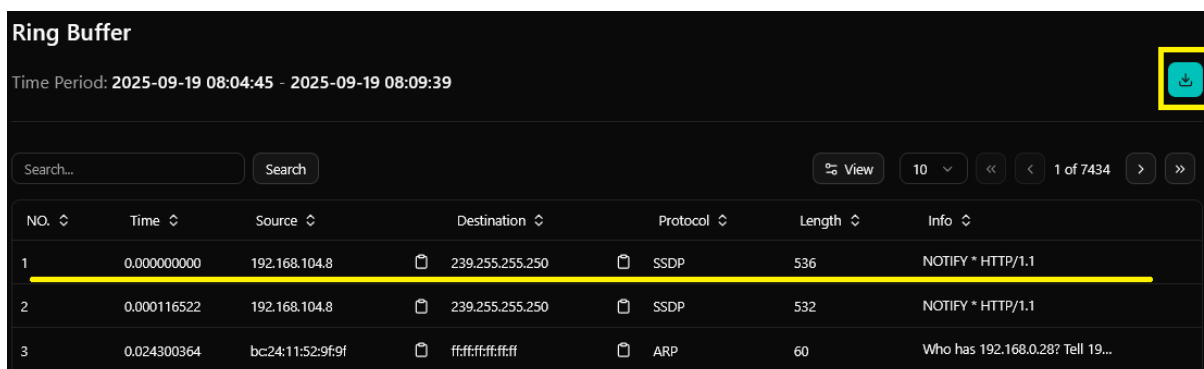


Viewing the Latest Time period

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.



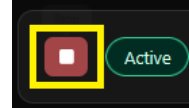
The screenshot shows the Ring Buffer page with a table of capture events. The table has the following columns: NO., Time, Source, Destination, Protocol, Length, and Info. The first event is highlighted in yellow.

| NO. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------------|-------------------|----------|--------|----------------------------------|
| 1 | 0.000000000 | 192.168.104.8 | 239.255.255.250 | SSDP | 536 | NOTIFY * HTTP/1.1 |
| 2 | 0.000116522 | 192.168.104.8 | 239.255.255.250 | SSDP | 532 | NOTIFY * HTTP/1.1 |
| 3 | 0.024300364 | bc:24:11:52:9f:9f | ff:ff:ff:ff:ff:ff | ARP | 60 | Who has 192.168.0.28? Tell 19... |

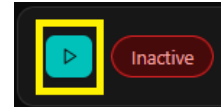
How To Use Wireshark With Nagios Network Analyzer 2026

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. The Ring Buffer must also be activated again if the system is rebooted.

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.

| ID | File Name | Interface |
|----|--|-----------|
| 6 | /usr/local/wireshark/temp_2025-09-04_19-04-25.pcap | ens160 |
| 5 | /usr/local/wireshark/temp_2025-09-04_18-53-39.pcap | ens160 |
| 4 | /usr/local/wireshark/temp_2025-09-04_18-34-21.pcap | nflg |

Top 10 Transmitters

| Source IP | Bytes |
|----------------|---------|
| 127.0.0.1 | 3518333 |
| 192.168.145.60 | 108572 |

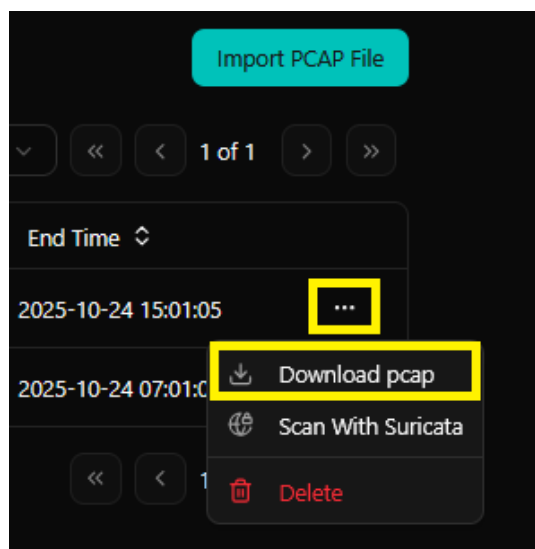
Top 10 Protocols

| Protocol | Count |
|----------|-------|
| HTTP | 1000 |
| TCP | 500 |
| UDP | 200 |

How To Use Wireshark With Nagios Network Analyzer 2026

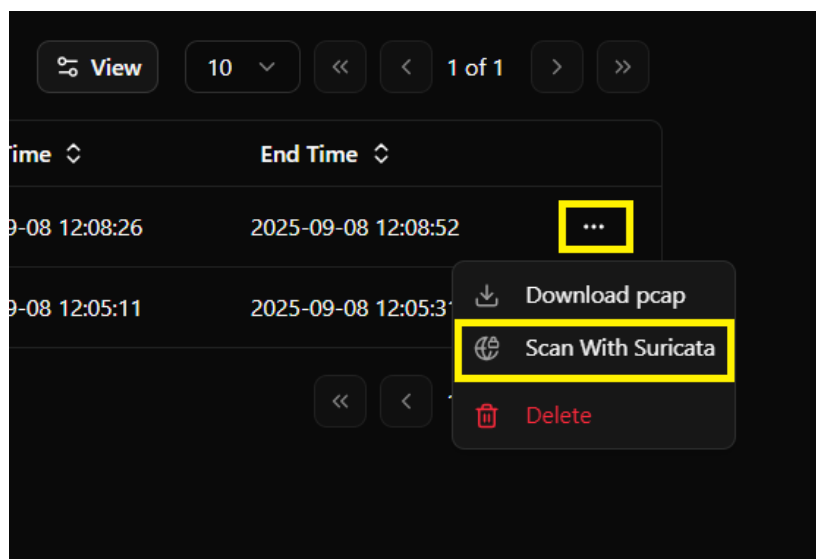
Downloading pcap Files

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



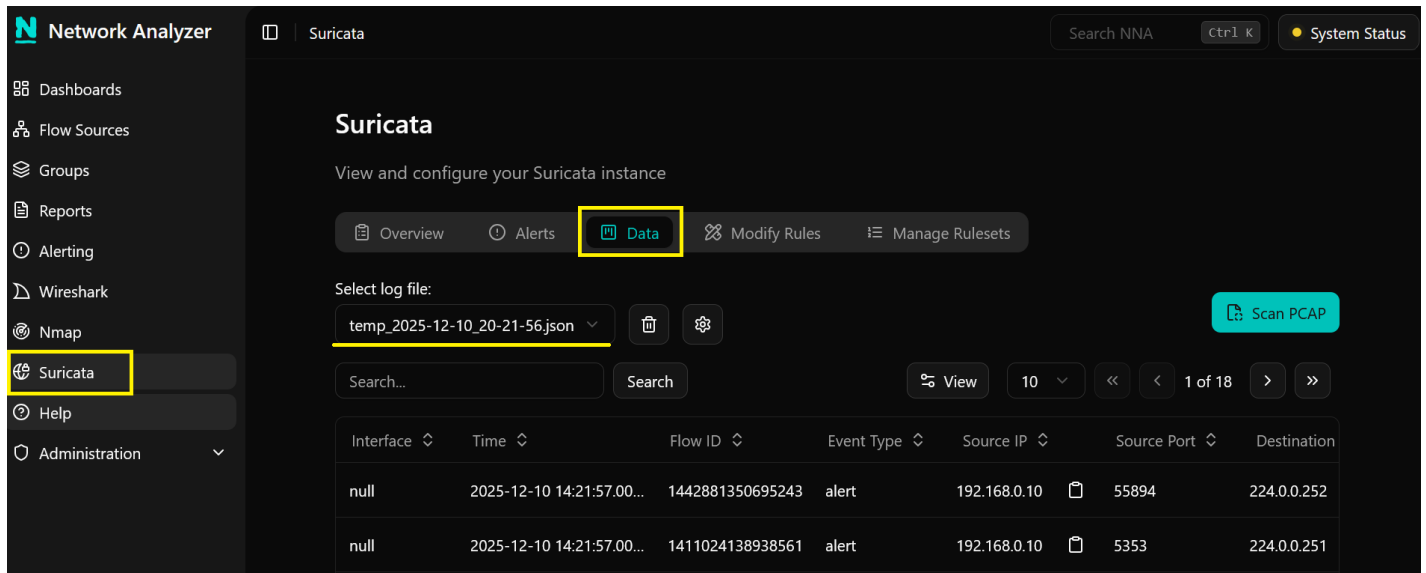
Scanning Pcap files with Suricata:

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



How To Use Wireshark With Nagios Network Analyzer 2026

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:

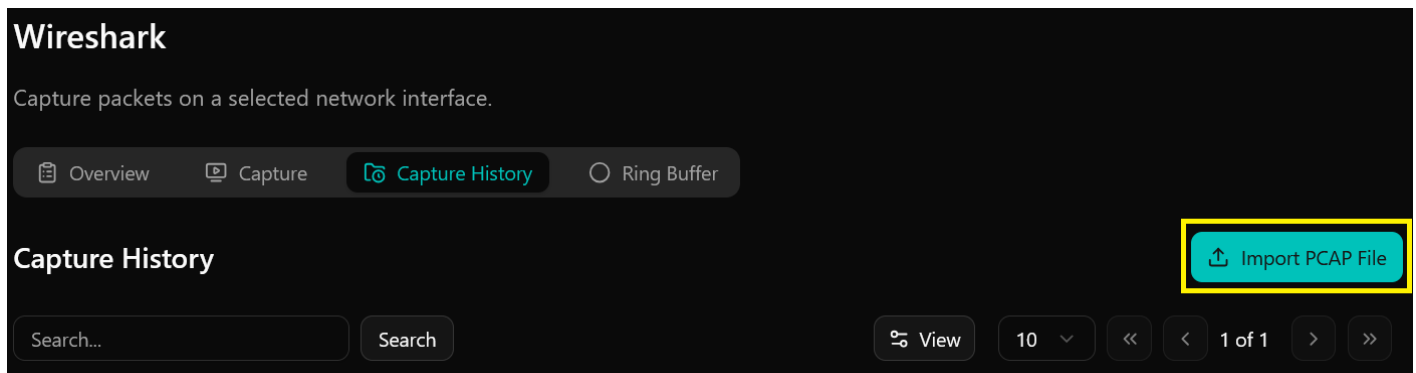


The screenshot shows the Nagios Network Analyzer interface for the Suricata section. The 'Data' tab is selected and highlighted with a yellow box. Below the tabs, the 'Select log file:' dropdown is set to 'temp_2025-12-10_20-21-56.json'. A 'Scan PCAP' button is visible. Below this, there is a search bar and a table of log entries.

| Interface | Time | Flow ID | Event Type | Source IP | Source Port | Destination |
|-----------|---------------------------|------------------|------------|--------------|-------------|-------------|
| null | 2025-12-10 14:21:57.00... | 1442881350695243 | alert | 192.168.0.10 | 55894 | 224.0.0.252 |
| null | 2025-12-10 14:21:57.00... | 1411024138938561 | alert | 192.168.0.10 | 5353 | 224.0.0.251 |

Importing pcap Files

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



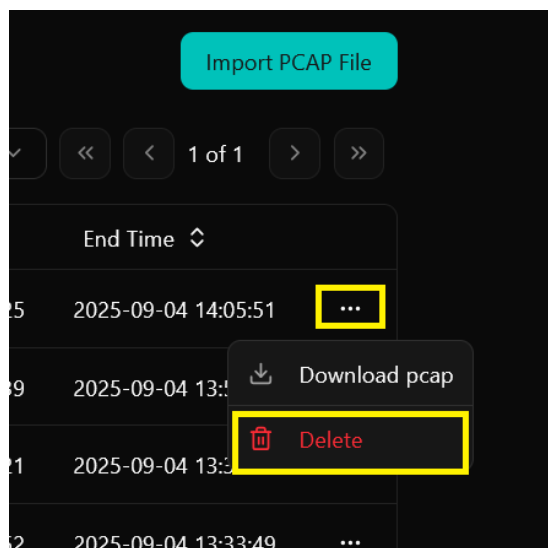
The screenshot shows the Nagios Network Analyzer interface for the Wireshark section. The 'Capture History' tab is selected. Below the tabs, there is a search bar and a table of capture history entries. The 'Import PCAP File' button is highlighted with a yellow box.

| Interface | Time | Flow ID | Event Type | Source IP | Source Port | Destination |
|-----------|---------------------------|------------------|------------|--------------|-------------|-------------|
| null | 2025-12-10 14:21:57.00... | 1442881350695243 | alert | 192.168.0.10 | 55894 | 224.0.0.252 |
| null | 2025-12-10 14:21:57.00... | 1411024138938561 | alert | 192.168.0.10 | 5353 | 224.0.0.251 |

How To Use Wireshark With Nagios Network Analyzer 2026

Deleting Captures

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



Finishing Up

This completes the documentation on Using Wireshark with NNA 2026. If you have additional questions or other support-related questions, please visit the Nagios Support Forum, Nagios Documentation Hub, or Nagios Library:

[Visit Nagios Support Forum](#)

[Visit Documentation Hub](#)

[Visit Nagios Library](#)