Analyze a packet capture file

Published: 2023-07-10

The offline capture mode enables administrators to upload and analyze a capture file recorded by packet analyzer software, such as Wireshark or tcpdump, in the ExtraHop system.

Here are some important considerations before enabling offline capture mode:

- When the capture is set to offline mode, the system datastore is reset. All previously recorded metrics are deleted from the datastore. When the system is set to online mode, the datastore is reset again.
- In offline mode, no metrics are collected from the capture interface until the system is set to online mode again.
- Only capture files in the pcap format are supported. Other formats such as pcapng are not supported.

Set the offline capture mode

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Capture**.
3. Click **Offline Capture File**.
4. Select **Upload** and then click **Save**.
5. Click **OK** to confirm the datastore reset.
   The capture process is stopped, the capture state is set to offline, and the datastore is cleared of all data. When the system has set the capture to offline mode, the Offline Capture File page appears.
6. Click **Choose File**, browse to the capture file that you want to upload, select the file, and then click **Open**.
7. Click **Upload**.
   The ExtraHop system displays the Offline Capture Results page when the capture file uploads successfully.
8. Click **View Results** to analyze the packet capture file as you would when the system is in live capture mode.

Return the system to live capture mode

1. In the System Configuration section, click **Capture (offline)**.
2. Click **Restart Capture**.
3. Select **Live**, and then click **Save**.

The system removes the performance metrics collected from the previous capture file and prepares the datastore for real-time analysis from the capture interface.