Packets

Published: 2025-03-25

A network packet is a small amount of data sent over Transmission Control Protocol/Internet Protocol (TCP/IP) networks. The ExtraHop system enables you to continuously collect, search, and download these packets with a Trace appliance, which can be useful to detect network intrusions and other suspicious activity.

You can search for and download packets from the Packets page in the ExtraHop system and through the Packet Search ⧉ resource in the ExtraHop REST API. Downloaded packets can then be analyzed through a third-party tool, such as Wireshark.

> **Note:** If you do not have a Trace appliance, you can still collect packets through triggers ⧉. See Initiate precision packet captures to analyze zero window conditions ⧉ for an example.

▶ Visit the related training: Packets ⧉

Navigating packets

Click **Packets** from the top menu to create a new packet query. From the New Packet Query page, you can specify a filter.
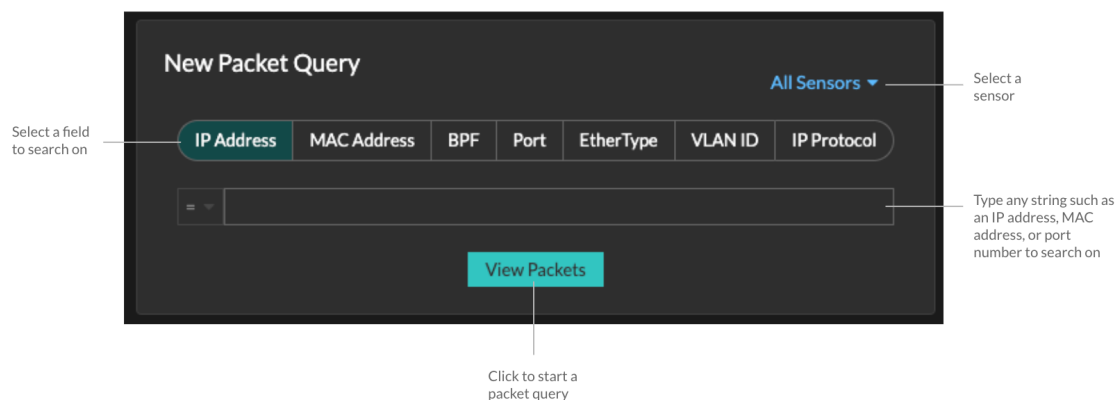
The results appear on the main Packets page. Launch another packet query by clicking **Packets** again from the top menu.

Set time interval   Filter the results   Start a packet query   Type an IP address in the global search field and then select Search Packets

If you change the time interval, the query starts again. Either end of the gray bar displays a timestamp, which is determined by the current time interval. The time on the right displays the starting point of the query and the time on the left displays the endpoint of the query. The blue bar indicates the time range during which the system found packets. You can drag to zoom on a period of time in the blue bar to run a query again for that selected time interval.

> **Tip:** Filter packets with Berkeley Packet Filter syntax ↗.

> **Note:** You can only view packets that match the privileges granted by your ExtraHop administrator. If you do not see your expected query results, contact your ExtraHop administrator.

Downloading packets

You can download query results into a packet capture (PCAP) file for analysis, along with TLS session keys and files associated with the packets.

Download options are available in the top-right drop-down menu. Click an option to enable your browser to download the file to your local machine.

Here are some considerations about downloading packets and extracting files:

- The download options displayed from the drop-down menu depend on your query results. For example, if there are no session keys associated with the packets, you might only see options to Download PCAP and Extract Files.
- Downloads only contain packets that match the privileges granted by your ExtraHop administrator. For example, if you query two sensors but were assigned limited access to one of the sensors by your administrator, your download will only contain packet headers from the limited access sensor.

- If you download session keys ⬀, you can open the packet capture file in a tool such as Wireshark, which can apply the session keys and display the decrypted packets.
- File extraction (also known as file carving) is available if files are observed on packets with HTTP or SMB records.

> 💡 **Tip:** From the Records page, you can search for HTTP or SMB record types and filter by File Observed. Click the packets icon next to the record that contains files you want to extract.

- File extraction is limited to the first 100 MB of packet query results.
- Extracted files are downloaded in a .zip file and contain original, unencrypted content that might include malicious data. A password is required to open extracted .zip files. The password is specified in the RevealX Enterprise ⬀ or RevealX 360 ⬀ Administration settings and can be obtained from your ExtraHop administrator.
- If you do not see your expected download options, contact your ExtraHop administrator. You will have no or limited access to sensors that are not assigned to you through sensor access control. Additionally, your download options can be restricted by module access and user privileges. The module access and privileges required for each download option is described in the following table:

Download Option	Module Required	Packet Forensics Privileges Required
Download PCAP + Session Keys	NDR or NPM	Packets and session keys
Download PCAP	NDR or NPM	Packets only
Download PCAP Headers	NDR or NPM	Packet headers only
Download PCAP Slices	NDR or NPM	Packet slices only
Download Session Keys	NDR or NPM	Packets and session keys
Extract Files	NDR	Packets only or Packets and session keys

Query packets in the ExtraHop system

While the Packets page provides quick access to query all packets, there are indicators and links from which you can initiate a packet query throughout the ExtraHop system.

- Type an IP address in the global search field and then select the Search Packets icon ◎ .
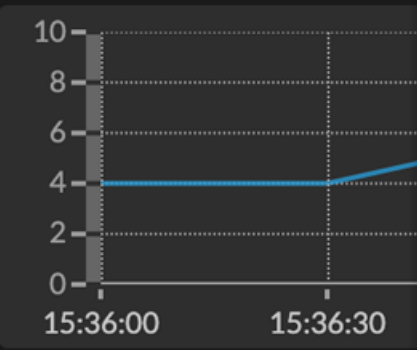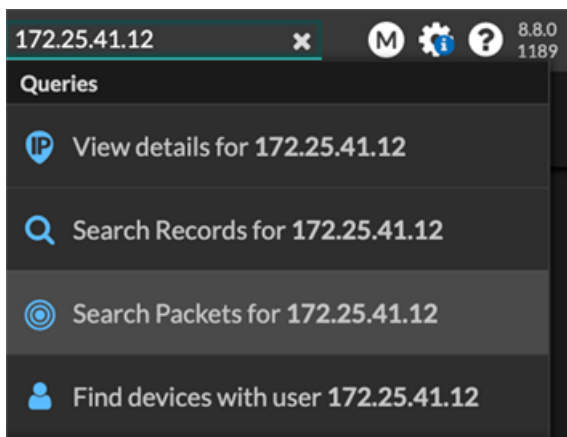

- Click **Packets** on a device page.

- Click the Packets icon ◎ next to any record on a record query results page.

- Click on an IP address or hostname in any chart with metrics for network bytes or packets by IP address to see a context menu. Then, click the Packets icon ◎ to query for the device and time interval.