

Packets

Published: 2022-06-09

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.

Query for packets

Launch a quick packet query by clicking **Packets** from the top menu. The ExtraHop system queries for all packets and displays the Packet Query page. 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.

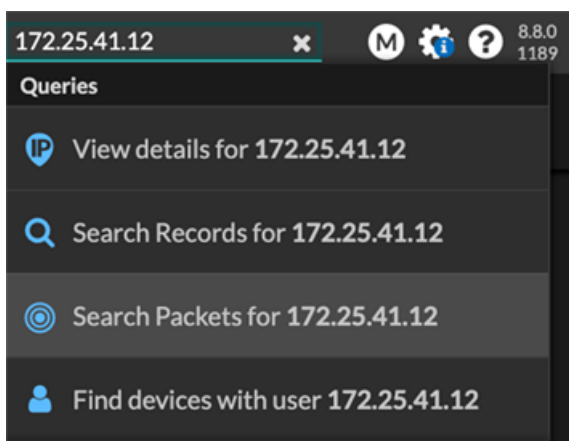
The following figure provides an overview of the Packet Query page and features:

The screenshot displays the ExtraHop Packet Query interface. At the top, there are navigation tabs: Overview, Dashboards, Detections, Alerts, Assets, Records, and Packets (selected). A search bar is visible in the top right. Below the navigation, the 'Packet Query Results' section is active. On the left, a 'Refine Results' sidebar shows a list of IP addresses and their corresponding data sizes (e.g., 135.140.88.252 (194.39 MB)). The main area contains a 'Packet Query' section with a time range bar. The bar shows a time interval from Feb 23, 1:51:02 pm to Feb 23, 1:56:02 pm. A blue bar indicates the time range during which packets were found. A 'Download PCAP' button is located to the right of the bar. Below the bar, there is a table of packet details. The table has the following columns: Time, Src IP, Dst IP, IP Proto, Src Port, Dst Port, Flags, Bytes, Src MAC, Dst MAC, EtherType, and VLAN ID. The table shows several rows of network traffic data.

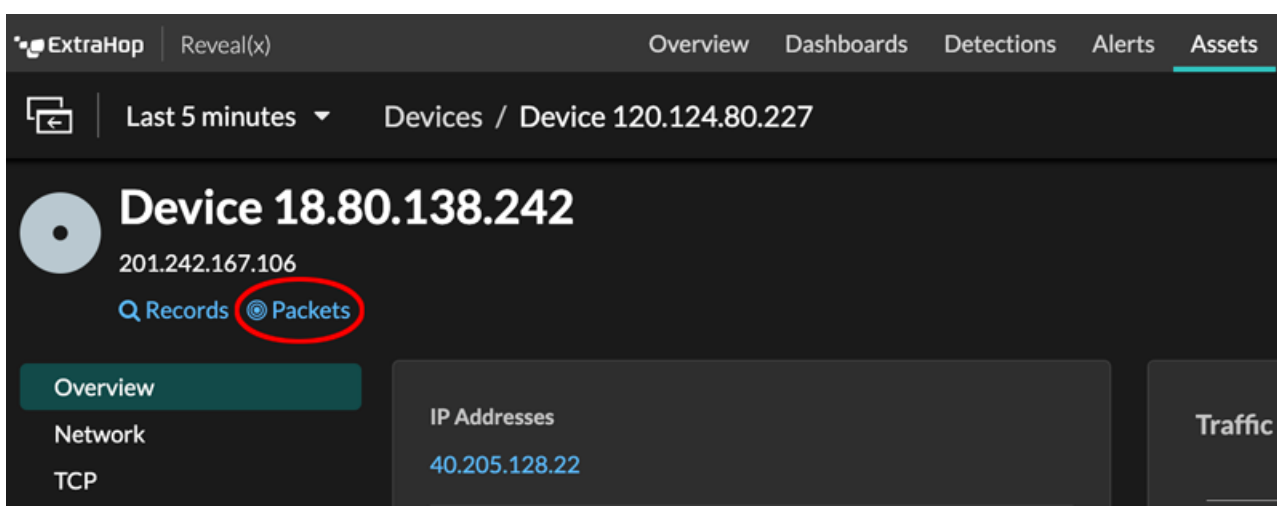
Tip: [Filter packets with Berkeley Packet Filter syntax](#).

There are multiple locations in the ExtraHop system from which you can initiate a packet query:

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



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



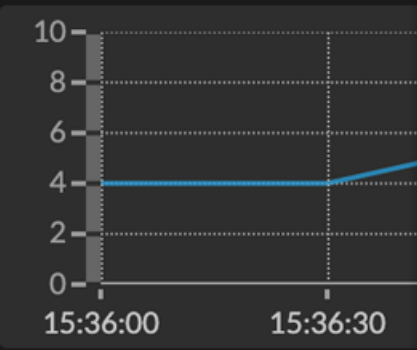
- Click the Packets icon next to any record on a record query results page.

	Time ↓	Record Type
	2022-02-23 15:04:08.999	DNS Response
	2022-02-23 15:04:08.999	DNS Request
	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	SSL Close

- 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.

Overview Dashboards Detections Alerts Assets

Threat Hunting / HTTP



10
8
6
4
2
0

15:36:00 15:36:30

Any Field ≈

	Client IP
<input type="text"/>	100.152.8.59
<input type="text"/>	192.168.23.82

100.152.8.59
External Endpoint
Las Vegas, Nevada, United States

myip.opendns.com

Go To

- [ARIN Whois Lookup](#)
- [Records](#)
- [Packets](#)

[Go to IP Address Details](#)