

Packets

Published: 2021-08-31

If your ExtraHop system is configured for continuous packet capture, you can search for and download packets from the Packets page in the ExtraHop system and the [Packet Search](#) resource in the ExtraHop REST API. The downloaded packets can then be analyzed through a third-party tool, such as Wireshark.

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:

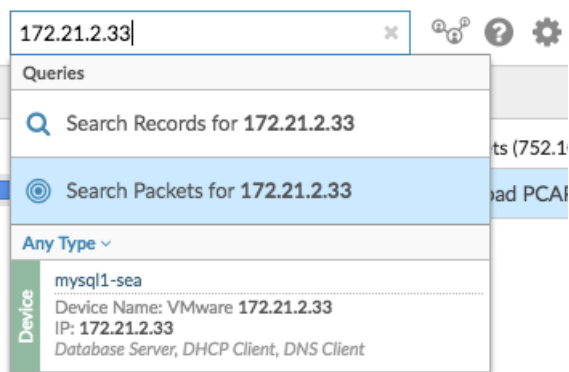
The screenshot shows the ExtraHop interface for the 'Packets' section. At the top, there are navigation tabs: Dashboards, Metrics, Records, and Packets. A search bar is present with the text 'Type an IP address in the global search field and then select Search Packets'. Below this, there's a 'Packet Query' section with a time range bar. The bar shows 'From Jun 30, 12:43:43 pm' and 'Until Jun 30, 1:13:43 pm'. A blue bar indicates the time range where packets were found. A 'Download PCAP' button is visible. Below the time range, there's a filter section with 'IP Address' and a search field. A table titled 'Previewing 20 packets around Jun 30, 1:13:43.103 pm' shows packet details. The table has columns: Time, Src IP, Dst IP, IP Proto, Src Port, Dst Port, Flags, Bytes, Src MAC, Dst MAC, EtherType, and VLAN ID. The table contains 8 rows of packet data.

Time	Src IP	Dst IP	IP Proto	Src Port	Dst Port	Flags	Bytes	Src MAC	Dst MAC	EtherType	VLAN ID
2017-06-30 13:13:43.10...	172.21.1.81	222.154.12.13...	TCP	8080	56696	ACK	1,51...	00:0C:29:5A:7D:3...	00:0C:29:D1:1F:E8	IPv4	—
2017-06-30 13:13:43.10...	172.21.1.81	222.154.12.13...	TCP	8080	56696	ACK	1,51...	00:0C:29:5A:7D:3...	00:0C:29:D1:1F:E8	IPv4	—
2017-06-30 13:13:43.10...	172.21.1.81	222.154.12.13...	TCP	8080	56696	PSH AC...	268	00:0C:29:5A:7D:3...	00:0C:29:D1:1F:E8	IPv4	—
2017-06-30 13:13:43.10...	222.154.12.13...	172.21.1.81	TCP	56696	8080	ACK	66	00:0C:29:D1:1F:E8	00:0C:29:5A:7D:3...	IPv4	—
2017-06-30 13:13:43.10...	222.154.12.13...	172.21.1.81	TCP	56696	8080	ACK	66	00:0C:29:D1:1F:E8	00:0C:29:5A:7D:3...	IPv4	—
2017-06-30 13:13:43.10...	222.154.12.13...	172.21.1.81	TCP	56696	8080	ACK	66	00:0C:29:D1:1F:E8	00:0C:29:5A:7D:3...	IPv4	—
2017-06-30 13:13:43.10...	222.154.12.13...	172.21.1.81	TCP	56696	8080	ACK	66	00:0C:29:D1:1F:E8	00:0C:29:5A:7D:3...	IPv4	—
2017-06-30 13:13:43.10...	222.154.12.13...	172.21.1.81	TCP	56696	8080	ACK	66	00:0C:29:D1:1F:E8	00:0C:29:5A:7D:3...	IPv4	—

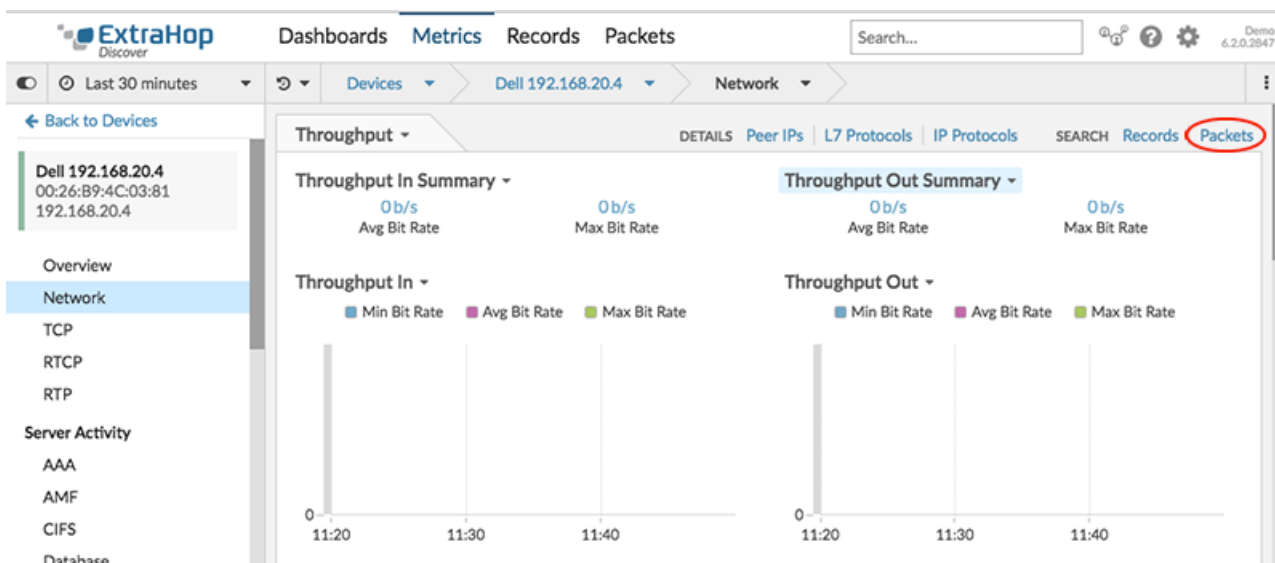
Tip: [Filter packets with Berkeley Packet Filter syntax](#).

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** from the upper right corner of a device page.



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

Any Field =

Packets	Time	Record Type
	2017-07-03 15:52:13.744	HTTP
	2017-07-03 15:52:13.744	HTTP
	2017-07-03 15:52:13.742	Flow
	2017-07-03 15:52:13.742	Flow
	2017-07-03 15:52:13.742	DB

- 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, select the Packets icon  to query for the device and time interval.

XenApp Client Network Health & Citrix Performance Impact ▾

Network Retransmissions ▾

192.168.2.128
192.168.6.180
192.168.10.211
192.168.2.11

Internal Client Dropped Packets ▾

192.168.6.180

Application Slowdowns ▾

192.168.2.128

Drill down by...

Group Member

Packets

Go to device...

[Device 0200c0a802800000 - TCP](#)

[Create chart from...](#)