

# Packets

Published: 2020-03-21

With a Reveal(x) system or an ExtraHop Trace appliance connected to a Discover appliance, you can search for and download packets for selected transactions through the Packets feature in the ExtraHop Web UI 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.

- For ExtraHop Reveal(x) systems that do not include continuous packet capture, you can [configure precision packet capture](#) by writing a trigger.
- For Discover appliances, you must deploy a Trace appliance. See the [deployment guides](#) for the ExtraHop Trace appliance.

## Query for packets

You can launch a quick packet query for the current time interval by clicking **Packets** from the top menu. The ExtraHop system queries packets for the selected time interval, such as the last 30 minutes, 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 Packets page. At the top, there are navigation tabs: Dashboards, Metrics, Records, and Packets. A search bar is located in the top right corner. Below the navigation, there's a 'Last 30 minutes an hour ago' dropdown and a 'Packet Queries' section with a 'New Packet Query' button. A 'Refine Results' sidebar on the left lists various IP addresses and their corresponding data sizes. The main area features a 'Packet Query' section with a time range bar from 'From Jun 30, 12:43:43 pm' to 'Until Jun 30, 1:13:43 pm'. A blue bar indicates the time range where packets were found. Below this, there's an 'IP Address' filter dropdown and a search input field. A table titled 'Previewing 20 packets around Jun 30, 1:13:43.103 pm' displays packet details including Time, Src IP, Dst IP, IP Proto, Src Port, Dst Port, Flags, Bytes, Src MAC, Dst MAC, EtherType, and VLAN ID.

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	-

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

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

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

172.21.2.33

Queries

- Search Records for 172.21.2.33
- Search Packets for 172.21.2.33**

Any Type ▾

Device

mysql1-sea

Device Name: VMware 172.21.2.33  
IP: 172.21.2.33  
Database Server, DHCP Client, DNS Client

- Click **Packets** from the upper right corner of a device page.

The screenshot shows the ExtraHop interface with the 'Packets' tab selected in the top navigation bar. The main content area displays throughput metrics for 'Dell 192.168.20.4'. The 'Packets' icon in the top right of the record view is circled in red. The interface includes a sidebar with navigation options like Overview, Network, TCP, and Server Activity.

- 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...](#)