

Packets concepts

Published: 2018-11-12

With 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. The downloaded packets can then be analyzed through a third-party tool, such as Wireshark.

Before you begin

You must have a configured ExtraHop Trace appliance before you can store and query for packets. See our [deployment guides](#) to get started.

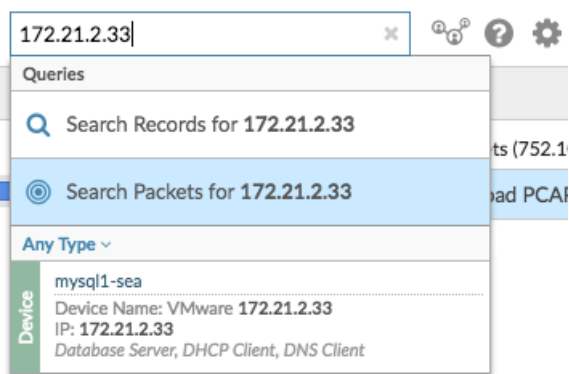
You can launch a quick packet query for the current time interval by clicking **Packets** from the top menu. The ExtraHop system queries packets for the selected time interval, such as the last 30 minutes, and displays the Packet Query page. If you change the time interval, the query starts again. Either 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:

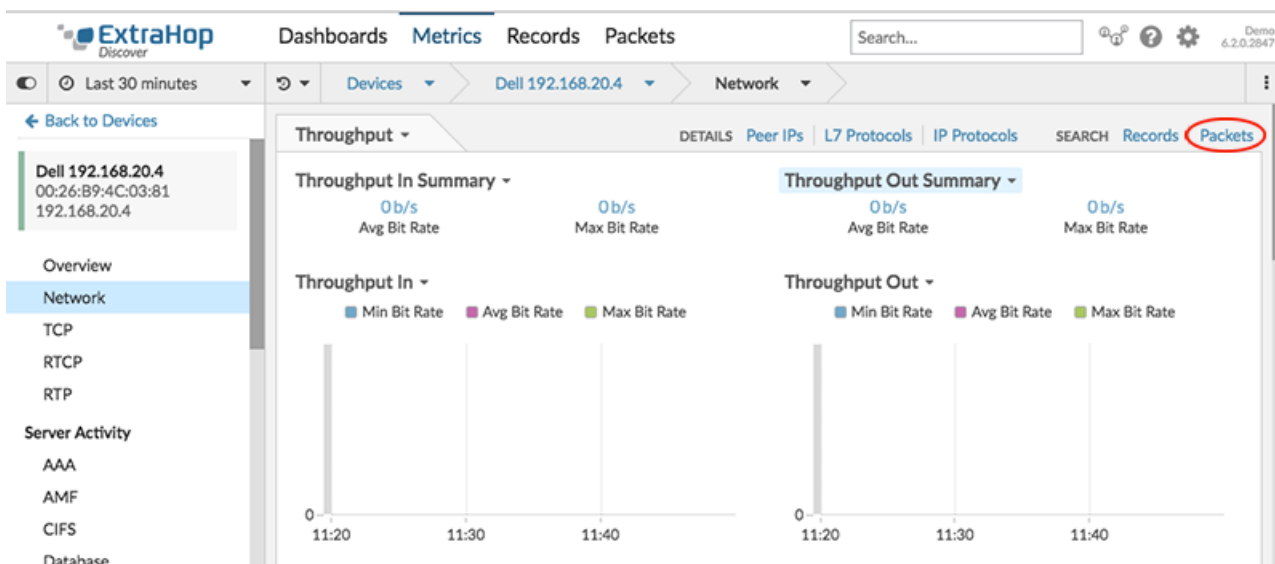
The screenshot shows the ExtraHop Web UI interface for the 'Packets' section. At the top, there's a navigation bar with 'Dashboards', 'Metrics', 'Records', and 'Packets'. Below this, there's a 'Packet Query' section. On the left, there's a 'Refine Results' sidebar with a list of IP addresses and their corresponding data sizes. The main area shows a search bar with the text 'Search...', a time range selector with 'From Jun 30, 12:43:43 pm' and 'Until Jun 30, 1:13:43 pm', and a 'Download PCAP' button. Below the time range selector, there's a table of packet details with columns for 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 packet data. Annotations with arrows point to various features: 'Set time interval' points to the time range selector; 'Filter the results' points to the search bar; 'Start a packet query' points to the 'New Packet Query' button; 'Time range where packets were found' points to the blue bar in the time range selector; and 'Type an IP address in the global search field and then select Search Packets' points to the search bar.


However, 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 .









- 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. (Only available with a connected Explore appliance.)

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...](#)