

Packets

Published: 2019-02-08

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 are navigation tabs for 'Dashboards', 'Metrics', 'Records', and 'Packets'. Below this is a search bar and a 'New Packet Query' button. A time range bar is visible, showing a blue segment for the current query. A table of packet details is displayed, including columns for Time, Src IP, Dst IP, IP Proto, Src Port, Dst Port, Flags, Bytes, Src MAC, Dst MAC, EtherType, and VLAN ID. Annotations with arrows point to various UI elements: 'Set time interval' points to the time range bar; 'Filter the results' points to the 'IP Address' filter; 'Start a packet query' points to the 'New Packet Query' button; 'Time range where packets were found' points to the blue bar on the time range; 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 .

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.

ExtraHop Discover Dashboards Metrics Records **Packets** Search... Demo 6.2.0.2847

Last 30 minutes Devices Dell 192.168.20.4 Network

← Back to Devices

Dell 192.168.20.4
00:26:B9:4C:03:81
192.168.20.4

Overview
Network
TCP
RTCP
RTP
Server Activity
AAA
AMF
CIFS
Database

Throughput In Summary - 0b/s Avg Bit Rate 0b/s Max Bit Rate

Throughput Out Summary - 0b/s Avg Bit Rate 0b/s Max Bit Rate

Throughput In - Min Bit Rate Avg Bit Rate Max Bit Rate

Throughput Out - Min Bit Rate Avg Bit Rate Max Bit Rate

SEARCH Records **Packets**

- Click the Packets icon next to any record on a record query results page in table view mode. (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

Application Slowdowns ▾

192.168.2.128

Drill down by...

- Group Member
- Packets

Go to device...

- [Device 0200c0a802800000 - TCP](#)
- [Create chart from...](#)

Internal Client Dropped Packets ▾

- 192.168.6.180