Packets

Published: 2024-04-07

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.

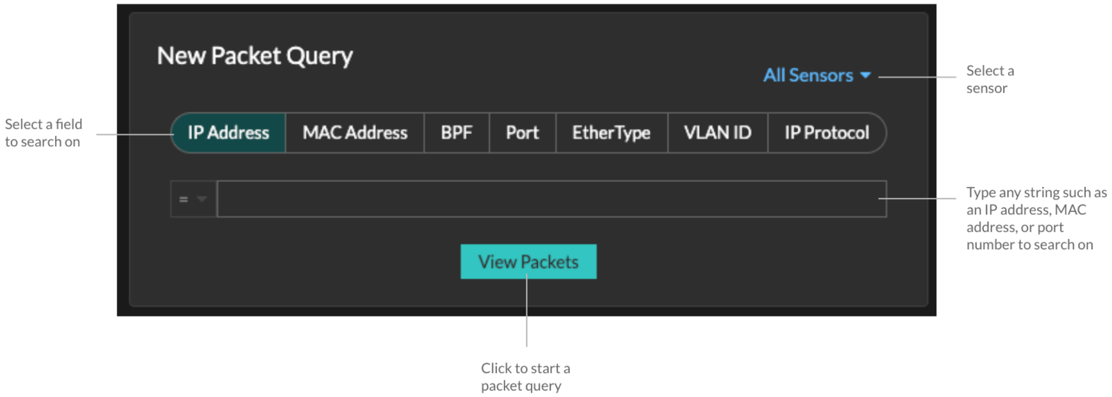
You can search for and download packets from the Packets page in the ExtraHop system and through the Packet Search resource in the ExtraHop REST API. Downloaded packets can then be analyzed through a third-party tool, such as Wireshark.

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.

Video: See the related training: Packets

Navigating packets

Click **Packets** from the top menu to create a new packet query. From the New Packet Query page, you can specify a filter.



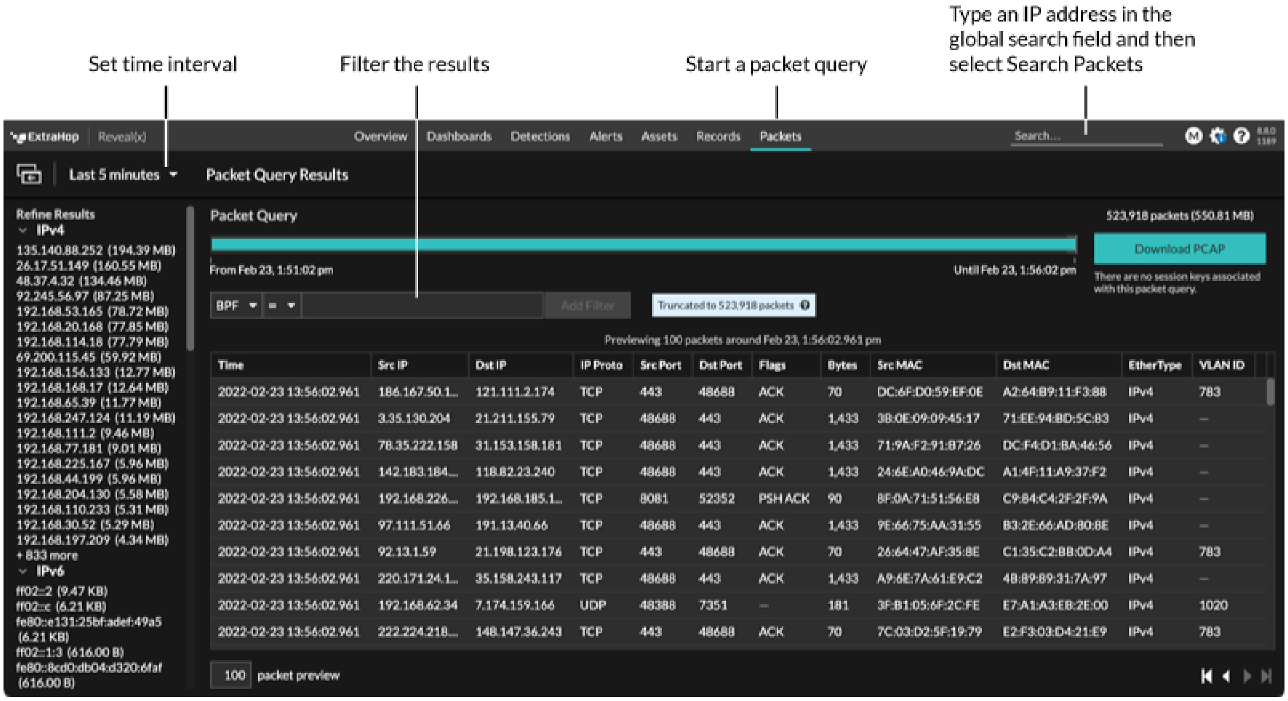
Select a sensor

Select a field to search on

Type any string such as an IP address, MAC address, or port number to search on

Click to start a packet query

The results appear on the main Packets page. Launch another packet query by clicking **Packets** again from the top menu.



Refine Results

IPv4

135.140.88.252 (194.39 MB)
26.17.51.149 (160.55 MB)
48.37.4.32 (134.46 MB)
92.245.56.97 (87.25 MB)
192.168.53.165 (78.72 MB)
192.168.20.168 (77.85 MB)
192.168.114.18 (77.79 MB)
69.200.115.45 (59.92 MB)
192.168.156.133 (12.77 MB)
192.168.168.17 (12.64 MB)
192.168.65.39 (11.77 MB)
192.168.247.124 (11.19 MB)
192.168.111.2 (9.46 MB)
192.168.77.181 (9.01 MB)
192.168.225.167 (5.96 MB)
192.168.44.199 (5.96 MB)
192.168.204.130 (5.58 MB)
192.168.110.233 (5.31 MB)
192.168.30.52 (5.29 MB)
192.168.197.209 (4.34 MB)
+ 833 more

IPv6

ff02::2 (9.47 KB)
ff02::c (6.21 KB)
fe80::e131:25bf:adef:49a5 (6.21 KB)
ff02::1:3 (616.00 B)
fe80::8cd0:db04:d320:6faf (616.00 B)

Packet Query

523,918 packets (550.81 MB)

From Feb 23, 1:51:02 pm

Until Feb 23, 1:56:02 pm

There are no session keys associated with this packet query.

Previewing 100 packets around Feb 23, 1:56:02.961 pm

Time	Src IP	Dst IP	IP Proto	Src Port	Dst Port	Flags	Bytes	Src MAC	Dst MAC	EtherType	VLAN ID
2022-02-23 13:56:02.961	186.167.50.1...	121.111.2.174	TCP	443	48688	ACK	70	DC:6F:D0:59:EF:0E	A2:64:B9:11:F3:88	IPv4	783
2022-02-23 13:56:02.961	3.35.130.204	21.211.155.79	TCP	48688	443	ACK	1,433	3B:0E:09:09:45:17	71:EE:94:8D:5C:83	IPv4	–
2022-02-23 13:56:02.961	78.35.222.158	31.153.158.181	TCP	48688	443	ACK	1,433	71:9A:F2:91:B7:26	DC:F4:D1:BA:46:56	IPv4	–
2022-02-23 13:56:02.961	142.183.184...	118.82.23.240	TCP	48688	443	ACK	1,433	24:6E:A0:46:9A:DC	A1:4F:11:A9:37:F2	IPv4	–
2022-02-23 13:56:02.961	192.168.226...	192.168.185.1...	TCP	8081	52352	PSH ACK	90	8F:0A:71:51:56:E8	C9:84:C4:2F:2F:9A	IPv4	–
2022-02-23 13:56:02.961	97.111.51.66	191.13.40.66	TCP	48688	443	ACK	1,433	9E:66:75:AA:31:55	B3:2E:66:AD:80:8E	IPv4	–
2022-02-23 13:56:02.961	92.13.1.59	21.198.123.176	TCP	443	48688	ACK	70	26:64:47:AF:35:8E	C1:35:C2:BB:0D:A4	IPv4	783
2022-02-23 13:56:02.961	220.171.24.1...	35.158.243.117	TCP	48688	443	ACK	1,433	A9:6E:7A:61:E9:C2	4B:89:89:31:7A:97	IPv4	–
2022-02-23 13:56:02.961	192.168.62.34	7.174.159.166	UDP	48388	7351	–	181	3F:B1:05:6F:2C:FE	E7:A1:A3:EB:2E:00	IPv4	1020
2022-02-23 13:56:02.961	222.224.218...	148.147.36.243	TCP	443	48688	ACK	70	7C:03:D2:5F:19:79	E2:F3:03:D4:21:E9	IPv4	783

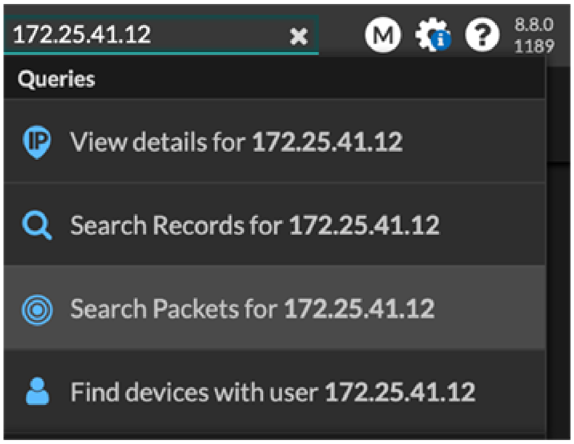
100 packet preview

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.

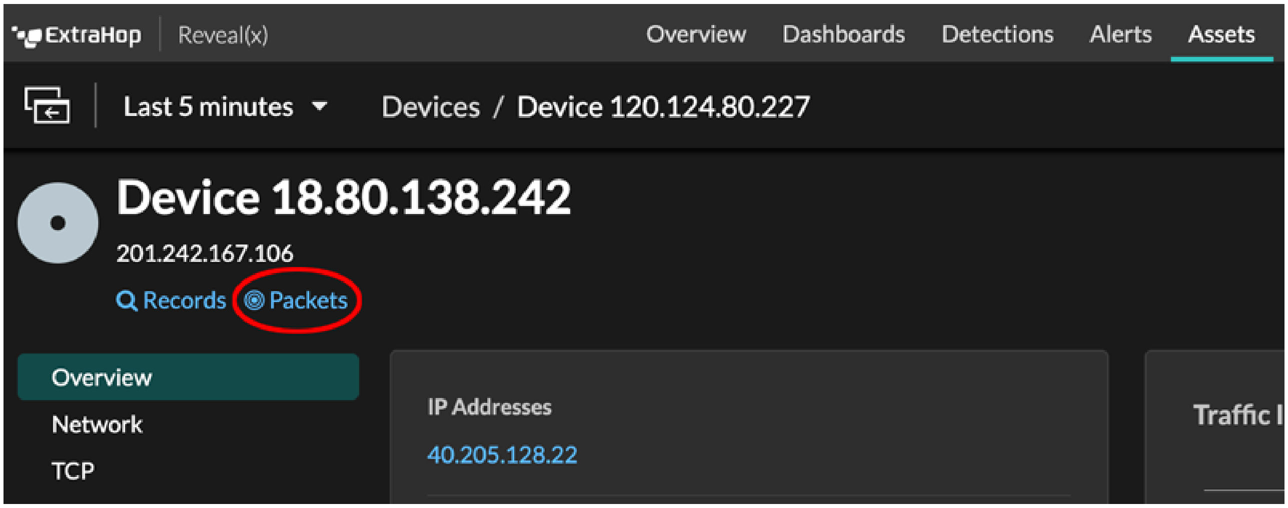
Tip: Filter packets with Berkeley Packet Filter syntax.

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

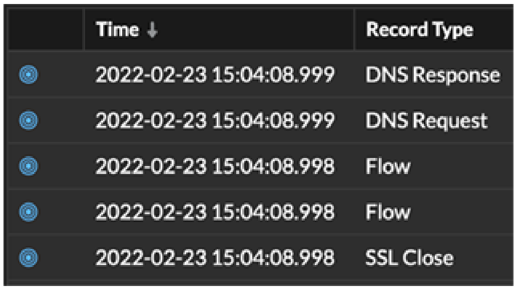
- Type an IP address in the global search field and then select the Search Packets icon ◎ .


172.25.41.12
8.8.0
1189
Queries
View details for 172.25.41.12
Search Records for 172.25.41.12
Search Packets for 172.25.41.12
Find devices with user 172.25.41.12

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

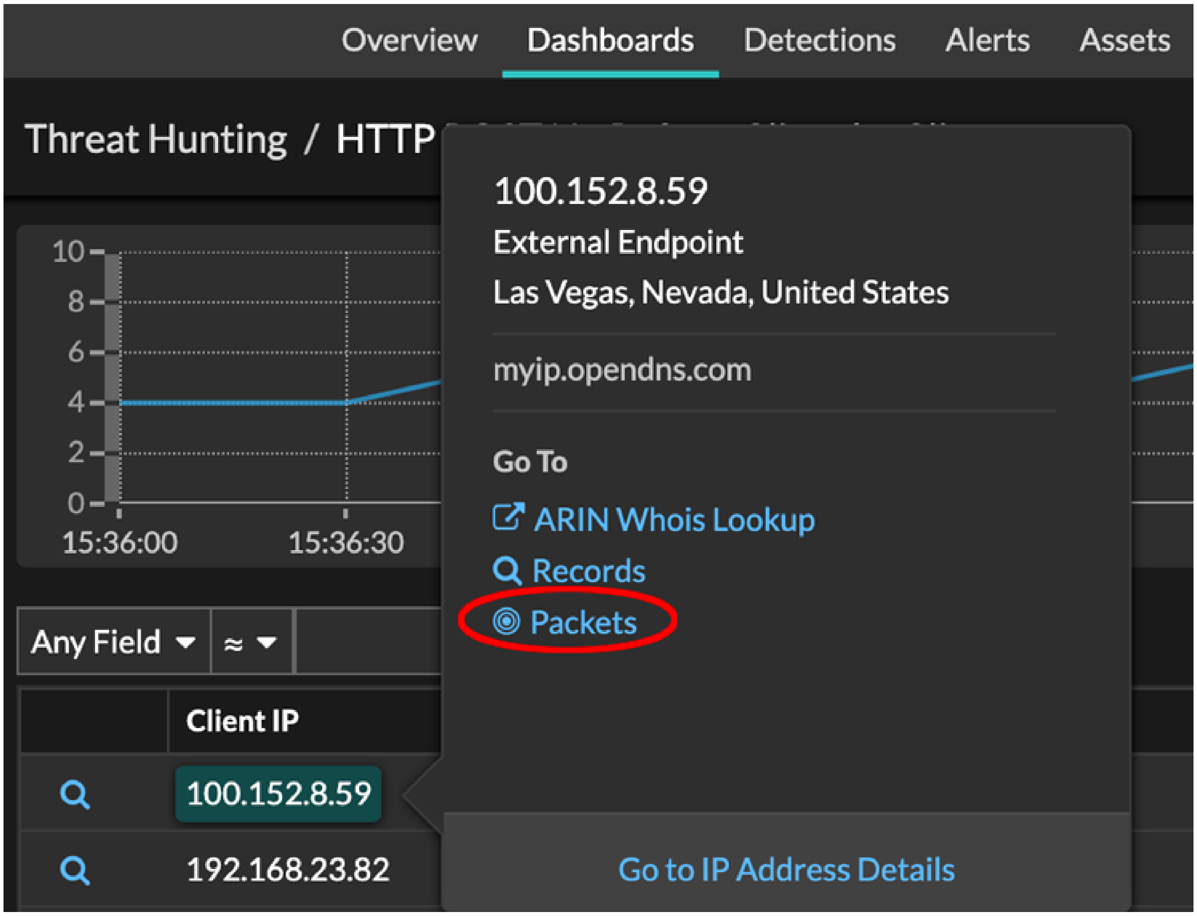


- Click the Packets icon ◎ next to any record on a record query results page.



	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
100.152.8.59
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