Packets

Published: 2022-09-27

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 **Z**. See Initiate precision packet captures to analyze zero window conditions **Z** for an example.

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.

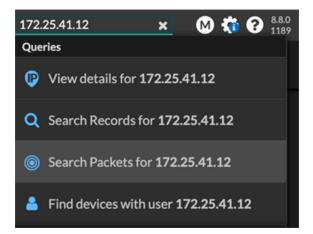
Set time inte	er the resu	e results			Start a packet query				Type an IP address in the global search field and then select Search Packets			
StraHop Reveal(x)	0	verview Dashbo	ards Detections	Alerts	Assets	Records	Packets			Search	(🕲 🆚 🕜 👫
🕞 🛛 Last 5 minutes 👻	Packet Query Results											
Refine Results	Packet Query									5	3,918 packets	(550.81 MB)
133.140.882.52 (194.39 MB) 26.17.51.149 (160.55 MB) 26.17.51.149 (160.55 MB) 48.37.432 (134.46 MB) 92.2465.531.65 (78.27 MB) 192.168.231.65 (78.27 MB) 192.168.231.65 (78.27 MB) 192.168.156.133 (12.77 MB) 192.168.156.133 (12.77 MB) 192.168.156.133 (12.77 MB) 192.168.451 (12.44 MB) 192.168.47 (12.44 MB) 192.168.47 (12.44 MB) 192.168.47 (12.44 MB) 192.168.47 (12.44 MB) 192.168.47 (12.44 MB) 192.168.47 (12.44 MB) 192.168.251.67 (5.96 MB) 192.168.4199 (5.96 MB) 192.168.252 (5.27 MB) 192.168.19.52 (5.27 MB) 192.168.19.52 (5.27 MB) 192.168.19.52 (5.27 MB) 192.168.197.209 (4.34 MB) 192.168.19	From Feb 23, 1:51:02 pm BPF 👻 🖷 👻		Add Filter			Truncated to 523,918 packets			Until Fe	Until Feb 23, 1:56:02 pm There are no session keys associated with this packet query.		
	Time	Src IP	Dat IP	Previ			nd Feb 23, 1:5		m Src MAC	Dit MAC	Filter Trees	VLAN ID
	Time 2022-02-23 13:56:02.961	186.167.50.1	121.111.2.174	TCP	Src Port	Dst Port 48688	Flags	Bytes 70	DC:6F:D0:59:EF:0E	A2:64:89:11:F3:88	EtherType IPv4	783
	2022-02-23 13:56:02.961	3.35.130.204	21.211.155.79	тср	48688	443	ACK	1.433	38:0E:09:09:45:17	71:EE:94:BD:5C:83	IPv4	-
	2022-02-23 13:56:02.961	78.35.222.158	31.153.158.181	тср	48688	443	ACK	1,433	71:9A:F2:91:87:26	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	тср	8081	52352	PSHACK	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	тср	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	тср	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
ff02::1:3 (616.00 B) fe80::8cd0:db04:d320:6faf (616.00 B)	100 packet preview											$\mathbf{H} \boldsymbol{\prec} \models \mathbb{H}$

The following figure provides an overview of the Packet Query page and features:

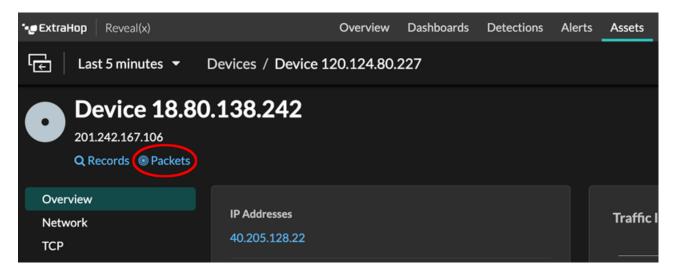
Tip: Filter packets with Berkeley Packet Filter syntax .

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** on a device page.



• Click the Packets icon <a>o next to any record on a record query results page.

	Time ↓	Record Type
۲	2022-02-23 15:04:08.999	DNS Response
	2022-02-23 15:04:08.999	DNS Request
۲	2022-02-23 15:04:08.998	Flow
۲	2022-02-23 15:04:08.998	Flow
۲	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 (1) to query for the device and time interval.

🕶 ExtraHop

