


Pakete

Veröffentlicht: 2024-04-10

Ein Netzwerkpaket ist eine kleine Datenmenge, die über TCP/IP-Netzwerke (Transmission Control Protocol/Internet Protocol) gesendet wird. Das ExtraHop-System ermöglicht es Ihnen, diese Pakete kontinuierlich mit einer Trace-Appliance zu sammeln, zu durchsuchen und herunterzuladen. Dies kann nützlich sein, um Netzwerkeinbrüche und andere verdächtige Aktivitäten zu erkennen.

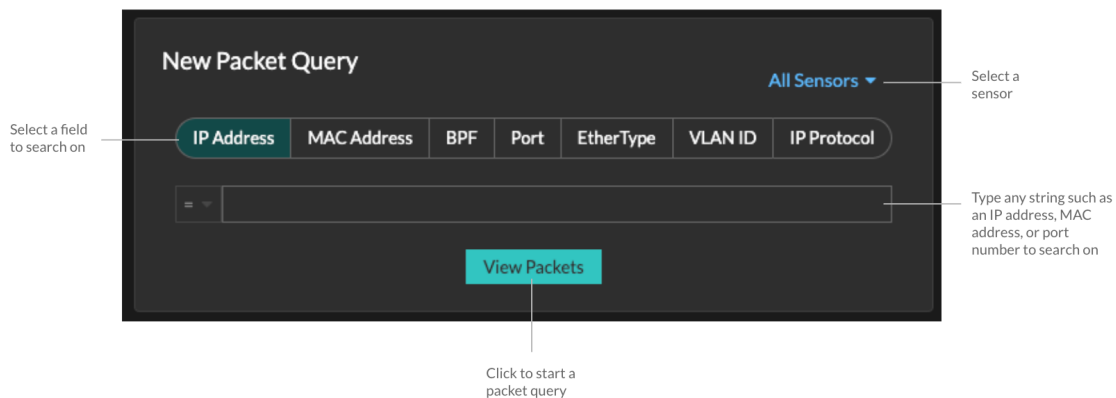
Sie können auf der Seite Pakete im ExtraHop-System nach Paketen suchen und diese herunterladen und über [Paketsuche](#) Ressource in der ExtraHop REST-API. Heruntergeladene Pakete können dann mit einem Drittanbieter-Tool wie Wireshark analysiert werden.

 **Hinweis** Wenn Sie keine Trace-Appliance haben, können Sie Pakete trotzdem über [löst aus](#). siehe [Initiieren Sie präzise Paketerfassungen, um Bedingungen ohne Fenster zu analysieren](#) für ein Beispiel.

 **Video** Sehen Sie sich die entsprechende Schulung an: [Pakete](#)

In Paketen navigieren

Klicken Sie **Pakete** aus dem oberen Menü, um eine neue Paketabfrage zu erstellen. Auf der Seite Neue Paketabfrage können Sie einen Filter angeben.



Die Ergebnisse erscheinen auf der Hauptseite Pakete Seite. Starten Sie eine weitere Paketabfrage, indem Sie auf **Pakete** wieder aus dem Hauptmenü.

Set time interval Filter the results Start a packet query Type an IP address in the global search field and then select Search Packets

Packet Query Results

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 (69.92 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)
 - 192.168.204.130 (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)

Download PCAP

From Feb 23, 1:51:02 pm Until Feb 23, 1:56:02 pm

BPF Add Filter Truncated to 523,918 packets

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:DD: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:BE	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

Wenn Sie das Zeitintervall ändern, beginnt die Abfrage erneut. An beiden Enden des grauen Balkens wird ein Zeitstempel angezeigt, der durch das aktuelle Zeitintervall bestimmt wird. Die Uhrzeit auf der rechten Seite zeigt den Startpunkt der Abfrage an und die Uhrzeit auf der linken Seite zeigt den Endpunkt der Abfrage an. Der blaue Balken gibt den Zeitraum an, in dem das System Pakete gefunden hat. Sie können einen Zeitraum in der blauen Leiste durch Ziehen vergrößern, um eine Abfrage für das ausgewählte Zeitintervall erneut auszuführen.





Hinweis: Pakete mit der Berkeley-Paketfilter-Syntax filtern [↗](#)

Es gibt mehrere Stellen im ExtraHop-System, von denen aus Sie eine Paketabfrage starten können:

- Geben Sie eine IP-Adresse in das globale Suchfeld ein und wählen Sie dann das Symbol Pakete durchsuchen aus. .

172.25.41.12

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

- Klicken Sie **Pakete** auf einer Geräteseite.

ExtraHop | Reveal(x) | Overview | Dashboards | Detections | Alerts | **Assets**

Last 5 minutes ▾ | Devices / Device 120.124.80.227

Device 18.80.138.242
201.242.167.106

Q Records **⊙ Packets**

Overview
Network
TCP

IP Addresses
40.205.128.22

Traffic I

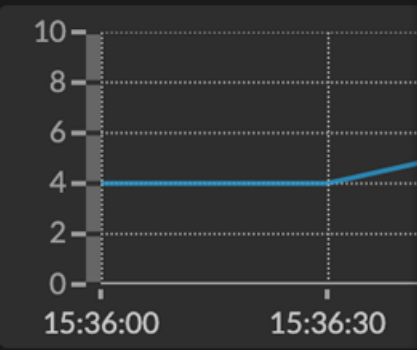
- Klicken Sie auf das Paketsymbol **⊙** neben einem beliebigen Datensatz auf der Ergebnisseite einer Datensatzabfrage.

	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

- Klicken Sie in einem Diagramm mit Metriken für Netzwerkbytes oder Pakete nach IP-Adresse auf eine IP-Adresse oder einen Hostnamen, um ein Kontextmenü aufzurufen. Klicken Sie dann auf das Paketsymbol **⊙** um das Gerät und das Zeitintervall abzufragen.

Overview Dashboards Detections Alerts Assets

Threat Hunting / HTTP



10
8
6
4
2
0

15:36:00 15:36:30

Any Field ≈

	Client IP
<input type="text"/>	100.152.8.59
<input type="text"/>	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](#)