

Pakete

Veröffentlicht: 2024-01-31

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 [Paketssuche](#) 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 Wenn Sie sich die entsprechende Schulung an: [Pakete](#)

Anfrage nach Paketen


Starten Sie eine schnelle Paketabfrage, indem Sie auf **Pakete** aus dem oberen Menü. Das ExtraHop-System fragt alle Pakete ab und zeigt die Seite Paketabfrage an. 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.

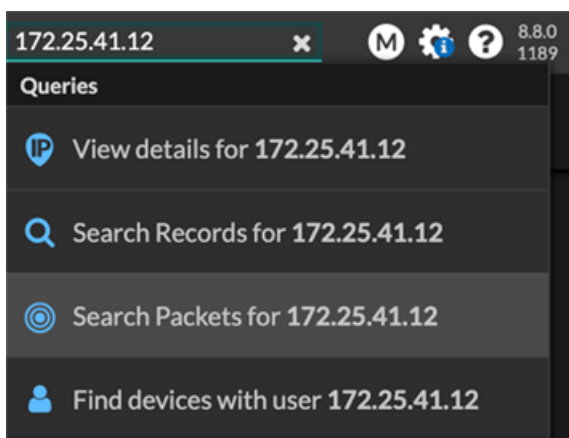
Die folgende Abbildung bietet einen Überblick über die Seite „Paketabfrage“ und ihre Funktionen:

The screenshot shows the 'Packets' section of the ExtraHop interface. At the top, there are navigation tabs: Overview, Dashboards, Detections, Alerts, Assets, Records, and **Packets**. A search bar is located in the top right corner. Below the navigation, there's a 'Packet Query Results' section. On the left, there's a 'Refine Results' sidebar with a tree view showing 'IPv4' and 'IPv6' categories, each with a list of IP addresses and their corresponding data sizes. The main area shows a 'Packet Query' section with a time range bar (From Feb 23, 1:51:02 pm to Until Feb 23, 1:56:02 pm) and a 'Download PCAP' button. Below this is a 'Filter' section with a 'BPF' dropdown and an 'Add Filter' button. The bottom part of the screenshot shows a table of packet details with columns: Time, Src IP, Dst IP, IP Proto, Src Port, Dst Port, Flags, Bytes, Src MAC, Dst MAC, EtherType, and VLAN ID. The table contains several rows of packet data.

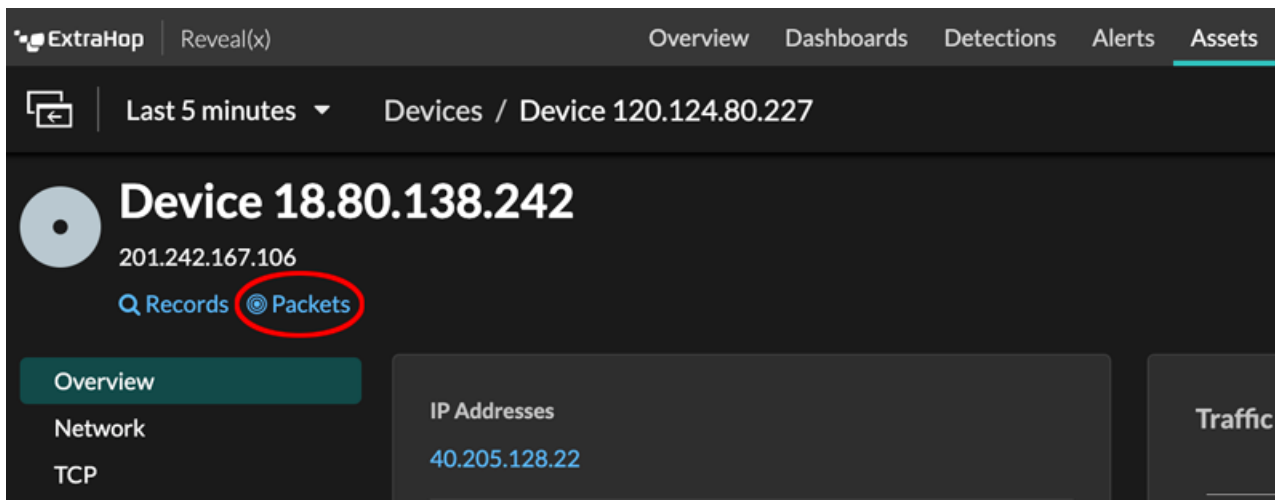
Hinweis [Pakete mit der Berkeley-Paketfilter-Syntax filtern](#).


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  .




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



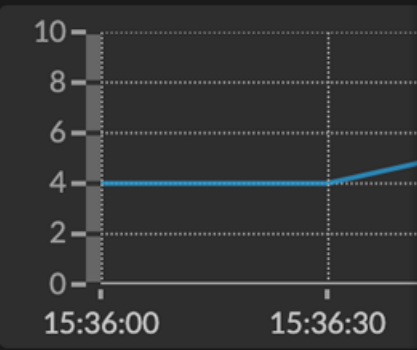
- Klicken Sie auf das Paketsymbol  neben einem beliebigen Datensatz auf der Ergebnisseite einer Datensatzabfrage.

	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](#)