

Network Security Tools

Home

List of Wireshark Display Filters

By [Robert Allen](#) | August 3, 2017 | 3 

When taking a packet capture it can display so much information that it can be difficult to find the information you need. Using Wireshark display filters, you can search for specific traffic or filter out unwanted traffic. This makes it much easier to analyze the packet capture and find the information you need.

The filtering capabilities of Wireshark can get very complex. There are so many different fields, operators and options for creating a filter that it can be hard to remember the syntax.

Below is a list of filters that I use often and have found to be very useful in my hunting for packets. If you have a good filter you want to share please add it to the comments below.

FREE BONUS: [Download the wireshark display list](#) of over 100 useful filters. This list has some easy and very powerful filters.

1. Filter traffic on specific IP address

This will display all traffic for the IP entered, source or destination.

```
ip.addr==192.168.1.2
```

2. Filter by source address

This will only show traffic where the source IP address is 192.168.1.2

```
ip.src==192.168.1.2
```

3. Filter by destination address

Displays only traffic for the matching destination IP.

```
ip.dst==192.168.1.2
```

4. Filter by IP subnet

Displays all traffic for the entered subnet, this will match on source or destination. Use CIDR format for subnet display filter.

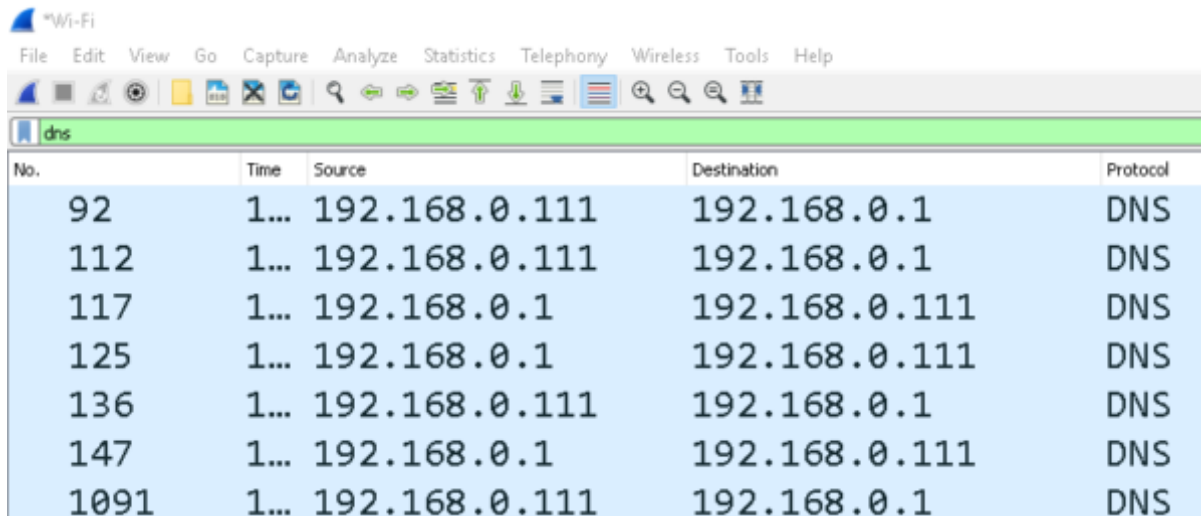
```
ip.addr==192.168.1.0/24
```

If you want to filter on a IP source subnet use `ip.src==subnet`

If you want to filter on IP destination subnet use `ip.dst==subnet`

5. Filter traffic based on protocol

To filter for a specific protocol just type in the name of the protocol. For example to display all DNS traffic just type DNS in the filter box.



No.	Time	Source	Destination	Protocol
92	1...	192.168.0.111	192.168.0.1	DNS
112	1...	192.168.0.111	192.168.0.1	DNS
117	1...	192.168.0.1	192.168.0.111	DNS
125	1...	192.168.0.1	192.168.0.111	DNS
136	1...	192.168.0.111	192.168.0.1	DNS
147	1...	192.168.0.1	192.168.0.111	DNS
1091	1...	192.168.0.111	192.168.0.1	DNS

Some other common protocols you could filter on: arp, http, ftp, smtp, ssh, telnet, bootp, icmp.

6. Exclude IP address

If you want to filter out an IP address so it's not displayed use this filter.

```
!ip.addr==192.168.1.2
```

7. Show traffic between two workstations or subnet

This first one will show only traffic between the two subnets

```
ip.addr==192.168.1.0/24 and ip.addr==192.168.2.0/24
```

This will show only traffic between the two specific IP address

```
ip.addr==192.168.1.2 and ip.addr==192.168.2.3
```

8. Filter by MAC address

If you only want to see traffic for a specific MAC address use this filter

```
eth.addr == 00:60:e0:53:13:d5
```

9. Filter on TCP port

```
tcp.port==80
```

Filter on TCP port source

```
tcp.srcport==80
```

or destination port

```
tcp.dstport==80
```

10. Find user agents

Its a good idea to understand what user agents are being used on your network, malicious traffic can often use unusual agent strings. To search for a user agent use this filter

```
http.user_agent contains Firefox
```

Replace Firefox with the user agent string you want to search for.

I like to use this one to exclude common user agents, this helps to quickly find possible malicious traffic.

```
!http.user_agent contains Firefox || !http.user_agent contains Chrome
```

This will filter out all user agents that contain Firefox or Chrome, I can continue to add on to the filter to exclude other common user agents.

11. Filter background network noise

There are several protocols that can be very noisy, it sometimes helps to filter this out so you can focus on other traffic.

```
!(arp or icmp or dns)
```

This will filter out arp, icmp and DNS traffic.

12. Filter on port and IP Address

If you want to see traffic from a certain IP on a specific port use this filter

```
tcp.port 80 && ip.addr == 192.168.1.2
```

This will show only port 80 (https) that has IP 192.168.1.2 in the source or destination.

13. Filter for all http get requests

```
http.request
```

14. Filter for http get and responses

```
http.request or http.response
```

15. Filter on three way handshake

The three way handshake is often used to calculate the network round trip time. This filter will display all the SYN, SYN ACK and SYN packets that should match the three way handshake.

```
tcp.flags.syn==1 or (tcp.seq==1 and tcp.ack==1 and tcp.len==0 and tcp.analysis.initial_rtt)
```

16. Find executable or other file types

Need to see if users are download .exe or other file types use this filter

```
frame contains "(attachment|tar|exe|zip|pdf) "
```

Just add in any other file extension you want to filter for.

17. Search traffic based on a keyword

```
tcp contains facebook
```

This displays all TCP packets that contain the word facebook. Just replace the word with what you want to search for. The only problem with this filter is it's limited to TCP packets only. To include all protocols use this filter

```
frame contains facebook
```

18. Detecting SYN Floods (Possible DDoS attacks)

DDos attacks can be done in a variety of ways, a large number of TCP connections is one of them.

To look for a large number of tcp connection attempts use this filter

```
tcp.flags.syn == 1 and tcp.flags.ack == 0
```

This will filter for the start of new TCP connections. If you see a constant new connections to the same destination IP, it could be a SYN or DDoS attack.

If you found this list useful, I recommend that you download the free display filter cheat sheet I made, it has over 100 useful display filters.

The list includes many filters not found in this post and includes an explanation to each filter.

Wireshark Display Filter Cheat Sheet

Ethernet Filters (MAC Address)	Explanation
eth.addr == MAC_Address	Filters for Mac address
eth.dst == MAC_Address	Filters for destination
eth.src == MAC_Address	Filters for source MAC
eth.addr == ff:ff:ff:ff:ff:ff	Shows only broadcast
eth.src == MAC_Address && eth.dst == MAC_Address	Filters for traffic with s address
DNS	Explanation
DNS	Shows all DNS traffic
!dns	excludes all DNS traffi
dns.qry.name == "yahoo.com"	Search for a specific I
dns.flags.response == 0	Filter for all DNS Quer
dns.flags.response == 1	Filters for all DNS resq
dns.qry.type == 1	Filter for DNS A recor
dns.qry.type == 15	Filter for CNAME reco
dns.arv.type == 12	Filter for PTR record I

[Download Now](#)

Posted in [wireshark-course1](#) and tagged [sniffers](#), [wireshark](#)

3 Comments

[How to filter http traffic using wireshark - Network Security Tools](#) on August 13, 2017 at 11:25 am

[...] also show some additional display filters for showing all http client [...]

[Reply](#)

How Wireshark Processes Packets - Network Security Tools on August 19, 2017 at 1:03 pm

[...] for Wireshark. This provides users the ability to interact with a packet capture, open, save, add display filters, [...]

[Reply](#)

When to use Wireshark - Network Security Tools on August 31, 2017 at 10:42 am

[...] capture I could see exactly what was happening. Since I knew it was a website issue, I applied a display filter to see all the DNS lookup requests. This would quickly show me all the domains that the client [...]

[Reply](#)

Leave a Comment

Comment

Name (required)

Email (will not be published) (required)

Website

Submit Comment

© 2019 Network Security Tools | Powered by [Beaver Builder](#)