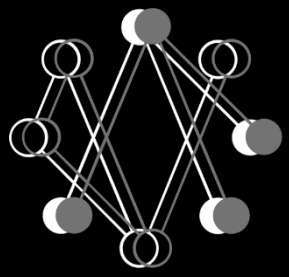

USEFUL WIRESHARK FILTERS

1. IP Address Filter

Filter: ip.addr == 192.168.1.1

Example Usage: This filter is used to display all packets involving the IP address 192.168.1.1. It includes both traffic to and from this address.

2. TCP Port Filter

Filter: tcp.port == 80

Example Usage: This filter shows all TCP packets where the source or destination port is 80, commonly associated with HTTP traffic.

3. Protocol Filter

Filter: http

Example Usage: This filter is used to display all HTTP packets. It's very useful for analyzing un-encrypted traffic.

4. Source and Destination Filter

Filter: ip.src == 192.168.1.1 && ip.dst == 192.168.1.2

Example Usage: This filter shows all packets originating from 192.168.1.1 and destined for 192.168.1.2, useful for tracking specific communication between two devices.

5. MAC Address Filter

Filter: eth.addr == 00:1B:44:11:3A:B7

Example Usage: This filter is used to display all packets that involve the Ethernet (MAC) address 00:1B:44:11:3A:B7.

6. Conversations Filter

Filter: (ip.addr == 192.168.1.1 && ip.addr == 10.1.2.3) && (tcp.port == 443)

Example Usage: This filter is used to display all traffic between the IP address 192.168.1.1 and 10.1.2.3 over TCP port 443, commonly used for HTTPS traffic.

7. Exclude Filter

Filter: !arp

Example Usage: This filter displays all packets except ARP packets. It's useful when you want to focus on higher-level protocols without ARP noise.

8. TCP Flags Filter

Filter: tcp.flags.syn == 1 && tcp.flags.ack == 0

Example Usage: This filter shows all TCP SYN packets that are used to initiate a TCP connection, useful for

analyzing connection setups.

9. DNS Queries Filter

Filter: dns.flags.response == 0

Example Usage: This filter displays all DNS query packets. It excludes DNS responses, focusing on the initial queries sent from clients.

10. Length or Size Filter

Filter: frame.len > 1000

Example Usage: This filter shows all packets with a frame length greater than 1000 bytes, useful for identifying larger packets in your traffic.

Don’t know what is Wireshark or how it is used?

/

Watch my Tutorial on YouTube!