Useful Display Filter

Layer 1

1. *frame.number* : display the selected frame/s according to their number

   Example:

   - frame.number == 123
   - frame.number >= 50 && frame.number <= 100

Layer 2

1. *eth.addr* : display frame/s with matching MAC address

   Example:

   - eth.addr == 01:00:53:54:00:fa
   - eth.addr == 0100.5354.00fa
2. *eth.src* : frame/s with the Ethernet source matching MAC address

   Example:

   - eth.src == 01:00:53:54:00:fa
3. *eth.dst* : frame/s with the Ethernet destination matching MAC address

   Example:

   - eth.dst == 01:00:53:54:00:fa

Layer 3

1. *ip.addr* : displays any matching source or destination IPv4 address

   Example:

   - ip.addr == 192.168.1.1
   - ip.addr == 192.168.1.0/24 (show packet where IP addr within the subnet range)
2. *ip.src* : displays frame/s with matching source IPv4 address

   Example:

   - ip.src == 192.168.1.1
3. *ip.dst* : displays frame/s with matching destination IPv4 address

   Example:

   - ip.dst == 192.168.1.1
4. *icmp.type* : display the selected ICMP types

   Example:

   - icmp.type == 0 (echo reply)
   - icmp.type == 3 (destination unreachable)
   - icmp.type == 8 (echo)

     *for full range of types, visit here

Layer 4

1. *tcp.stream* : display only the packets associated with a particular streams, typically from application layer

   Example:

   - tcp.stream == 1
   - tcp.stream >= 4
2. *udp.stream* : display only the packets associated with a particular streams, typically from application layer

   Example:

   - udp.stream == 1
   - udp.stream >= 4

*alternatively, you can select any frame containing TCP/UDP protocol, right click -> Follow -> TCP Stream or UDP stream

Layer 5

1. *dhcp* : show all frame/s containing the DHCP protocol

   Example:

   - dhcp
2. *dhcp.type* : display the selected DHCP message type such as DHCP Discover, DHCP Request, and etc.

   Example:

   - dhcp.type == 1 (Discover/Request)
   - dhcp.type == 2 (ACK/Offer)
3. *browser.command* : display selected browser messages

   Example:

   - browser.command == 1 (HostAnnouncement message)
   - browser.command == 9 (GetBackupListRequest message)

Guides/References

DHCP

1. https://avocado89.medium.com/getting-dynamic-ip-with-dhcp-ee1ee1e722b0
2. https://avocado89.medium.com/dhcp-packet-analysis-c84827e162f0

Example Approach to Packet Analysis

1. https://josh-vr.medium.com/hackthebox-chase-forensics-challenge-writeup-eebf72d6051f