Wireshark tasks

- Download PDF
- To access the updated handouts, please click on the following link: https://yasirbhutta.github.io/wireshark/index.html

To filter specific traffic using **Wireshark**, you can use display filters to narrow down the packets of interest. Here are some common Wireshark filter tasks that can be helpful for practical scenarios:

1. **Filter by Protocol**

- **HTTP Traffic:**

```
http
```

- **TCP Traffic:**

```
tcp
```

- **UDP Traffic:**

```
udp
```

- **DNS Traffic:**

```
dns
```

    - **DNS Traffic:**

```
dhcp
```

2. **Filter by IP Address**

- **Traffic to/from a Specific IP Address:**

```
ip.addr == 192.168.1.1
```

- **Traffic from a Specific IP Address:**

```
ip.src == 192.168.1.1
```

- **Traffic to a Specific IP Address:**

```
ip.dst == 192.168.1.1
```

3. Filter by Port Number

- **Traffic on a Specific Port:**

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

- **Filter HTTP (port 80) or HTTPS (port 443) Traffic:**

```
tcp.port == 80 or tcp.port == 443
```

4. Filter by MAC Address

- **Traffic from a MAC Address:**

```
eth.src == 00:11:22:33:44:55
```

- **Traffic to a MAC Address:**

```
eth.dst == 00:11:22:33:44:55
```

5. Filter by Subnet

- **Traffic from a Subnet (e.g., 192.168.1.0/24):**

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

The IP address `192.168.1.0/24` represents a **subnet** in the world of IP addressing. Let's break it down:

Components of `192.168.1.0/24`:

1. `192.168.1.0` **(Network Address)**:

    - This is the **base IP address** of the subnet.
    - It's a **private IP address** reserved for internal use within local networks (it won't be routed on the public internet).
    - `192.168.x.x` is a common range for home and small business networks.

2. `/24` **(Subnet Mask)**:

    - This is **CIDR (Classless Inter-Domain Routing) notation** that represents the subnet mask.
    - `/24` means that the first 24 bits of the IP address are reserved for the **network portion**, and the remaining 8 bits are used for the **host portion** (devices within the network).
    - In dotted decimal format, the subnet mask for `/24` is **255.255.255.0**, which is equivalent to 24 network bits.

What Does `192.168.1.0/24` Represent?

- **Network Address**: `192.168.1.0` is the **network identifier** for the subnet. It is not assigned to any device.

- **Range of Usable IP Addresses**:

    - The **usable IP range** in this subnet is from **192.168.1.1** to **192.168.1.254**.
    - **192.168.1.1** would typically be assigned to a router or gateway.
    - You can assign IP addresses from **192.168.1.2** to **192.168.1.254** to devices within the network.

- **Broadcast Address**: The **broadcast address** for this subnet is **192.168.1.255**. This address is used to send messages to all devices on the network.

Structure of an IP Address

An IPv4 address is 32 bits, and in CIDR notation, we divide this into two parts:

- **Network portion** (first 24 bits in this case): Identifies the network (e.g., 192.168.1.x).
- **Host portion** (last 8 bits in this case): Identifies individual devices within the network (e.g., `.1`, `.2`, `.3`, ... up to `.254`).

Example:

For the network `192.168.1.0/24`:

- **Network address**: 192.168.1.0
- **Subnet mask**: 255.255.255.0
- **Usable IP range**: 192.168.1.1 to 192.168.1.254
- **Broadcast address**: 192.168.1.255

This setup allows for **254 usable IP addresses** (from `.1` to `.254`) that can be assigned to hosts (e.g., computers, printers, phones) on the network.

Summary:

- `192.168.1.0` is the network identifier, and the `/24` means the first 24 bits are used for the network, leaving 8 bits for the hosts.

- **Subnet mask** `/24` allows for 254 devices on the network (usable IPs from **192.168.1.1** to **192.168.1.254**).

This type of subnetting is typical in home and small office networks.

6. **Filter by HTTP Request Method**

- **HTTP GET Requests:**

```
http.request.method == "GET"
```

- **HTTP POST Requests:**

```
http.request.method == "POST"
```

7. **Filter by Time**

- **Packets within a specific time range (e.g., capture between two timestamps):**

```
 frame.time >= "Sep 26, 2024 14:00:00" && frame.time <= "Sep 26, 2024
14:30:00"
```

8. **Filter by Packet Size**

- **Packets larger than a specific size (e.g., greater than 1000 bytes):**

```
frame.len > 1000
```

9. **Filter by HTTP Requests in Info Column**

- **Filter HTTP GET requests:**

```
http.request and frame contains "GET"
```

- **Filter HTTP POST requests:**

```
http.request and frame contains "POST"
```

10. **Filter ICMP Packets (Ping) in Info Column**

- **Filter ICMP Echo Requests (ping):**

```
icmp.type == 8
```

- **Filter ICMP Echo Replies:**

```
icmp.type == 0
```

11. Filter by Specific String or Text in Info Column

- **Filter by any text string in the Info column, e.g., a URL:**

```
frame contains "https://example.com"
```

- **Filter by specific phrases, e.g., `ACK` in TCP packet info:**

```
frame contains "ACK"
```

12. Filter by HTTP Response Code in Info Column

- **Filter HTTP 200 OK responses:**

```
http.response.code == 200
```

- **Filter HTTP 404 Not Found responses:**

```
http.response.code == 404
```