CyberForge
ACADEMY

# Wireshark 101

Packet Capture & Analysis

# $ whoami

- Software Engineer and Researcher at CyberForge Academy
- Research, Creating course content/setups, developing SaaS software and open source tools
- For past 6 months, interned with Singapore based Web3 education startup
- Final year, B. Tech. CSE @ LPU Jalandhar
- Interests:
  - Tech 👨‍💻
  - Cricket 🏏
  - Food 🍕

CyberForge ACADEMY

# Table of contents



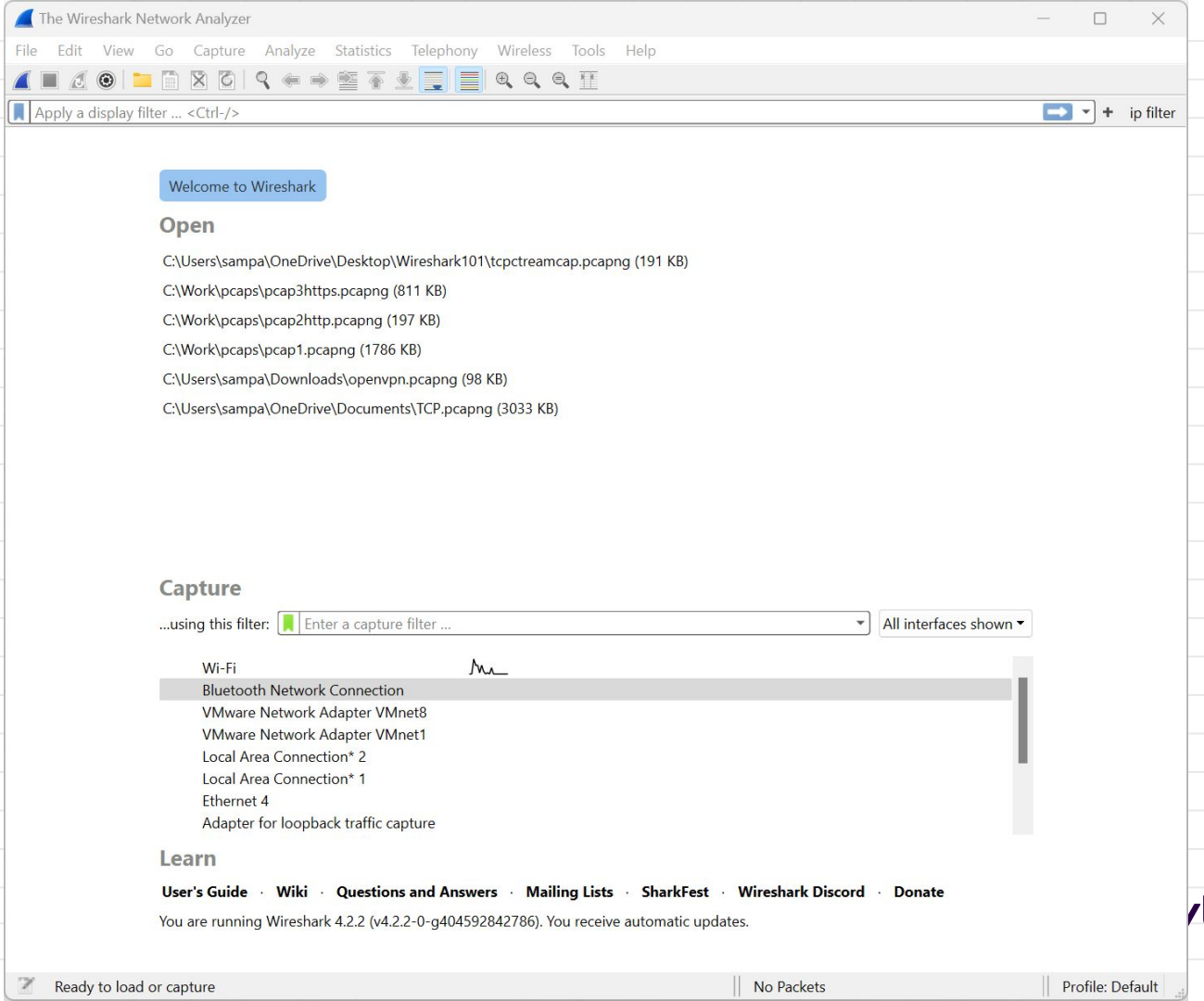
CyberForge ACADEMY

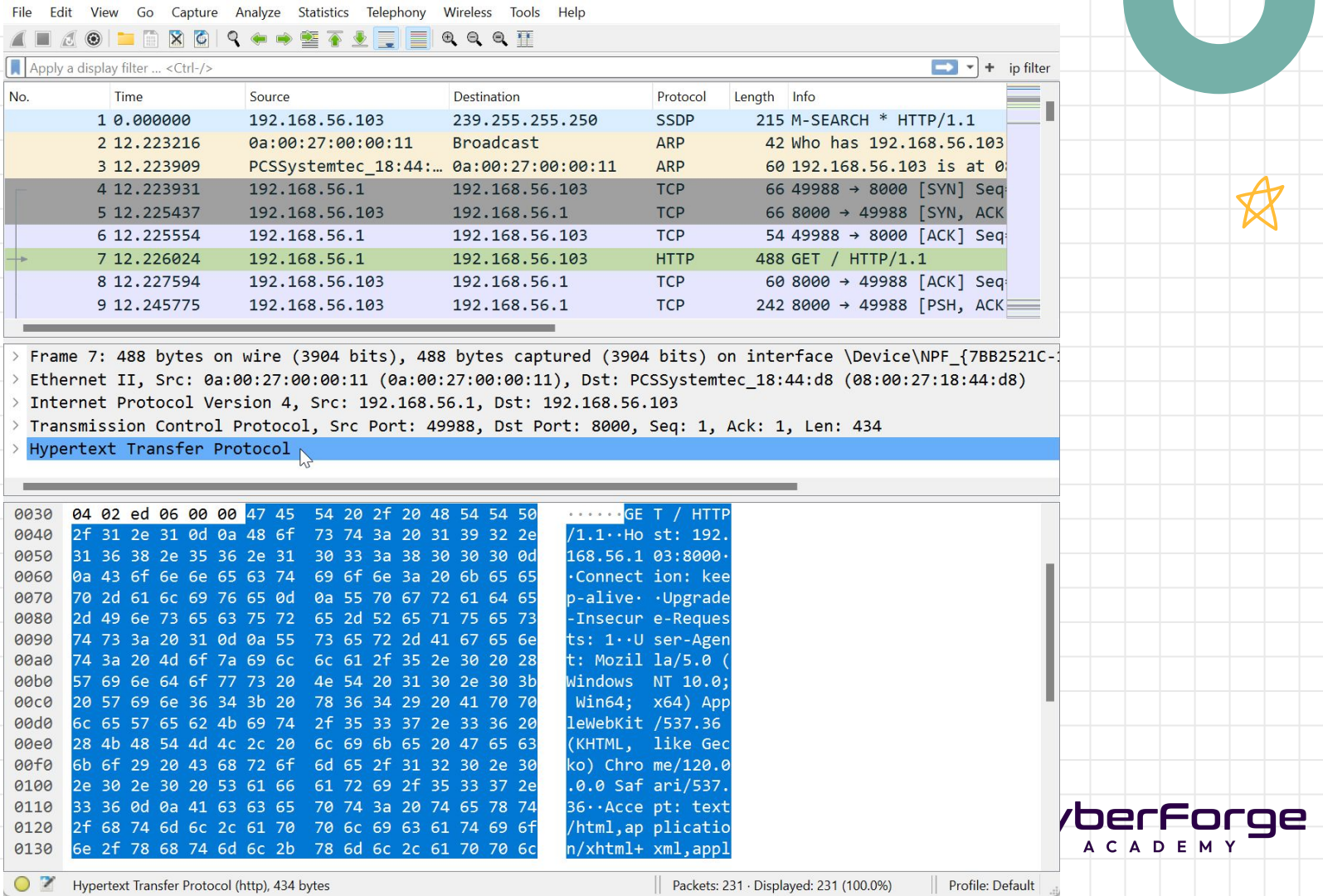
# What is Wireshark ?

- Most popular Network Protocol Analyzer
- Micro and macro analysis of captured packet data
- Released in 1998 by **Gerald Combs** as **Ethereal**
- Free and Open Source
  https://github.com/wireshark/wireshark
- Cross-platform (Windows/Linux/MacOS)
- Can be extended in C or Lua
- Support plugins, easy way to extend functionality

WIRESHARK

CyberForge ACADEMY


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
ip filter
Welcome to Wireshark
Open
C:\Users\sampa\OneDrive\Desktop\Wireshark101\tcpctreamcap.pcapng (191 KB)
C:\Work\pcaps\pcap3https.pcapng (811 KB)
C:\Work\pcaps\pcap2http.pcapng (197 KB)
C:\Work\pcaps\pcap1.pcapng (1786 KB)
C:\Users\sampa\Downloads\openvpn.pcapng (98 KB)
C:\Users\sampa\OneDrive\Documents\TCP.pcapng (3033 KB)
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
Wi-Fi
Bluetooth Network Connection
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 2
Local Area Connection* 1
Ethernet 4
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.2.2 (v4.2.2-0-g404592842786). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default



# Why Packet Analysis?

- Diagnosing Network Issues
  Example: Observe number of retransmissions in TCP packets.

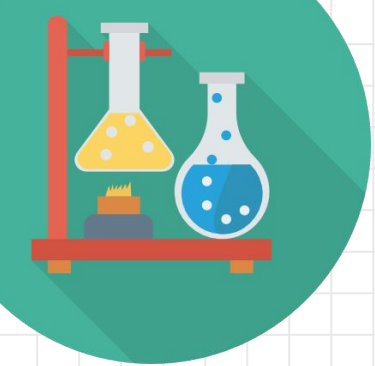
- Performance Monitoring
  Example:  To monitor the response time of a web server.

- Security Analysis
  Example:  Analyzing network traffic to uncover abnormal communication, connections to malicious IPs, or unexpected data transfers.

- Protocol Analysis
  Example:  Troubleshooting VoIP (Voice over IP) call quality issues.

- Forensic Analysis
  Example:  Analyzing packets over time to reconstruct events and pinpoint the compromise point.

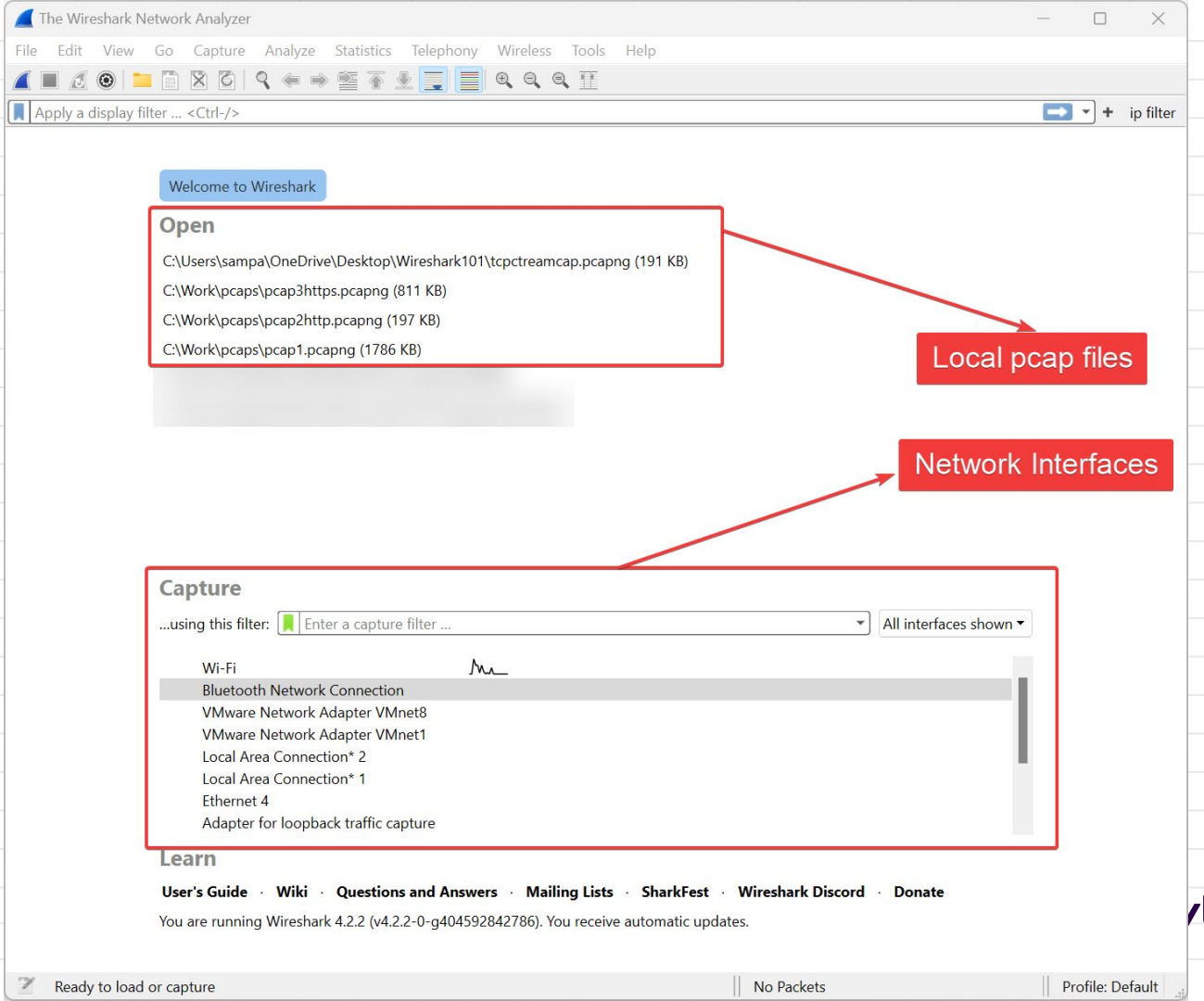
CyberForge ACADEMY

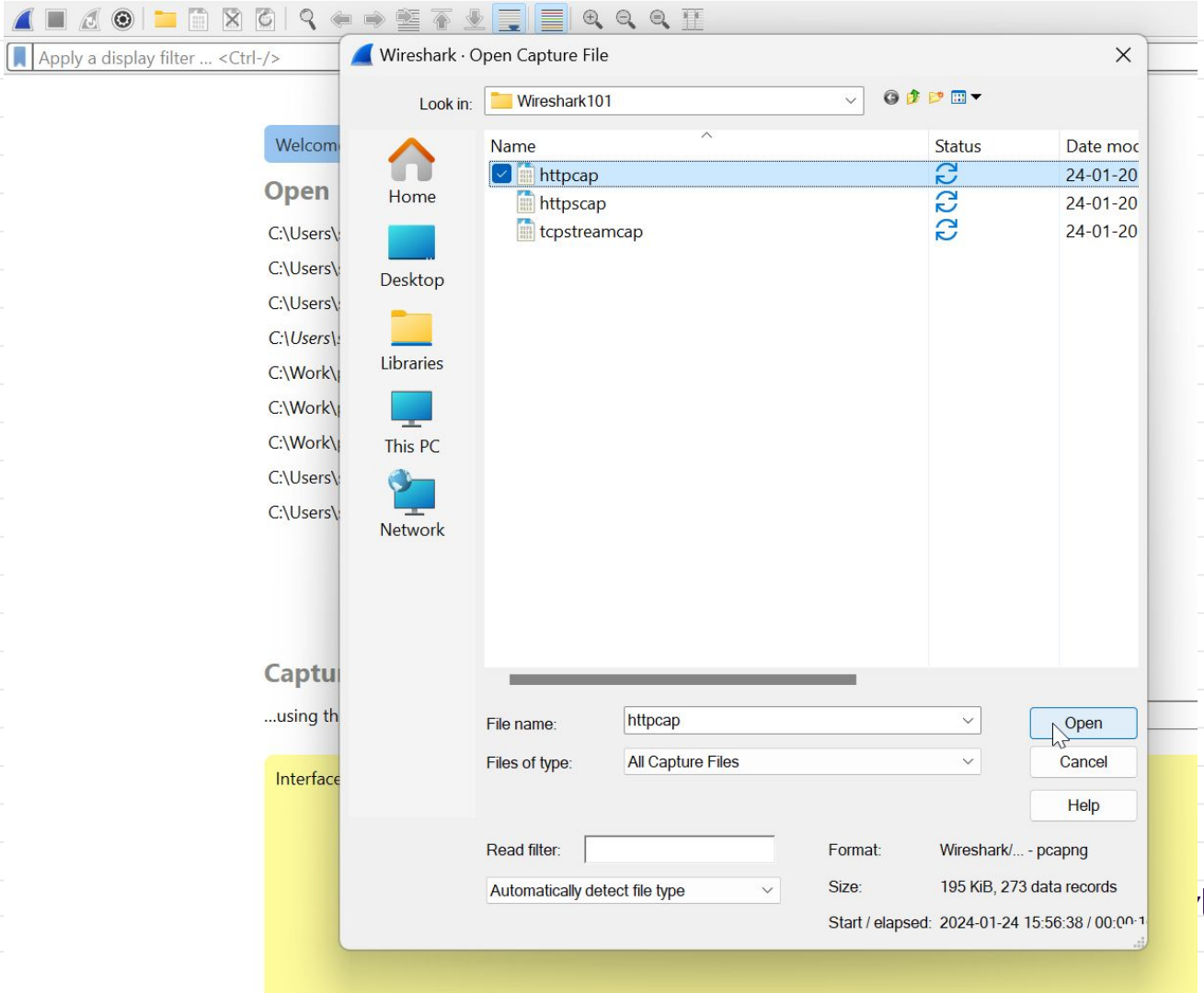


# Capturing HTTP Packet

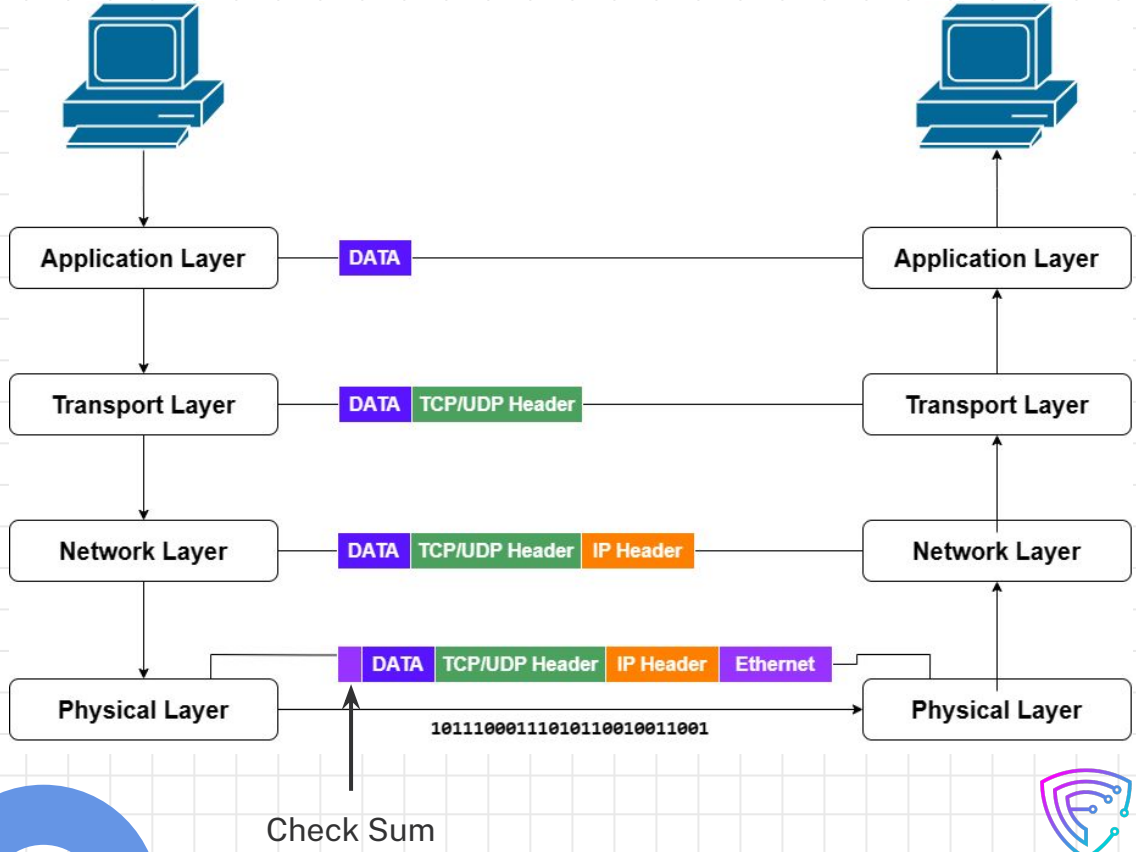
- Pcap: Workshops/Wireshark101-OWASP/pcaps/httpcap-CyberForgeAcademy
- Video: Capturing HTTP Traffic using Wireshark (youtube.com)

CyberForge ACADEMY


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
ip filter
Welcome to Wireshark
Open
C:\Users\sampa\OneDrive\Desktop\Wireshark101\tcpctreamcap.pcapng (191 KB)
C:\Work\pcaps\pcap3https.pcapng (811 KB)
C:\Work\pcaps\pcap2http.pcapng (197 KB)
C:\Work\pcaps\pcap1.pcapng (1786 KB)
Local pcap files
Network Interfaces
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wi-Fi
Bluetooth Network Connection
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 2
Local Area Connection* 1
Ethernet 4
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.2.2 (v4.2.2-0-g404592842786). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

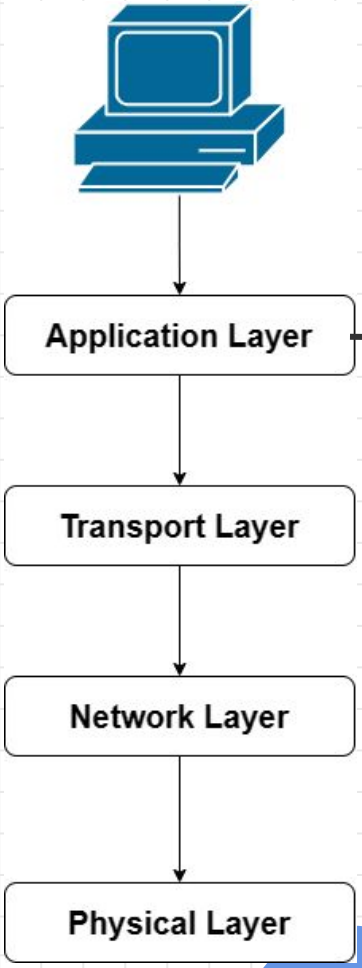

Apply a display filter ... <Ctrl-/>
Welcom
Open
C:\Users\
C:\Users\
C:\Users\
C:\Users\
C:\Work\
C:\Work\
C:\Work\
C:\Users\
C:\Users\
Captu
...using th
Interface
Wireshark · Open Capture File
Look in:
Wireshark101
Home
Desktop
Libraries
This PC
Network
Name
Status
Date mod
httpcap
24-01-20
httpscap
24-01-20
tcpstreamcap
24-01-20
File name:
httpcap
Files of type:
All Capture Files
Open
Cancel
Help
Read filter:
Automatically detect file type
Format:
Wireshark/... - pcapng
Size:
195 KiB, 273 data records
Start / elapsed:
2024-01-24 15:56:38 / 00:00:1

# TCP/IP Model



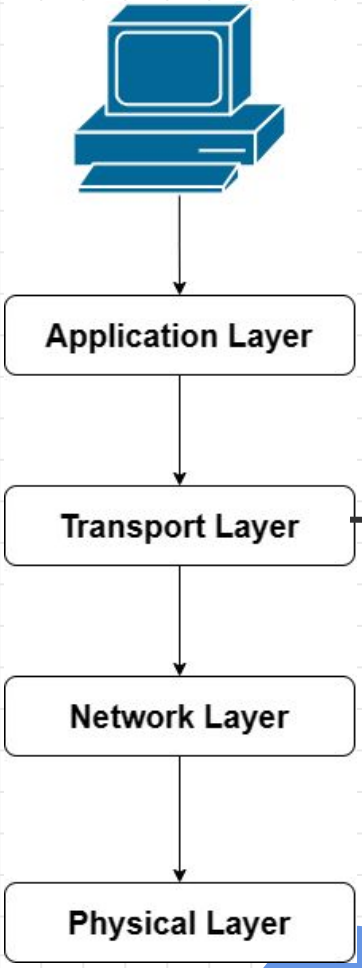

CyberForge ACADEMY

# HTTP Response Packet with 200 code and page content




```
Hypertext Transfer Protocol
  HTTP/1.0 200 OK\r\n
  Server: SimpleHTTP/0.6 Python/3.10.12\r\n
  Date: Wed, 24 Jan 2024 10:11:07 GMT\r\n
  Content-type: text/html\r\n
  Content-Length: 1654\r\n
  Last-Modified: Tue, 23 Jan 2024 19:46:49 GMT\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.009803000 seconds]
  [Request in frame: 8]
  [Request URI: http://192.168.56.103:8000/]
  File Data: 1654 bytes
Line-based text data: text/html (40 lines)
  <!DOCTYPE html>\n
  <html lang="en">\n
  <head>\n
      <meta charset="UTF-8">\n
      <meta http-equiv="X-UA-Compatible" content="IE=edge">\n
      <meta name="viewport" content="width=device-width, initial-scale=1.0">
      <style>\n
```

CyberForge ACADEMY




## TCP Source port 8000 and Destination port 57066

```
Transmission Control Protocol, Src Port: 8000, Dst Port: 57066, Seq: 1649, A
  Source Port: 8000
  Destination Port: 57066
  [Stream index: 0]
> [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 194]
  Sequence Number: 1649    (relative sequence number)
  Sequence Number (raw): 947992284
  [Next Sequence Number: 1844    (relative sequence number)]
  Acknowledgment Number: 435    (relative ack number)
  Acknowledgment number (raw): 4092790033
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x019 (FIN, PSH, ACK)
  Window: 501
  [Calculated window size: 64128]
  [Window size scaling factor: 128]
  Checksum: 0x33df [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
  TCP payload (194 bytes)
  TCP segment data (194 bytes)
```

CyberForge ACADEMY

Application Layer

Transport Layer

Network Layer

Physical Layer

## IPv4 Header, Source IP 192.168.56.103, Destination IP 192.168.56.1

```
Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 234
    Identification: 0x7546 (30022)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xd30e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.56.103
    Destination Address: 192.168.56.1
```

CyberForge ACADEMY

Application Layer

Transport Layer

Network Layer

Physical Layer

## MAC Header
## Source MAC 08:00:27:18:44:d8, Destination MAC 0a:00:27:00:00:11

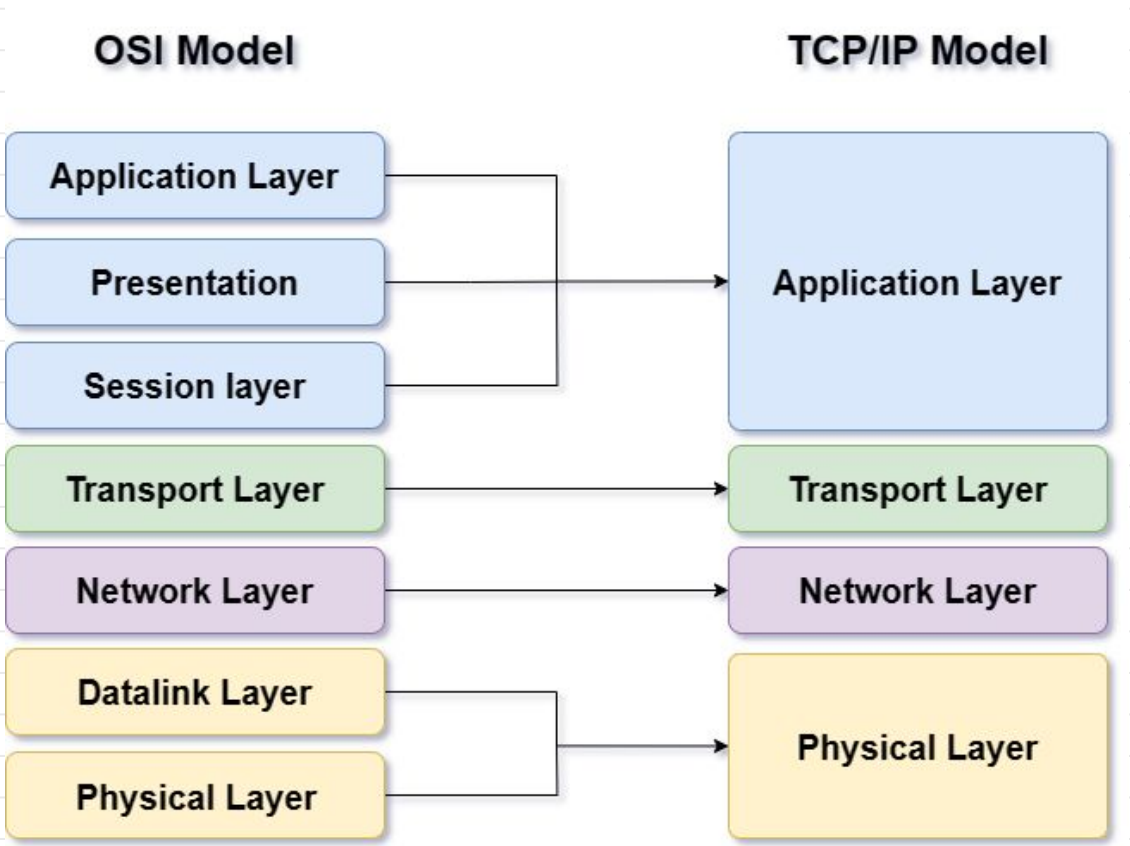
```
> Frame 13: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface \
v Ethernet II, Src: PCSSystemtec_18:44:d8 (08:00:27:18:44:d8), Dst: 0a:00:27:00:00:11 (0
  v Destination: 0a:00:27:00:00:11 (0a:00:27:00:00:11)
      Address: 0a:00:27:00:00:11 (0a:00:27:00:00:11)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: PCSSystemtec_18:44:d8 (08:00:27:18:44:d8)
      Address: PCSSystemtec_18:44:d8 (08:00:27:18:44:d8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.1
> Transmission Control Protocol, Src Port: 8000, Dst Port: 57066, Seq: 1649, Ack: 435, L
> [3 Reassembled TCP Segments (1842 bytes): #10(188), #11(1460), #13(194)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (40 lines)
```

PCAP: Workshops/Wireshark101-OWASP/pcaps/httpcap-CyberForgeAcademy

CyberForge ACADEMY

# Quiz

| | |
|---|---|
| **Can we show the OSI model in Wireshark ?** | a) YES, we can !! |
| | b) NO!!!!! |
| | c) Don’t Know :( |




CyberForge ACADEMY

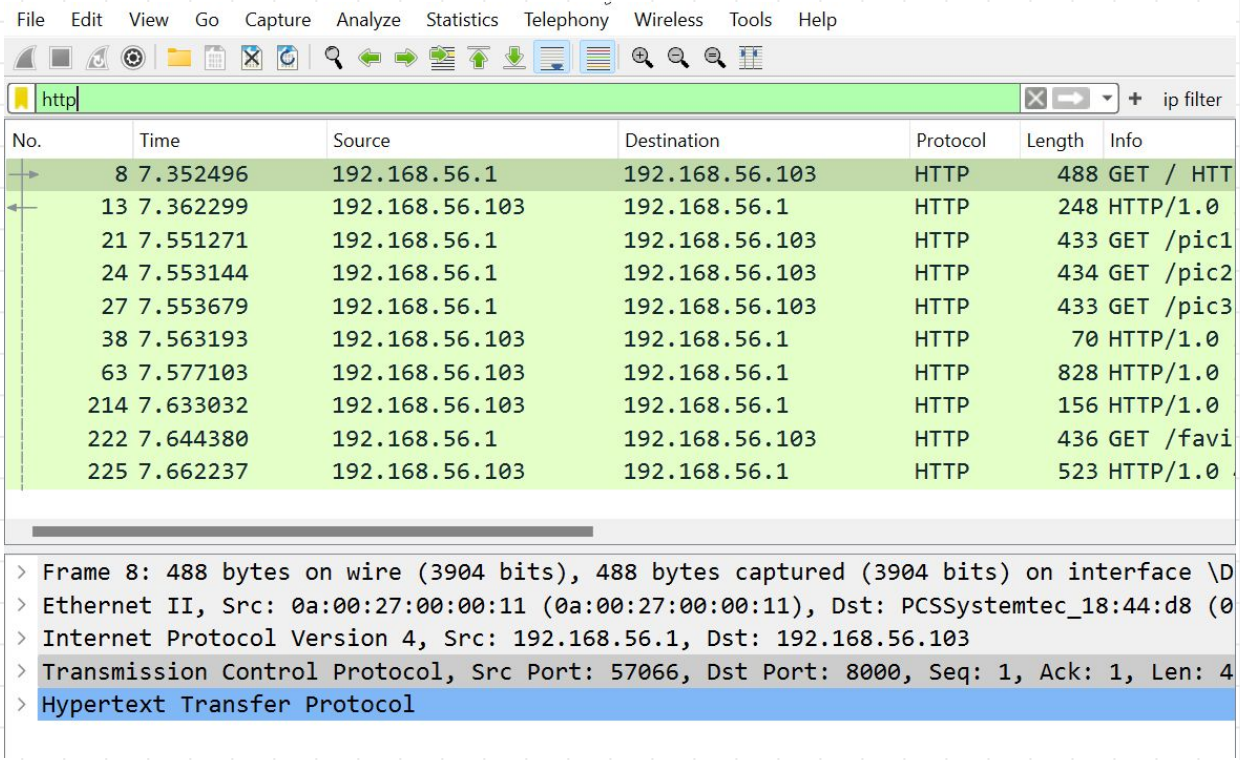
# Wireshark Filters

- Criteria applied to captured packet data for targeting specific network traffic.

- Purpose:
  - Efficient analysis
  - Noise reduction
  - Troubleshooting

- Types of Filters:
  - Display Filters
  - Capture Filters

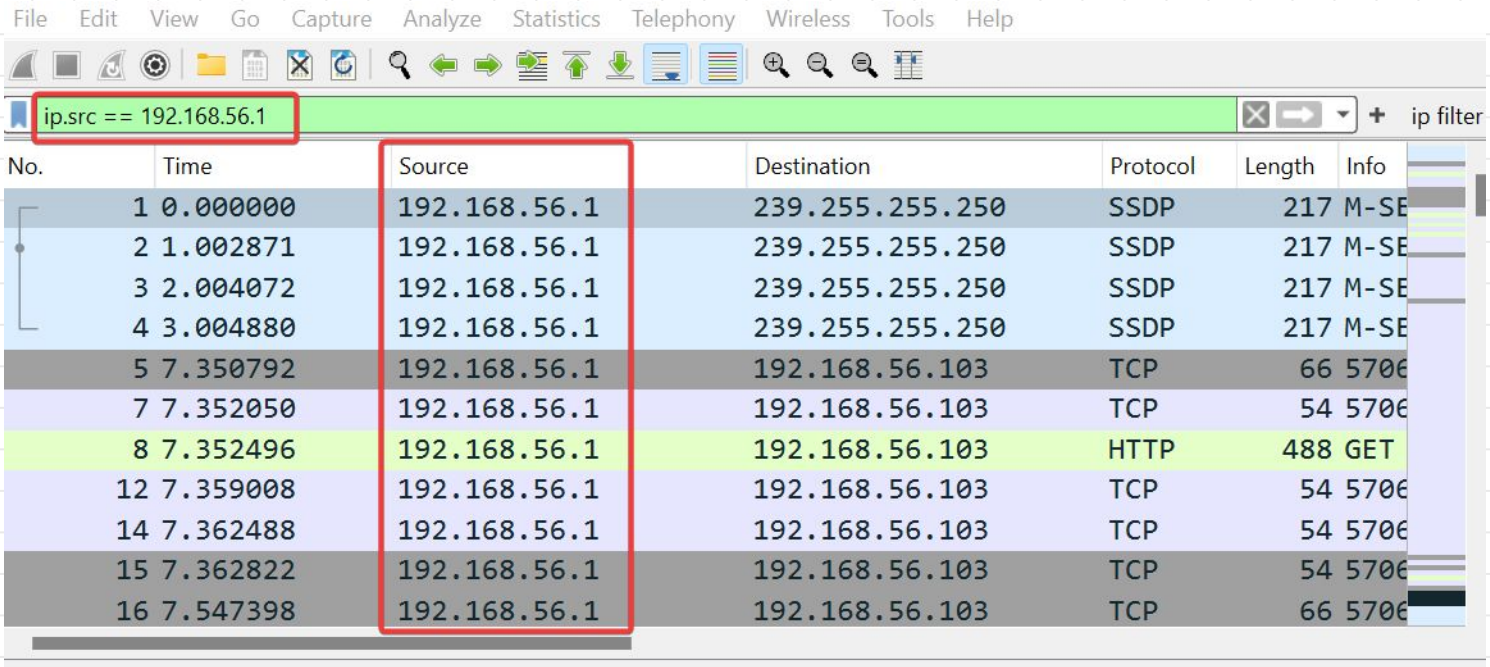
# 1. Protocol Based Filter




Filtered for http traffic

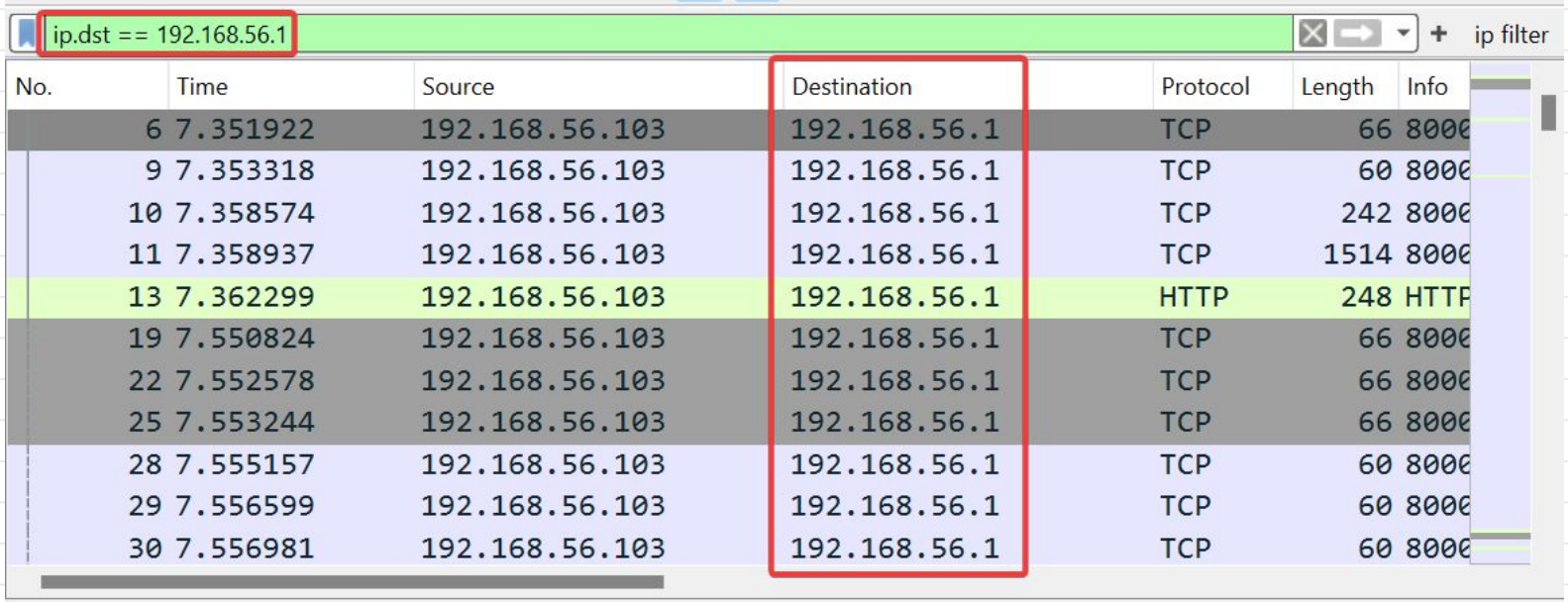
CyberForge ACADEMY

## 2. Filter by IP Address




Filtered for source IP: 192.168.56.1

CyberForge ACADEMY




| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 6 | 7.351922 | 192.168.56.103 | 192.168.56.1 | TCP | 66 | 8000 |
| 9 | 7.353318 | 192.168.56.103 | 192.168.56.1 | TCP | 60 | 8000 |
| 10 | 7.358574 | 192.168.56.103 | 192.168.56.1 | TCP | 242 | 8000 |
| 11 | 7.358937 | 192.168.56.103 | 192.168.56.1 | TCP | 1514 | 8000 |
| 13 | 7.362299 | 192.168.56.103 | 192.168.56.1 | HTTP | 248 | HTTP |
| 19 | 7.550824 | 192.168.56.103 | 192.168.56.1 | TCP | 66 | 8000 |
| 22 | 7.552578 | 192.168.56.103 | 192.168.56.1 | TCP | 66 | 8000 |
| 25 | 7.553244 | 192.168.56.103 | 192.168.56.1 | TCP | 66 | 8000 |
| 28 | 7.555157 | 192.168.56.103 | 192.168.56.1 | TCP | 60 | 8000 |
| 29 | 7.556599 | 192.168.56.103 | 192.168.56.1 | TCP | 60 | 8000 |
| 30 | 7.556981 | 192.168.56.103 | 192.168.56.1 | TCP | 60 | 8000 |

Filtered for Destination IP: 192.168.56.1

CyberForge ACADEMY

ip.addr == 192.168.56.1

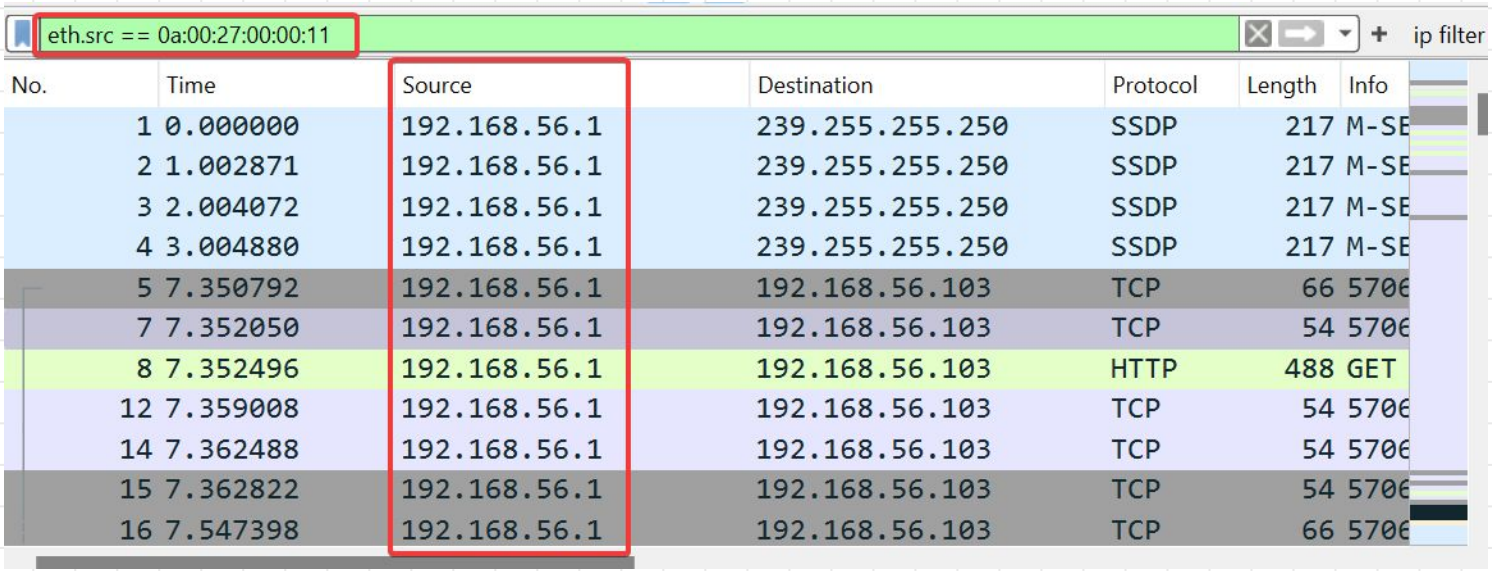
ip filter

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.56.1 | 239.255.255.250 | SSDP | 217 | M-SE |
| 2 | 1.002871 | 192.168.56.1 | 239.255.255.250 | SSDP | 217 | M-SE |
| 3 | 2.004072 | 192.168.56.1 | 239.255.255.250 | SSDP | 217 | M-SE |
| 4 | 3.004880 | 192.168.56.1 | 239.255.255.250 | SSDP | 217 | M-SE |
| 5 | 7.350792 | 192.168.56.1 | 192.168.56.103 | TCP | 66 | 5706 |
| 6 | 7.351922 | 192.168.56.103 | 192.168.56.1 | TCP | 66 | 8000 |
| 7 | 7.352050 | 192.168.56.1 | 192.168.56.103 | TCP | 54 | 5706 |
| 8 | 7.352496 | 192.168.56.1 | 192.168.56.103 | HTTP | 488 | GET |
| 9 | 7.353318 | 192.168.56.103 | 192.168.56.1 | TCP | 60 | 8000 |
| 10 | 7.358574 | 192.168.56.103 | 192.168.56.1 | TCP | 242 | 8000 |
| 11 | 7.358937 | 192.168.56.103 | 192.168.56.1 | TCP | 1514 | 8000 |

Filtered for both source and destination IP: 192.168.56.1

CyberForge ACADEMY

## 3. Filter by MAC Address

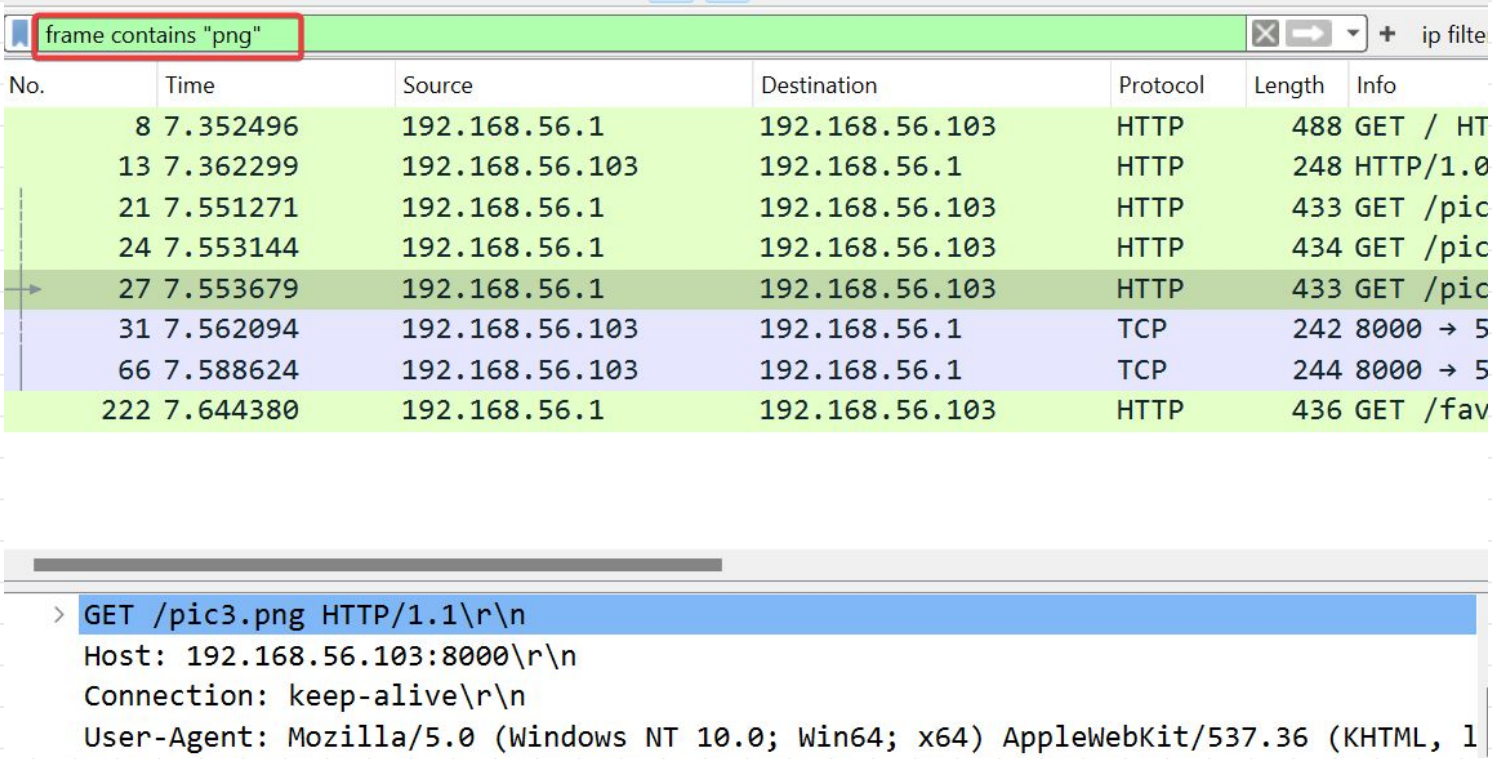



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.56.1 | 239.255.255.250 | SSDP | 217 | M-SE |
| 2 | 1.002871 | 192.168.56.1 | 239.255.255.250 | SSDP | 217 | M-SE |
| 3 | 2.004072 | 192.168.56.1 | 239.255.255.250 | SSDP | 217 | M-SE |
| 4 | 3.004880 | 192.168.56.1 | 239.255.255.250 | SSDP | 217 | M-SE |
| 5 | 7.350792 | 192.168.56.1 | 192.168.56.103 | TCP | 66 | 5706 |
| 7 | 7.352050 | 192.168.56.1 | 192.168.56.103 | TCP | 54 | 5706 |
| 8 | 7.352496 | 192.168.56.1 | 192.168.56.103 | HTTP | 488 | GET |
| 12 | 7.359008 | 192.168.56.1 | 192.168.56.103 | TCP | 54 | 5706 |
| 14 | 7.362488 | 192.168.56.1 | 192.168.56.103 | TCP | 54 | 5706 |
| 15 | 7.362822 | 192.168.56.1 | 192.168.56.103 | TCP | 54 | 5706 |
| 16 | 7.547398 | 192.168.56.1 | 192.168.56.103 | TCP | 66 | 5706 |

Filtered for source MAC: 0a:00:27:00:11

CyberForge ACADEMY

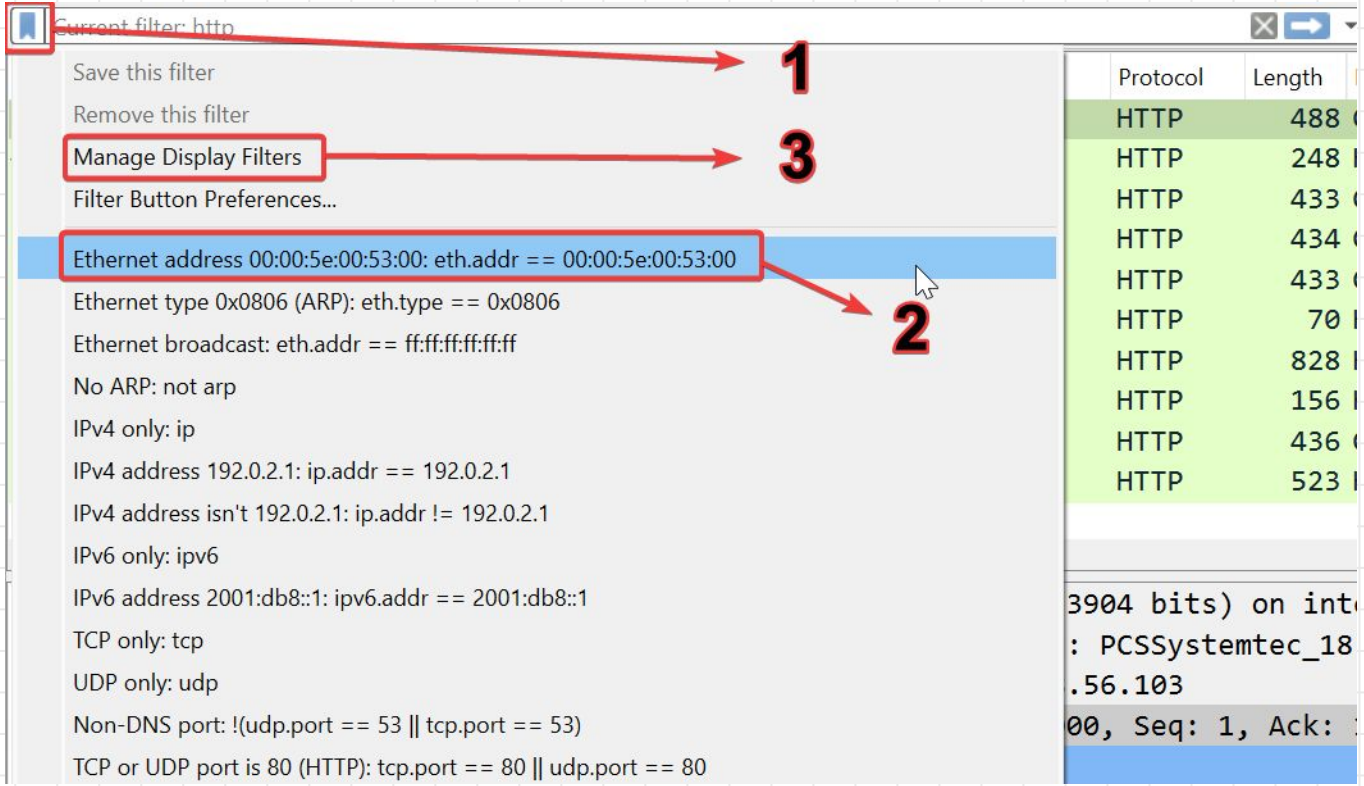
## 4. Filter by Frame content




Filtered bye frame content: “png”

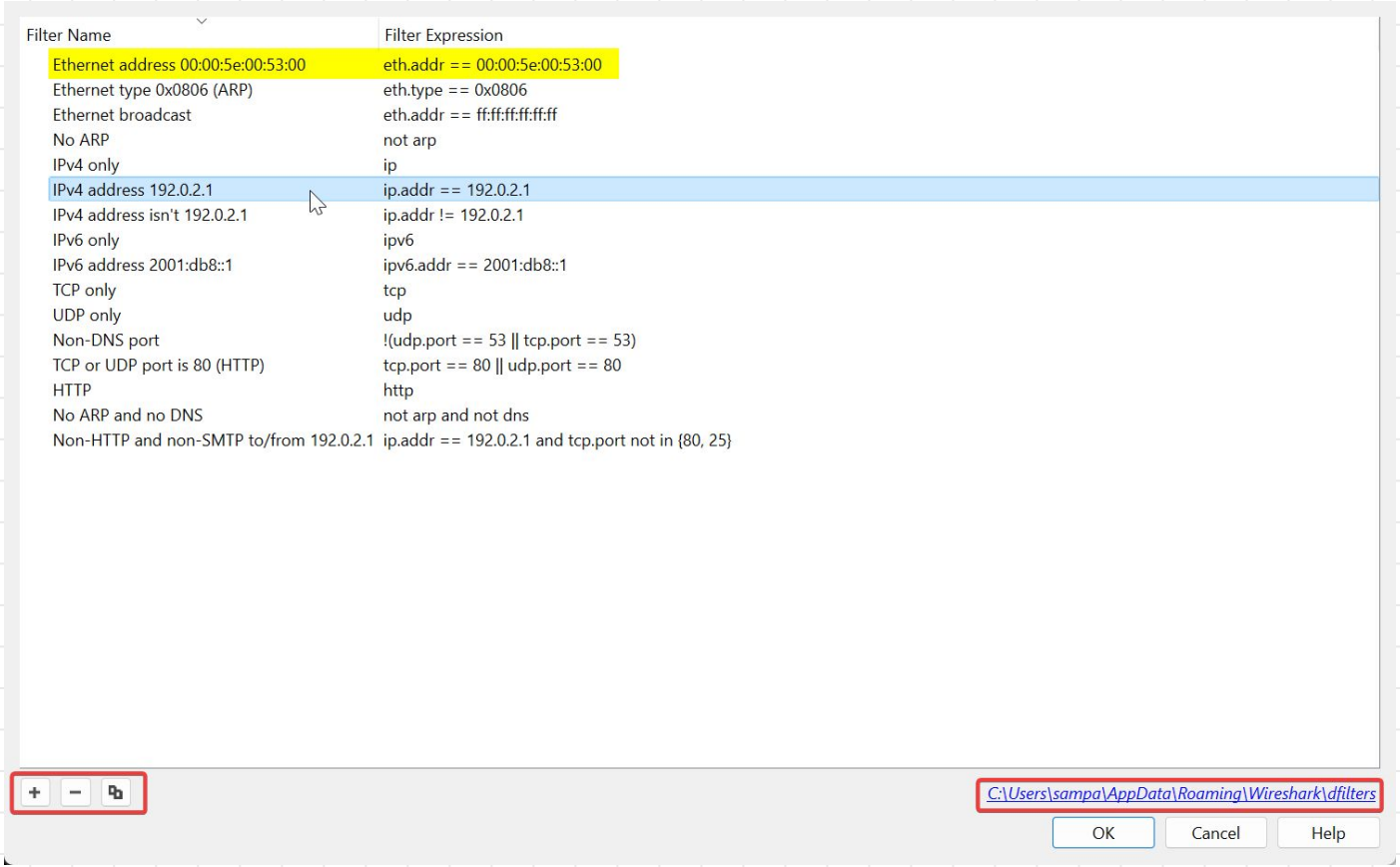
CyberForge ACADEMY

## 5. Saving Filters by custom names



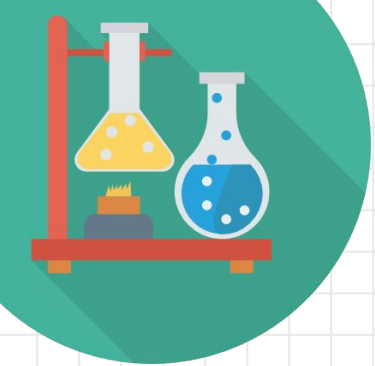

1. Open saved filters 2. Select from saved 3. Add custom name

CyberForge ACADEMY




Menu to add custom names

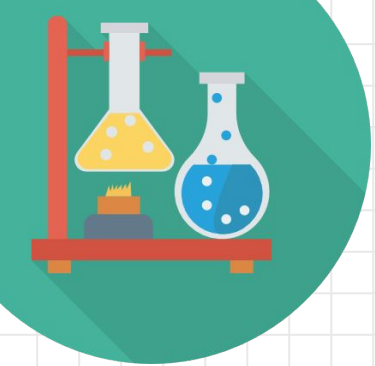
CyberForge ACADEMY



# TCP Stream Reconstruction

- Pcap: Workshops/Wireshark101-OWASP/pcaps/tcpstreampcap-CyberForge Academy
- Video: Reconstructing TCP Stream (youtube.com)

CyberForge ACADEMY

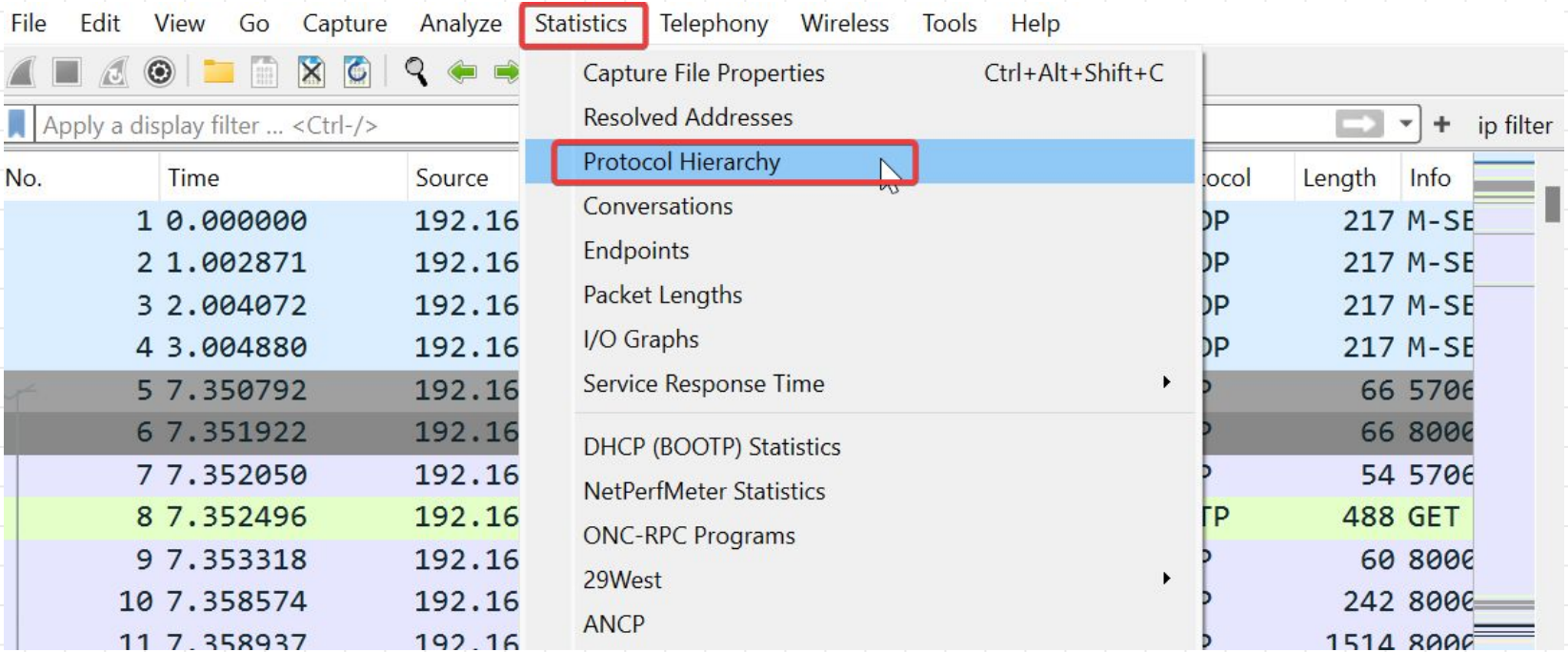


# Extracting Resources from Traffic

- Pcap: Workshops/Wireshark101 - OWASP/pcaps/objectcapture - CyberForgeAcademy
- Video: Exporting Objects from HTTP Traffic (youtube.com)

CyberForge ACADEMY

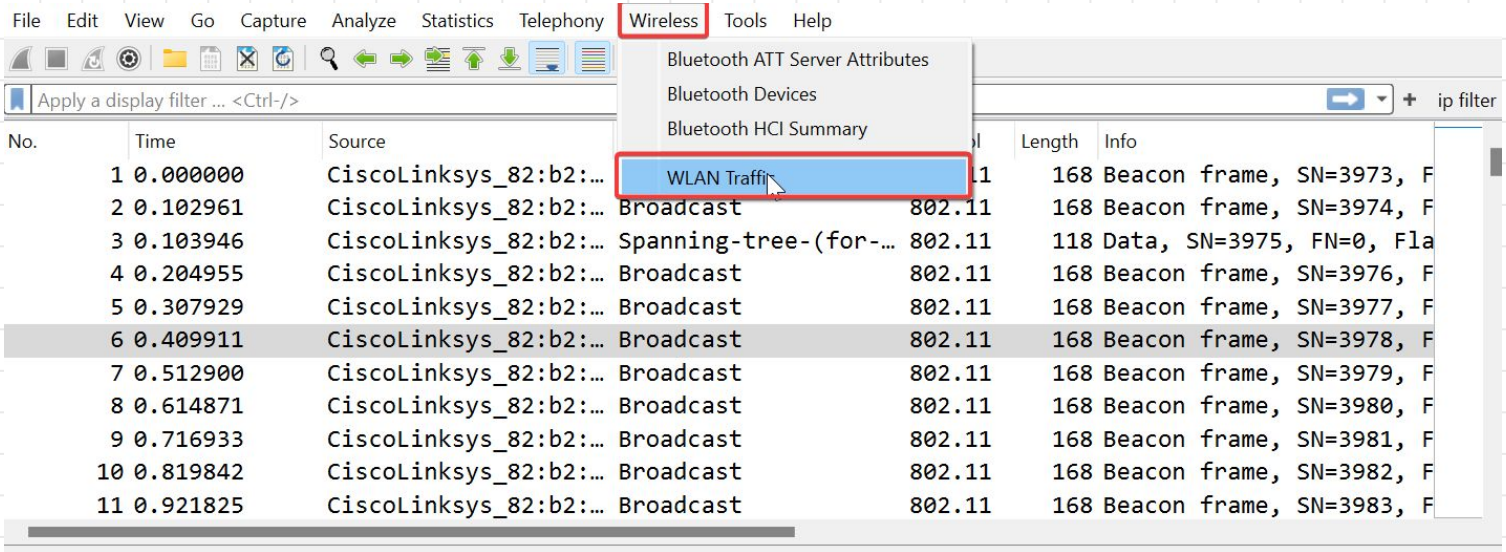
## **Hack 1:** Using Protocol Hierarchy




CyberForge ACADEMY

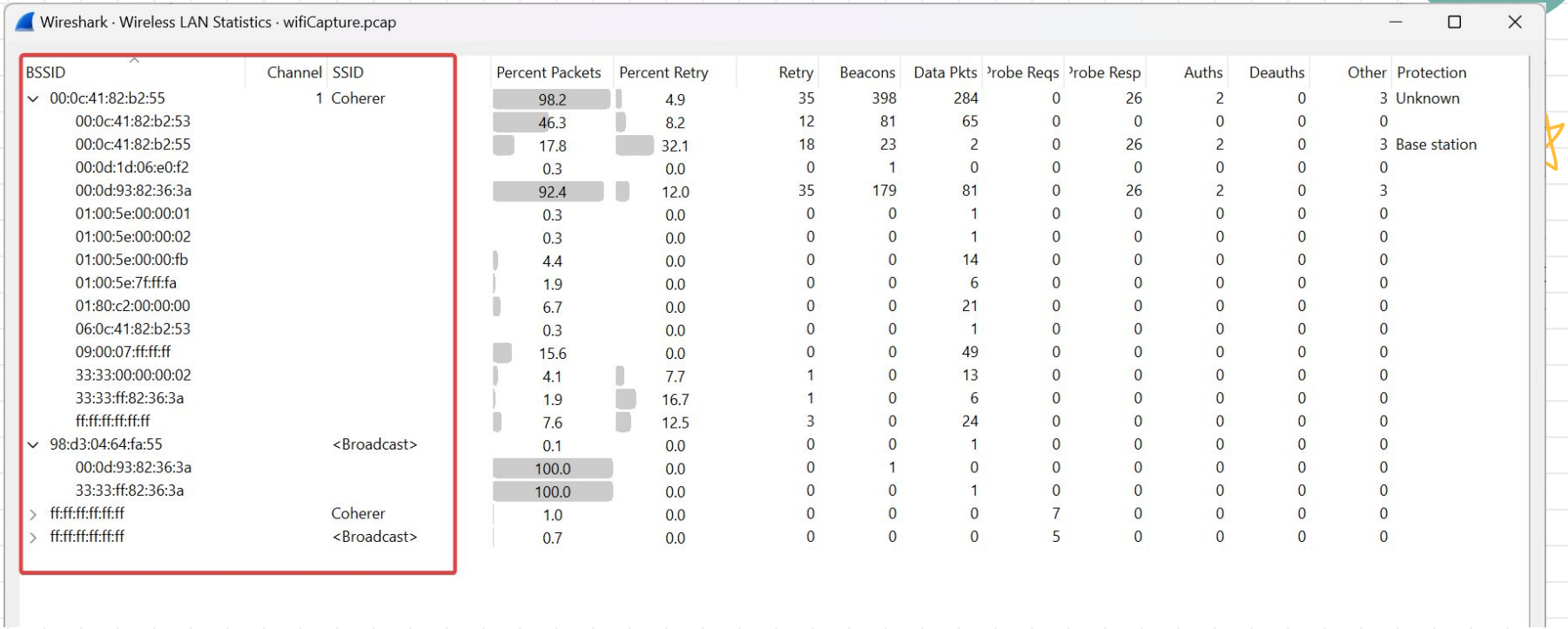
| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s | PDUs |
|---|---|---|---|---|---|---|---|---|---|
| Frame | 100.0 | 244 | 100.0 | 190245 | 21 k | 0 | 0 | 0 | 244 |
| Ethernet | 100.0 | 244 | 1.8 | 3494 | 388 | 0 | 0 | 0 | 244 |
| Internet Protocol Version 4 | 99.2 | 242 | 2.5 | 4840 | 538 | 0 | 0 | 0 | 242 |
| User Datagram Protocol | 4.9 | 12 | 0.1 | 96 | 10 | 0 | 0 | 0 | 12 |
| Simple Service Discovery Protocol | 4.9 | 12 | 1.1 | 2096 | 233 | 12 | 2096 | 233 | 12 |
| Transmission Control Protocol | 94.3 | 230 | 94.4 | 179663 | 19 k | 220 | 175954 | 19 k | 230 |
| Hypertext Transfer Protocol | 4.1 | 10 | 92.0 | 174943 | 19 k | 5 | 1954 | 217 | 10 |
| Portable Network Graphics | 0.8 | 2 | 78.2 | 148710 | 16 k | 2 | 148710 | 16 k | 2 |
| Line-based text data | 0.8 | 2 | 1.1 | 2123 | 236 | 2 | 2123 | 236 | 2 |
| JPEG File Interchange Format | 0.4 | 1 | 11.2 | 21214 | 2359 | 1 | 21214 | 2359 | 1 |
| Address Resolution Protocol | 0.8 | 2 | 0.0 | 74 | 8 | 2 | 74 | 8 | 2 |

## **Hack 2:** Checking nearby devices over Wifi network




PCAP: Workshops/Wireshark101-OWASP/pcaps/wifiCapture.pcap CyberForgeAcademy

CyberForge ACADEMY

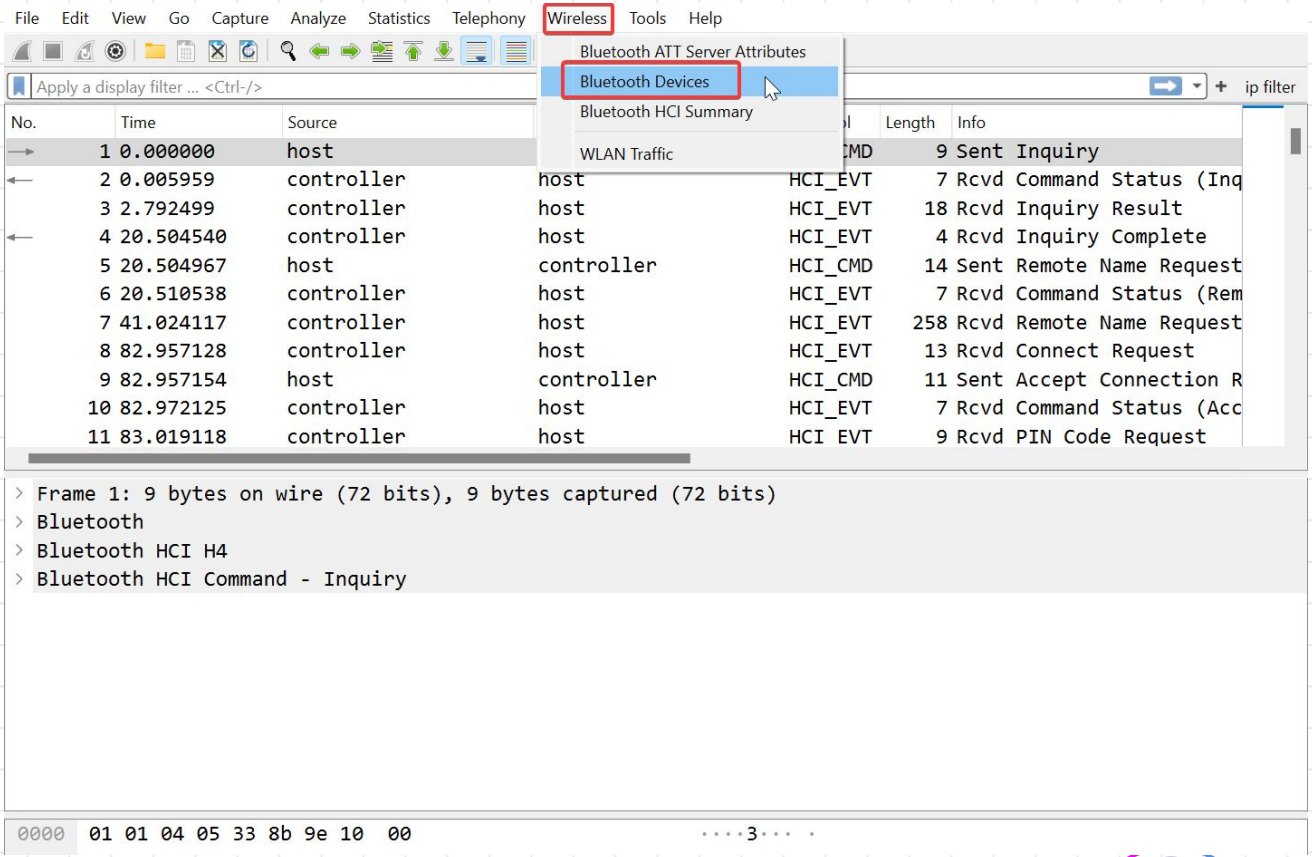



| BSSID | Channel | SSID | Percent Packets | Percent Retry | Retry | Beacons | Data Pkts | Probe Reqs | Probe Resp | Auths | Deauths | Other | Protection |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00:0c:41:82:b2:55 | 1 | Coherer | 98.2 | 4.9 | 35 | 398 | 284 | 0 | 26 | 2 | 0 | 3 | Unknown |
| 00:0c:41:82:b2:53 | | | 46.3 | 8.2 | 12 | 81 | 65 | 0 | 0 | 0 | 0 | 0 | |
| 00:0c:41:82:b2:55 | | | 17.8 | 32.1 | 18 | 23 | 2 | 0 | 26 | 2 | 0 | 3 | Base station |
| 00:0d:1d:06:e0:f2 | | | 0.3 | 0.0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 00:0d:93:82:36:3a | | | 92.4 | 12.0 | 35 | 179 | 81 | 0 | 26 | 2 | 0 | 3 | |
| 01:00:5e:00:00:01 | | | 0.3 | 0.0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | |
| 01:00:5e:00:00:02 | | | 0.3 | 0.0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | |
| 01:00:5e:00:00:fb | | | 4.4 | 0.0 | 0 | 0 | 14 | 0 | 0 | 0 | 0 | 0 | |
| 01:00:5e:7f:ff:fa | | | 1.9 | 0.0 | 0 | 0 | 6 | 0 | 0 | 0 | 0 | 0 | |
| 01:80:c2:00:00:00 | | | 6.7 | 0.0 | 0 | 0 | 21 | 0 | 0 | 0 | 0 | 0 | |
| 06:0c:41:82:b2:53 | | | 0.3 | 0.0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | |
| 09:00:07:ff:ff:ff | | | 15.6 | 0.0 | 0 | 0 | 49 | 0 | 0 | 0 | 0 | 0 | |
| 33:33:00:00:00:02 | | | 4.1 | 7.7 | 1 | 0 | 13 | 0 | 0 | 0 | 0 | 0 | |
| 33:33:ff:82:36:3a | | | 1.9 | 16.7 | 1 | 0 | 6 | 0 | 0 | 0 | 0 | 0 | |
| ff:ff:ff:ff:ff:ff | | | 7.6 | 12.5 | 3 | 0 | 24 | 0 | 0 | 0 | 0 | 0 | |
| 98:d3:04:64:fa:55 | | <Broadcast> | 0.1 | 0.0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | |
| 00:0d:93:82:36:3a | | | 100.0 | 0.0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 33:33:ff:82:36:3a | | | 100.0 | 0.0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | |
| ff:ff:ff:ff:ff:ff | | Coherer | 1.0 | 0.0 | 0 | 0 | 0 | 7 | 0 | 0 | 0 | 0 | |
| ff:ff:ff:ff:ff:ff | | <Broadcast> | 0.7 | 0.0 | 0 | 0 | 0 | 5 | 0 | 0 | 0 | 0 | |

List of all the nearby devices that are connected to Wifi pcap:

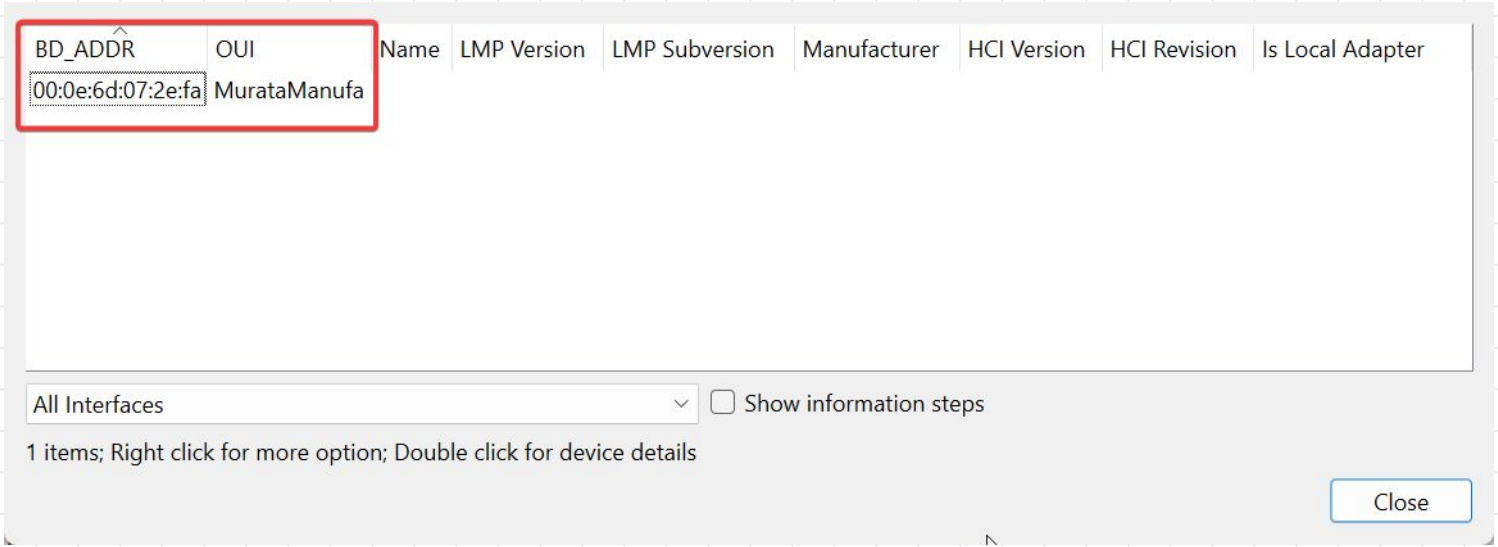
CyberForge ACADEMY

# **Hack 3:** Check bluetooth connected devices




PCAP: Workshops/Wireshark101-OWASP/pcaps/BluetoothCapture.cap CyberForgeAcademy

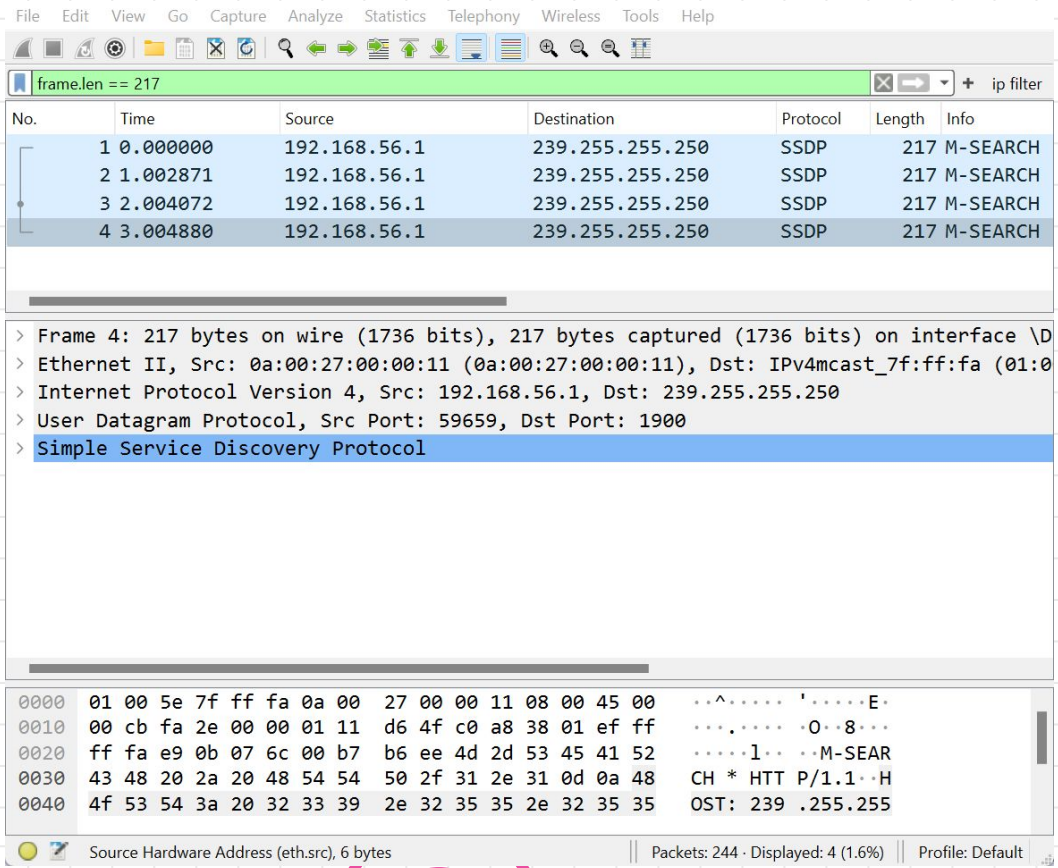
CyberForge ACADEMY




Bluetooth address of the connected user

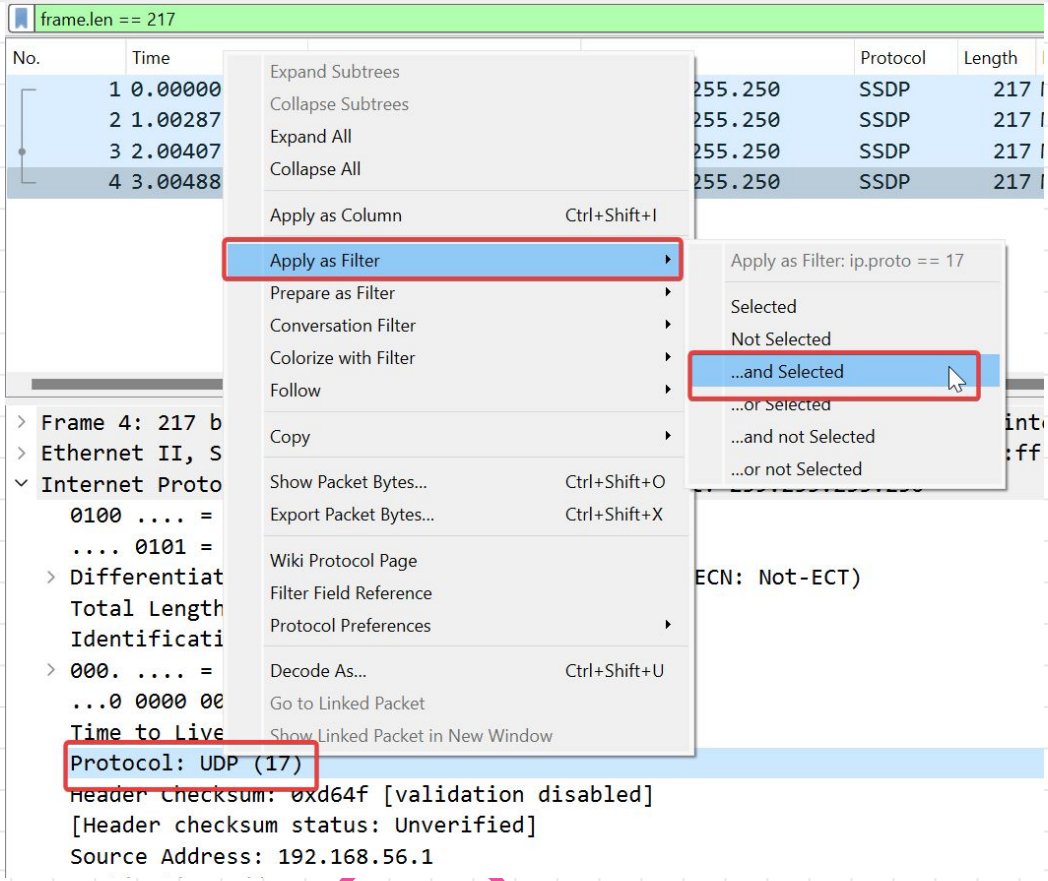
CyberForge ACADEMY

# **Hack 4:** Type Less & Drag More

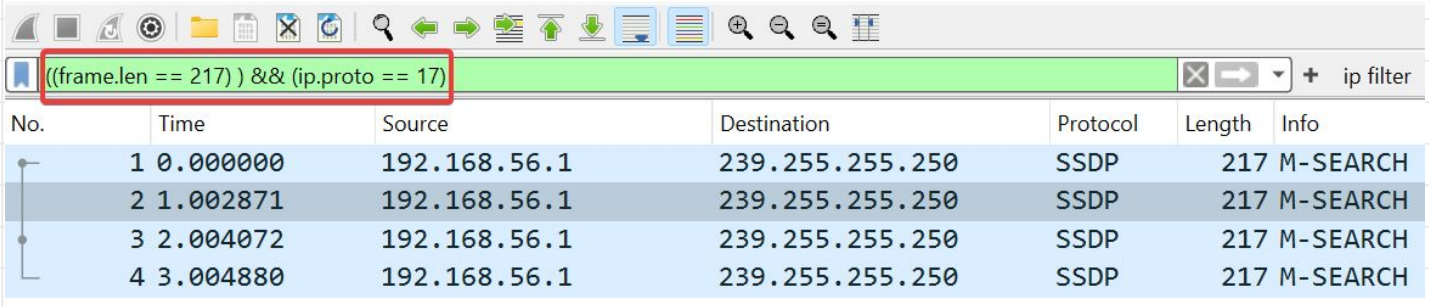



CyberForge ACADEMY

# **Hack 5:** Combine Filters




CyberForge ACADEMY




Combined frame length and protocol filters by AND operation

CyberForge ACADEMY

# But, What on CLI?

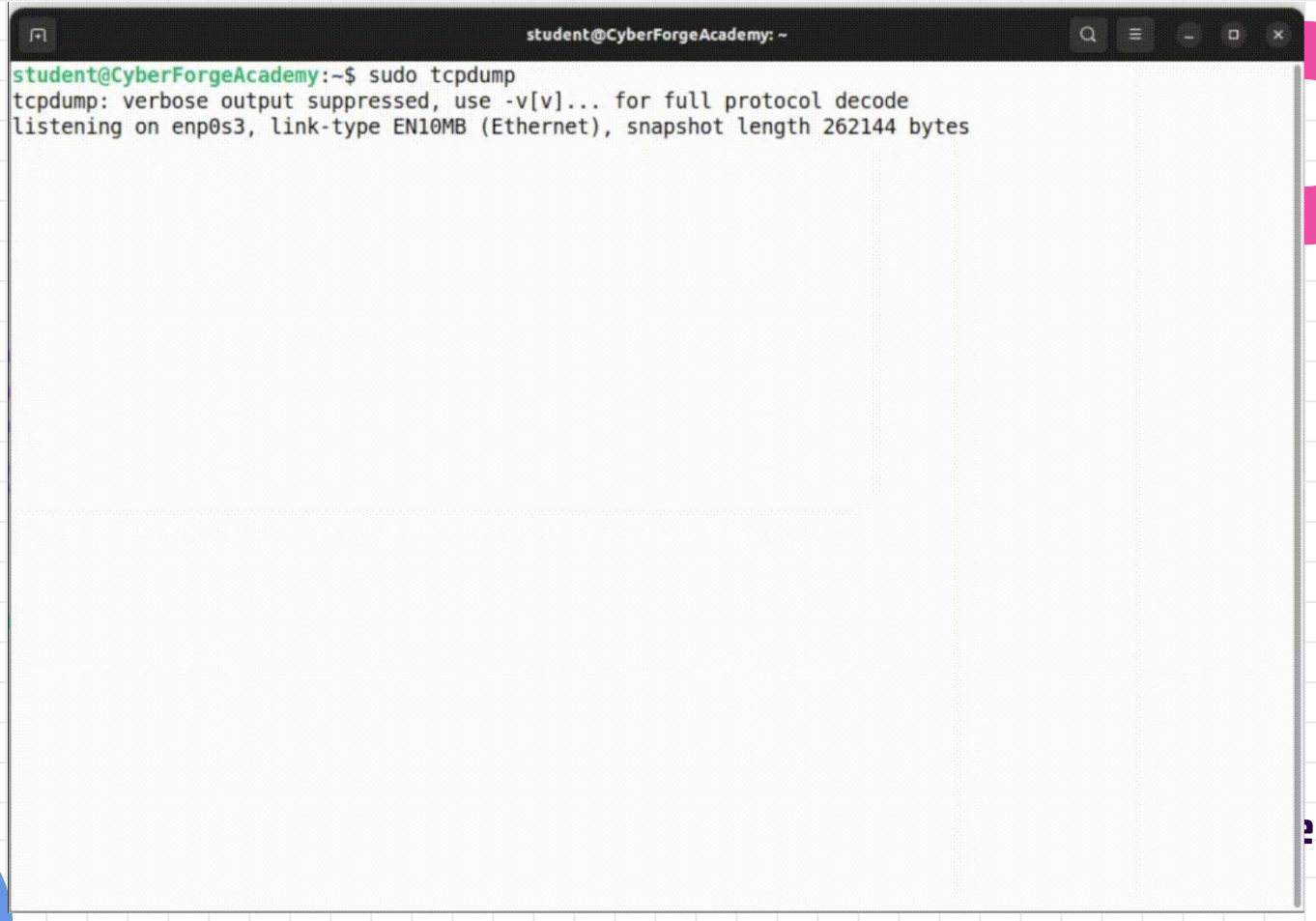
**Tshark** (https://tshark.dev)

Documentation:
https://www.wireshark.org/docs/wsug_html_chunked/AppToolstshark.html

# But, Can we do better?

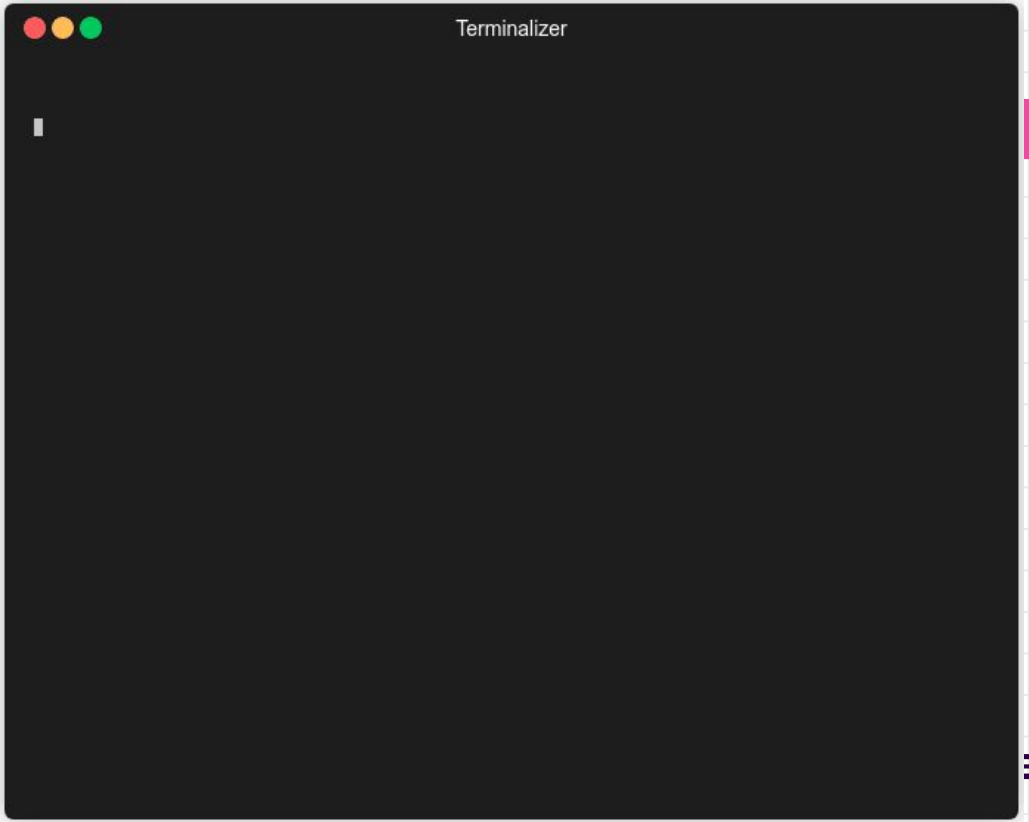
## Tcpdump

(https://www.tcpdump.org/)



# Ok, but I want it like GUI :)

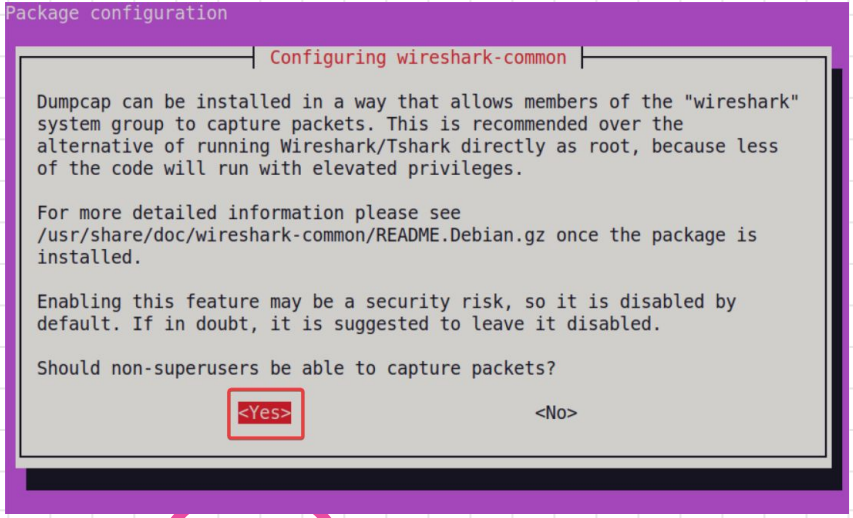
**Termshark** (https://github.com/gcla/termshark)



# Install Wireshark on Linux

**Step 1:** Update device packages
**Command:** sudo apt-get update

**Step 2:** Download and install wireshark
**Command:** sudo apt install wireshark




CyberForge ACADEMY

# Install Wireshark on Linux

**Step 4:** Add your current user to the wireshark group
**Command:** sudo adduser $USER wireshark

**Step 5:** Restart system to start using Wireshark.

CyberForge ACADEMY

# Thanks!

## Do you have any questions?

contact@cyberforge.academy
+91 837537763
https://cyberforge.academy
https://github.com/CyberForgeAcademy/Workshops