



## Academic Year: 2022-2023

### Filters in Wireshark

#### 1. Ip:

##### a. Src

The screenshot shows the Wireshark interface with the filter bar set to `ip.src`. The packet list on the left shows various network protocols, including ICMP, TCP, and UDP. The packet details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane at the bottom shows the raw data of the selected packet.

##### b. Dst

The screenshot shows the Wireshark interface with the filter bar set to `ip.dst`. The packet list on the left shows various network protocols, including ICMP, TCP, and UDP. The packet details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane at the bottom shows the raw data of the selected packet.



**SHRI VILEPARLE KELAVANI MANDAL'S  
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**  
(Autonomous College Affiliated to the University of Mumbai)  
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)



**Academic Year: 2022-2023**

**c. Addr**

Wireshark packet capture showing a list of network traffic. The list includes various protocols like HTTP, DNS, and SMTP. The packet details pane on the right shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

**2. Tcp:**

**a. Tcp**

Wireshark packet capture showing a list of network traffic. The list includes various protocols like HTTP, DNS, and SMTP. The packet details pane on the right shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.





**SHRI VILEPARLE KELAVANI MANDAL'S  
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**  
(Autonomous College Affiliated to the University of Mumbai)  
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)



**b. Port**

Wireshark packet capture for port 80. The packet list shows a series of HTTP requests and responses. The packet details pane shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

**c. Ack**

Wireshark packet capture for ACK. The packet list shows a series of ACK packets. The packet details pane shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.



**Capturing from Wi-Fi**

File Edit View Go Capture Analysis Statistics Telephony Windows Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
25199	20.835537	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22161456 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25200	20.835556	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22161516 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25201	20.835572	34.184.35.123	36.128.112.125	TCP	94	57680 → 80 [ACK] Seq=22164376 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25202	20.835589	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22164376 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25203	20.835603	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22155836 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25204	20.835615	34.184.35.123	36.128.112.125	TCP	94	57680 → 80 [ACK] Seq=221617296 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25205	20.835630	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22167396 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25206	20.835643	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22167396 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25207	20.835656	34.184.35.123	36.128.112.125	TCP	94	57680 → 80 [ACK] Seq=221702016 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25208	20.835668	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22170316 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25209	20.835680	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22170316 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25210	20.835698	34.184.35.123	36.128.112.125	TCP	94	57680 → 80 [ACK] Seq=221731316 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25211	20.835908	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=221731316 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25212	20.835721	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22174096 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25213	20.835734	34.184.35.123	36.128.112.125	TCP	94	57680 → 80 [ACK] Seq=22175096 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25214	20.835749	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22175096 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25215	20.835759	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22177516 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25216	20.835782	34.184.35.123	36.128.112.125	TCP	94	57680 → 80 [ACK] Seq=22177976 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25217	20.835795	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22178076 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25218	20.835825	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22180436 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25219	20.835842	34.184.35.123	36.128.112.125	TCP	94	57680 → 80 [ACK] Seq=22181896 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25220	20.835857	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22181896 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25221	20.835876	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22183356 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25222	20.835893	34.184.35.123	36.128.112.125	TCP	94	57680 → 80 [ACK] Seq=22184816 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25223	20.835907	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22184816 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]
25224	20.835924	34.184.35.123	36.128.112.125	TCP	1514	80 → 57680 [ACK] Seq=22186276 Ack=7715 Win=718 Len=0 [TCP segment of a reassembled PDU]

Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface Wi-Fi\#{41FC362-8057-48B1-AA2E-58BFD200C1A4}

Ethernet II, Src: Intel(R) Wi-Fi 6E AX210 (8C:8E:62:8E:58:B0), Dst: Intel(R) Wi-Fi 6E AX210 (8C:8E:62:8E:58:B0)

Internet Protocol Version 4, Src: 34.184.35.123, Port: 80, Dst: 36.128.112.125, Port: 57680

User Datagram Protocol, Src Port: 57573, Dst Port: 1900

[Sample Source Discovery Protocol](#)

```


```

[illegible]





**SHRI VILEPARLE KELAVANI MANDAL'S  
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**  
(Autonomous College Affiliated to the University of Mumbai)  
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)



#### 4. Udp:

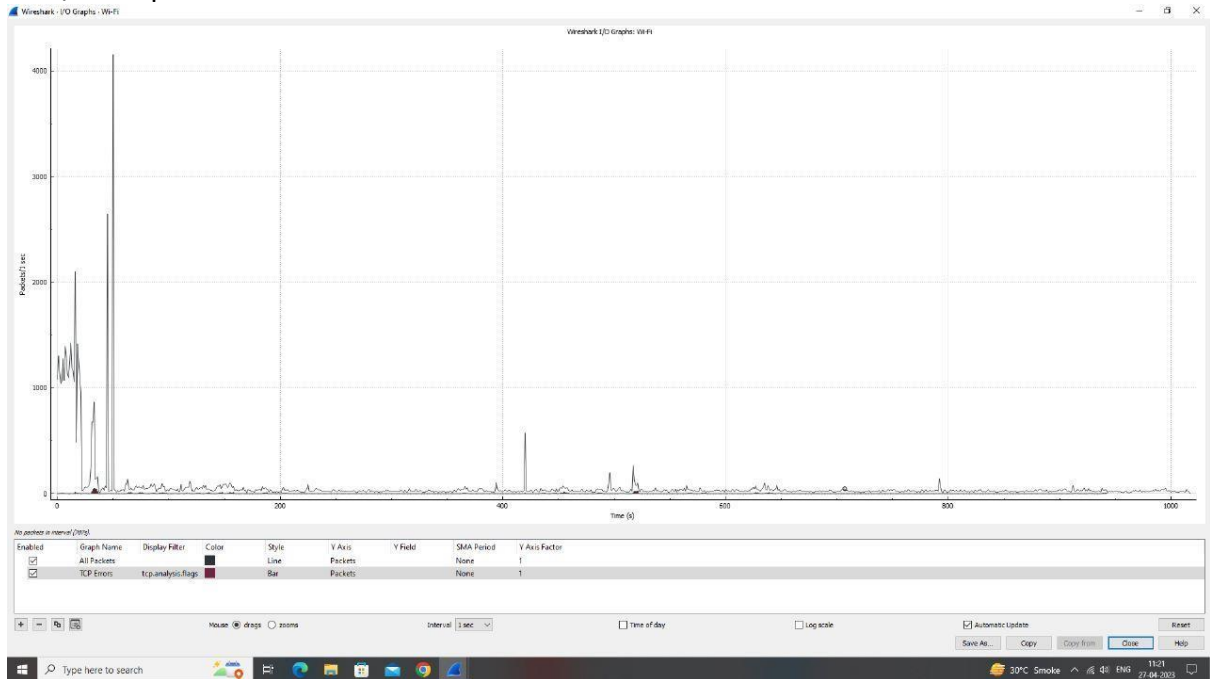
Wireshark packet capture for UDP traffic. The packet list shows multiple UDP packets from 10.126.112.15 to 125.10004. The packet details pane shows the structure of a UDP packet, including Ethernet II, Internet Protocol Version 4, and Data (43 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

#### 5. Http:

Wireshark packet capture for HTTP traffic. The packet list shows multiple HTTP packets from 10.126.112.225 to 34.104.35.123. The packet details pane shows the structure of an HTTP packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.



## 6. I/O Graph:



**Conclusion:** Thus, we have simulated Packet Capturing in Wireshark.