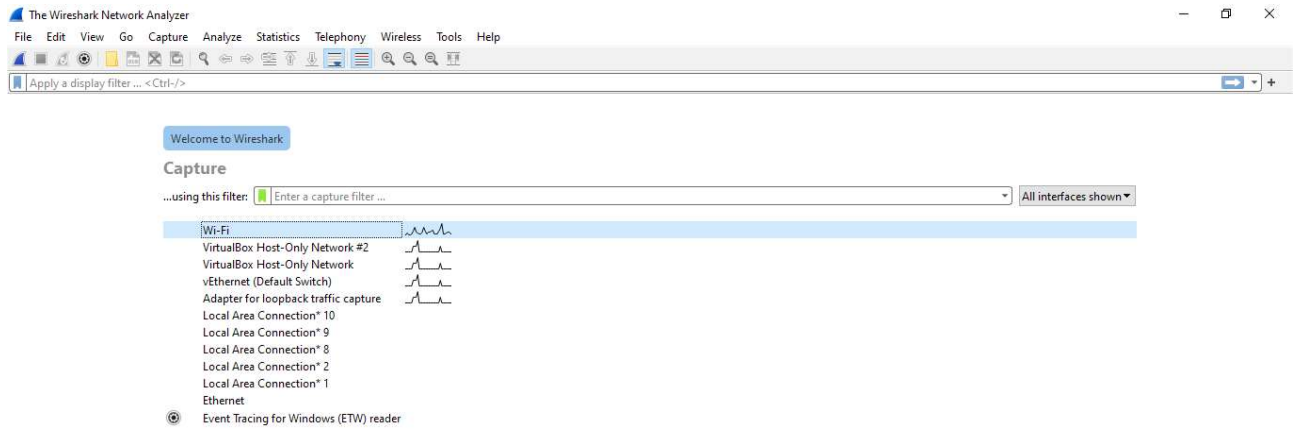
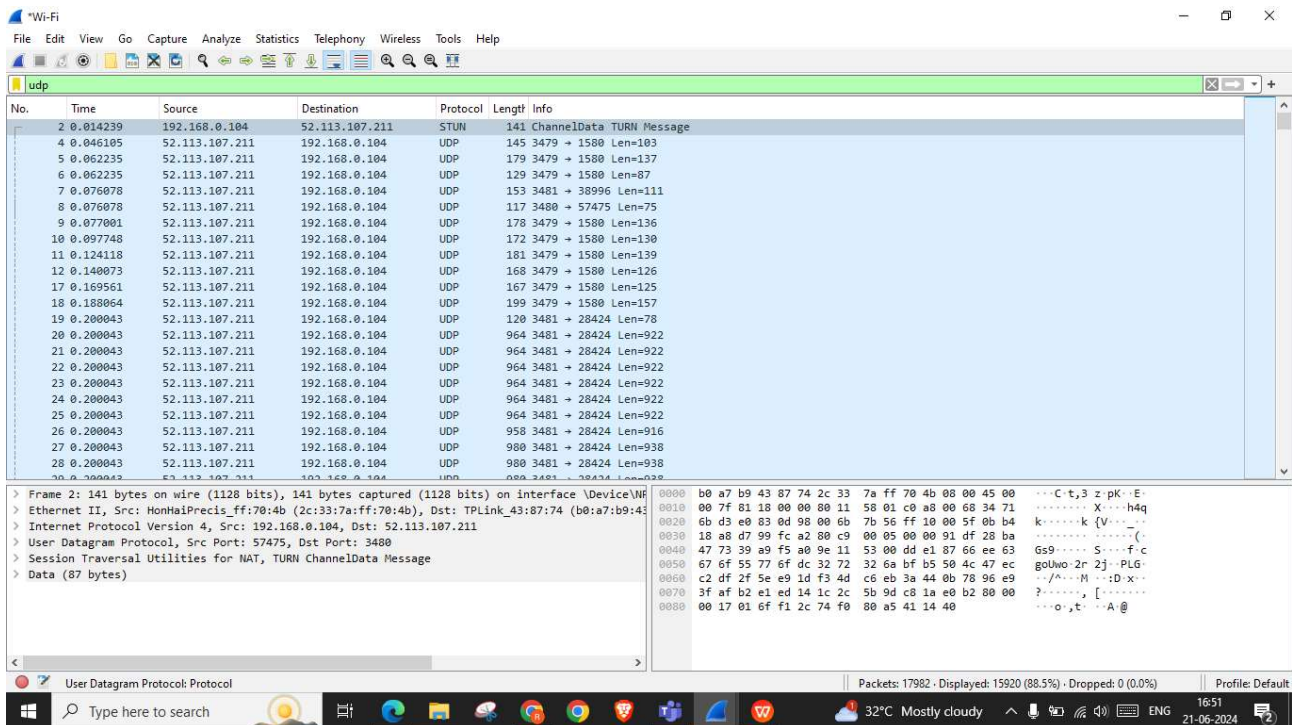


# Lab Exercise – UDP & TCP (21-06)

## Capture a UDP Trace:



## Selecting the Wi-Fi Interface



## Capture the packets of UDP traffic

## Open the Trace:

The screenshot shows the Wireshark interface with a network trace loaded. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, analysis, and display. The display filter bar shows "Apply a display filter ... <Ctrl-/>". The packet list pane on the left shows a list of 23 packets. The packet details pane on the right shows the details of the selected packet (No. 1). The packet bytes pane on the right shows the raw data of the selected packet. The status bar at the bottom shows "Packets: 1172 - Displayed: 1172 (100.0%)".

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.122	64.238.147.113	TCP	78	60643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=256679793 TSecr=0 SACK_PERM
2	0.008010	64.238.147.113	192.168.1.122	TCP	74	80 → 60643 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SACK_PERM TSval=4016893437 TSecr=256679793 WS=4
3	0.008080	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=256679881 TSecr=4016893437
4	0.008579	192.168.1.122	64.238.147.113	HTTP	257	GET /sigcomm/2011/papers/sigcomm/p2.pdf HTTP/1.1
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 → 60643 [ACK] Seq=1 Ack=192 Win=6864 Len=0 TSval=4016893527 TSecr=256679881
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 → 60643 [PSH, ACK] Seq=1 Ack=192 Win=6864 Len=245 TSval=4016893528 TSecr=256679881 [TCP segment of a re...
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=246 Win=524280 Len=0 TSval=256679970 TSecr=4016893528
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=246 Ack=192 Win=6864 Len=1368 TSval=4016893538 TSecr=256679881 [TCP segment of a reas...
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=1614 Ack=192 Win=6864 Len=1368 TSval=4016893615 TSecr=256679970 [TCP segment of a reas...
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=2982 Win=523944 Len=0 TSval=256680057 TSecr=4016893538
11	0.267657	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=2982 Ack=192 Win=6864 Len=1368 TSval=4016893615 TSecr=256679970 [TCP segment of a reas...
12	0.354612	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=4350 Ack=192 Win=6864 Len=1368 TSval=4016893703 TSecr=256680057 [TCP segment of a reas...
13	0.354647	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=5718 Win=523944 Len=0 TSval=256680144 TSecr=4016893615
14	0.355174	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=5718 Ack=192 Win=6864 Len=1368 TSval=4016893703 TSecr=256680057 [TCP segment of a reas...
15	0.355561	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=7086 Ack=192 Win=6864 Len=1368 TSval=4016893703 TSecr=256680057 [TCP segment of a reas...
16	0.355579	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=8454 Win=523944 Len=0 TSval=256680144 TSecr=4016893703
17	0.440719	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=8454 Ack=192 Win=6864 Len=1368 TSval=4016893789 TSecr=256680144 [TCP segment of a reas...
18	0.441973	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=9822 Ack=192 Win=6864 Len=1368 TSval=4016893789 TSecr=256680144 [TCP segment of a reas...
19	0.442003	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=11190 Win=523944 Len=0 TSval=256680230 TSecr=4016893789
20	0.442648	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [PSH, ACK] Seq=11190 Ack=192 Win=6864 Len=1368 TSval=4016893789 TSecr=256680144 [TCP segment of...
21	0.442716	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=12558 Win=523944 Len=0 TSval=256680230 TSecr=4016893789
22	0.445916	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=12558 Ack=192 Win=6864 Len=1368 TSval=4016893793 TSecr=256680144 [TCP segment of a re...
23	0.446386	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=13926 Ack=192 Win=6864 Len=1368 TSval=4016893793 TSecr=256680144 [TCP segment of a re...

## Selecting the Ethernet Interface

## TCP Connection Setup/Teardown:

## Search for packets with the SYN flag on using the filter expression “tcp.flags.syn==1” :

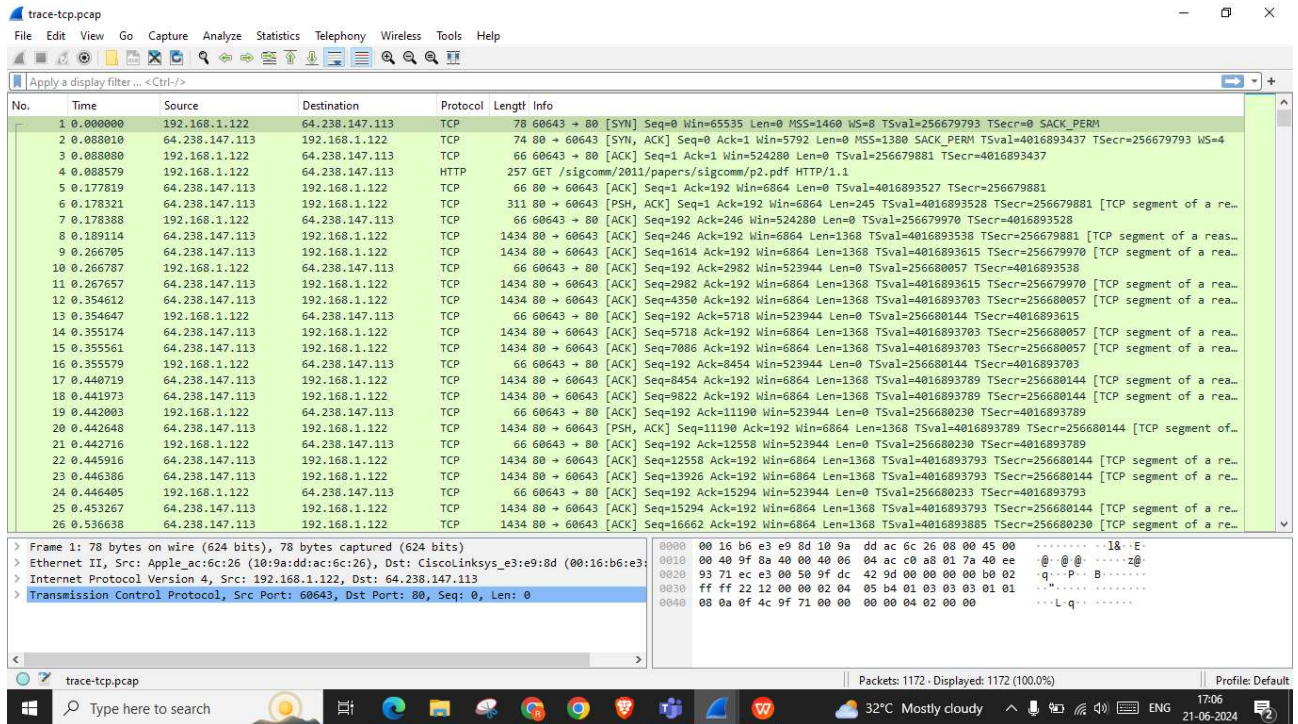
The screenshot shows the Wireshark interface with a network trace filtered by the expression "tcp.flags.syn==1". The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, analysis, and display. The display filter bar shows "tcp.flags.syn==1". The packet list pane on the left shows a list of 2 packets. The packet details pane on the right shows the details of the selected packet (No. 1). The packet bytes pane on the right shows the raw data of the selected packet. The status bar at the bottom shows "Packets: 1172 - Displayed: 2 (0.2%)".

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.122	64.238.147.113	TCP	78	60643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=256679793 TSecr=0 SACK_PERM
2	0.008010	64.238.147.113	192.168.1.122	TCP	74	80 → 60643 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SACK_PERM TSval=4016893437 TSecr=256679793 WS=4

## TCP segment with SYN flag on



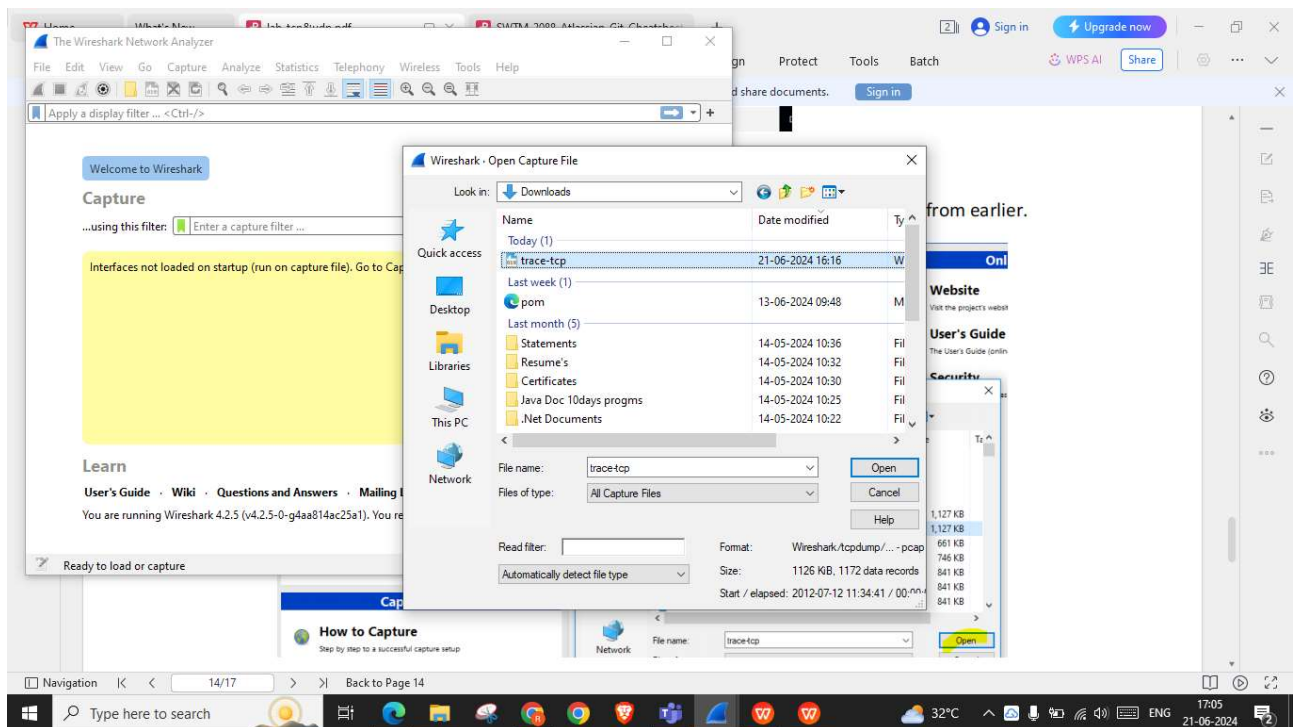
## Clearing the display filter TCP segment with SYN flag on and Viewing the complete trace:

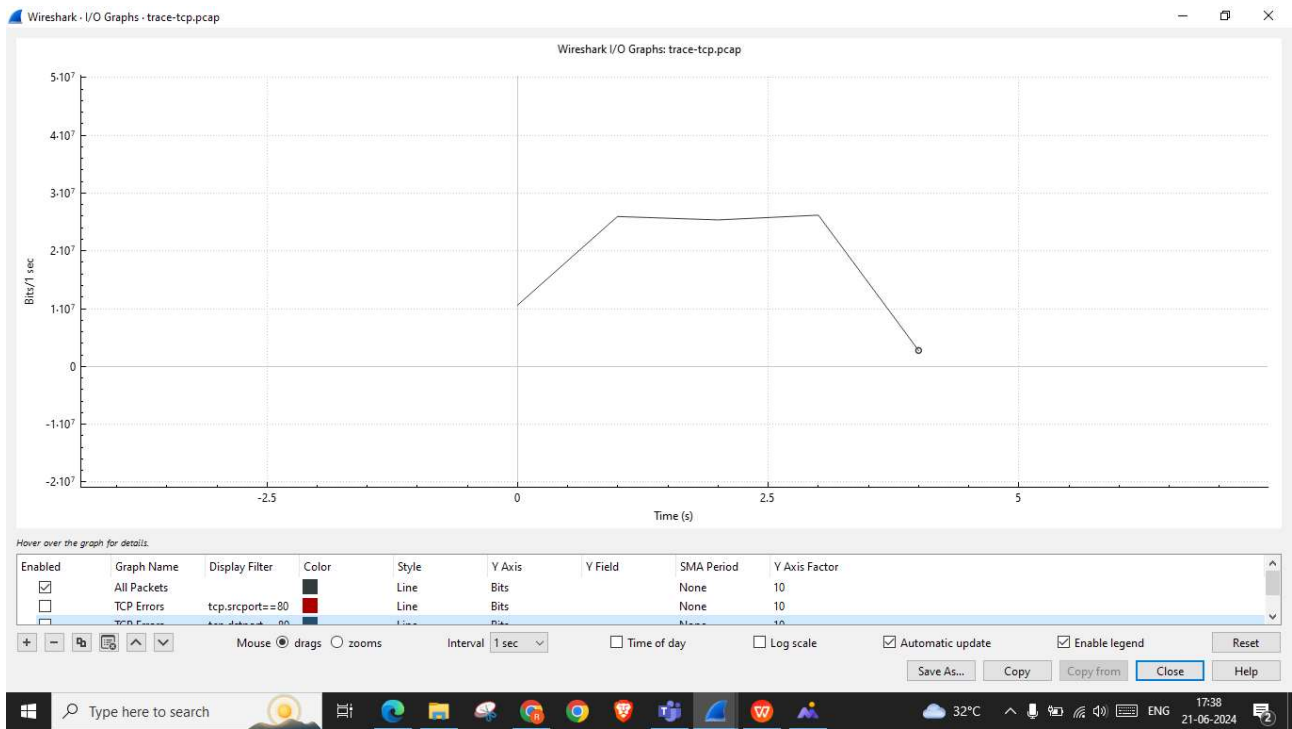


## Viewing the complete trace

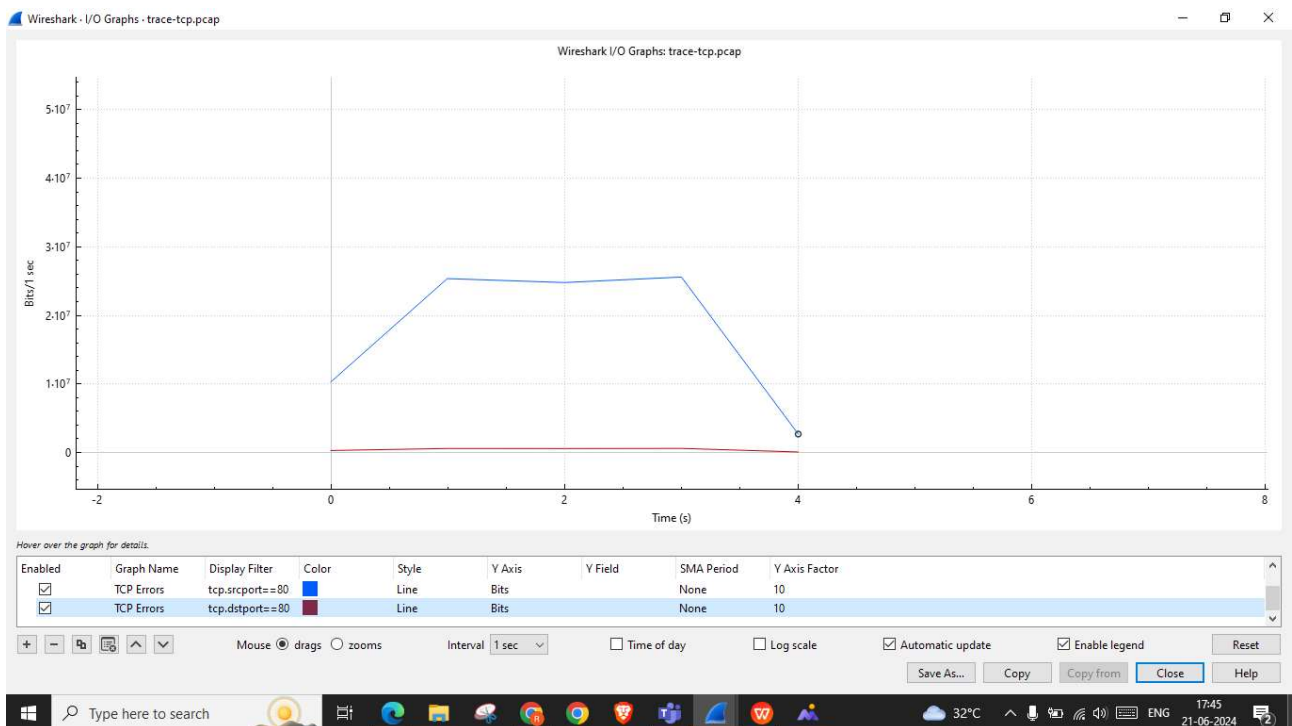
## TCP Data Transfer:

open the trace-tcp file which is in downloads folder:





The IO graph



TCP download rate over time via an IO graph