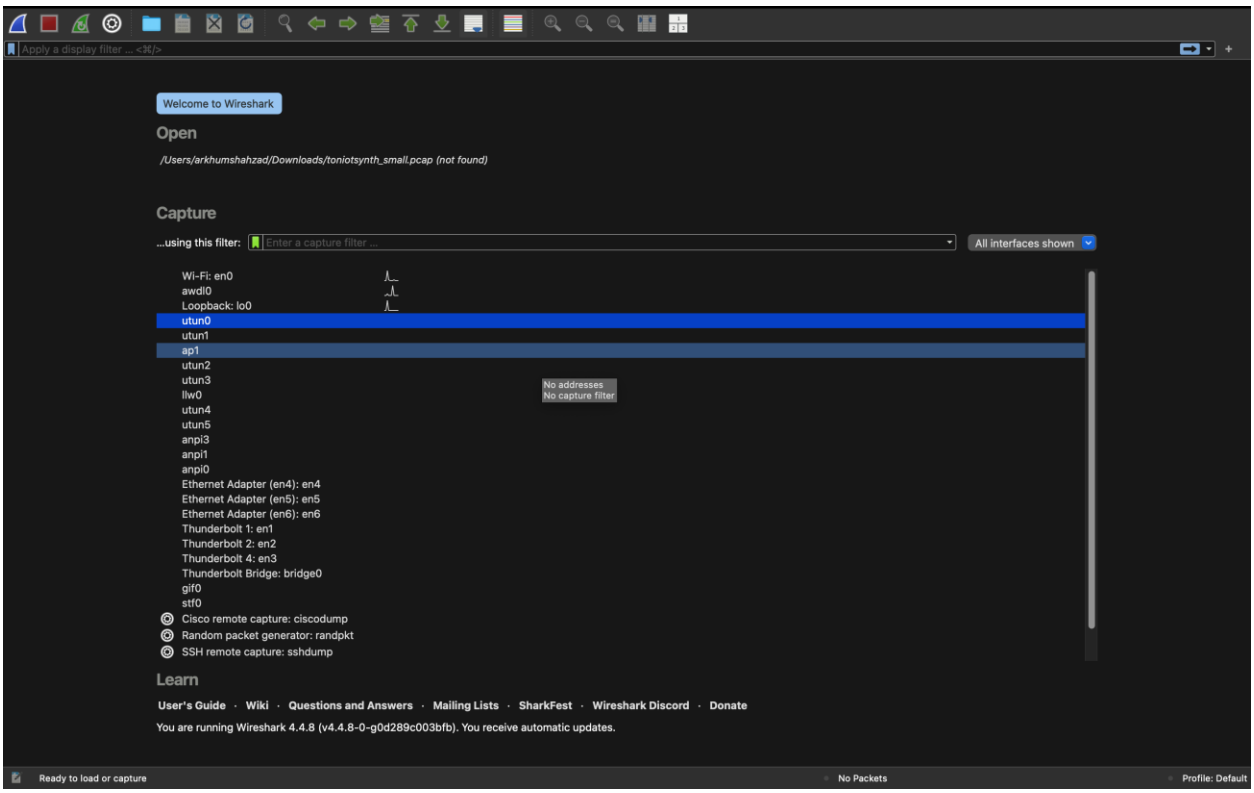
Tutorial: Traffic Analysis using Wireshark

🎯 Objective

Learn how to capture, filter, and analyze network traffic using Wireshark to detect normal and attack patterns (TON_IoT dataset context).

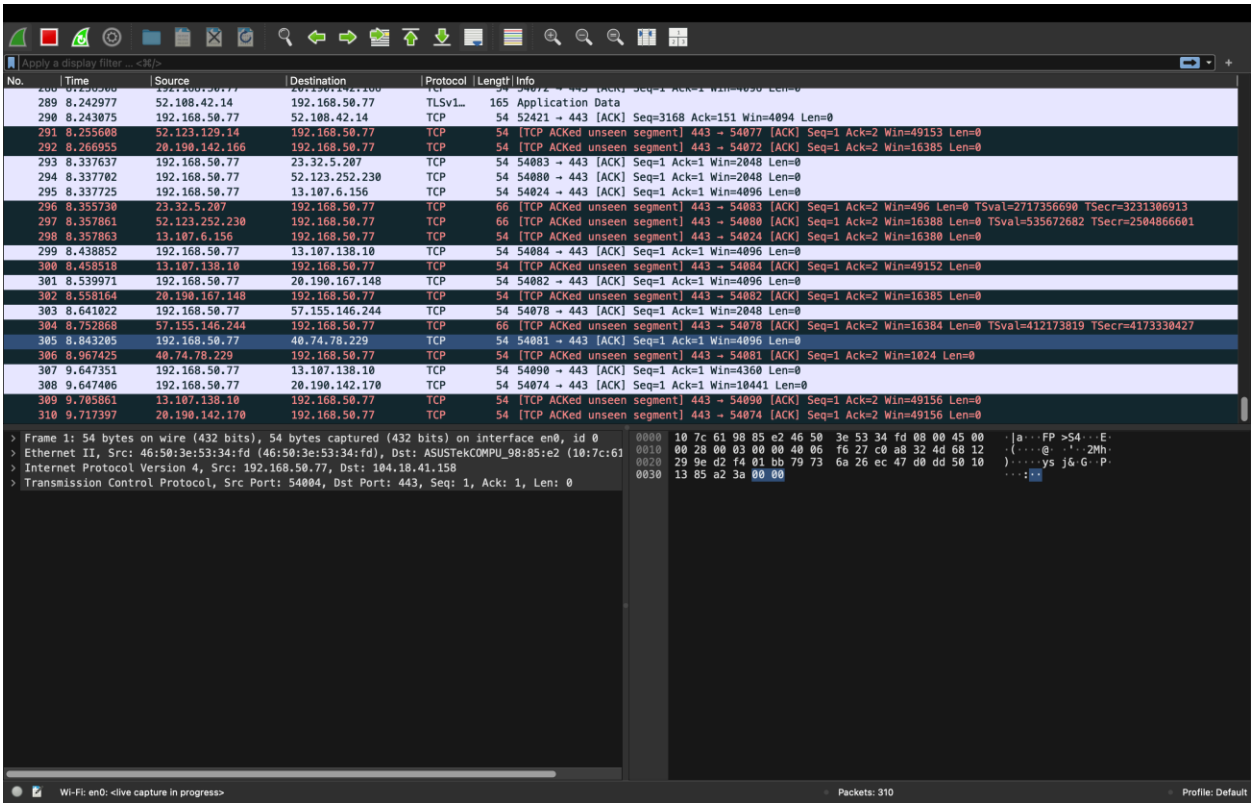
🛠️ Step 1: Launch Wireshark

- Open Wireshark from your applications or via terminal (wireshark &).
- Select the **active network interface** (e.g., eth0, wlan0, or the virtual adapter for your VM).



🛠️ Step 2: Capture Traffic

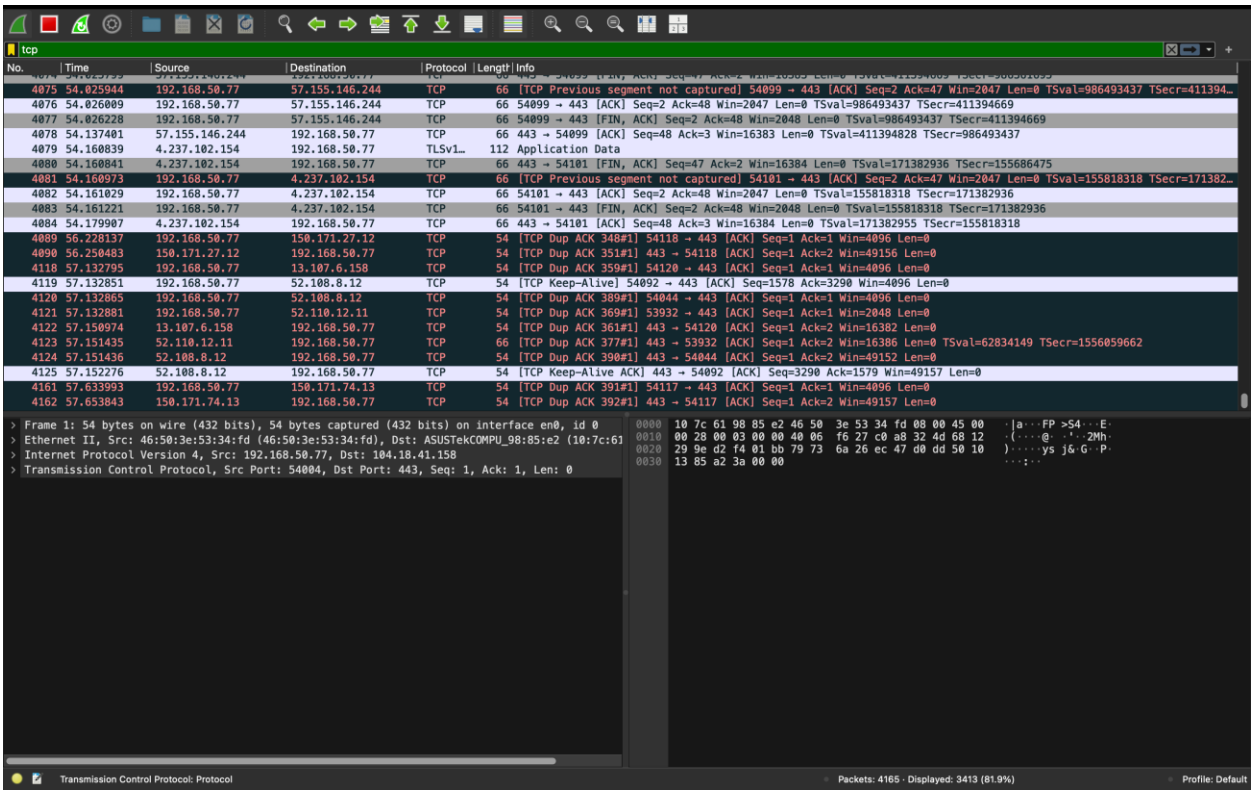
- Click on the interface to begin live capture.
- Packets will start populating in the main Wireshark window.



🛠️ Step 3: Apply Filters

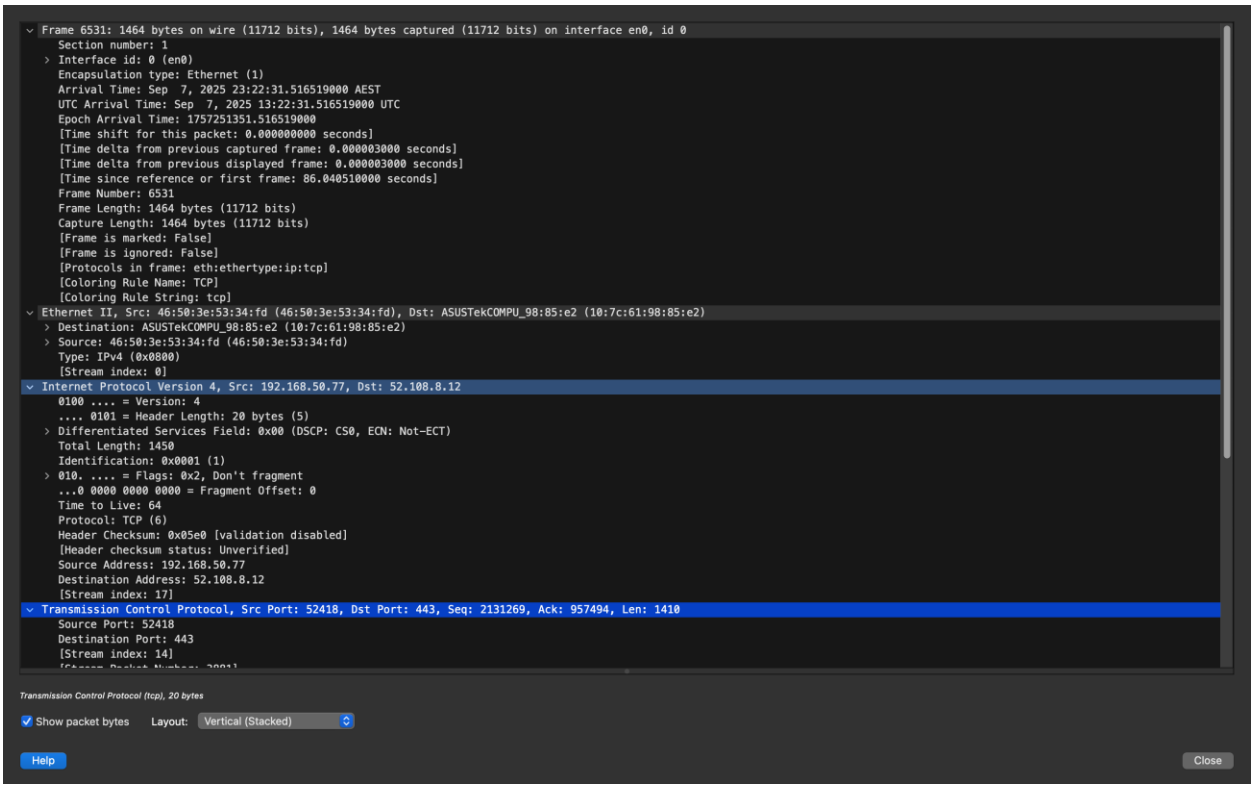
- Use **display filters** to focus on specific protocols:
  - tcp → show only TCP traffic
  - udp → show only UDP traffic

- icmp → show only ping requests
- ip.addr == 192.168.1.1 → show traffic involving a specific host



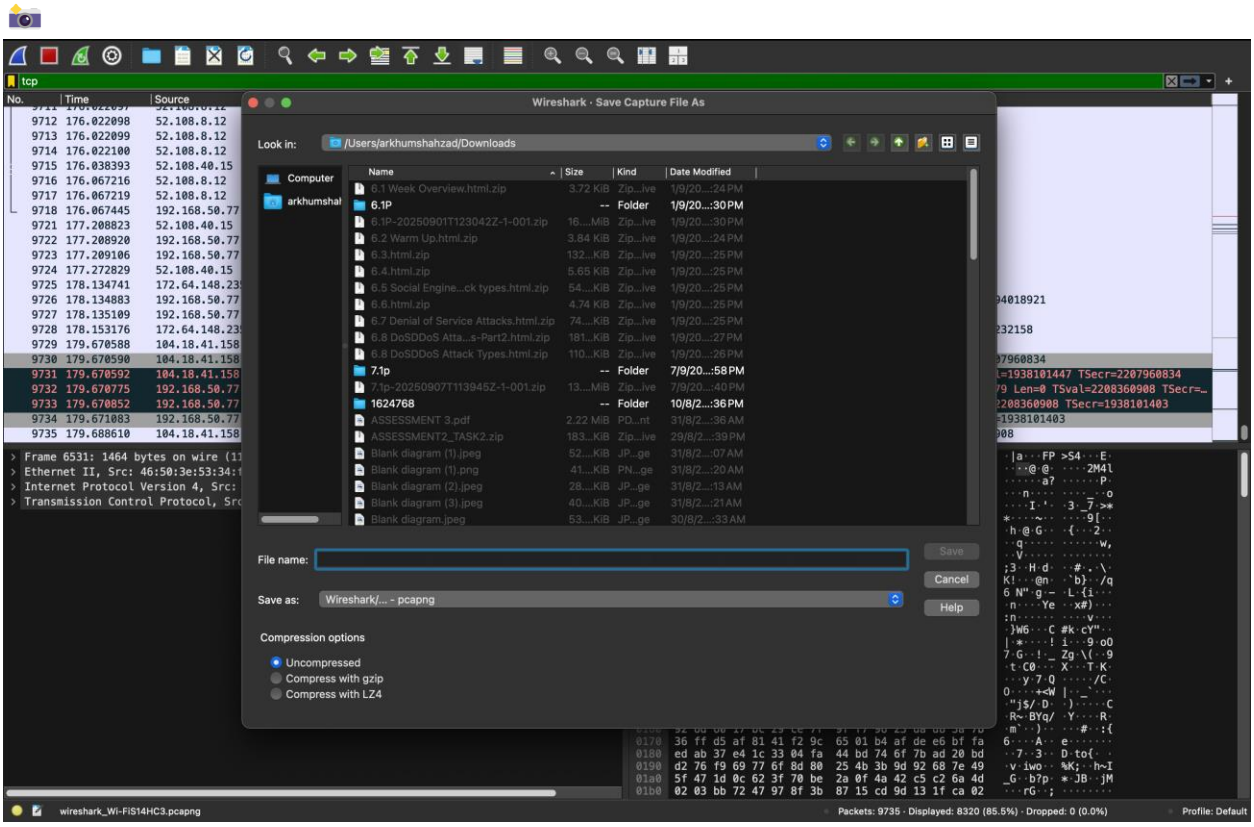
🛠️ Step 4: Analyze Packets

- Select a packet and expand details in the middle panel (Ethernet, IP, TCP layers).
- Inspect source/destination IP, port numbers, flags (e.g., SYN, ACK).
- Compare normal vs suspicious flows (e.g., repeated SYNs → SYN flood).



🛠️ Step 5: Save Captures

- Stop the capture.
- Save the file (File → Save As...) in .pcapng format for replay or analysis.


tcp
No. Time Source
Wireshark · Save Capture File As
Look in: /Users/arkhumshahzad/Downloads
Computer
arkhumshal
Name Size Kind Date Modified
6.1 Week Overview.html.zip 3.72 KiB Zip...ive 1/9/20...:24 PM
6.1P -- Folder 1/9/20...:30 PM
6.1P-20250901T123042Z-1-001.zip 16....MiB Zip...ive 1/9/20...:30 PM
6.2 Warm Up.html.zip 3.84 KiB Zip...ive 1/9/20...:24 PM
6.3.html.zip 132...KiB Zip...ive 1/9/20...:25 PM
6.4.html.zip 5.65 KiB Zip...ive 1/9/20...:25 PM
6.5 Social Engine...ck types.html.zip 54....KiB Zip...ive 1/9/20...:25 PM
6.6.html.zip 4.74 KiB Zip...ive 1/9/20...:25 PM
6.7 Denial of Service Attacks.html.zip 74....KiB Zip...ive 1/9/20...:25 PM
6.8 DoSDDoS Atta...s-Part2.html.zip 181...KiB Zip...ive 1/9/20...:27 PM
6.8 DoSDDoS Attack Types.html.zip 110...KiB Zip...ive 1/9/20...:26 PM
7.1p -- Folder 7/9/20...:58 PM
7.1p-20250907T113945Z-1-001.zip 13....MiB Zip...ive 7/9/20...:40 PM
1624768 -- Folder 10/8/2...:36 PM
ASSESSMENT 3.pdf 2.22 MiB PD...nt 31/8/2...:36 AM
ASSESSMENT2_TASK2.zip 183...KiB Zip...ive 29/8/2...:39 PM
Blank diagram (1).jpeg 52....KiB JP...ge 31/8/2...:07 AM
Blank diagram (1).png 41....KiB PN...ge 31/8/2...:20 AM
Blank diagram (2).jpeg 28....KiB JP...ge 31/8/2...:13 AM
Blank diagram (3).jpeg 40....KiB JP...ge 31/8/2...:21 AM
Blank diagram.jpeg 53....KiB JP...ge 30/8/2...:33 AM
File name:
Save as: Wireshark/... - pcapng
Save
Cancel
Help
Compression options
Uncompressed
Compress with gzip
Compress with LZ4
Frame 6531: 1464 bytes on wire (11
Ethernet II, Src: 46:50:3e:53:34:
Internet Protocol Version 4, Src:
Transmission Control Protocol, Sr
wireshark_Wi-FiS14HC3.pcapng
Packets: 9735 · Displayed: 8320 (85.5%) · Dropped: 0 (0.0%)
Profile: Default