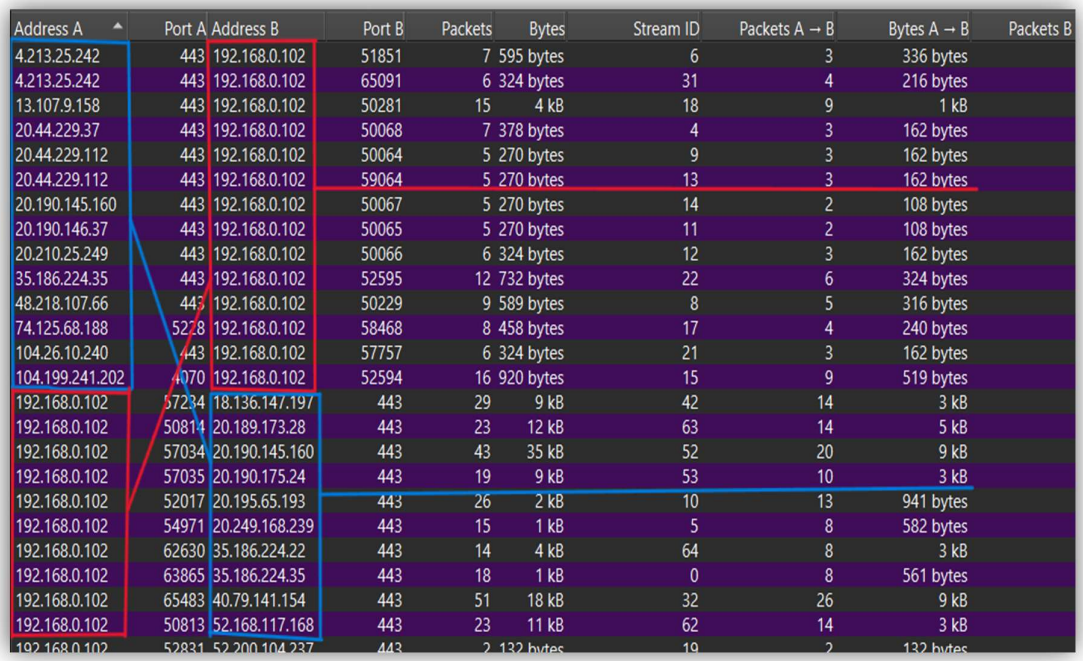
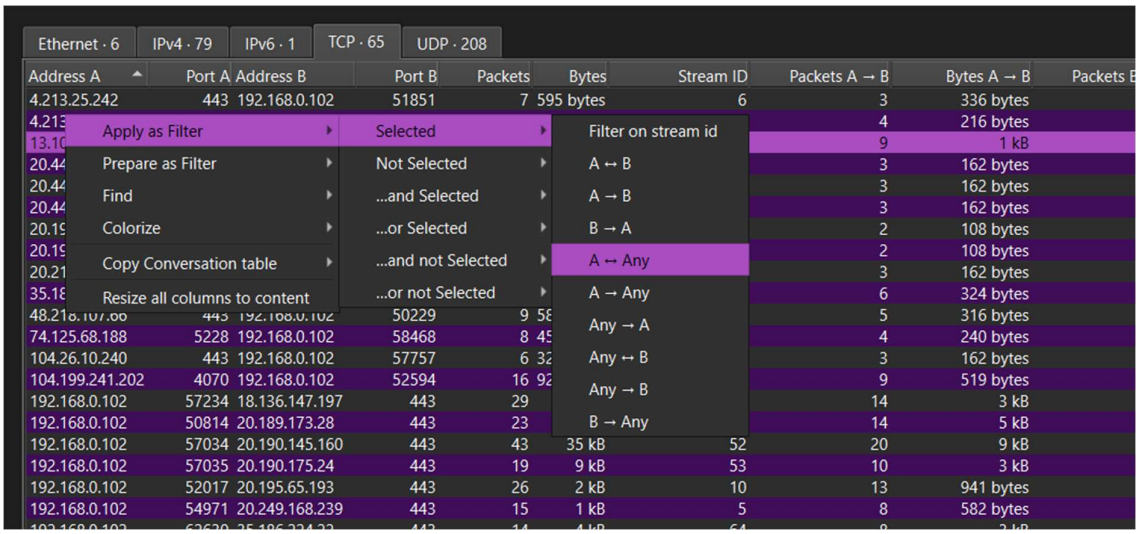


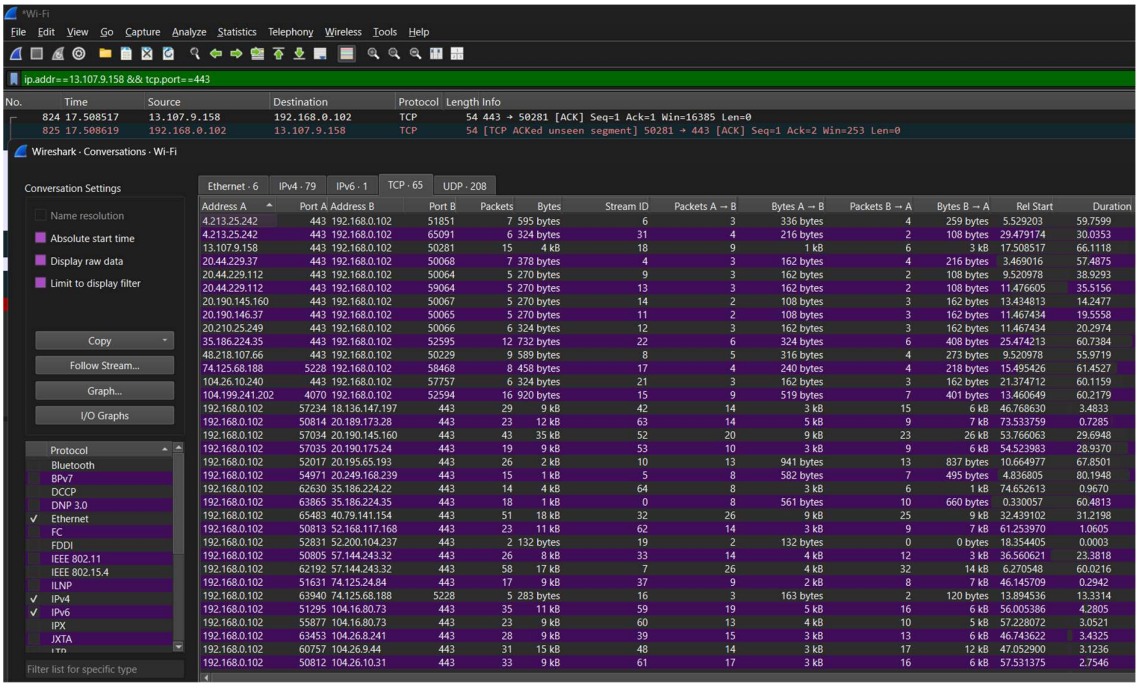
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B
4.213.25.242	443	192.168.0.102	51851	7	595 bytes	6	3	336 bytes	
4.213.25.242	443	192.168.0.102	65091	6	324 bytes	31	4	216 bytes	
13.107.9.158	443	192.168.0.102	50281	15	4 kB	18	9	1 kB	
20.44.229.37	443	192.168.0.102	50068	7	378 bytes	4	3	162 bytes	
20.44.229.112	443	192.168.0.102	50064	5	270 bytes	9	3	162 bytes	
20.44.229.112	443	192.168.0.102	59064	5	270 bytes	13	3	162 bytes	
20.190.145.160	443	192.168.0.102	50067	5	270 bytes	14	2	108 bytes	
20.190.146.37	443	192.168.0.102	50065	5	270 bytes	11	2	108 bytes	
20.210.25.249	443	192.168.0.102	50066	6	324 bytes	12	3	162 bytes	
35.186.224.35	443	192.168.0.102	52595	12	732 bytes	22	6	324 bytes	
48.218.107.66	443	192.168.0.102	50229	9	589 bytes	8	5	316 bytes	
74.125.68.188	5228	192.168.0.102	58468	8	458 bytes	17	4	240 bytes	
104.26.10.240	443	192.168.0.102	57757	6	324 bytes	21	3	162 bytes	
104.199.241.202	4070	192.168.0.102	52594	16	920 bytes	15	9	519 bytes	
192.168.0.102	57234	18.136.147.197	443	29	9 kB	42	14	3 kB	
192.168.0.102	50814	20.189.173.28	443	23	12 kB	63	14	5 kB	
192.168.0.102	57034	20.190.145.160	443	43	35 kB	52	20	9 kB	
192.168.0.102	57035	20.190.175.24	443	19	9 kB	53	10	3 kB	
192.168.0.102	52017	20.195.65.193	443	26	2 kB	10	13	941 bytes	
192.168.0.102	54971	20.249.168.239	443	15	1 kB	5	8	582 bytes	
192.168.0.102	62630	35.186.224.22	443	14	4 kB	64	8	3 kB	
192.168.0.102	63865	35.186.224.35	443	18	1 kB	0	8	561 bytes	
192.168.0.102	65483	40.79.141.154	443	51	18 kB	32	26	9 kB	
192.168.0.102	50813	52.168.117.168	443	23	11 kB	62	14	3 kB	
192.168.0.102	52831	52.200.104.237	443	2	132 bytes	19	2	132 bytes	

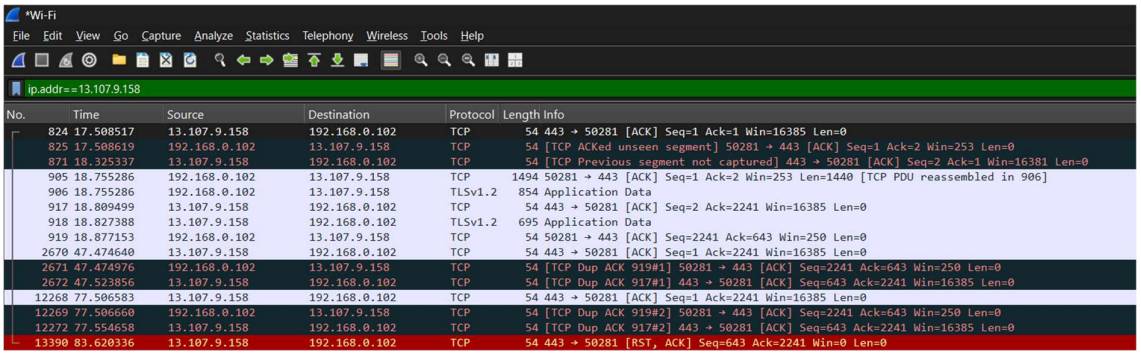
My Computer

Conversation Partner

- **My Computer (Local Address):** The red boxes highlight the IP address 192.168.0.102, which represents your local machine's internal IP address.
- **Conversation Partner (Remote Addresses):** The blue boxes highlight various external IP addresses (e.g., 20.190.145.160, 35.186.224.35) belonging to servers you are communicating with.
- **Ports & Protocols:** * Most connections shown use **Port 443**. This indicates **HTTPS** traffic, which is **encrypted**.
- High-numbered ports (e.g., 57234, 63865) on "My Computer" are **ephemeral ports** used to initiate the connection.
- **Data Volume:** The "Bytes" columns show the size of the data transferred, helping you identify which "Conversation Partner" sent or received the most information.







1. Connection Overview (Conversations)

The images show the "Conversations" window, which lists active network dialogues between your computer and various servers.

- **My Computer (Address A/B):** Your local IP address is identified as **192.168.0.102**.
- **Conversation Partners:** These are external IP addresses such as **13.107.9.158** or **20.190.145.160**.
- **Port Analysis:** Most connections use **Port 443**, which indicates **HTTPS** traffic. Your computer uses high-numbered random ports (e.g., 50281, 57234) to establish these sessions.

2. Identifying Encrypted Traffic

You have applied a filter for ip.addr==13.107.9.158 to isolate traffic with a specific server.

- **TLS Protocol:** Within this filtered view, you can see the **TLSv1.2** protocol in use.
- **Application Data:** Packets labeled as "**Application Data**" (e.g., packets #906 and #918) contain the actual information being sent, which is **encrypted** and cannot be read in plain text.

3. TCP Traffic Observations

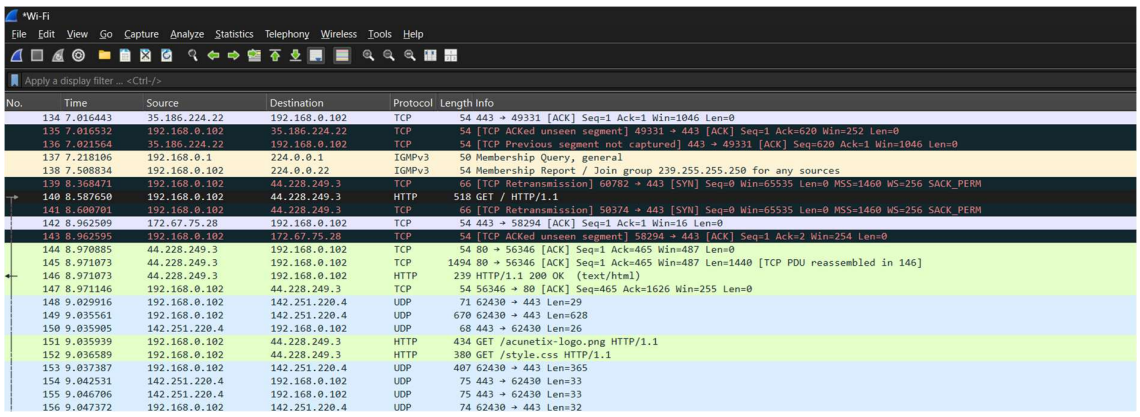
The packet list reveals several technical details about the health and status of your TCP connections:

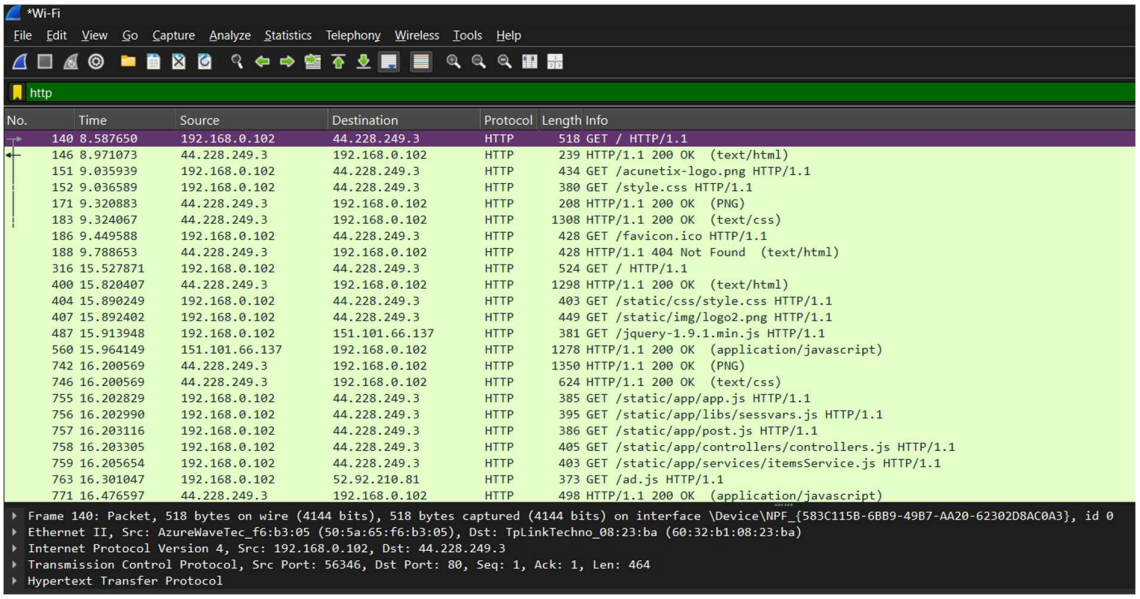
- **Standard Traffic:** You can see standard **[ACK]** (Acknowledgment) packets being exchanged to confirm data receipt.
- **Connection Errors:** Some packets are highlighted in dark colors, indicating network issues like **"TCP Dup ACK"** (Duplicate Acknowledgment) or **"TCP Previous segment not captured,"** which happen when data is lost or delayed in transit.
- **Connection Termination:** Packet #13390 shows a **[RST, ACK]** (Reset/Acknowledgment) in red, indicating the connection was abruptly closed.

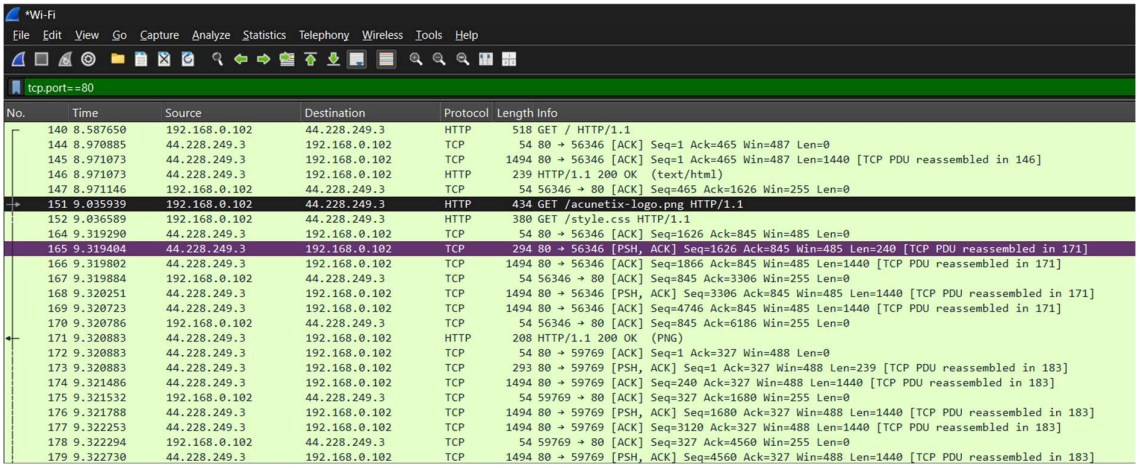
4. Filtering and Analysis

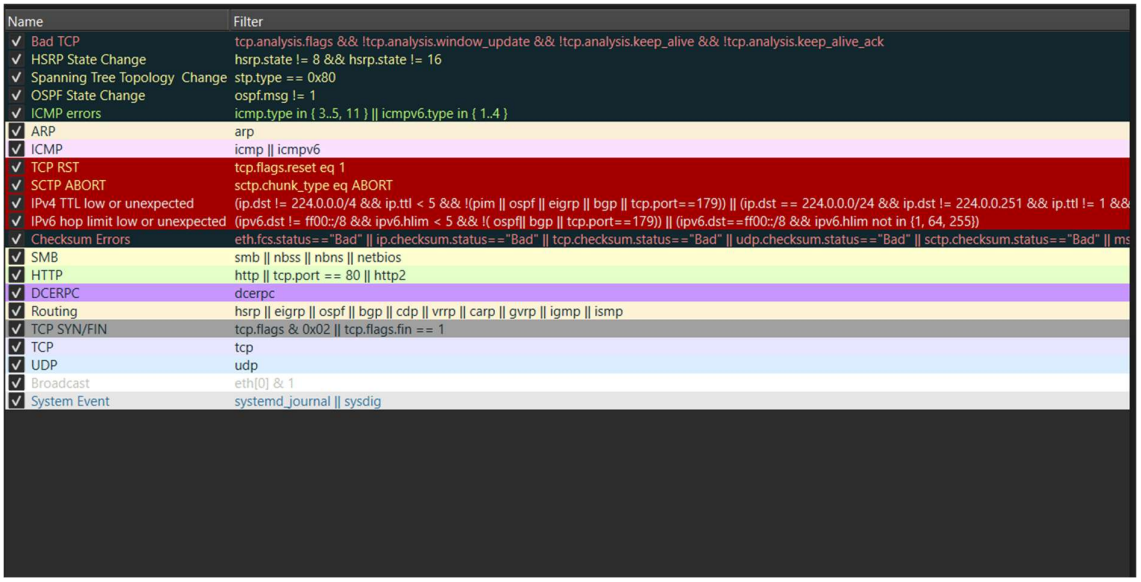
One screenshot demonstrates how to perform analysis by right-clicking a conversation and selecting **"Apply as Filter"** -> **"Selected"** -> **"A <-> Any"**. This is a key skill for Task 3, as it allows an analyst to isolate a specific stream of data for deeper inspection.

Http Filtering:

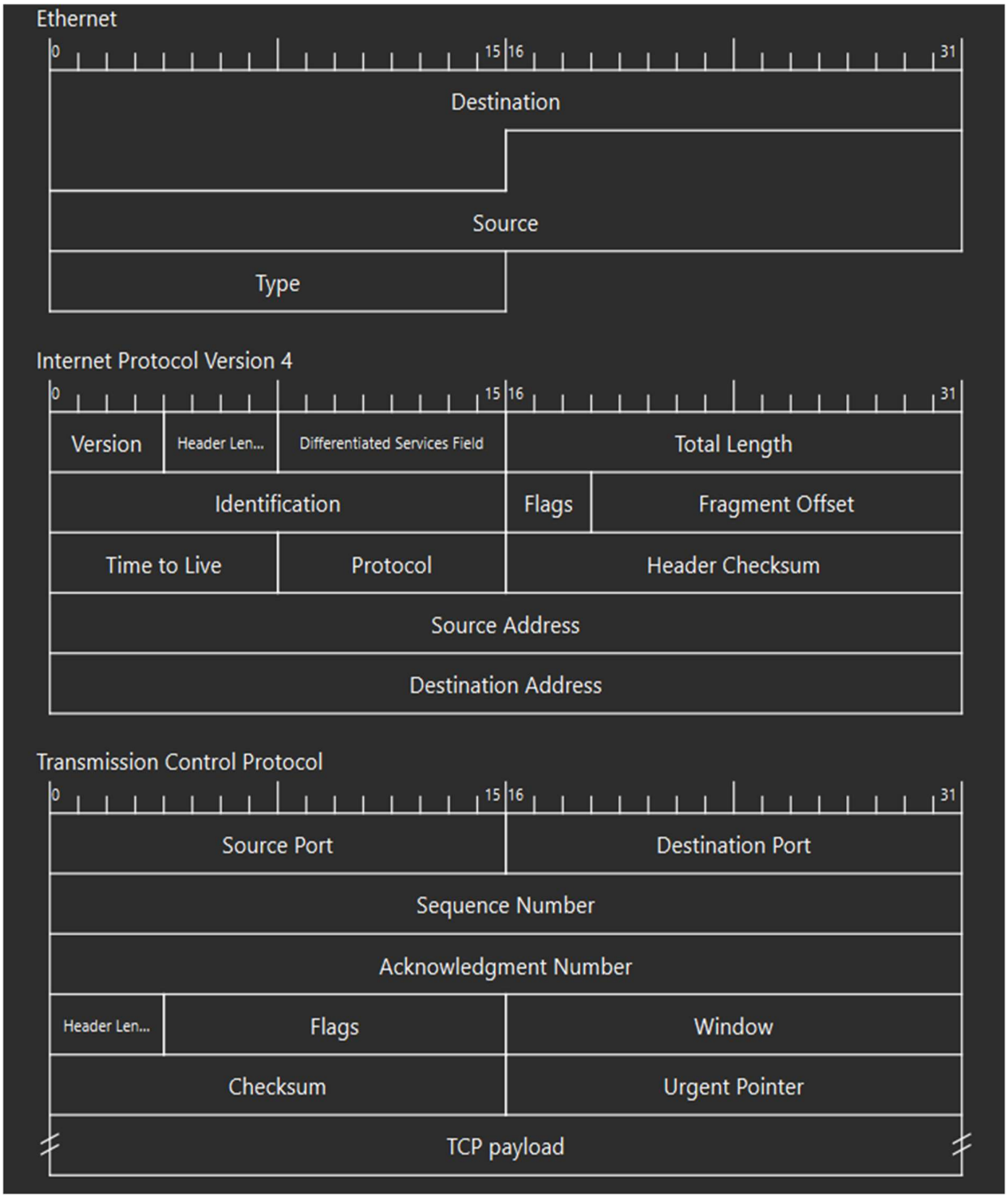


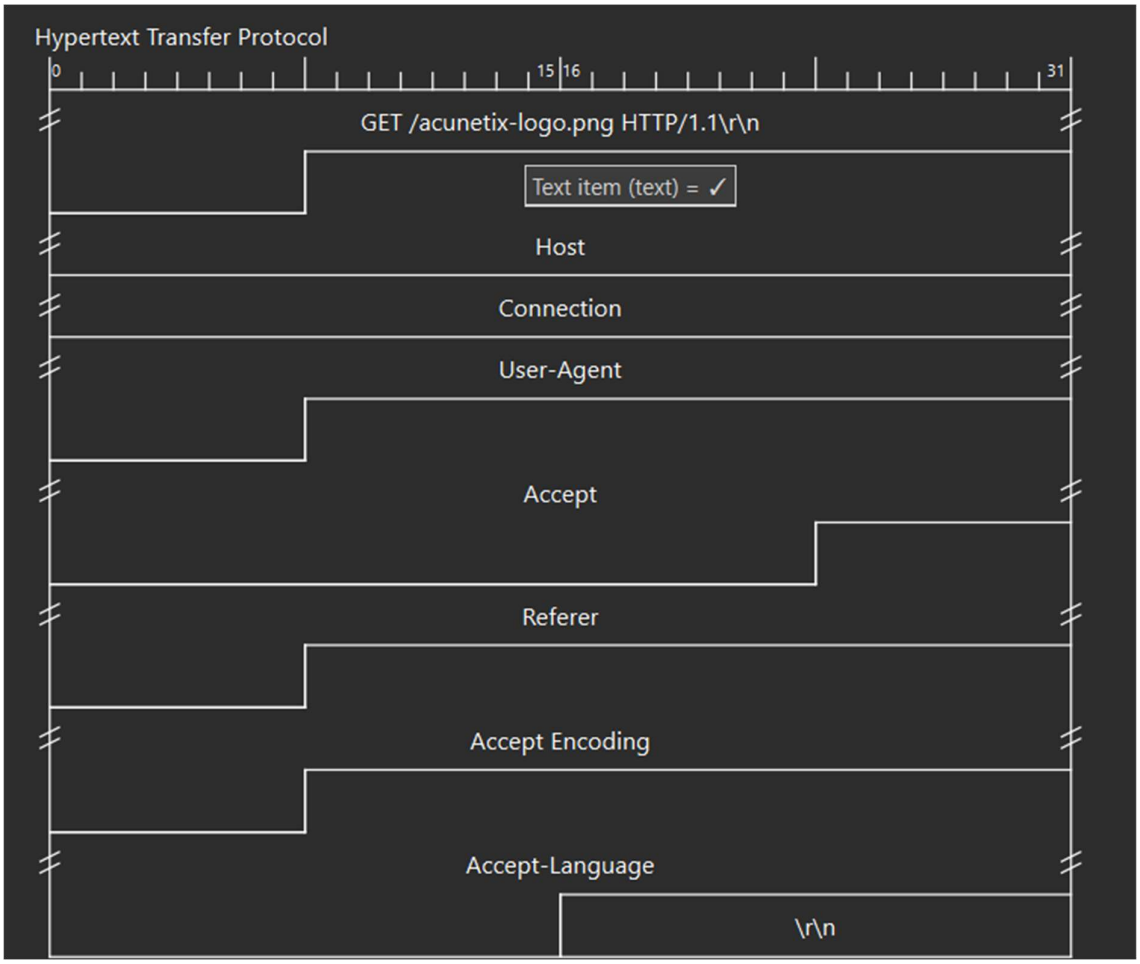

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
140 8.587650 192.168.0.102 44.228.249.3 HTTP 518 GET / HTTP/1.1
146 8.971073 44.228.249.3 192.168.0.102 HTTP 239 HTTP/1.1 200 OK (text/html)
151 9.035939 192.168.0.102 44.228.249.3 HTTP 434 GET /acunetix-logo.png HTTP/1.1
152 9.036589 192.168.0.102 44.228.249.3 HTTP 380 GET /style.css HTTP/1.1
171 9.320883 44.228.249.3 192.168.0.102 HTTP 208 HTTP/1.1 200 OK (PNG)
183 9.324067 44.228.249.3 192.168.0.102 HTTP 1308 HTTP/1.1 200 OK (text/css)
186 9.449588 192.168.0.102 44.228.249.3 HTTP 428 GET /favicon.ico HTTP/1.1
188 9.788653 44.228.249.3 192.168.0.102 HTTP 428 HTTP/1.1 404 Not Found (text/html)
316 15.527871 192.168.0.102 44.228.249.3 HTTP 524 GET / HTTP/1.1
400 15.820407 44.228.249.3 192.168.0.102 HTTP 1298 HTTP/1.1 200 OK (text/html)
404 15.890249 192.168.0.102 44.228.249.3 HTTP 403 GET /static/css/style.css HTTP/1.1
407 15.892402 192.168.0.102 44.228.249.3 HTTP 449 GET /static/img/logo2.png HTTP/1.1
487 15.913948 192.168.0.102 151.101.66.137 HTTP 381 GET /jquery-1.9.1.min.js HTTP/1.1
560 15.964149 151.101.66.137 192.168.0.102 HTTP 1278 HTTP/1.1 200 OK (application/javascript)
742 16.200569 44.228.249.3 192.168.0.102 HTTP 1350 HTTP/1.1 200 OK (PNG)
746 16.200569 44.228.249.3 192.168.0.102 HTTP 624 HTTP/1.1 200 OK (text/css)
755 16.202829 192.168.0.102 44.228.249.3 HTTP 385 GET /static/app/app.js HTTP/1.1
756 16.202990 192.168.0.102 44.228.249.3 HTTP 395 GET /static/app/libs/sessvars.js HTTP/1.1
757 16.203116 192.168.0.102 44.228.249.3 HTTP 386 GET /static/app/post.js HTTP/1.1
758 16.203305 192.168.0.102 44.228.249.3 HTTP 405 GET /static/app/controllers/controllers.js HTTP/1.1
759 16.205654 192.168.0.102 44.228.249.3 HTTP 403 GET /static/app/services/itemsService.js HTTP/1.1
763 16.301047 192.168.0.102 52.92.210.81 HTTP 373 GET /ad.js HTTP/1.1
771 16.476597 44.228.249.3 192.168.0.102 HTTP 498 HTTP/1.1 200 OK (application/javascript)
Frame 140: Packet, 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits) on interface \Device\NPF_{583C115B-6BB9-49B7-AA20-62302D8AC0A3}, id 0
Ethernet II, Src: AzureWaveTec_f6:b3:05 (50:5a:65:f6:b3:05), Dst: TpLinkTechno_08:23:ba (60:32:b1:08:23:ba)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 56346, Dst Port: 80, Seq: 1, Ack: 1, Len: 464
Hypertext Transfer Protocol


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port==80
No. Time Source Destination Protocol Length Info
140 8.587650 192.168.0.102 44.228.249.3 HTTP 518 GET / HTTP/1.1
144 8.970885 44.228.249.3 192.168.0.102 TCP 54 80 → 56346 [ACK] Seq=1 Ack=465 Win=487 Len=0
145 8.971073 44.228.249.3 192.168.0.102 TCP 1494 80 → 56346 [ACK] Seq=1 Ack=465 Win=487 Len=1440 [TCP PDU reassembled in 146]
146 8.971073 44.228.249.3 192.168.0.102 HTTP 239 HTTP/1.1 200 OK (text/html)
147 8.971146 192.168.0.102 44.228.249.3 TCP 54 56346 → 80 [ACK] Seq=465 Ack=1626 Win=255 Len=0
151 9.035939 192.168.0.102 44.228.249.3 HTTP 434 GET /acunetix-logo.png HTTP/1.1
152 9.036589 192.168.0.102 44.228.249.3 HTTP 380 GET /style.css HTTP/1.1
164 9.319290 44.228.249.3 192.168.0.102 TCP 54 80 → 56346 [ACK] Seq=1626 Ack=845 Win=485 Len=0
165 9.319404 44.228.249.3 192.168.0.102 TCP 294 80 → 56346 [PSH, ACK] Seq=1626 Ack=845 Win=485 Len=240 [TCP PDU reassembled in 171]
166 9.319802 44.228.249.3 192.168.0.102 TCP 1494 80 → 56346 [ACK] Seq=1866 Ack=845 Win=485 Len=1440 [TCP PDU reassembled in 171]
167 9.319884 192.168.0.102 44.228.249.3 TCP 54 56346 → 80 [ACK] Seq=845 Ack=3306 Win=255 Len=0
168 9.320251 44.228.249.3 192.168.0.102 TCP 1494 80 → 56346 [PSH, ACK] Seq=3306 Ack=845 Win=485 Len=1440 [TCP PDU reassembled in 171]
169 9.320723 44.228.249.3 192.168.0.102 TCP 1494 80 → 56346 [ACK] Seq=4746 Ack=845 Win=485 Len=1440 [TCP PDU reassembled in 171]
170 9.320786 192.168.0.102 44.228.249.3 TCP 54 56346 → 80 [ACK] Seq=845 Ack=6186 Win=255 Len=0
171 9.320883 44.228.249.3 192.168.0.102 HTTP 208 HTTP/1.1 200 OK (PNG)
172 9.320883 44.228.249.3 192.168.0.102 TCP 54 80 → 59769 [ACK] Seq=1 Ack=327 Win=488 Len=0
173 9.320883 44.228.249.3 192.168.0.102 TCP 293 80 → 59769 [PSH, ACK] Seq=1 Ack=327 Win=488 Len=239 [TCP PDU reassembled in 183]
174 9.321486 44.228.249.3 192.168.0.102 TCP 1494 80 → 59769 [ACK] Seq=240 Ack=327 Win=488 Len=1440 [TCP PDU reassembled in 183]
175 9.321532 192.168.0.102 44.228.249.3 TCP 54 59769 → 80 [ACK] Seq=327 Ack=1680 Win=255 Len=0
176 9.321788 44.228.249.3 192.168.0.102 TCP 1494 80 → 59769 [PSH, ACK] Seq=1680 Ack=327 Win=488 Len=1440 [TCP PDU reassembled in 183]
177 9.322253 44.228.249.3 192.168.0.102 TCP 1494 80 → 59769 [ACK] Seq=3120 Ack=327 Win=488 Len=1440 [TCP PDU reassembled in 183]
178 9.322294 192.168.0.102 44.228.249.3 TCP 54 59769 → 80 [ACK] Seq=327 Ack=4560 Win=255 Len=0
179 9.322730 44.228.249.3 192.168.0.102 TCP 1494 80 → 59769 [PSH, ACK] Seq=4560 Ack=327 Win=488 Len=1440 [TCP PDU reassembled in 183]


Name Filter
Bad TCP tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
HSRP State Change hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change stp.type == 0x80
OSPF State Change ospf.msg != 1
ICMP errors icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
ARP arp
ICMP icmp || icmpv6
TCP RST tcp.flags.reset eq 1
SCTP ABORT sctp.chunk_type eq ABORT
IPv4 TTL low or unexpected (ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !(pim || ospf || eigrp || bgp || tcp.port==179)) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 &&
IPv6 hop limit low or unexpected (ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf|| bgp || tcp.port==179)) || (ipv6.dst==ff00::/8 && ipv6.hlim not in {1, 64, 255})
Checksum Errors eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || ms
SMB smb || nbss || nbns || netbios
HTTP http || tcp.port == 80 || http2
DCERPC dcerpc
Routing hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN tcp.flags & 0x02 || tcp.flags.fin == 1
TCP tcp
UDP udp
Broadcast eth[0] & 1
System Event systemd_journal || sysdig

Packet Diagram:





1. Identifying Core Networking Concepts

Your screenshots show a deep dive into the protocol layers required by the task:

- **Layer 2 (Ethernet II):** You have captured the physical hardware communication between **AzureWaveTec** (your machine) and a **TpLinkTechno** device.
- **Layer 3 (IPv4):** Your local IP is clearly identified as **192.168.0.102**, communicating with an external web server at **44.228.249.3**.
- **Layer 4 (TCP):** You are monitoring traffic on **Port 80** (HTTP) and **Port 443** (HTTPS).
- **Application Layer (HTTP):** You have successfully isolated a **GET request** for /acunetix-logo.png, which shows the browser asking for a specific image file.

2. Identifying Plain-Text vs. Encrypted Traffic

One of the most important parts of your task is distinguishing between readable and hidden data.

- **Plain-Text (HTTP):** Your screenshots show active **HTTP** traffic where the "Info" column displays clear text like GET /style.css and HTTP/1.1 200 OK. This is "plain-text" because an attacker could read exactly what you are viewing.
- **Encrypted (HTTPS/TLS):** In contrast, other screenshots show **TLSv1.2** traffic to IP **13.107.9.158**. These packets are labeled "**Application Data**," meaning the content is scrambled and unreadable to anyone intercepting it.

3. Traffic Analysis & Filtering

You have demonstrated advanced use of Wireshark tools to organize your data:

- **Conversation Tracking:** You opened the **Conversations** window to see a summary of all active "talks" between your computer and the internet, allowing you to see which servers are sending the most data (Bytes).
- **Advanced Filtering:** You used the right-click menu to **"Apply as Filter"** a specific stream (A <-> Any), which cleared out background noise to focus only on one connection.
- **Display Filters:** You successfully used filters like http and tcp.port == 80 to narrow down your search.

4. Technical Observations (Security Analysis)

Your capture caught several real-world networking behaviors:

- **TCP Health:** You observed **"TCP Dup ACK"** and **"TCP Retransmissions"**. In security, high rates of these can sometimes indicate a network attack or a very unstable connection.
- **Connection Reset:** You captured a **[RST, ACK]** packet (highlighted in red), showing a connection being abruptly terminated by the server.
- **Packet Structure:** You have generated visual maps of the **Ethernet, IP, and TCP headers**, showing exactly how data is "wrapped" before being sent over the wire.