

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.

Ethernet · 6 IPv4 · 79 IPv6 · 1 TCP · 65 UDP · 208									
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	

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==13.107.9.158 && tcp.port==443

No.	Time	Source	Destination	Protocol	Length	Info
824	17.508517	13.107.9.158	192.168.0.102	TCP	54	443 → 50281 [ACK] Seq=1 Ack=1 Win=16385 Len=0
825	17.508619	192.168.0.102	13.107.9.158	TCP	54	[TCP ACKed unseen segment] 50281 → 443 [ACK] Seq=1 Ack=2 Win=253 Len=0

Wireshark - Conversations - Wi-Fi

Conversation Settings

Name resolution
Absolute start time
Display raw data
Limit to display filter

Copy
Follow Stream...
Graph...
I/O Graphs

Protocol
Bluetooth
BIP7
DCCP
DNP 3.0
✓ Ethernet
FC
FDIO
IEEE 802.11
IEEE 802.15.4
ILNP
IPV4
✓ IPV6
IPX
JXTA
...
Filter list for specific type

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
4.213.25.242	443	192.168.0.102	51851	7	595 bytes	6	3	336 bytes	4	259 bytes	5.529203	59.7599
4.213.25.242	443	192.168.0.102	65091	6	324 bytes	31	4	216 bytes	2	108 bytes	29.479174	30.0353
13.107.9.158	443	192.168.0.102	50281	15	4 kB	18	9	1 kB	6	3 kB	17.508517	66.1118
20.44.229.37	443	192.168.0.102	50068	7	378 bytes	4	3	162 bytes	4	216 bytes	3.469016	57.4875
20.44.229.112	443	192.168.0.102	50064	5	270 bytes	9	3	162 bytes	2	108 bytes	9.520978	38.9293
20.44.229.112	443	192.168.0.102	59064	5	270 bytes	13	3	162 bytes	2	108 bytes	11.476605	35.5155
20.190.145.160	443	192.168.0.102	50067	5	270 bytes	14	2	108 bytes	3	162 bytes	13.434813	14.2477
20.190.146.37	443	192.168.0.102	50065	5	270 bytes	11	2	108 bytes	3	162 bytes	11.467434	19.5558
20.210.25.249	443	192.168.0.102	50066	6	324 bytes	12	3	162 bytes	3	162 bytes	11.467434	20.2974
35.186.224.35	443	192.168.0.102	52595	12	732 bytes	22	6	324 bytes	6	408 bytes	25.474213	60.7384
48.218.107.66	443	192.168.0.102	50229	9	589 bytes	8	5	316 bytes	4	273 bytes	9.520978	55.9719
74.126.68.188	5228	192.168.0.102	59468	8	458 bytes	17	4	240 bytes	4	218 bytes	15.499426	61.4527
104.26.10.240	443	192.168.0.102	57757	6	324 bytes	21	3	162 bytes	3	162 bytes	21.374712	60.1159
104.199.241.202	4070	192.168.0.102	52594	16	920 bytes	15	9	519 bytes	7	401 bytes	16.460649	60.2179
192.168.0.102	57234	18.136.147.197	443	29	9 kB	42	14	3 kB	15	6 kB	46.768630	3.4833
192.168.0.102	50814	20.189.173.28	443	23	12 kB	63	14	5 kB	9	7 kB	73.533759	0.7285
192.168.0.102	57034	20.190.145.160	443	43	35 kB	52	20	9 kB	23	26 kB	53.766063	29.6948
192.168.0.102	57035	20.190.175.24	443	19	9 kB	53	10	3 kB	9	6 kB	54.523933	28.9370
192.168.0.102	52017	20.195.65.193	443	26	2 kB	10	13	941 bytes	13	837 bytes	10.664977	67.8501
192.168.0.102	54971	20.249.168.239	443	15	1 kB	5	8	582 bytes	7	495 bytes	4.836805	80.1948
192.168.0.102	62630	35.186.224.22	443	14	4 kB	64	8	3 kB	6	1 kB	74.652613	0.9670
192.168.0.102	63865	35.186.224.35	443	18	1 kB	0	8	561 bytes	10	660 bytes	0.330057	60.4813
192.168.0.102	65483	40.79.141.154	443	51	18 kB	32	26	9 kB	25	9 kB	32.439102	31.2198
192.168.0.102	50813	52.168.117.168	443	23	11 kB	62	14	3 kB	9	7 kB	61.233970	1.0605
192.168.0.102	52831	52.200.104.237	443	2	132 bytes	19	2	132 bytes	0	0 bytes	18.354405	0.0003
192.168.0.102	50805	57.144.243.32	443	26	8 kB	33	14	4 kB	12	3 kB	36.560621	23.3818
192.168.0.102	62192	57.144.243.32	443	58	17 kB	7	26	4 kB	32	14 kB	6.270548	60.0216
192.168.0.102	51631	74.125.24.84	443	17	9 kB	37	9	2 kB	8	7 kB	46.145709	0.2942
192.168.0.102	63940	74.125.68.188	5228	5	283 bytes	16	3	163 bytes	2	120 bytes	13.894536	13.3314
192.168.0.102	51295	104.16.80.73	443	35	11 kB	59	19	5 kB	16	6 kB	56.005366	4.2805
192.168.0.102	55877	104.16.80.73	443	23	9 kB	60	10	4 kB	10	5 kB	57.228072	3.0521
192.168.0.102	63453	104.26.8.241	443	28	9 kB	39	15	3 kB	13	6 kB	46.743622	3.4325
192.168.0.102	60757	104.26.9.44	443	31	15 kB	48	14	3 kB	17	12 kB	47.052900	3.1236
192.168.0.102	50812	104.26.10.31	443	33	9 kB	61	17	3 kB	16	6 kB	57.531375	2.7546

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==13.107.9.158

No.	Time	Source	Destination	Protocol	Length	Info
824	17.508517	13.107.9.158	192.168.0.102	TCP	54	443 → 50281 [ACK] Seq=1 Ack=1 Win=16385 Len=0
825	17.508619	192.168.0.102	13.107.9.158	TCP	54	[TCP ACKed unseen segment] 50281 → 443 [ACK] Seq=1 Ack=2 Win=253 Len=0
871	18.325337	13.107.9.158	192.168.0.102	TCP	54	[TCP Previous segment not captured] 443 → 50281 [ACK] Seq=2 Ack=1 Win=16381 Len=0
905	18.755286	192.168.0.102	13.107.9.158	TCP	1494	50281 → 443 [ACK] Seq=1 Ack=2 Win=253 Len=1440 [TCP PDU reassembled in 906]
906	18.755286	192.168.0.102	13.107.9.158	TLSv1.2	854	Application Data
917	18.809499	13.107.9.158	192.168.0.102	TCP	54	443 → 50281 [ACK] Seq=2 Ack=2241 Win=16385 Len=0
918	18.827388	13.107.9.158	192.168.0.102	TLSv1.2	695	Application Data
919	18.877153	192.168.0.102	13.107.9.158	TCP	54	50281 → 443 [ACK] Seq=2241 Ack=643 Win=250 Len=0
2670	47.474640	192.168.0.102	13.107.9.158	TCP	54	443 → 50281 [ACK] Seq=1 Ack=2241 Win=16385 Len=0
2671	47.474976	192.168.0.102	13.107.9.158	TCP	54	[TCP Dup ACK 919#1] 50281 → 443 [ACK] Seq=2241 Ack=643 Win=250 Len=0
2672	47.523856	192.168.0.102	13.107.9.158	TCP	54	[TCP Dup ACK 917#1] 443 → 50281 [ACK] Seq=643 Ack=2241 Win=16385 Len=0
12268	77.506583	13.107.9.158	192.168.0.102	TCP	54	443 → 50281 [ACK] Seq=1 Ack=2241 Win=16385 Len=0
12269	77.506660	192.168.0.102	13.107.9.158	TCP	54	[TCP Dup ACK 919#2] 50281 → 443 [ACK] Seq=2241 Ack=643 Win=250 Len=0
12272	77.554658	13.107.9.158	192.168.0.102	TCP	54	[TCP Dup ACK 917#2] 443 → 50281 [ACK] Seq=643 Ack=2241 Win=16385 Len=0
13390	83.620336	13.107.9.158	192.168.0.102	TCP	54	443 → 50281 [RST, ACK] Seq=643 Ack=2241 Win=0 Len=0

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

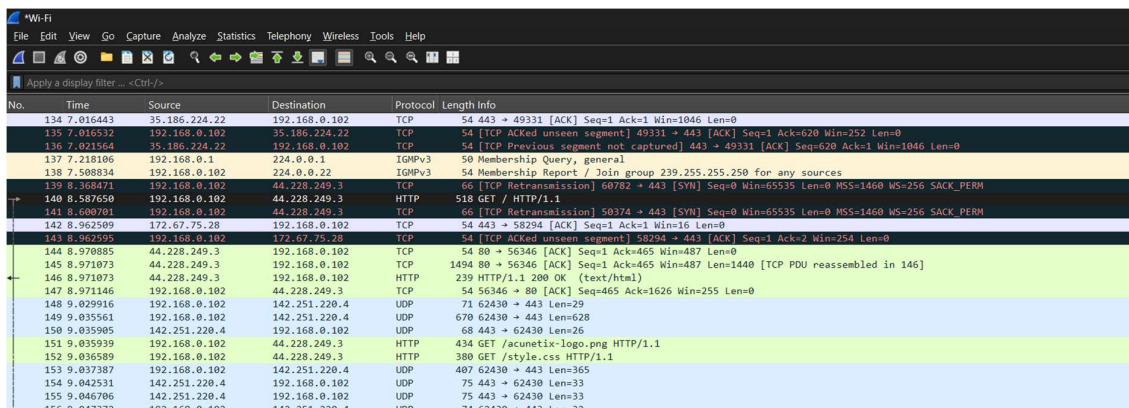
The packet list reveals several technical details about the health and status of your TCP connections:

- **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:



The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for file operations, capture control, and analysis. A filter bar at the top of the packet list shows the active filter: `Apply a display filter ... <Ctrl-/>`.

The packet list table displays the following data:

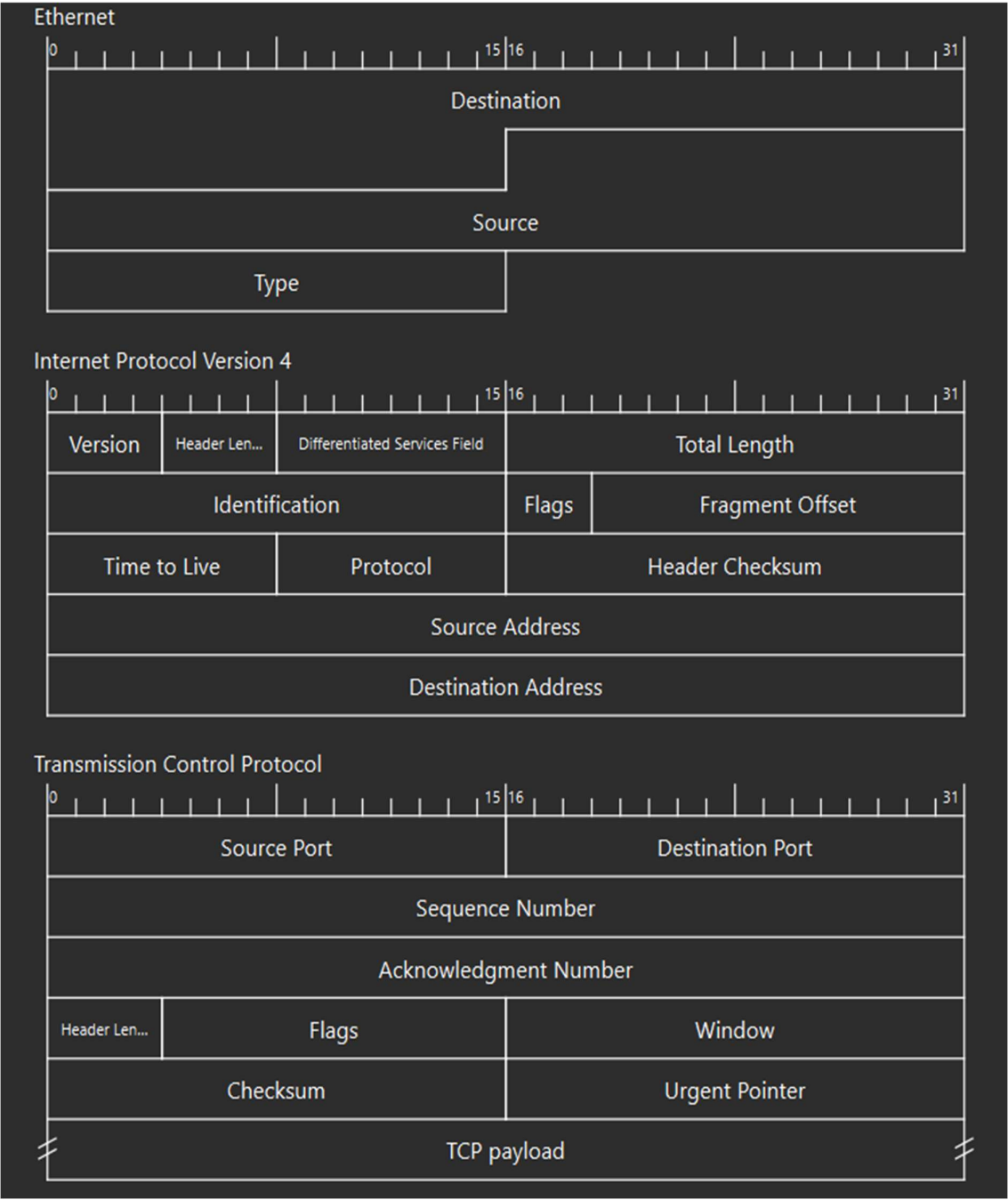
No.	Time	Source	Destination	Protocol	Length	Info
134	7.016443	35.186.224.22	192.168.0.102	TCP	54	443 → 49331 [ACK] Seq=1 Ack=1 Win=1046 Len=0
135	7.016532	192.168.0.102	35.186.224.22	TCP	54	[TCP ACKed unseen segment] 49331 → 443 [ACK] Seq=1 Ack=620 Win=252 Len=0
136	7.021564	35.186.224.22	192.168.0.102	TCP	54	[TCP Previous segment not captured] 443 → 49331 [ACK] Seq=620 Ack=1 Win=1046 Len=0
137	7.218106	192.168.0.1	224.0.0.1	IGMPv3	50	Membership Query, general
138	7.508834	192.168.0.102	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
139	8.368471	192.168.0.102	44.228.249.3	TCP	66	[TCP Retransmission] 60782 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
140	8.587650	192.168.0.102	44.228.249.3	HTTP	518	GET / HTTP/1.1
141	8.600761	192.168.0.102	44.228.249.3	TCP	66	[TCP Retransmission] 50274 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
142	8.962509	172.67.75.28	192.168.0.102	TCP	54	443 → 58294 [ACK] Seq=1 Ack=1 Win=16 Len=0
143	8.962595	192.168.0.102	172.67.75.28	TCP	54	[TCP ACKed unseen segment] 58294 → 443 [ACK] Seq=1 Ack=2 Win=254 Len=0
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
148	9.029916	192.168.0.102	142.251.220.4	UDP	71	62430 → 443 Len=29
149	9.035561	192.168.0.102	142.251.220.4	UDP	670	62430 → 443 Len=628
150	9.035905	142.251.220.4	192.168.0.102	UDP	68	443 → 62430 Len=26
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
153	9.037387	192.168.0.102	142.251.220.4	UDP	407	62430 → 443 Len=365
154	9.042531	142.251.220.4	192.168.0.102	UDP	75	443 → 62430 Len=33
155	9.046706	142.251.220.4	192.168.0.102	UDP	75	443 → 62430 Len=33
156	9.047372	192.168.0.102	142.251.220.4	UDP	74	62430 → 443 Len=32

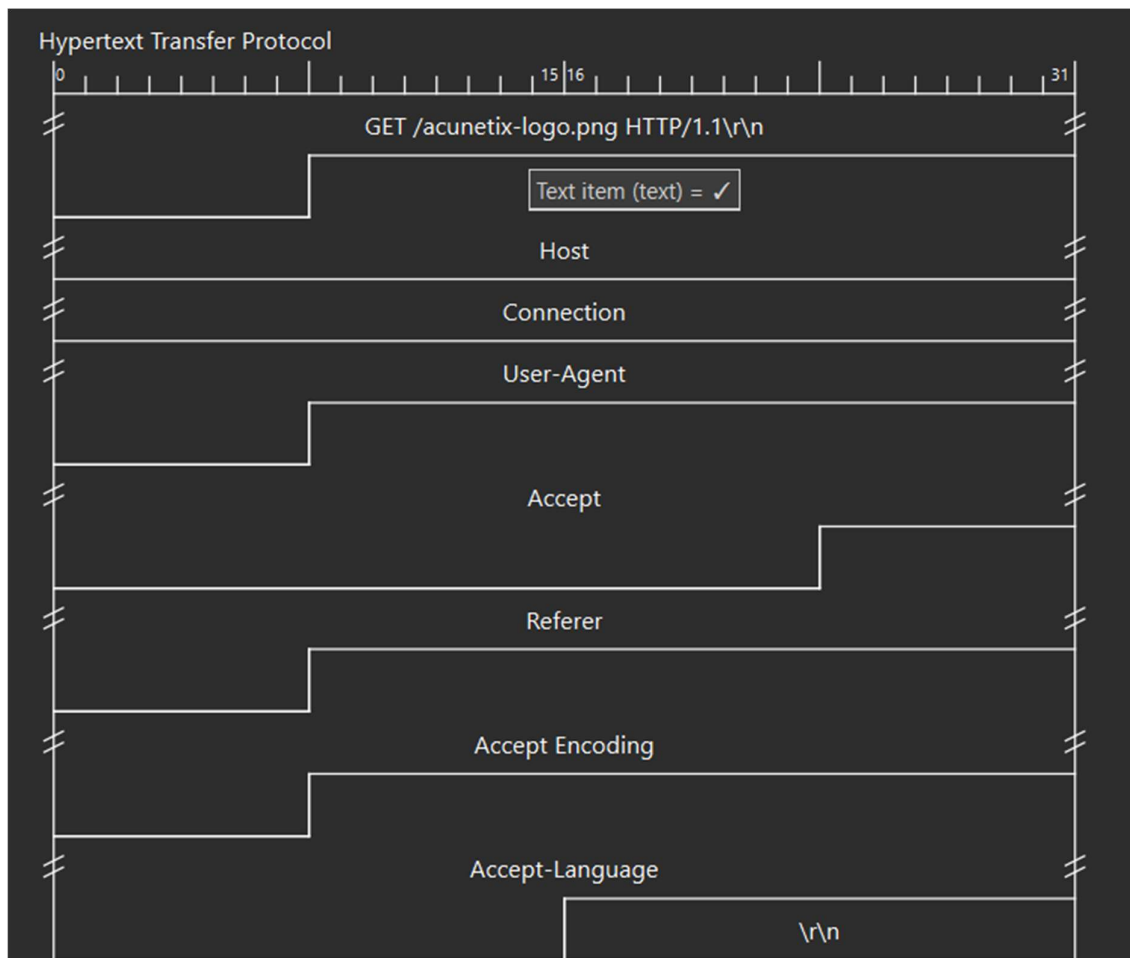
*Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length Info	
140	8.587650	192.168.0.102	44.228.249.3	HTTP	518	GET / HTTP/1.1
146	8.971073	44.228.249.3	192.168.0.102	HTTP	239	HTTP/1.1 200 OK (text/html)
151	9.035939	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/sockjs.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-68B9-49B7-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	9.071146	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 && !ip.in [ospf] bgp tcp.port == 179)) (ip.dst == 224.0.0.0/4 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !ip.in [ospf] bgp tcp.port == 179))
✓ IPv6 hop limit low or unexpected	(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !ip.in [ospf] bgp tcp.port == 179)) (ipv6.dst == ff00::/8 && ipv6.hlim not in { 1, 64, 255 })
✓ Checksum Errors	eth.fcsh.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.