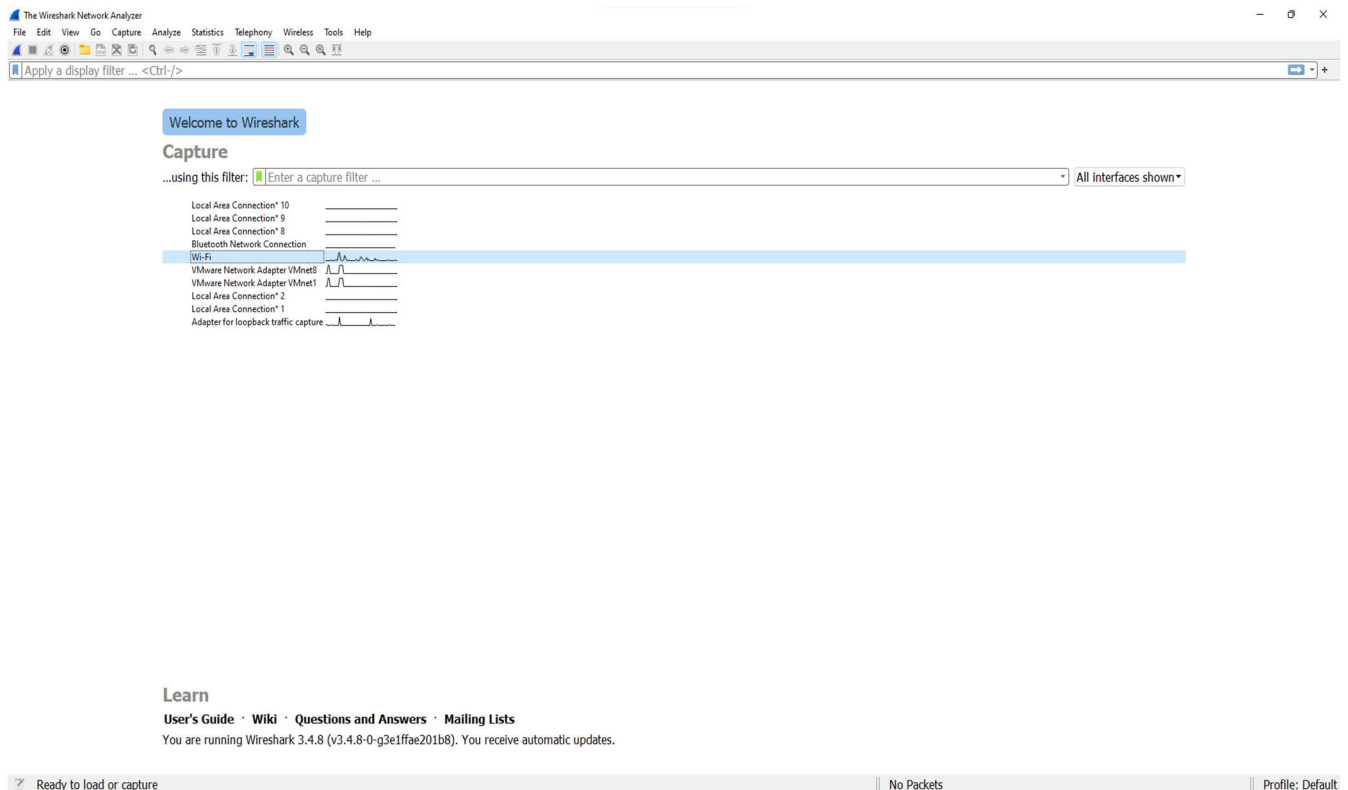


Packet Capture using Wireshark

This is a project where I captured the packets using Wireshark and analyzed different protocols. At the end of this project, I entered my **credentials** in a testing website which uses http protocol and captured that packet to **reveal** the entered credentials. I have analyzed captured packets, packet details and bytes.

Picking correct interface from all the interfaces available in Wireshark. I selected Wi-Fi



Applying a display filter ... <Ctrl-/>
+

No.	Time	Source	Destination	Protocol	Length	Info
93	8.739315	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
94	9.540401	54.147.21.139	192.168.1.69	TCP	56	443 → 64107 [ACK] Seq=1 Ack=1 Win=0 Len=0
95	9.540464	192.168.1.69	54.147.21.139	TCP	54	[TCP ACKed unseen segment] 64107 → 443 [ACK] Seq=1 Ack=2 Win=513 Len=0
96	9.733753	192.168.1.69	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _companion-link_tcp.local, "QI" question PTR _homekit_tcp.local, "QI" question PTR _sleep-proxy_udp.local, "QI" question OPT
97	9.733753	f680:c58:cl3a:fc6a::f802::fb	224.0.0.251	MDNS	174	Standard query 0x0000 PTR _companion-link_tcp.local, "QI" question PTR _homekit_tcp.local, "QI" question PTR _sleep-proxy_udp.local, "QI" question OPT
98	9.760772	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
99	11.051954	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
100	11.972802	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
101	12.740797	192.168.1.69	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _companion-link_tcp.local, "QI" question PTR _homekit_tcp.local, "QI" question PTR _sleep-proxy_udp.local, "QI" question OPT
102	12.740757	f680:c58:cl3a:fc6a::f802::fb	224.0.0.251	MDNS	174	Standard query 0x0000 PTR _companion-link_tcp.local, "QI" question PTR _homekit_tcp.local, "QI" question PTR _sleep-proxy_udp.local, "QI" question OPT
103	12.895251	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
104	14.124145	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
105	15.040420	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
106	15.067708	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
107	16.543364	2600:1700:1166:3600::2603:1036:2407:1::17	TSv1.2	102	Application Data	
108	16.596897	2603:1036:2407:1::17	2600:1700:1166:3600::	TCP	74	443 → 64649 [ACK] Seq=1 Ack=29 Win=2050 Len=0
109	16.621367	2600:1700:1166:3600::2603:1036:2407:1::17	TSv1.2	102	Application Data	
110	16.674331	2603:1036:2407:1::17	2600:1700:1166:3600::	TCP	74	443 → 64650 [ACK] Seq=1 Ack=29 Win=2051 Len=0
111	17.199139	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
112	17.197919	2600:1700:1166:3600::2607:f8b0:4023:1002::	TCP	75	64906 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]	
113	17.202879	2607:f8b0:4023:1002::2600:1700:1166:3600::	TCP	86	443 → 64906 [ACK] Seq=1 Ack=2 Min=285 Len=0 SLE=1 SRE=2	
114	17.185734	2600:1700:1166:3600::2600:1404:c00:111::	TCP	75	64879 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]	
115	17.189802	2600:1404:c00:111::2600:1700:1166:3600::	TCP	86	443 → 64879 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2	
116	18.123201	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
117	18.041507	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
118	20.279553	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
119	21.045971	192.168.1.69	20.10.31.115	TCP	55	64458 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
120	21.092408	20.10.31.115	192.168.1.69	TCP	66	443 → 64455 [ACK] Seq=1 Ack=1 Win=7873 Len=0 SLE=1 SRE=2
121	21.105995	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II
122	22.111383	NokiaSol_F4:31:48	Broadcast	0x7373	121	Ethernet II

> Frame 1: 253 bytes on wire (2024 bits), 253 bytes captured (2024 bits) on interface Device\NPF_{F4F53B05-480B-431F-AF49-66A409E8FAF4}, id 0

> Ethernet II, Src: 1a:9c:12:7b:b9:b2c (1a:9c:12:7b:b9:b2c), Dst: IPV4cast_fb (01:00:5e:00:00:00:fb)

> Internet Protocol Version 4, Src: 192.168.1.98, Dest: 224.0.0.251

> User Datagram Protocol, Src Port: 5353, Dst Port: 5353

> Multicast Domain Name System (query)

[Community ID: 1:3E5bWp560Lq7p9b0cziTaaI2Pbcv]

```

0000  01 00 5e 00 00 00 fb 1a 9c 02 7b b9 b2 c0 00 00 45 00  ---.....f---E-
0010  00 ef fd 77 00 00 ff 11 3c 80 c0 a8 01 62 e0 00 00  ---.....b---
0020  00 0f 14 e9 14 e9 00 db 50 02 00 00 00 00 00 00 02  ---.....
0030  00 00 00 00 00 01 0a 
```

```

C:\Users\tiwar>ipconfig /all

Connection-specific DNS Suffix . : attlocal.net
IPv6 Address. . . . . : 2600:1700:11e6:3600::20
IPv6 Address. . . . . : 2600:1700:11e6:3600:6dd6:158d:c166:a65e
Temporary IPv6 Address. . . . . : 2600:1700:11e6:3600:9125:be40:1da:2e77
Link-local IPv6 Address . . . . . : fe80::bddd:13d1:166:a65e%21
IPv4 Address. . . . . : 192.168.1.69
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::3aa0:67ff:fef4:3142%21
                          192.168.1.254

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\tiwar>ping 192.168.1.69

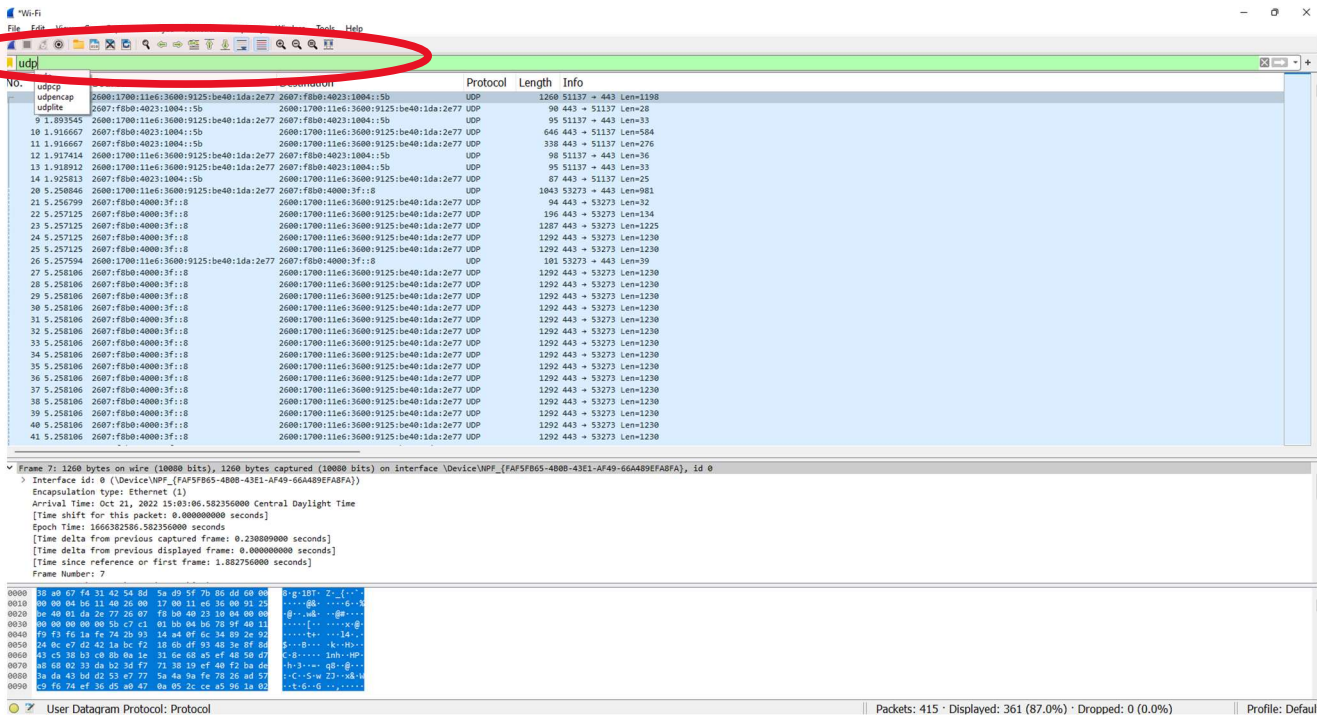
Pinging 192.168.1.69 with 32 bytes of data:
Reply from 192.168.1.69: bytes=32 time<1ms TTL=128
Reply from 192.168.1.69: bytes=32 time<1ms TTL=128
Reply from 192.168.1.69: bytes=32 time<1ms TTL=128
Reply from 192.168.1.69: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\tiwar>

```

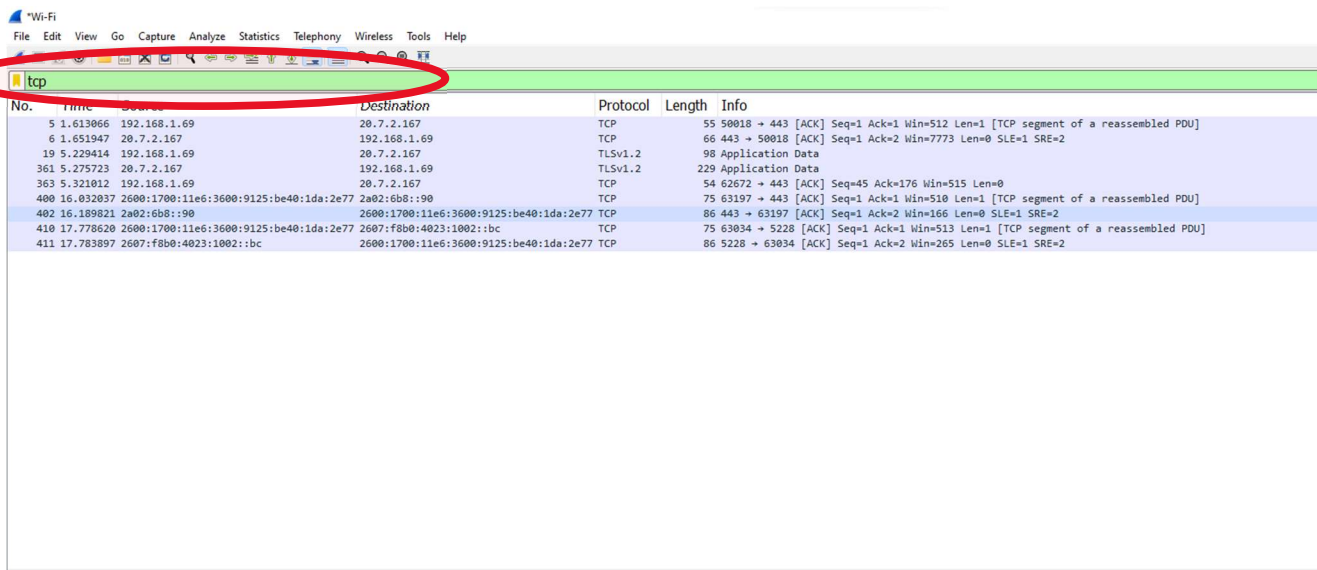

Observing UDP Protocols by applying a display filter



The screenshot shows the Wireshark network protocol analyzer interface. The top toolbar contains various icons for file operations, capture, analysis, and display. A red circle highlights the 'Display Filter' field, which contains the filter 'udp'. Below the filter, the packet list pane shows a list of captured packets, with the first packet (No. 1) selected. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane shows the raw data of the selected packet.

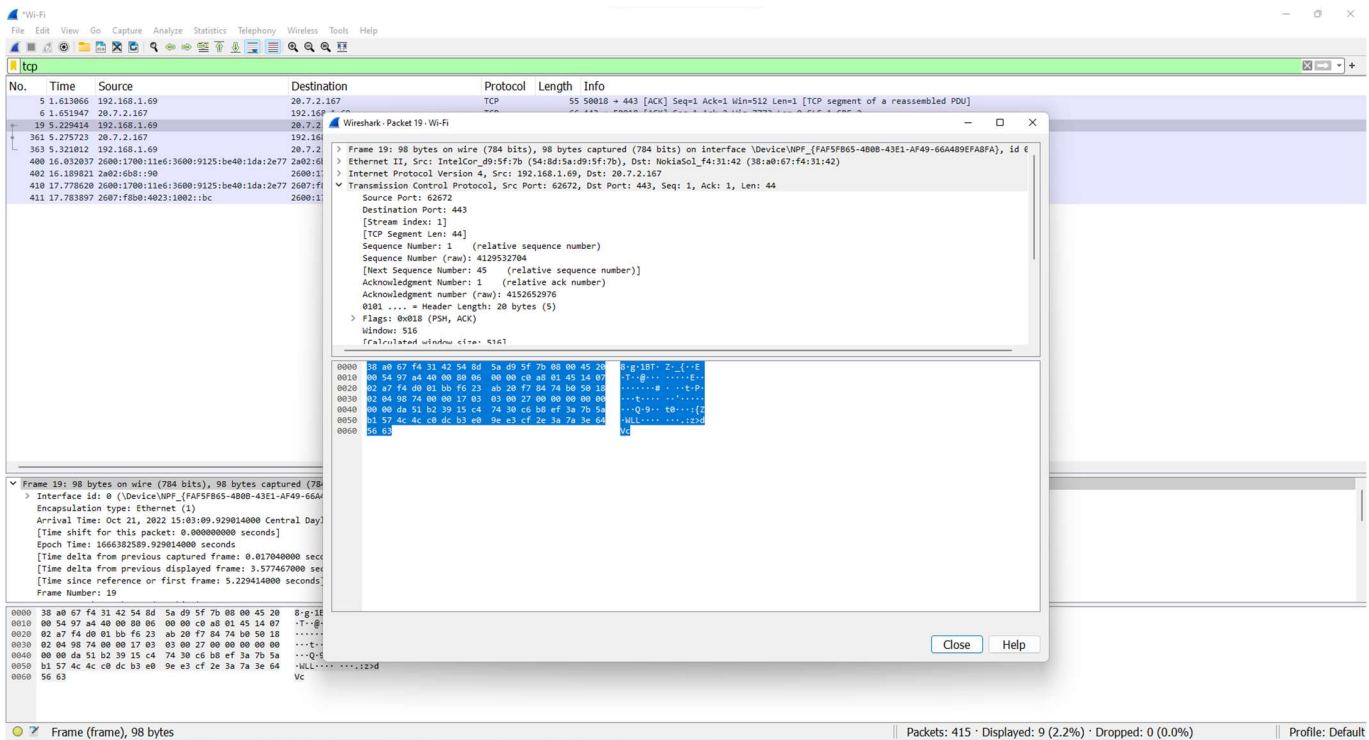
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	192.168.1.102	UDP	1260	51137 → 443 Len=1198
2	0.000000	192.168.1.101	192.168.1.102	UDP	90	443 → 51137 Len=28
3	0.000000	192.168.1.101	192.168.1.102	UDP	95	51137 → 443 Len=33
4	0.000000	192.168.1.101	192.168.1.102	UDP	646	443 → 51137 Len=584
5	0.000000	192.168.1.101	192.168.1.102	UDP	338	443 → 51137 Len=276
6	0.000000	192.168.1.101	192.168.1.102	UDP	98	51137 → 443 Len=36
7	0.000000	192.168.1.101	192.168.1.102	UDP	95	51137 → 443 Len=33
8	0.000000	192.168.1.101	192.168.1.102	UDP	87	443 → 51137 Len=25
9	0.000000	192.168.1.101	192.168.1.102	UDP	1063	53273 → 443 Len=981
10	0.000000	192.168.1.101	192.168.1.102	UDP	94	443 → 53273 Len=32
11	0.000000	192.168.1.101	192.168.1.102	UDP	196	443 → 53273 Len=134
12	0.000000	192.168.1.101	192.168.1.102	UDP	1287	443 → 53273 Len=1225
13	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
14	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
15	0.000000	192.168.1.101	192.168.1.102	UDP	101	53273 → 443 Len=39
16	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
17	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
18	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
19	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
20	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
21	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
22	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
23	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
24	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
25	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
26	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
27	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
28	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
29	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
30	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
31	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
32	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
33	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
34	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
35	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
36	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
37	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
38	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
39	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
40	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230
41	0.000000	192.168.1.101	192.168.1.102	UDP	1292	443 → 53273 Len=1230

Observing TCP Protocols by applying filters

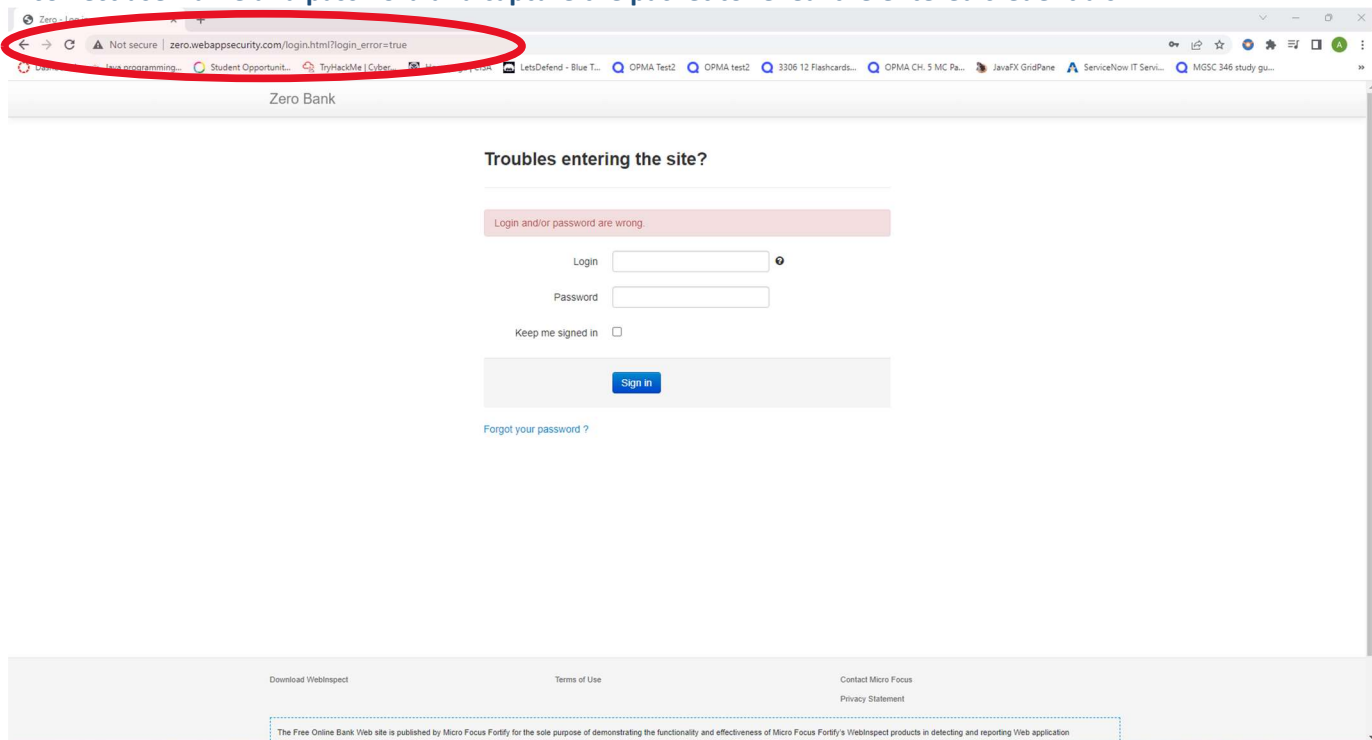


The screenshot shows the Wireshark network protocol analyzer interface. The top toolbar contains various icons for file operations, capture, analysis, and display. A red circle highlights the 'Display Filter' field, which contains the filter 'tcp'. Below the filter, the packet list pane shows a list of captured packets, with the first packet (No. 1) selected. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	5.1613066	192.168.1.69	20.7.2.167	TCP	55	50018 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
2	6.1651947	20.7.2.167	192.168.1.69	TCP	66	443 → 50018 [ACK] Seq=1 Ack=2 Win=7773 Len=0 SLE=1 SRE=2
3	5.229414	192.168.1.69	20.7.2.167	TLSv1.2	98	Application Data
4	5.275723	20.7.2.167	192.168.1.69	TLSv1.2	229	Application Data
5	5.321012	192.168.1.69	20.7.2.167	TCP	54	62672 → 443 [ACK] Seq=45 Ack=176 Win=515 Len=0
6	15.032837	2600:1700:11e6:3600:9125:be40:1da:2e77	2a02:b80::90	TCP	75	63157 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
7	16.189021	2a02:b80::90	2600:1700:11e6:3600:9125:be40:1da:2e77	TCP	86	443 → 63197 [ACK] Seq=1 Ack=2 Win=166 Len=0 SLE=1 SRE=2
8	17.778620	2600:1700:11e6:3600:9125:be40:1da:2e77	2607:f8b0:4023:1002:1bc	TCP	75	63034 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
9	17.783897	2607:f8b0:4023:1002:1bc	2600:1700:11e6:3600:9125:be40:1da:2e77	TCP	86	5228 → 63034 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2



Logging in to **zero.webappsecurity.com**. This website uses http protocol which is not secure. I will try to login with the incorrect username and password and capture the packet to reveal the entered credentials.



Apply http only filter to see the http packets

Wireshark interface showing an HTTP filter applied to the packet list. The filter is `http`. The packet list shows various HTTP GET requests. The packet details pane shows the structure of an HTTP packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data of the selected packet.

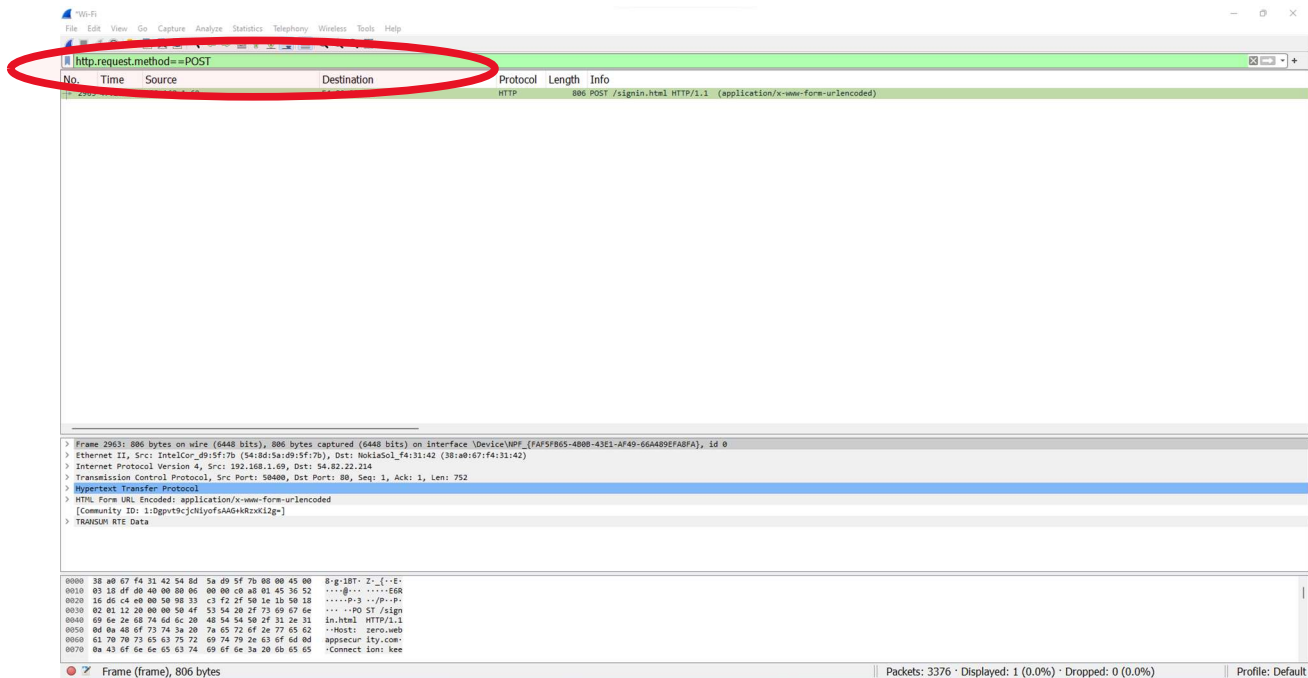
No.	Time	Source	Destination	Protocol	Length	Info
1199	29.413780	192.168.1.69	54.82.22.214	HTTP	1199	HTTP/1.1 200 OK (text/html)
418	29.420294	192.168.1.69	54.82.22.214	HTTP	418	GET /resources/css/bootstrap.min.css HTTP/1.1
417	29.468797	192.168.1.69	54.82.22.214	HTTP	417	GET /resources/css/font-awesome.css HTTP/1.1
409	29.468799	192.168.1.69	54.82.22.214	HTTP	409	GET /resources/css/main.css HTTP/1.1
404	29.468802	192.168.1.69	54.82.22.214	HTTP	404	GET /resources/js/jquery-1.8.2.min.js HTTP/1.1
401	29.468805	192.168.1.69	54.82.22.214	HTTP	401	GET /resources/js/bootstrap.min.js HTTP/1.1
404	29.471349	54.82.22.214	192.168.1.69	HTTP	404	GET /resources/js/placeholders.min.js HTTP/1.1
232	29.503339	54.82.22.214	192.168.1.69	HTTP	232	HTTP/1.1 200 OK (text/css)
340	29.511758	54.82.22.214	192.168.1.69	HTTP	340	HTTP/1.1 200 OK (text/css)
845	29.514172	54.82.22.214	192.168.1.69	HTTP	845	HTTP/1.1 200 OK (text/css)
651	29.541372	54.82.22.214	192.168.1.69	HTTP	651	HTTP/1.1 200 OK (application/javascript)
266	29.548184	54.82.22.214	192.168.1.69	HTTP	266	HTTP/1.1 200 OK (application/javascript)
466	29.552365	192.168.1.69	54.82.22.214	HTTP	466	GET /resources/img/main_carousel_1.jpg HTTP/1.1
349	29.595262	54.82.22.214	192.168.1.69	HTTP	349	HTTP/1.1 200 OK (application/javascript)
466	29.598855	192.168.1.69	54.82.22.214	HTTP	466	GET /resources/img/main_carousel_2.jpg HTTP/1.1
466	29.608681	192.168.1.69	54.82.22.214	HTTP	466	GET /resources/img/main_carousel_3.jpg HTTP/1.1
489	29.648825	192.168.1.69	54.82.22.214	HTTP	489	GET /resources/font/fontawesome-webfont.woff?v=3.0.1 HTTP/1.1
797	29.702041	54.82.22.214	192.168.1.69	HTTP	797	HTTP/1.1 200 OK (image/jpeg)
659	29.715472	54.82.22.214	192.168.1.69	HTTP	659	HTTP/1.1 200 OK (image/jpeg)
1252	29.761322	54.82.22.214	192.168.1.69	HTTP	1252	HTTP/1.1 200 OK (application/x-font-woff)
1213	29.797047	54.82.22.214	192.168.1.69	HTTP	1213	HTTP/1.1 200 OK (image/jpeg)
444	29.812750	192.168.1.69	54.82.22.214	HTTP	444	GET /favicon.ico HTTP/1.1
1312	29.853543	54.82.22.214	192.168.1.69	HTTP	1312	HTTP/1.1 404 Not Found (text/html)
544	29.7162843	192.168.1.69	54.82.22.214	HTTP	544	GET /login.html HTTP/1.1
410	29.7162843	192.168.1.69	54.82.22.214	HTTP	410	HTTP/1.1 200 OK (text/html)
806	29.724090	54.82.22.214	192.168.1.69	HTTP	806	POST /signin.html HTTP/1.1 (application/x-www-form-urlencoded)
426	29.724090	54.82.22.214	192.168.1.69	HTTP	426	HTTP/1.1 302 Found
626	29.724090	54.82.22.214	192.168.1.69	HTTP	626	GET /login.html?login_error=true HTTP/1.1
546	29.724090	54.82.22.214	192.168.1.69	HTTP	546	HTTP/1.1 200 OK (text/html)
468	29.724090	54.82.22.214	192.168.1.69	HTTP	468	HTTP/1.1 408 Request Time-out (text/html)

To view the credentials entered in the insecure website, look for POST method in Info column.

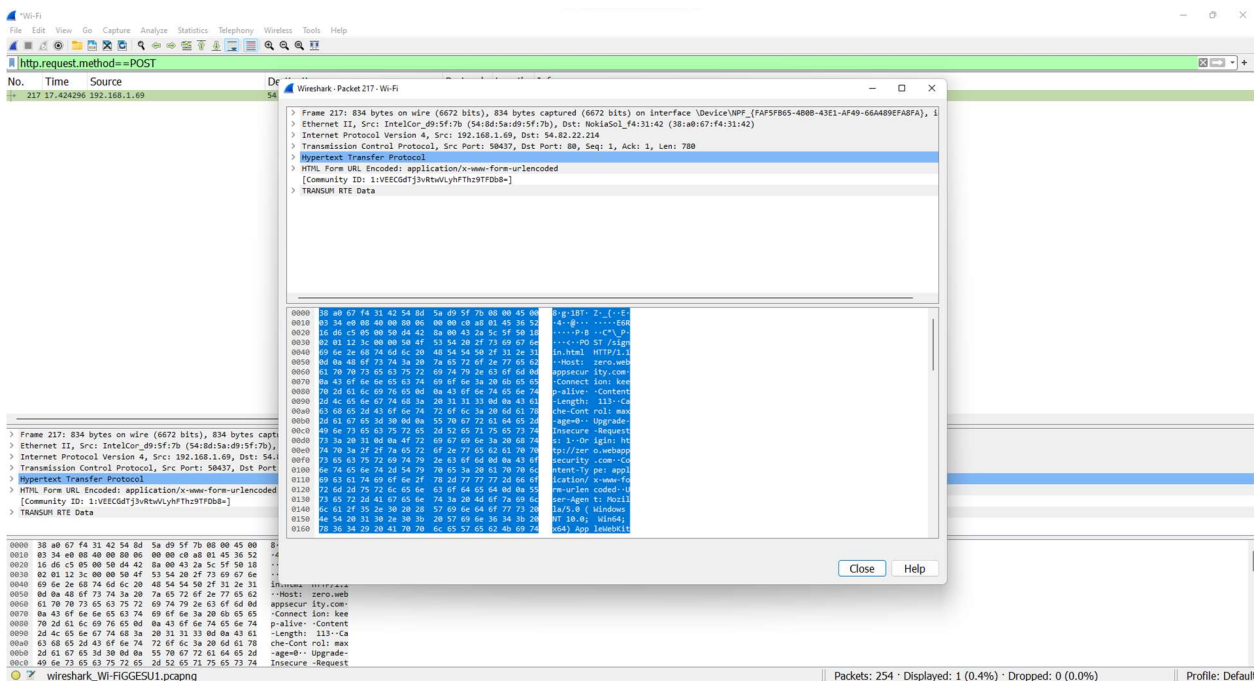
Wireshark interface showing an HTTP filter applied to the packet list. The filter is `http`. The packet list shows various HTTP GET requests. The packet details pane shows the structure of an HTTP packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1199	29.413780	192.168.1.69	54.82.22.214	HTTP	1199	HTTP/1.1 200 OK (text/html)
418	29.420294	192.168.1.69	54.82.22.214	HTTP	418	GET /resources/css/bootstrap.min.css HTTP/1.1
417	29.468797	192.168.1.69	54.82.22.214	HTTP	417	GET /resources/css/font-awesome.css HTTP/1.1
409	29.468799	192.168.1.69	54.82.22.214	HTTP	409	GET /resources/css/main.css HTTP/1.1
404	29.468802	192.168.1.69	54.82.22.214	HTTP	404	GET /resources/js/jquery-1.8.2.min.js HTTP/1.1
401	29.468805	192.168.1.69	54.82.22.214	HTTP	401	GET /resources/js/bootstrap.min.js HTTP/1.1
404	29.471349	54.82.22.214	192.168.1.69	HTTP	404	GET /resources/js/placeholders.min.js HTTP/1.1
232	29.503339	54.82.22.214	192.168.1.69	HTTP	232	HTTP/1.1 200 OK (text/css)
340	29.511758	54.82.22.214	192.168.1.69	HTTP	340	HTTP/1.1 200 OK (text/css)
845	29.514172	54.82.22.214	192.168.1.69	HTTP	845	HTTP/1.1 200 OK (text/css)
651	29.541372	54.82.22.214	192.168.1.69	HTTP	651	HTTP/1.1 200 OK (application/javascript)
266	29.548184	54.82.22.214	192.168.1.69	HTTP	266	HTTP/1.1 200 OK (application/javascript)
466	29.552365	192.168.1.69	54.82.22.214	HTTP	466	GET /resources/img/main_carousel_1.jpg HTTP/1.1
349	29.595262	54.82.22.214	192.168.1.69	HTTP	349	HTTP/1.1 200 OK (application/javascript)
466	29.598855	192.168.1.69	54.82.22.214	HTTP	466	GET /resources/img/main_carousel_2.jpg HTTP/1.1
466	29.608681	192.168.1.69	54.82.22.214	HTTP	466	GET /resources/img/main_carousel_3.jpg HTTP/1.1
489	29.648825	192.168.1.69	54.82.22.214	HTTP	489	GET /resources/font/fontawesome-webfont.woff?v=3.0.1 HTTP/1.1
797	29.702041	54.82.22.214	192.168.1.69	HTTP	797	HTTP/1.1 200 OK (image/jpeg)
659	29.715472	54.82.22.214	192.168.1.69	HTTP	659	HTTP/1.1 200 OK (image/jpeg)
1252	29.761322	54.82.22.214	192.168.1.69	HTTP	1252	HTTP/1.1 200 OK (application/x-font-woff)
1213	29.797047	54.82.22.214	192.168.1.69	HTTP	1213	HTTP/1.1 200 OK (image/jpeg)
444	29.812750	192.168.1.69	54.82.22.214	HTTP	444	GET /favicon.ico HTTP/1.1
1312	29.853543	54.82.22.214	192.168.1.69	HTTP	1312	HTTP/1.1 404 Not Found (text/html)
544	29.7162843	192.168.1.69	54.82.22.214	HTTP	544	GET /login.html HTTP/1.1
410	29.7162843	192.168.1.69	54.82.22.214	HTTP	410	HTTP/1.1 200 OK (text/html)
806	29.724090	54.82.22.214	192.168.1.69	HTTP	806	POST /signin.html HTTP/1.1 (application/x-www-form-urlencoded)
426	29.724090	54.82.22.214	192.168.1.69	HTTP	426	HTTP/1.1 302 Found
626	29.724090	54.82.22.214	192.168.1.69	HTTP	626	GET /login.html?login_error=true HTTP/1.1
546	29.724090	54.82.22.214	192.168.1.69	HTTP	546	HTTP/1.1 200 OK (text/html)
468	29.724090	54.82.22.214	192.168.1.69	HTTP	468	HTTP/1.1 408 Request Time-out (text/html)

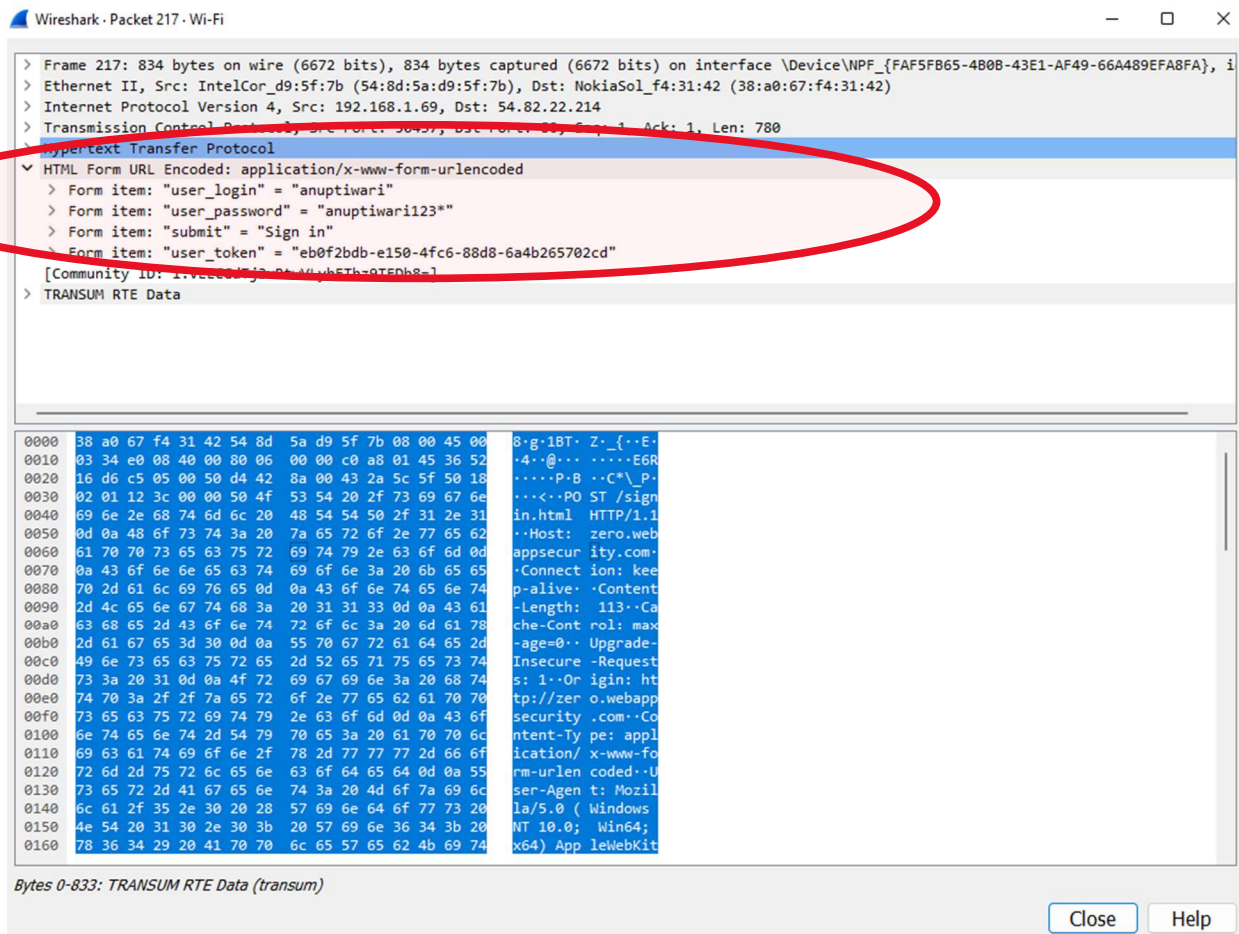
It can also be searched by typing `http.request.method==POST`



Clicking on the packet details to see more information about the http packet.



Clicking on HTML form URL to see the credentials entered in the insecure website.



Right click on POST method and click on Follow TCP or Http to see more detailed information.

