

1/

No.	Time	Source	Destination	Protocol	Length	Info
3009	11.630367	213.179.202.16	192.168.2.26	UDP	1225	50004 → 62092 Len=1183
3010	11.640365	213.179.202.16	192.168.2.26	UDP	1225	50004 → 62092 Len=1183
3011	11.641918	128.119.245.12	192.168.2.26	TCP	66	80 → 49691 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM=1 WS=128
3012	11.642006	192.168.2.26	128.119.245.12	TCP	54	49691 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
3013	11.643924	128.119.245.12	192.168.2.26	TCP	54	80 → 49735 [ACK] Seq=1 Ack=491 Win=30336 Len=0
3014	11.645552	128.119.245.12	192.168.2.26	HTTP	492	HTTP/1.1 200 OK (text/html)
3015	11.646323	213.179.202.16	192.168.2.26	UDP	1225	50004 → 62092 Len=1183
3016	11.653445	213.179.202.16	192.168.2.26	UDP	1225	50004 → 62092 Len=1183
3017	11.655846	192.168.2.26	213.179.202.16	UDP	94	62092 → 50004 Len=52
3018	11.659522	213.179.202.16	192.168.2.26	UDP	1225	50004 → 62092 Len=1183
3019	11.663524	213.179.202.16	192.168.2.26	UDP	1225	50004 → 62092 Len=1183
3020	11.663772	192.168.2.26	13.78.111.198	TCP	54	63615 → 443 [ACK] Seq=65752 Ack=11701 Win=131072 Len=0

> Frame 3014: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
> Ethernet II, Src: zte_23:91:50 (38:54:9b:23:91:50), Dst: AzureWav_e2:39:db (ec:2e:98:e2:39:db)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.26
> Transmission Control Protocol, Src Port: 80, Dst Port: 49735, Seq: 1, Ack: 491, Len: 438
> Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
<html>\n
Congratulations! You've downloaded the first Wireshark lab file!\n
</html>\n

3 different protocols: HTTP, TCP, UDP

2/ To get a clearer view, we get only the http filter:

No.	Time	Source	Destination	Protocol	Length	Info
225	2021-10-22 22:59:11.453238	192.168.2.26	128.119.245.12	HTTP	535	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
242	2021-10-22 22:59:11.712874	128.119.245.12	192.168.2.26	HTTP	492	HTTP/1.1 200 OK (text/html)

Time: 22:59:11.712874 - 22:59:11.453238 = 0.259 s

3/ the **gaia.cs.umass.edu** address is: 128.119.245.12

My computer's Internet address: 192.168.2.26

4/ First HTTP GET information:

C:\Users\ASUS\AppData\Local\Temp\wireshark_Wi-FiFRQ4B1.pcapng 347 total packets, 2 shown

No.	Time	Source	Destination	Protocol	Length	Info
225	2021-10-22 22:59:11.453238	192.168.2.26	128.119.245.12	HTTP	535	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 225: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
Ethernet II, Src: AzureWav_e2:39:db (ec:2e:98:e2:39:db), Dst: zte_23:91:50 (38:54:9b:23:91:50)
Internet Protocol Version 4, Src: 192.168.2.26, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 65173, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
Hypertext Transfer Protocol

Second HTTP information:

No.	Time	Source	Destination	Protocol	Length	Info
242	2021-10-22 22:59:11.712874	128.119.245.12	192.168.2.26	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 242: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
Ethernet II, Src: zte_23:90:31 (38:54:9b:23:90:31), Dst: AzureWav_e2:39:db (ec:2e:98:e2:39:db)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.26
Transmission Control Protocol, Src Port: 80, Dst Port: 65173, Seq: 1, Ack: 482, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
<html>\n
Congratulations! You've downloaded the first Wireshark lab file!\n
</html>\n