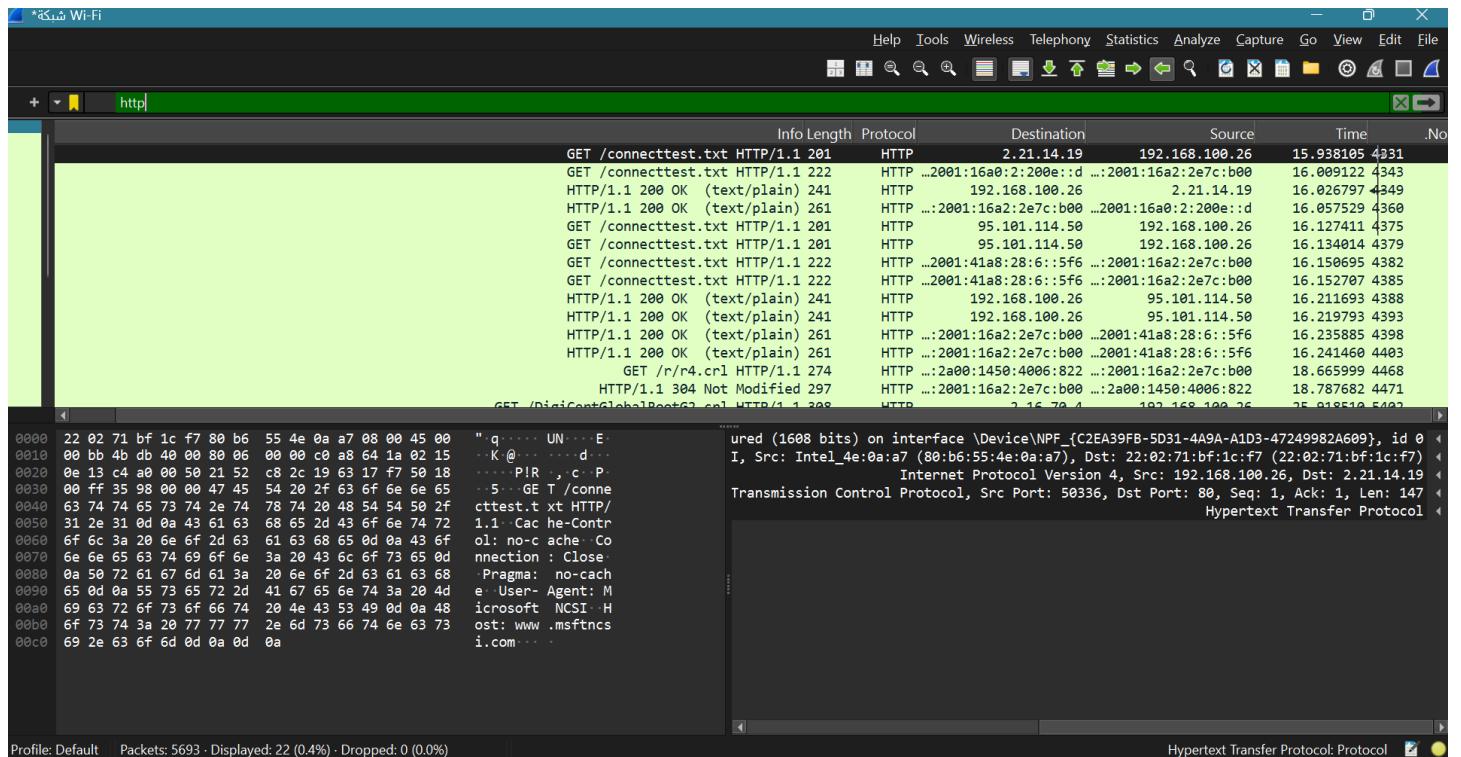


LAB1 - the internet protocol

Capturing HTTP Traffic

Shows the complete packet capture in Wireshark after stopping the traffic from the URL, including all protocols observed during the session.



HTTP Stream Analysis

Shows the result of using **Follow → HTTP Stream**, displaying the complete HTTP communication between the client and server, including request and response messages.

```
GET /connecttest.txt HTTP/1.1
Cache-Control: no-cache
Connection: Close
Pragma: no-cache
User-Agent: Microsoft NCSI
Host: www.msftncsi.com
```

```
HTTP/1.1 200 OK
Content-Length: 22
Date: Sun, 08 Feb 2026 13:47:59 GMT
Connection: close
Content-Type: text/plain
Cache-Control: max-age=30, must-revalidate
```

Microsoft Connect Test

HTTP Protocol Details

Displays the **Hypertext Transfer Protocol** section expanded, showing HTTP request and response details such as method, host, and status code.

```
Hypertext Transfer Protocol ▾
HTTP/1.1 200 OK\r\n
Content-Length: 22\r\n
Date: Sun, 08 Feb 2026 13:47:59 GMT\r\n
Connection: close\r\n
Content-Type: text/plain\r\n
Cache-Control: max-age=30, must-revalidate\r\n
r\n
[Request in frame: 4375]
[Time since request: 84.282000 milliseconds]
[Request URI: /connecttest.txt]
[Full request URI: http://www.msftncsi.com/connecttest.txt]
File Data: 22 bytes
```

TCP Packet Filtering

Shows Wireshark with the tcpdisplay filter applied, isolating TCP packets for connection analysis.

Wi-Fi

tcp

	Info	Length	Protocol	Destination	Source	Time	No
Seq=149 Ack=189 Win=65280 Len=0 [FIN, ACK] 80 → 50337 74	TCP ...:2001:16a0:2:200e::d ...:2001:16a2:2e7c:b00	16.057690 4363					
Seq=0 Win=65535 Len=0 MSS=1432 WS=256 SACK_PERM [SYN] 80 → 50341 86	TCP ...:2001:41a8:28:6::5f6 ...:2001:16a2:2e7c:b00	16.065982 4365					
Seq=0 Win=65535 Len=0 MSS=1432 WS=256 SACK_PERM [SYN] 80 → 50340 86	TCP ...:2001:41a8:28:6::5f6 ...:2001:16a2:2e7c:b00	16.065982 4366					
Seq=1 Ack=750 Win=29960 Len=0 [ACK] 50335 → 443 54	TCP 192.168.100.26 38.106.231.208	16.084831 4369	Server Hello, Change Cipher Spec, Application Data, Application Data 299	192.168.100.26 38.106.231.208		16.088395 4370	
Seq=189 Ack=158 Win=64768 Len=0 [ACK] 50337 → 80 74	TCP ...:2001:16a2:2e7c:b00 ...:2001:16a0:2:200e::d	16.089698 4371	Change Cipher Spec, Application Data, Application Data 292	TLSv1.3 38.106.231.208 192.168.100.26		16.095489 4372	
Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128 [SYN, ACK] 50338 → 80 66	TCP 192.168.100.26 95.101.114.50	16.127180 4373					
Seq=1 Ack=1 Win=65280 Len=0 [ACK] 80 → 50338 54	TCP 95.101.114.50 192.168.100.26	16.127286 4374					
GET /connecttest.txt HTTP/1.1 201	HTTP 95.101.114.50 192.168.100.26	16.127411 4375					
Seq=189 Ack=149 Win=64128 Len=0 [ACK] 50336 → 80 54	TCP 192.168.100.26 2.21.14.19	16.128894 4376					
Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128 [SYN, ACK] 50339 → 80 66	TCP 192.168.100.26 95.101.114.50	16.133872 4377					
Seq=1 Ack=1 Win=65280 Len=0 [ACK] 80 → 50339 54	TCP 95.101.114.50 192.168.100.26	16.133987 4378					
GET /connecttest.txt HTTP/1.1 201	HTTP 95.101.114.50 192.168.100.26	16.134014 4379					
Seq=0 Ack=1 Win=64240 Len=0 MSS=1432 SACK_PERM WS=178 [SYN, ACK] 50341 → 80 86	TCP ...:2001:16a0:2:200e::d ...:2001:41a8:28:6::5f6	16.150222 4380					
0000 80 b6 55 4e 0a a7 22 02 71 bf 1c f7 08 00 45 00 ..UN.. q...E..	tured (432 bits) on interface \Device\NPF_{C2EA39FB-5D31-4A9A-A1D3-47249982A609}, id 0 I, Src: 22:02:71:bf:1c:f7 (22:02:71:bf:1c:f7), Dst: Intel_4e:0:a7 (80:b6:55:4e:0:a7)						
0010 00 28 00 00 40 00 38 06 0d e6 02 15 0e 13 c0 a8 (..@8..	Internet Protocol Version 4, Src: 2.21.14.19, Dst: 192.168.100.26						
0020 64 1a 00 50 c4 a0 19 63 18 b3 21 52 c8 c0 50 10 d..P..c..IR..P..	ansmission Control Protocol, Src Port: 80, Dst Port: 50336, Seq: 189, Ack: 149, Len: 0						
0030 01 f5 97 db 00 00							

TCP Data Transfer Packets

Shows TCP packets filtered using `tcp.len > 0`, indicating packets that carry actual data during the TCP connection.

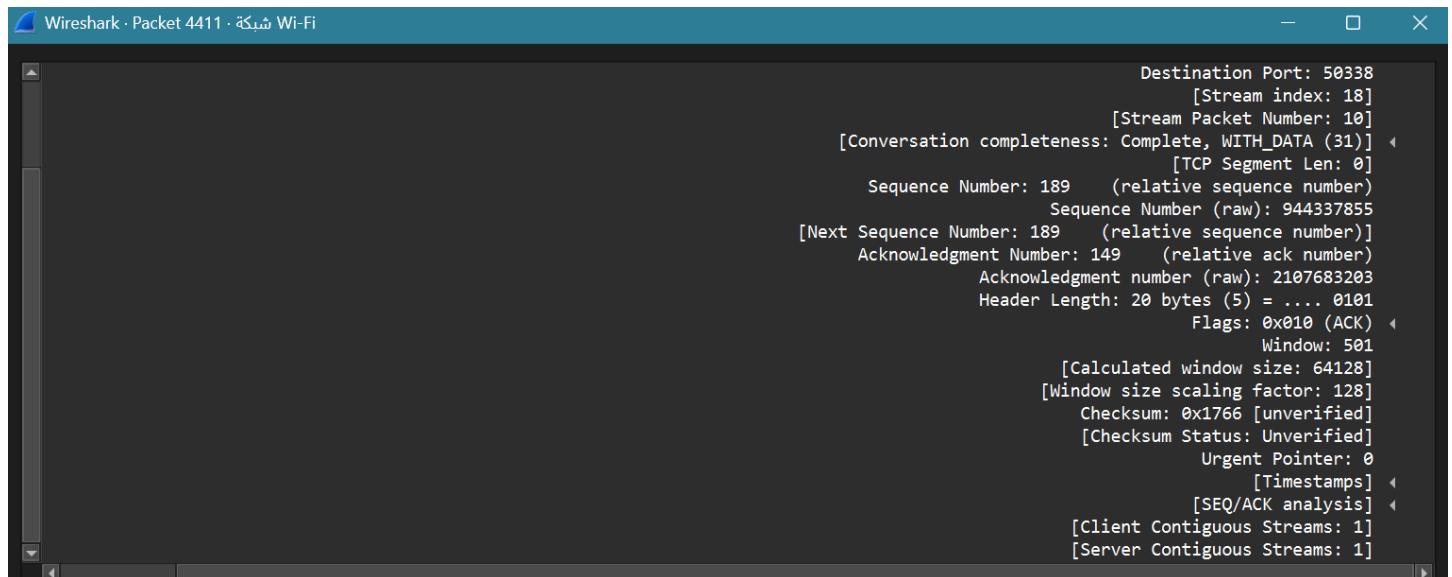
Wi-Fi

tcp.len > 0

	Info	Length	Protocol	Destination	Source	Time	No
Application Data 341	TLSv1.3 192.168.100.26 38.106.231.208	16.273114 4407					
Application Data 101	TLSv1.3 192.168.100.26 38.106.231.208	16.273114 4448					
Application Data 725	TLSv1.3 38.106.231.208 192.168.100.26	16.274423 4410					
Application Data 616	TLSv1.3 192.168.100.26 38.106.231.208	16.459315 4416					
Client Hello (SNI=chifsr.lenovomm.com) 803	TLSv1.3 38.106.231.208 192.168.100.26	16.882482 4425					
Server Hello, Change Cipher Spec, Application Data, Application Data 299	TLSv1.3 192.168.100.26 38.106.231.208	17.078750 4429					
Change Cipher Spec, Application Data, Application Data 292	TLSv1.3 38.106.231.208 192.168.100.26	17.081289 4430					
Application Data 341	TLSv1.3 192.168.100.26 38.106.231.208	17.297517 4431					
Application Data 101	TLSv1.3 192.168.100.26 38.106.231.208	17.297517 4432					
Application Data 953	TLSv1.3 38.106.231.208 192.168.100.26	17.299291 4434					
Application Data 616	TLSv1.3 192.168.100.26 38.106.231.208	17.496034 4438					
Client Hello (SNI=chifsr.lenovomm.com) 803	TLSv1.3 38.106.231.208 192.168.100.26	17.908795 4446					
Server Hello, Change Cipher Spec, Application Data, Application Data 299	TLSv1.3 192.168.100.26 38.106.231.208	18.085748 4448					
Change Cipher Spec, Application Data, Application Data 293	TLSv1.3 38.106.231.208 192.168.100.26	18.090783 4449					
Application Data 341	TLSv1.3 192.168.100.26 38.106.231.208	18.266854 4450					
Application Data 101	TLSv1.3 192.168.100.26 38.106.231.208	18.266854 4451					
Application Data 1138	TLSv1.3 38.106.231.208 192.168.100.26	18.268315 4453					
Application Data 616	TLSv1.3 192.168.100.26 38.106.231.208	18.451929 4455					
GET /r/r4.crl HTTP/1.1 274	HTTP ...:2a00:1450:4006:822 ...:2001:16a2:2e7c:b00	18.665999 4468					
HTTP/1.1 304 Not Modified 297	HTTP ...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:822	18.787682 4471					
Client Hello (SNI=chifsr.lenovomm.com) 803	TLSv1.3 38.106.231.208 192.168.100.26	18.871726 4475					
Server Hello, Change Cipher Spec, Application Data, Application Data 299	TLSv1.3 192.168.100.26 38.106.231.208	19.057384 4478					
Change Cipher Spec, Application Data, Application Data 293	TLSv1.3 38.106.231.208 192.168.100.26	19.065478 4479					
Application Data 341	TLSv1.3 192.168.100.26 38.106.231.208	19.281675 4480					
Application Data 101	TLSv1.3 192.168.100.26 38.106.231.208	19.281675 4481					
Application Data 1389	TLSv1.3 38.106.231.208 192.168.100.26	19.283304 4483					

TCP Protocol Details

Displays the **Transmission Control Protocol** section expanded, showing TCP header fields including sequence and acknowledgment numbers.



UDP Packet Filtering

Shows Wireshark with the `udpdisplay` filter applied, displaying only UDP packets generated during the capture.

	Info	Length	Protocol	Destination	Source	Time	No
	Len=201 443 → 51396 263	263	UDP	...:2a00:1450:4006:808 ...:2001:16a2:2e7c:b00		4.411949 69	
	Len=1226 56937 → 443 1288	1288	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:81d		4.440203 70	
	Len=1230 56937 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:81d		4.440203 71	
	Len=673 56937 → 443 735	735	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:81d		4.440203 72	
	Len=37 443 → 56937 99	99	UDP	...:2a00:1450:4006:81d ...:2001:16a2:2e7c:b00		4.477297 73	
	Len=1226 51396 → 443 1288	1288	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.493382 74	
	Len=1220 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.493382 75	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.493382 76	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.493382 77	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.493382 78	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.493382 79	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.493382 80	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.493382 81	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.493382 82	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.493382 83	
	Len=36 443 → 51396 98	98	UDP	...:2a00:1450:4006:808 ...:2001:16a2:2e7c:b00		4.494035 84	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.496161 85	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.496161 86	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.496161 87	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.496161 88	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.496161 89	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.496161 90	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.496161 91	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.496161 92	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.496161 93	
	Len=1230 51396 → 443 1292	1292	UDP	...:2001:16a2:2e7c:b00 ...:2a00:1450:4006:808		4.496161 94	

UDP Protocol Details

Displays the **User Datagram Protocol** section expanded, showing source port, destination port, packet length, checksum, and payload information.

	Source Port:	443	Destination Port:	51396
	Length:	1238	Checksum:	0x7690 [unverified]
	[Checksum Status: Unverified]		[Stream index: 3]	
	[Stream Packet Number: 12]		[Timestamps]	
	UDP payload (1230 bytes)		Data (1230 bytes)	

part 4: comparison between TCP and UDP

	tcp or udp	reasons
Reliability and Connection Establishment	TCP	<ul style="list-style-type: none"> • Establishes connection (three-way handshake) • Guaranteed delivery with retransmissions
Data Integrity and Ordering	TCP	<ul style="list-style-type: none"> • Maintains order using sequence numbers • Checks and retransmits corrupted packets

	tcp	udp
use cases	Slower, more overhead, reliable, ensures order	Web browsing, email, file transfer, HTTPS
performance	Faster, low overhead, unreliable, no order guarantee	Streaming, VoIP, online gaming, DNS