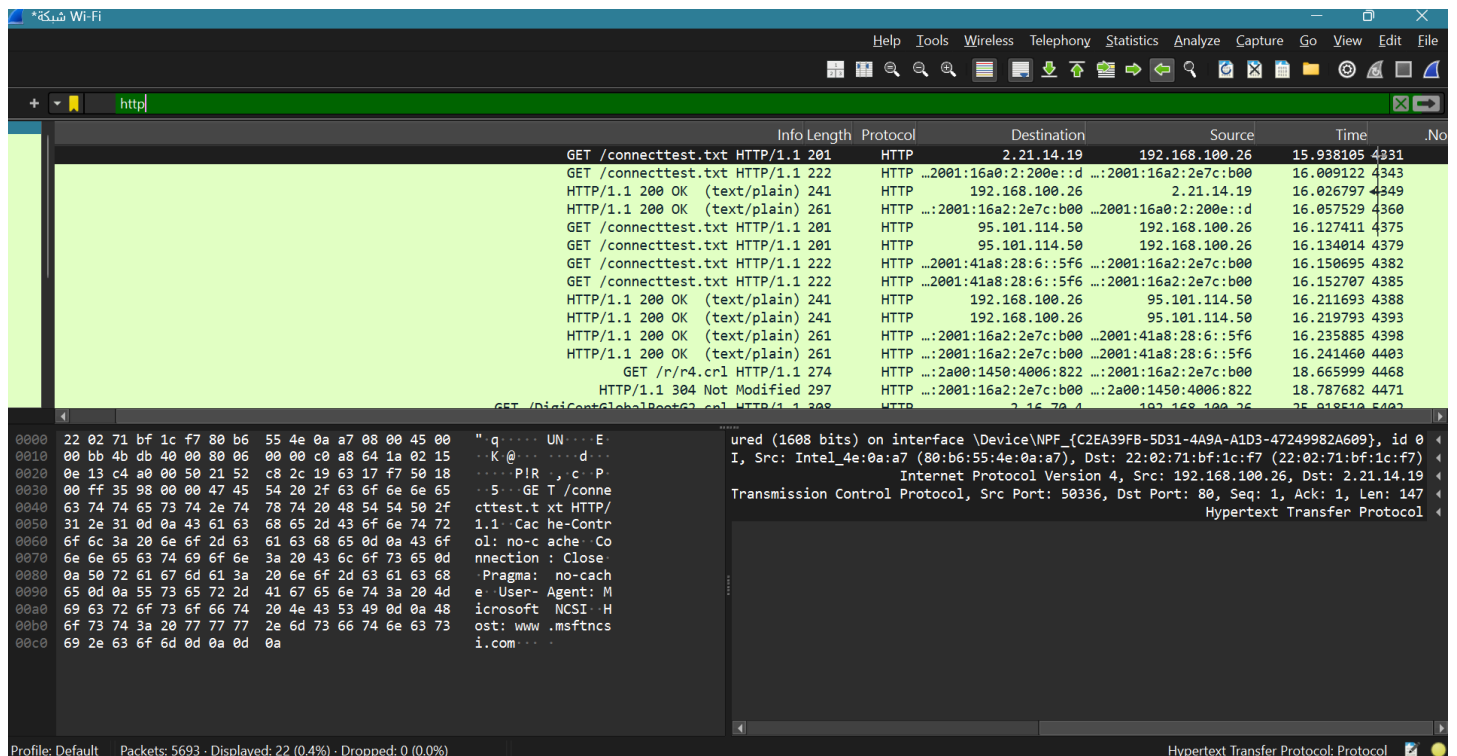


LAB1 - the internet protocol

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.

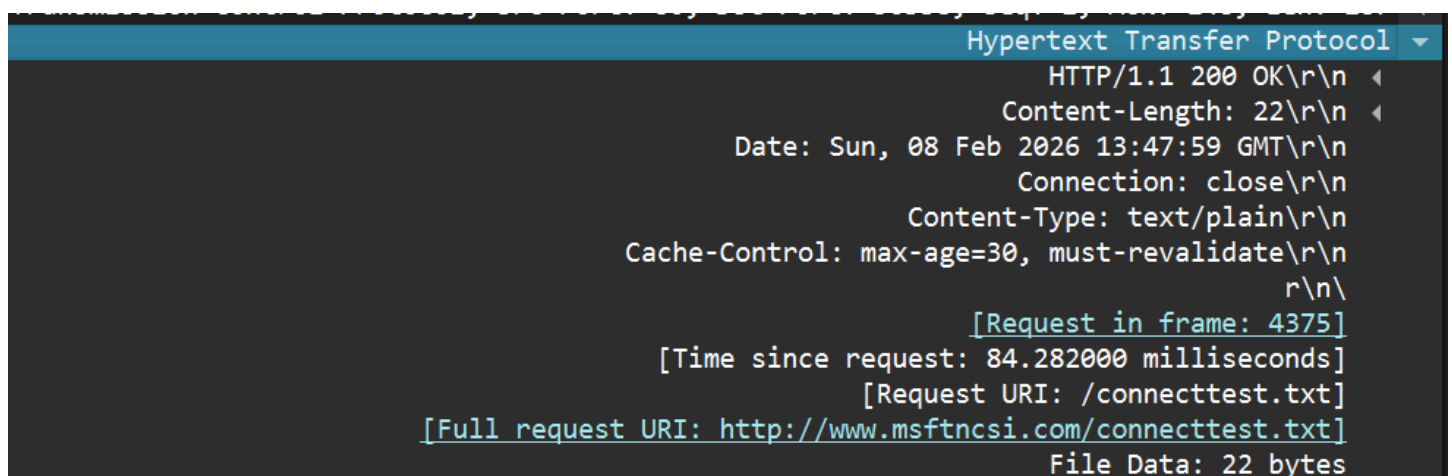
```
GET /connecttest.txt HTTP/1.1
Cache-Control: no-cache
Connection: Close
Pragma: no-cache
User-Agent: Microsoft NCSI
Host: www.msftncsi.com
```

```
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.



TCP Packet Filtering

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

No	Time	Source	Destination	Protocol	Length	Info
4363	16.057690	192.168.100.26	192.168.100.26	TCP	74	Seq=149 Ack=189 Win=65280 Len=0 [FIN, ACK] 80 → 50337
4365	16.065902	192.168.100.26	192.168.100.26	TCP	86	Seq=0 Win=65535 Len=0 MSS=1432 WS=256 SACK_PERM [SYN] 80 → 50341
4366	16.065902	192.168.100.26	192.168.100.26	TCP	86	Seq=0 Win=65535 Len=0 MSS=1432 WS=256 SACK_PERM [SYN] 80 → 50340
4369	16.084831	192.168.100.26	192.168.100.26	TCP	54	Seq=1 Ack=750 Win=29960 Len=0 [ACK] 50335 → 443
4370	16.088395	192.168.100.26	192.168.100.26	TLSv1.3	299	Server Hello, Change Cipher Spec, Application Data
4371	16.089698	192.168.100.26	192.168.100.26	TCP	74	Seq=189 Ack=150 Win=64768 Len=0 [ACK] 50337 → 80
4372	16.095489	192.168.100.26	192.168.100.26	TLSv1.3	292	Change Cipher Spec, Application Data
4373	16.127180	192.168.100.26	192.168.100.26	TCP	66	Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128 [SYN, ACK] 50338 → 80
4374	16.127286	192.168.100.26	192.168.100.26	TCP	54	Seq=1 Ack=1 Win=65280 Len=0 [ACK] 80 → 50338
4375	16.127411	192.168.100.26	192.168.100.26	HTTP	201	GET /connecttest.txt HTTP/1.1
4376	16.128894	192.168.100.26	192.168.100.26	TCP	54	Seq=189 Ack=149 Win=64128 Len=0 [ACK] 50336 → 80
4377	16.133872	192.168.100.26	192.168.100.26	TCP	66	Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128 [SYN, ACK] 50339 → 80
4378	16.133907	192.168.100.26	192.168.100.26	TCP	54	Seq=1 Ack=1 Win=65280 Len=0 [ACK] 80 → 50339
4379	16.134014	192.168.100.26	192.168.100.26	HTTP	201	GET /connecttest.txt HTTP/1.1

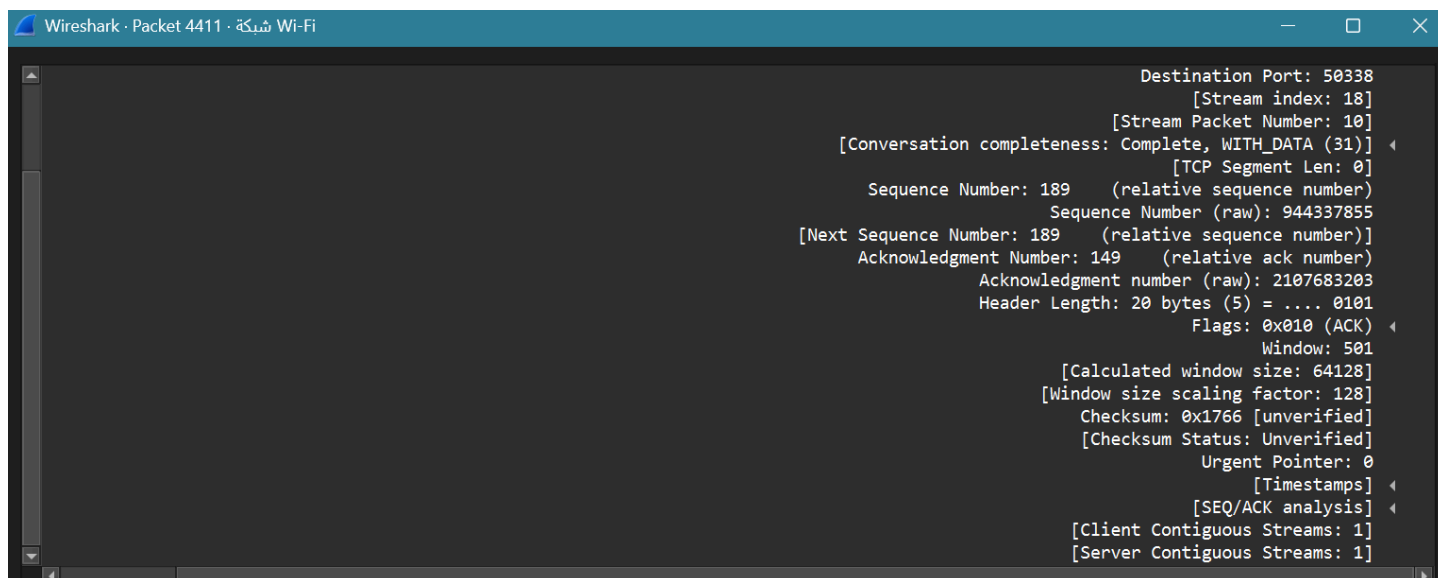
TCP Data Transfer Packets

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

No	Time	Source	Destination	Protocol	Length	Info
4407	16.273114	192.168.100.26	192.168.100.26	TLSv1.3	341	Application Data
4408	16.273114	192.168.100.26	192.168.100.26	TLSv1.3	101	Application Data
4410	16.274423	192.168.100.26	192.168.100.26	TLSv1.3	725	Application Data
4416	16.459315	192.168.100.26	192.168.100.26	TLSv1.3	616	Application Data
4425	16.882482	192.168.100.26	192.168.100.26	TLSv1.3	803	Client Hello (SNI=chifsr.lenovomm.com)
4429	17.078750	192.168.100.26	192.168.100.26	TLSv1.3	299	Server Hello, Change Cipher Spec, Application Data
4430	17.081209	192.168.100.26	192.168.100.26	TLSv1.3	292	Change Cipher Spec, Application Data
4431	17.297517	192.168.100.26	192.168.100.26	TLSv1.3	341	Application Data
4432	17.297517	192.168.100.26	192.168.100.26	TLSv1.3	101	Application Data
4434	17.299291	192.168.100.26	192.168.100.26	TLSv1.3	953	Application Data
4438	17.496034	192.168.100.26	192.168.100.26	TLSv1.3	616	Application Data
4446	17.908795	192.168.100.26	192.168.100.26	TLSv1.3	803	Client Hello (SNI=chifsr.lenovomm.com)
4448	18.085748	192.168.100.26	192.168.100.26	TLSv1.3	299	Server Hello, Change Cipher Spec, Application Data
4449	18.090783	192.168.100.26	192.168.100.26	TLSv1.3	293	Change Cipher Spec, Application Data
4450	18.266854	192.168.100.26	192.168.100.26	TLSv1.3	341	Application Data
4451	18.266854	192.168.100.26	192.168.100.26	TLSv1.3	101	Application Data
4453	18.268315	192.168.100.26	192.168.100.26	TLSv1.3	1138	Application Data
4455	18.451929	192.168.100.26	192.168.100.26	TLSv1.3	616	Application Data
4468	18.665999	192.168.100.26	192.168.100.26	HTTP	274	GET /r/r4.cr1 HTTP/1.1
4471	18.787682	192.168.100.26	192.168.100.26	HTTP	297	HTTP/1.1 304 Not Modified
4475	18.871726	192.168.100.26	192.168.100.26	TLSv1.3	803	Client Hello (SNI=chifsr.lenovomm.com)
4478	19.057384	192.168.100.26	192.168.100.26	TLSv1.3	299	Server Hello, Change Cipher Spec, Application Data
4479	19.065478	192.168.100.26	192.168.100.26	TLSv1.3	293	Change Cipher Spec, Application Data
4480	19.281675	192.168.100.26	192.168.100.26	TLSv1.3	341	Application Data
4481	19.281675	192.168.100.26	192.168.100.26	TLSv1.3	101	Application Data
4483	19.283304	192.168.100.26	192.168.100.26	TLSv1.3	1389	Application Data

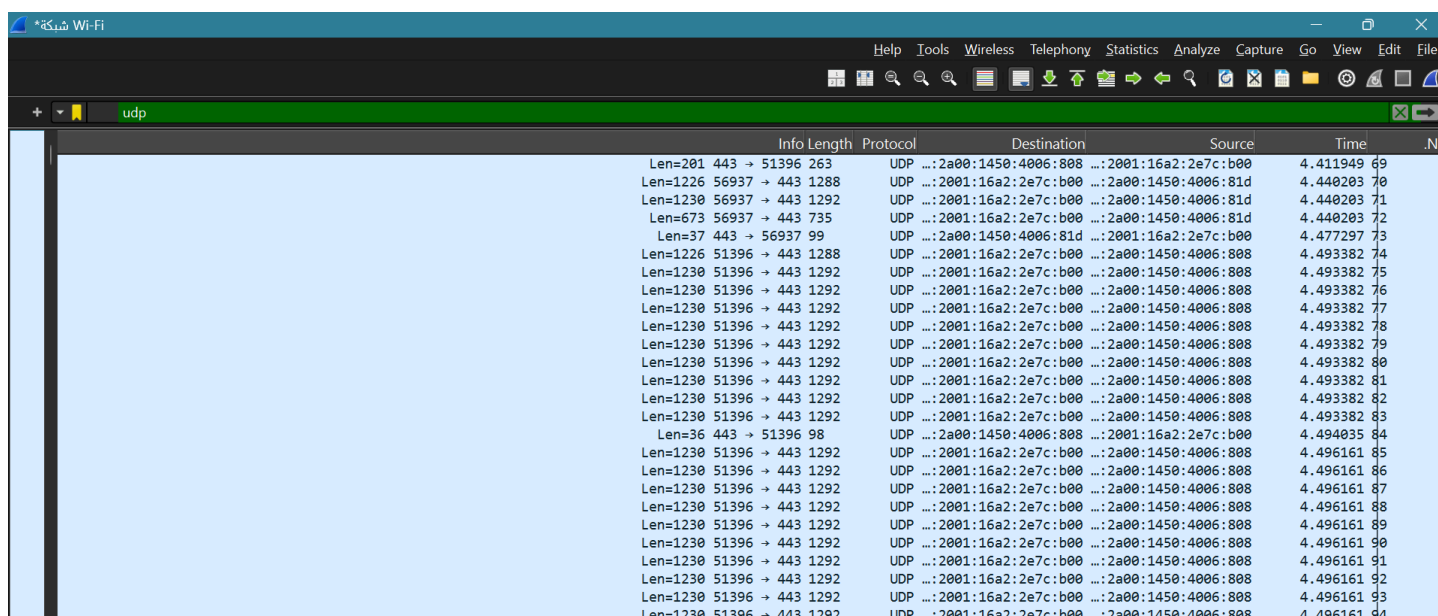
TCP Protocol Details

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



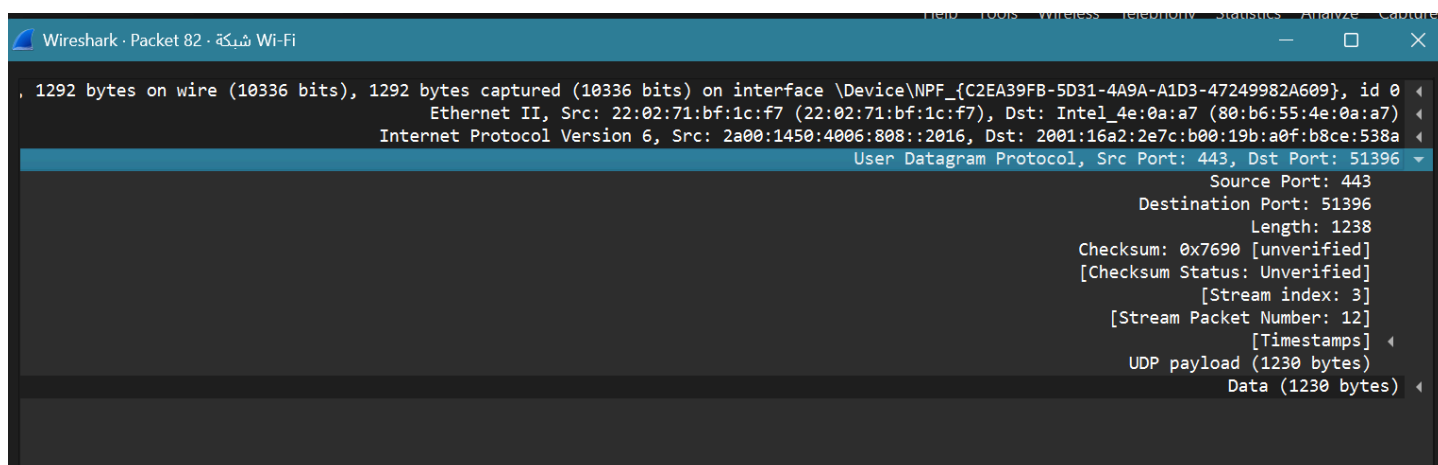
UDP Packet Filtering

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



UDP Protocol Details

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



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