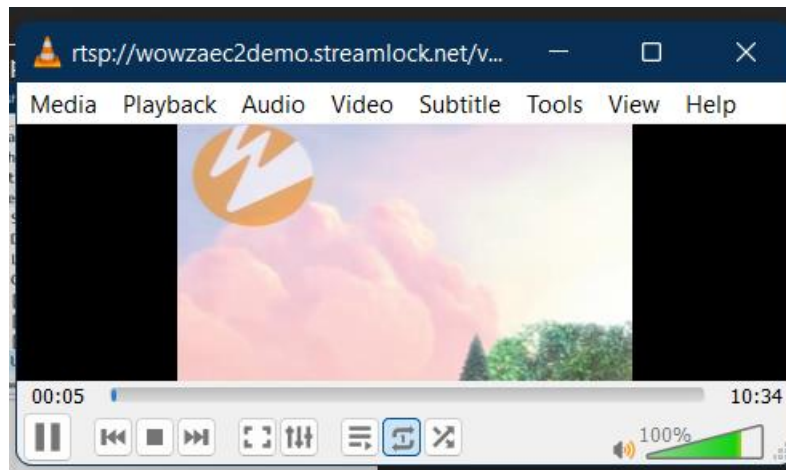
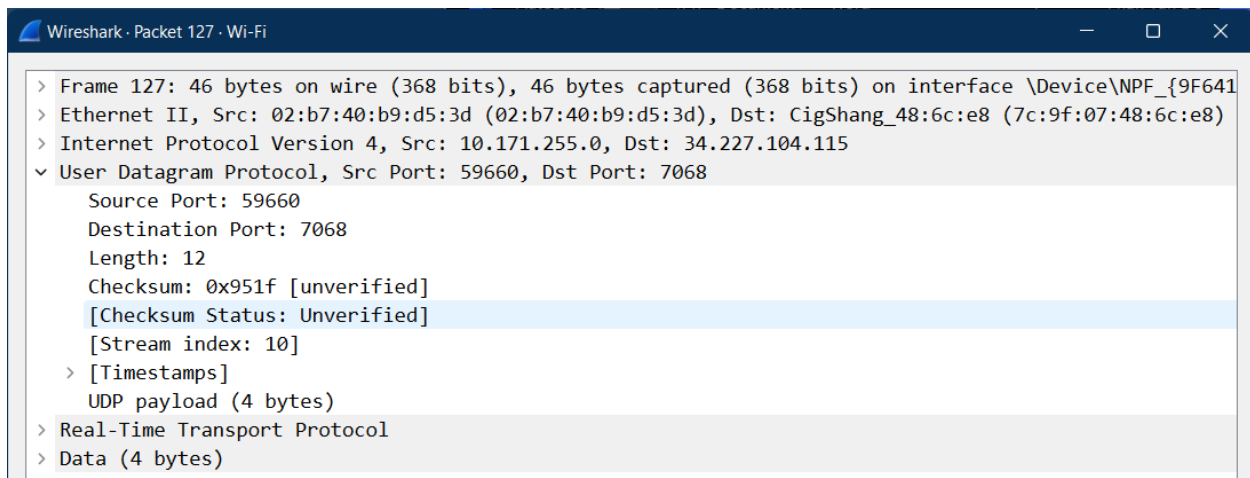


Phần UDP:

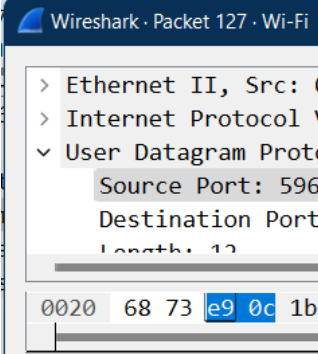
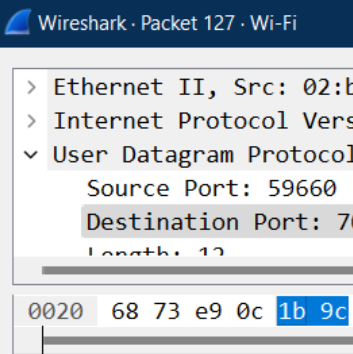
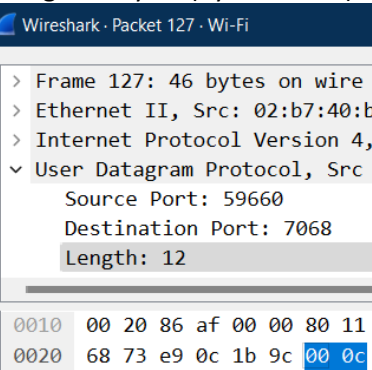
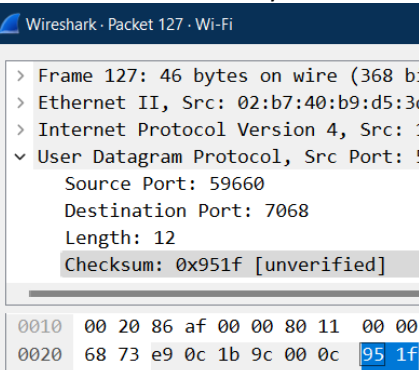
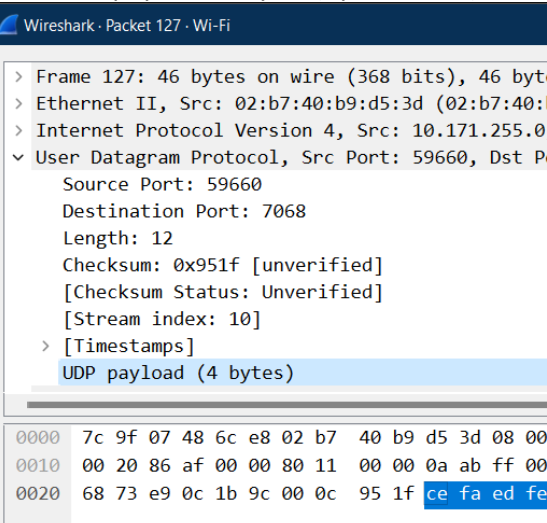


1.

- Source Port: cổng kết nối của bên gửi
- Destination Port: cổng kết nối của bên nhận
- Length: độ dài header và payload
- Checksum: dùng để xác thực nội dung payload có bị lỗi không.
- UDP payload: dữ liệu chính của UDP packet.



2.

<p>Source Port: 2 bytes (byte 34 – 35)</p>  <p>Bytes 34-35: Source Port (udp.srcport)</p>	<p>Destination Port: 2 bytes (byte 36 – 37)</p>  <p>Bytes 36-37: Destination Port (udp.dstport)</p>
<p>Length: 2 bytes (byte 38 – 39)</p>  <p>Bytes 38-39: Length (udp.length)</p>	<p>Checksum: 2 bytes</p>  <p>Bytes 40-41: Checksum (udp.checksum)</p>
<p>UDP payload: 4 bytes (byte 42 – 45)</p>  <p>Bytes 42-45: Data (data.data)</p>	

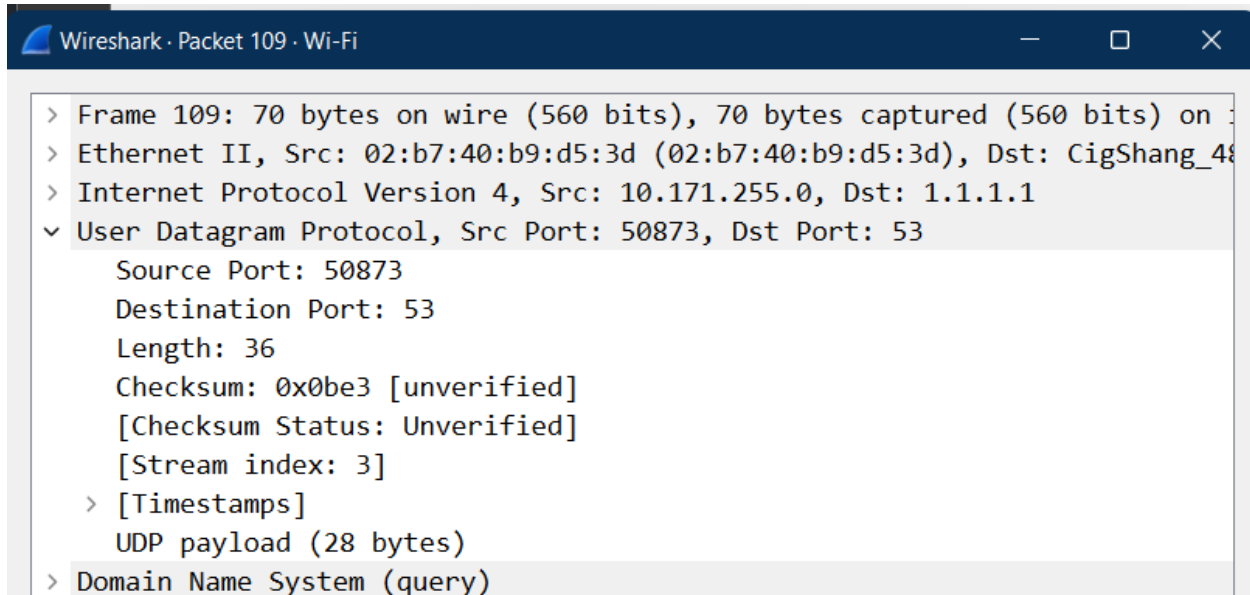
3. Giá trị của trường Length trong UDP header là độ dài của header và payload của UDP packet. Tổng = 12 bytes = Source Port (2 bytes) + Destination Port (2 bytes) + Length (2 bytes) + Checksum (2 bytes) + UDP payload (4 bytes).

4. Length chiếm 2 bytes (0x000c) => Max length là 0xffff hay 65535 bytes (không tính UDP header và IP header). Vậy UDP payload có thể chứa 65535 bytes.

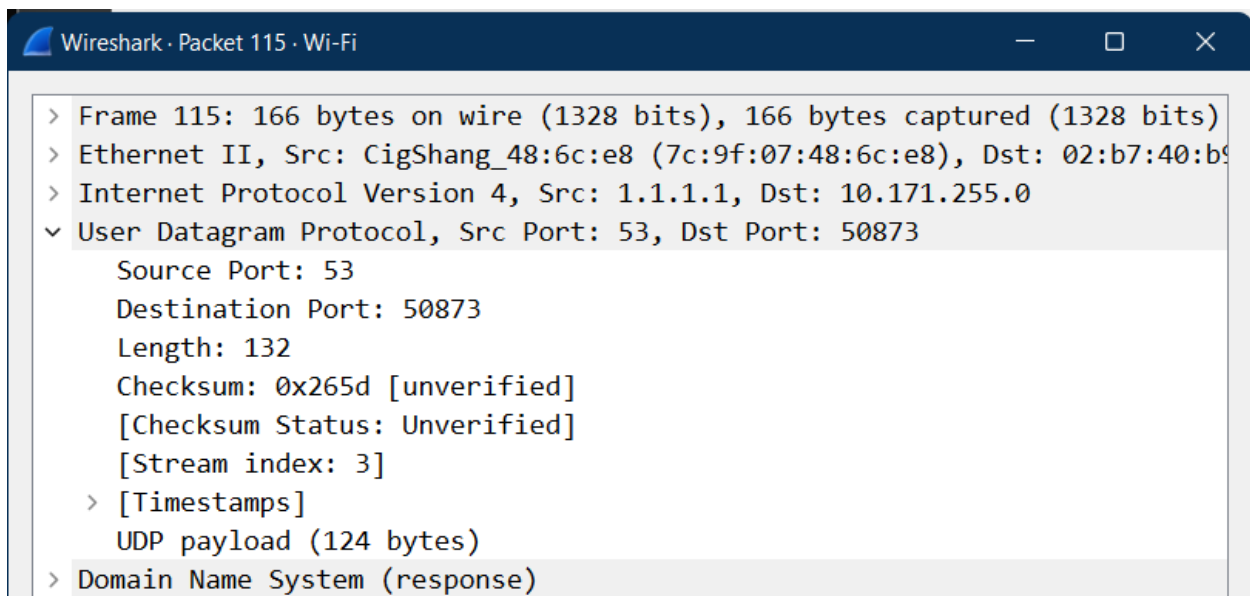
5. Source port chiếm 2 bytes (0xe90c) => Max source port là 0xffff hay 65535.

6. Trong file 21520722-DNS.pcap:

- Gói tin do máy mình gửi:

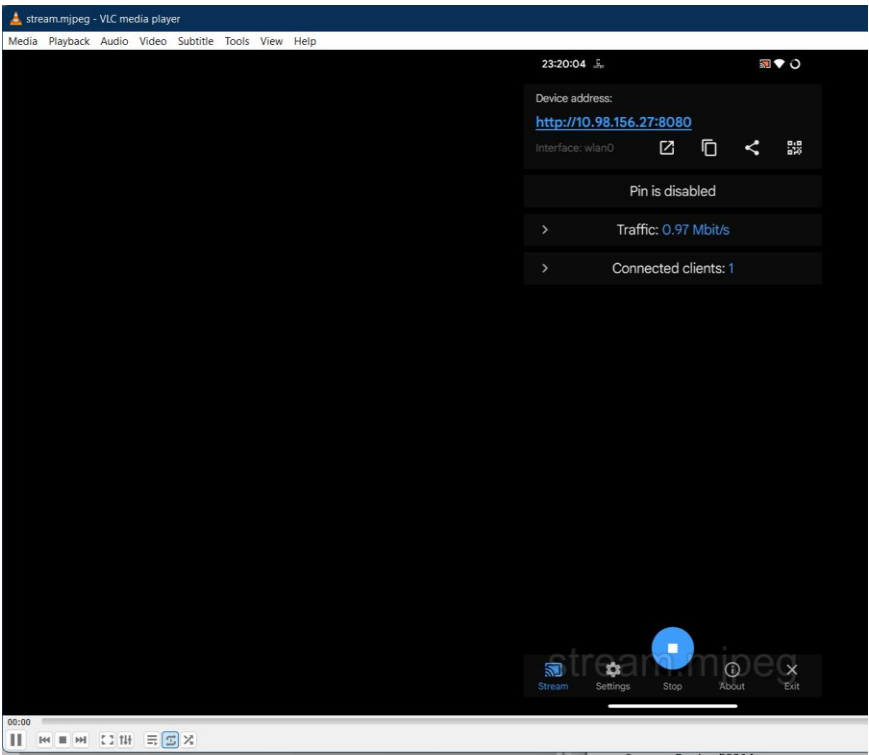


- Gói tin phản hồi của gói tin đó:



- Port của máy mình là source port trong gói tin do máy mình gửi, đồng thời là destination port trong gói tin phản hồi của gói tin đó. Tương tự, source port trong gói tin phản hồi cũng là destination port trong gói tin do máy mình gửi.

Phần TCP:



7. Client có IP là 10.171.255.0 và TCP port là 63099:

84	8.967969	10.171.255.0	10.98.156.27
89	9.054163	10.98.156.27	10.171.255.0
90	9.054226	10.171.255.0	10.98.156.27
91	9.054288	10.171.255.0	10.98.156.27
95	9.078683	10.98.156.27	10.171.255.0
97	9.219625	10.98.156.27	10.171.255.0
98	9.222195	10.98.156.27	10.171.255.0

> Frame 84: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

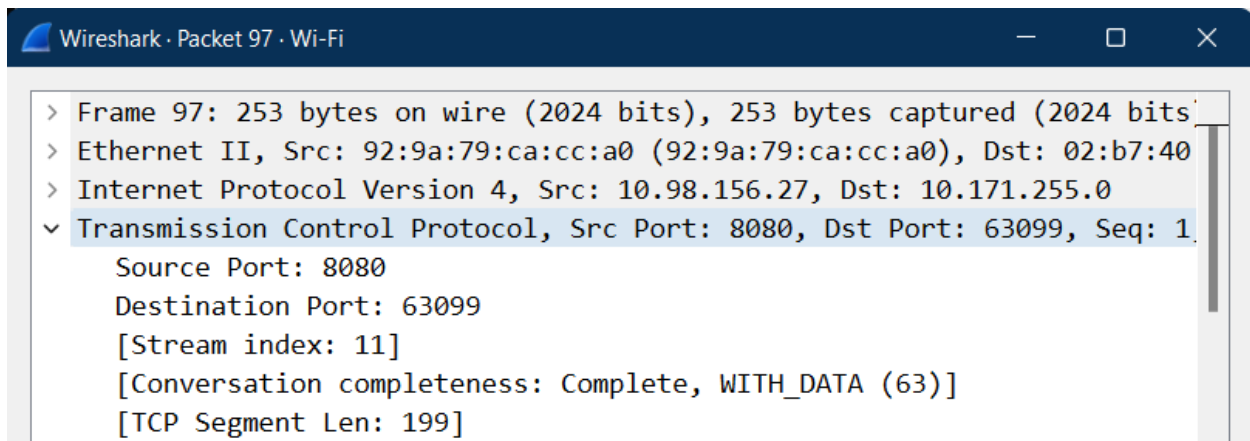
> Ethernet II, Src: 02:b7:40:b9:d5:3d (02:b7:40:b9:d5:3d), Dst: 02:00:00:00:00:00

> Internet Protocol Version 4, Src: 10.171.255.0, Dst: 10.98.156.27

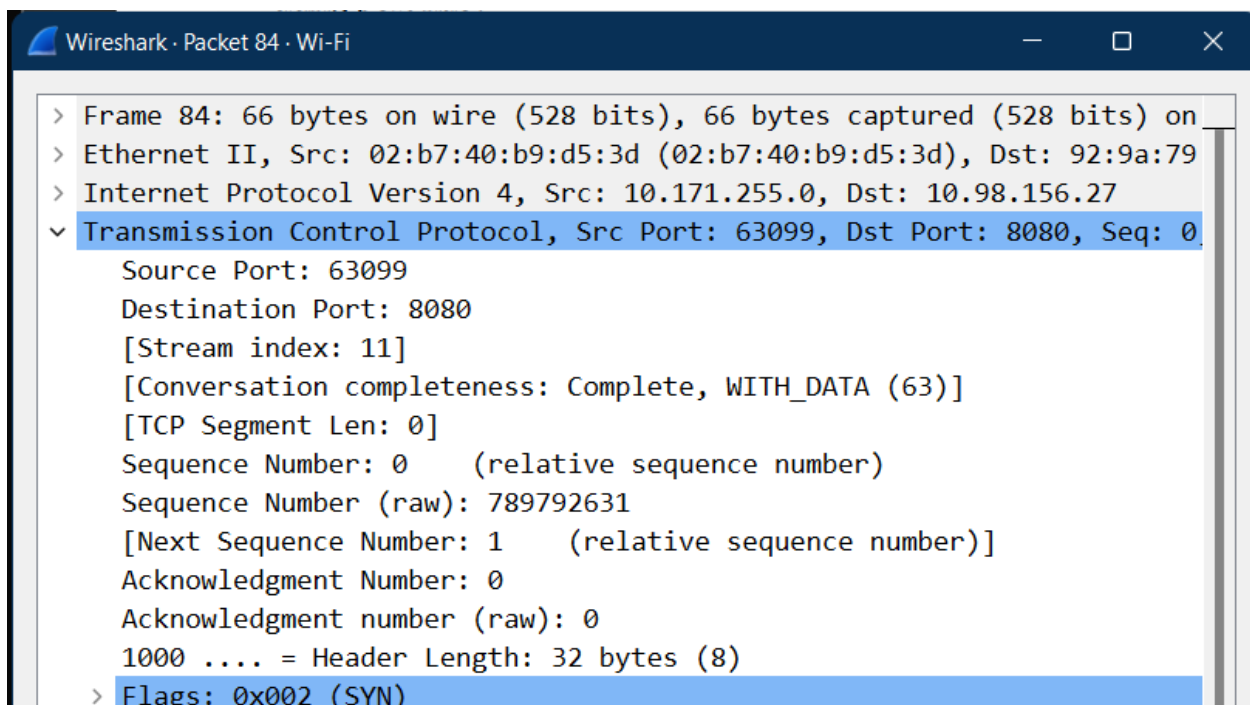
> Transmission Control Protocol, Src Port: 63099, Dst Port: 8080

Source Port: 63099

8. Server có IP là 10.98.156.27. Kết nối TCP dùng để gửi các segments sử dụng port 8080, dùng để nhận các segments sử dụng port 63099:



9. Sequence number = 0 khi khởi tạo kết nối TCP giữa client và server. Trường Flags = 0x002 cho ta biết segment đó là TCP SYN segment.

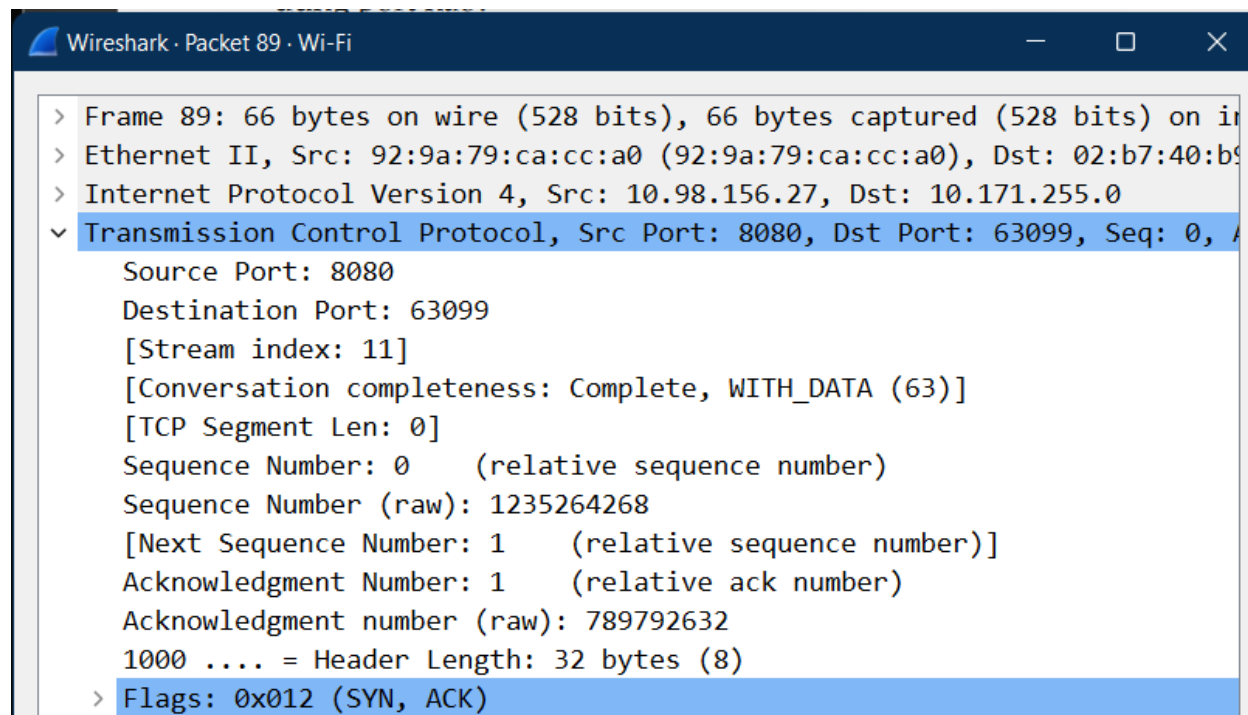


10.

- Sequence number = 0.

- Giá trị Acknowledgement = 1.

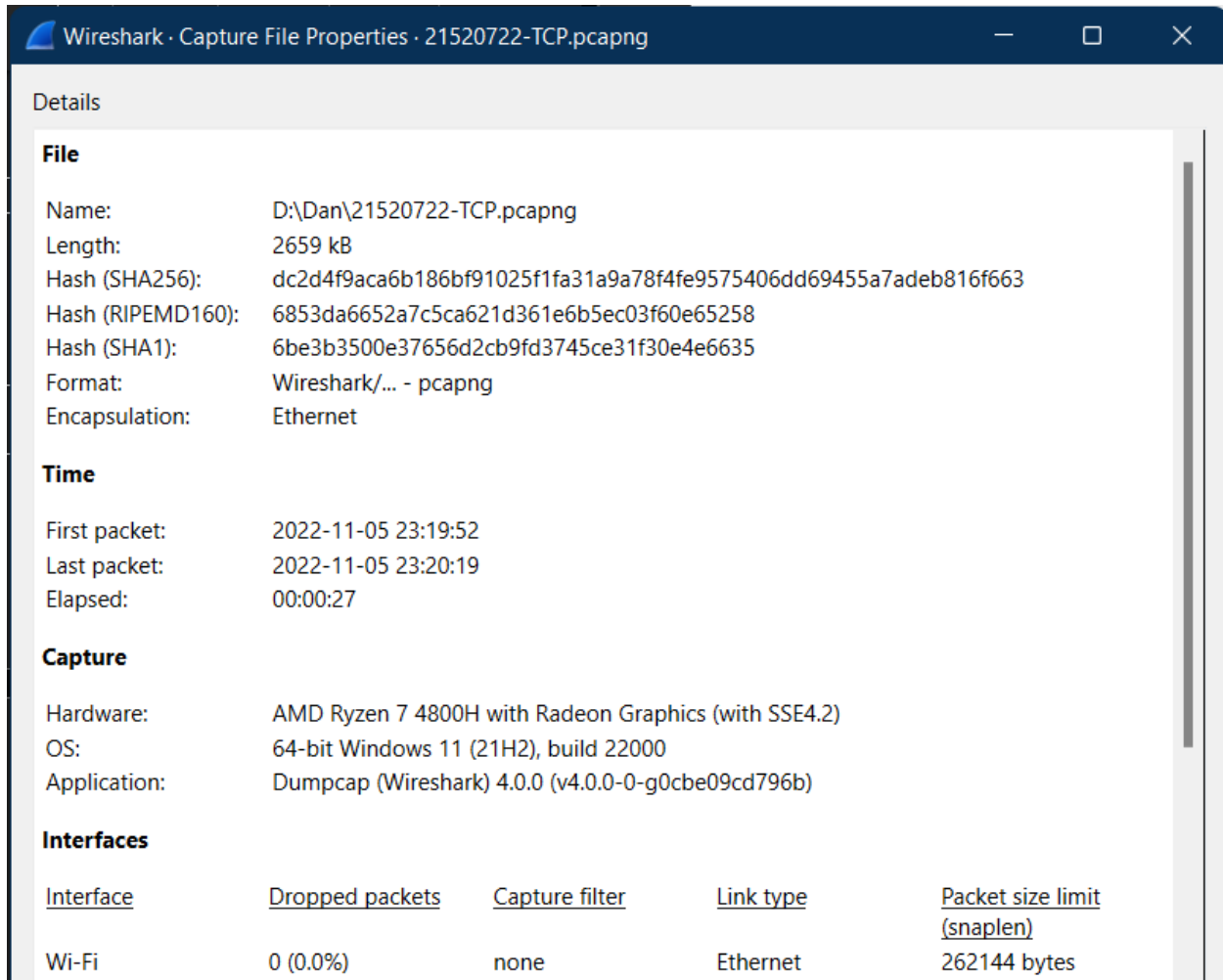
- Server xác định được giá trị Acknowledgement vì Client đã gửi Acknowledgement number = 0 trước đó ở packet 84. Thành phần Flags = 0x012 cho ta biết đó là SYN/ACK segment.



11.

STT	Các SEQ	Thời gian gửi	Thời gian nhận ACK	RTT (Round trip time)
97 – 104	1, 200, 1660, 310, 4089, 4288, 4295, 5755	9.219625	9.222236 tại packet 105	0.000041
106 – 107	7215, 8177	9.222736	9.222754 tại packet 108	0.000018
109 – 123	8383, 9625, 11085, 12545, 14005, 15465, 16925, 18385, 19845, 21305, 22765, 24225, 25685, 27145, 28605	9.245859	9.245924 tại packet 124	0.000065
125 – 128	30065, 31525, 32985, 34445	9.247653	9.247688 tại packet 129	0.000035
130 – 145	35905, 37256, 28498, 39740, 40982, 42224, 43466, 4444708, 45950, 47192, 48434, 49676, 50918, 52160, 53402, 54644	9.270841	9.270950 tại packet 146	0.000109
147 – 153	55886, 57128, 58370, 59612, 60854, 62096, 63338	9.271179	9.271179 tại packet 154	0.000039

12. Không có. Trong mục Statistics > Capture File Properties (Ctrl+Alt+Shift+C) cho ta biết số packet bị drop là 0, tức là không có segment nào được gửi lại.



The image shows the 'Wireshark · Capture File Properties · 21520722-TCP.pcapng' window. It contains details about the capture file, including file metadata, time range, capture hardware, and a table of interfaces with their respective dropped packets and capture filters.

Details

File

Name: D:\Dan\21520722-TCP.pcapng
Length: 2659 kB
Hash (SHA256): dc2d4f9aca6b186bf91025f1fa31a9a78f4fe9575406dd69455a7adeb816f663
Hash (RIPEMD160): 6853da6652a7c5ca621d361e6b5ec03f60e65258
Hash (SHA1): 6be3b3500e37656d2cb9fd3745ce31f30e4e6635
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2022-11-05 23:19:52
Last packet: 2022-11-05 23:20:19
Elapsed: 00:00:27

Capture

Hardware: AMD Ryzen 7 4800H with Radeon Graphics (with SSE4.2)
OS: 64-bit Windows 11 (21H2), build 22000
Application: Dumpcap (Wireshark) 4.0.0 (v4.0.0-0-g0cbe09cd796b)

Interfaces

<u>Interface</u>	<u>Dropped packets</u>	<u>Capture filter</u>	<u>Link type</u>	<u>Packet size limit (snaplen)</u>
Wi-Fi	0 (0.0%)	none	Ethernet	262144 bytes