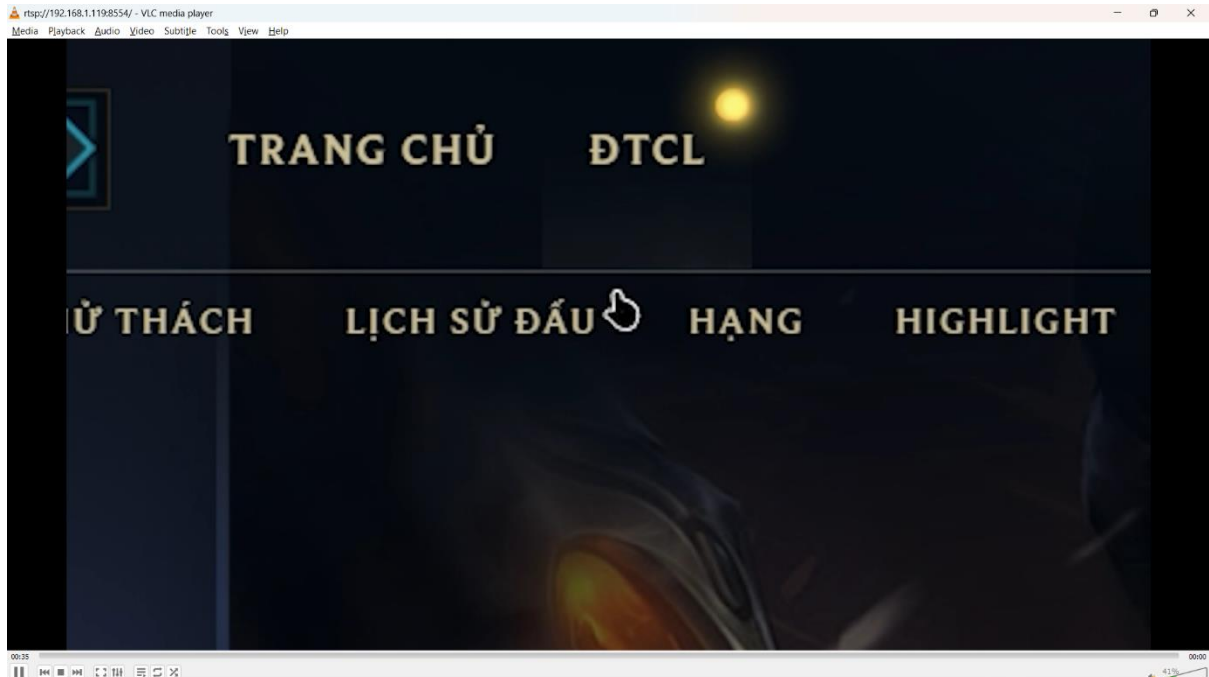


Tên: Ngô Vũ Minh Đạt

MSSV:21521935

Task 1: Phân tích hoạt động giao thức UDP



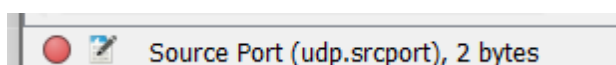
Câu 1: Chọn một gói tin UDP, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó?

```
Internet Protocol Version 4, Src: 192.168.1.123, Dst: 192.168.1.1
  User Datagram Protocol, Src Port: 58376, Dst Port: 59562
    Source Port: 58376
    Destination Port: 59562
    Length: 12
    Checksum: 0xf179 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 48]
```


- *Source Port: port nguồn*
- *Destination: port đích*
- *Length: độ dài gói tin (bytes)*
- *Checksum: Giá trị kiểm tra*

Câu 2: Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?



- Source port : 2 bytes




- Destination port: 2 bytes

 Destination Port (udp.dstport), 2 bytes

- Length: 2 bytes

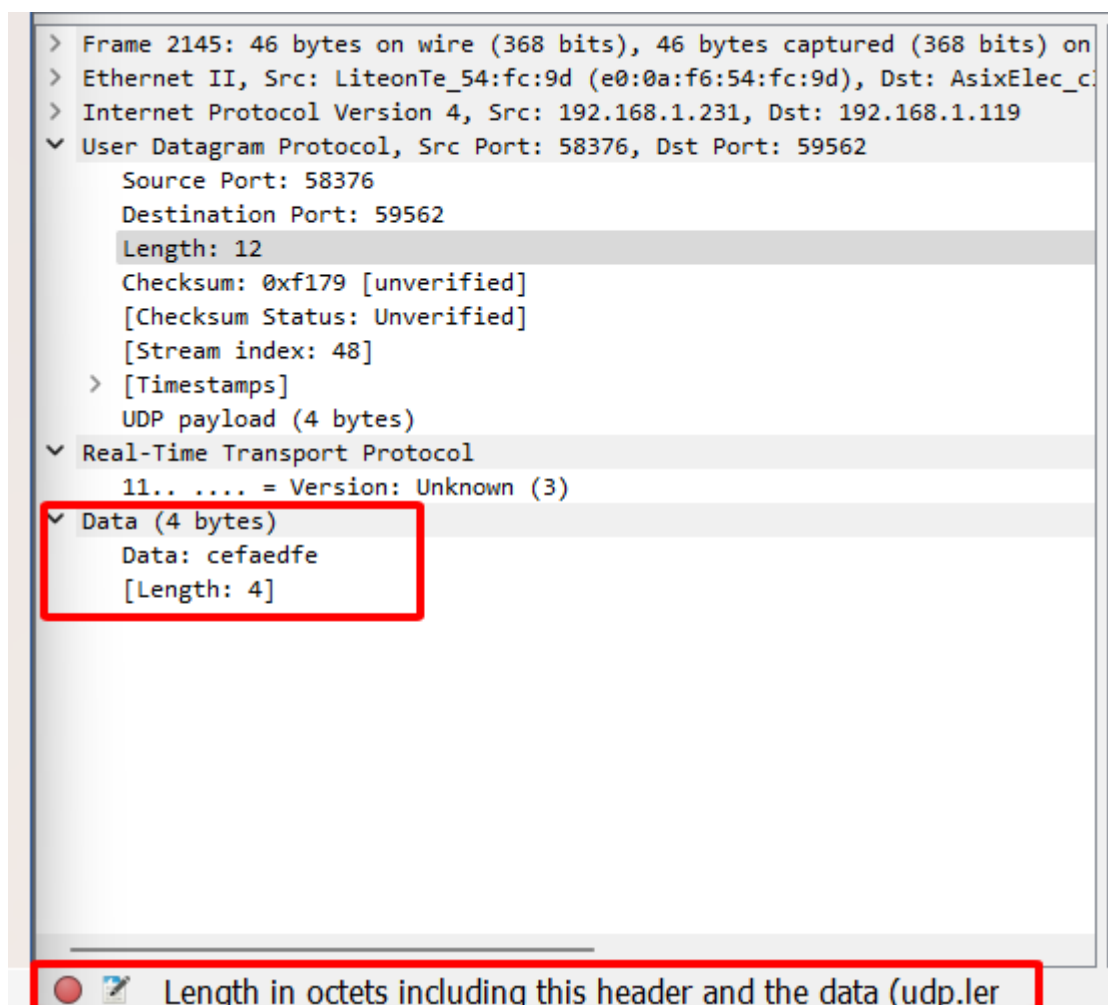
  Length in octets including this header and the data (udp.length), 2 bytes

- Checksum : 2 bytes

  Details at: <https://www.wireshark.org/docs/develop/Checksums.html> (udp.checksum), 2 bytes

Câu 3: Giá trị của trường Length trong UDP header là độ dài của gì? Chứng minh nhận định này?

- Giá trị *length*=12 trong UDP là độ dài bao gồm 8 byte header (bao gồm source port, destination port, length, checksum) và 4 byte data



Câu 4: Số bytes lớn nhất mà payload (phần chứa dữ liệu gốc, không tính UDP header và IP header) của UDP có thể chứa?

- Giá trị lớn nhất mà UDP payload có thể có là $2^{16} - 1$ (do giá trị lưu trong 16 bit) trừ đi 8 bytes header. Bằng $65535 - 8 = 65527$ bytes

Câu 5: Giá trị lớn nhất có thể có của port nguồn (Source port)?

- $Max\ source\ port = 2^{16} - 1 = 65535$

Câu 6: Tìm và kiểm tra một cặp gói tin sử dụng giao thức UDP gồm: gói tin do máy mình gửi và gói tin phản hồi của gói tin đó. Miêu tả mối quan hệ về port number của 2 gói tin này. Gợi ý: Có thể bắt gói tin UDP ở một tình huống khác để tìm được 1 cặp gói tin như trên.

- *Source port của bên sender sẽ thành destination port của bên receiver gửi lại*
- *Destination port của bên sender sẽ thành source port của bên gửi*

Bên gửi

No.	Time	Source	Destination	Protocol	Length	Info
2145	113.688456	192.168.1.231	192.168.1.119	RTP	46	Unknown RTP version 3
2147	113.688582	192.168.1.231	192.168.1.119	RTP	46	Unknown RTP version 3
2149	113.688663	192.168.1.231	192.168.1.119	RTP	46	Unknown RTP version 3
2151	113.688763	192.168.1.231	192.168.1.119	RTP	46	Unknown RTP version 3
2154	113.700047	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8033, Time=434688359
2155	113.702407	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8034, Time=434688359
2156	113.707204	192.168.1.119	192.168.1.231	RTP	1164	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8035, Time=434688359, Ma
2157	113.710934	192.168.1.119	192.168.1.231	RTP	60	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8036, Time=434689859
2158	113.712189	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8037, Time=434689859
2159	113.712189	192.168.1.119	192.168.1.231	RTP	539	PT=DynamicRTP-Type-96, SSRC=0xEB5FFA9, Seq=5078, Time=231834655, Mar
2160	113.715301	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8038, Time=434689859
2161	113.720562	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8039, Time=434689859
2163	113.723599	192.168.1.119	192.168.1.231	RTP	619	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8040, Time=434689859, Ma
2164	113.726908	192.168.1.119	192.168.1.231	RTP	60	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8041, Time=434691360
2165	113.732363	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8042, Time=434691360
2166	113.732363	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8043, Time=434691360
2167	113.733039	192.168.1.119	192.168.1.231	RTP	564	PT=DynamicRTP-Type-96, SSRC=0xEB5FFA9, Seq=5079, Time=231835680, Mar
2168	113.737469	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8044, Time=434691360
2169	113.740693	192.168.1.119	192.168.1.231	RTP	280	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8045, Time=434691360, Ma
2170	113.743841	192.168.1.119	192.168.1.231	RTP	60	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8046, Time=434692859
2171	113.746935	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8047, Time=434692859
2172	113.750916	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8048, Time=434692859
2173	113.752372	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8049, Time=434692859
2174	113.755185	192.168.1.119	192.168.1.231	RTP	563	PT=DynamicRTP-Type-96, SSRC=0xEB5FFA9, Seq=5080, Time=231836703, Mar
2175	113.759601	192.168.1.119	192.168.1.231	RTP	81	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8050, Time=434692859, Ma
2176	113.760912	192.168.1.119	192.168.1.231	RTP	60	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8051, Time=434694359
2177	113.766322	192.168.1.119	192.168.1.231	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8052, Time=434694359

> Frame 2145: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{E4BF8B19-222E-4832-86E4-3E45A2217ABA}, id 0
 > Ethernet II, Src: LiteonTe_54:fc:9d (e0:0a:f6:54:fc:9d), Dst: AsixElec_c3:6e:b3 (00:0e:c6:c3:6e:b3)
 > Internet Protocol Version 4, Src: 192.168.1.231, Dst: 192.168.1.119
 > User Datagram Protocol, Src Port: 58376, Dst Port: 59562
 Source Port: 58376
 Destination Port: 59562

Bên nhận

2151	113.688763	192.168.1.231	192.168.1.119	RTP	46 Unknown RTP version 3
2154	113.700047	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8033, Time=434688359
2155	113.702487	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8034, Time=434688359
2156	113.707204	192.168.1.119	192.168.1.231	RTP	1164 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8035, Time=434688359, Mark
2157	113.710934	192.168.1.119	192.168.1.231	RTP	60 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8036, Time=434688359
2158	113.712189	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8037, Time=434688359
2159	113.712189	192.168.1.119	192.168.1.231	RTP	539 PT=DynamicRTP-Type-96, SSRC=0xE85FFA9, Seq=5078, Time=231834655, Mark
2160	113.715301	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8038, Time=434688359
2161	113.720562	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8039, Time=434688359
2163	113.723599	192.168.1.119	192.168.1.231	RTP	619 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8040, Time=434688359, Mark
2164	113.726908	192.168.1.119	192.168.1.231	RTP	60 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8041, Time=434691360
2165	113.732363	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8042, Time=434691360
2166	113.732363	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8043, Time=434691360
2167	113.733039	192.168.1.119	192.168.1.231	RTP	564 PT=DynamicRTP-Type-96, SSRC=0xE85FFA9, Seq=5079, Time=231835680, Mark
2168	113.737469	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8044, Time=434691360
2169	113.740693	192.168.1.119	192.168.1.231	RTP	280 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8045, Time=434691360, Mark
2170	113.743841	192.168.1.119	192.168.1.231	RTP	60 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8046, Time=434692859
2171	113.746935	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8047, Time=434692859
2172	113.750916	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8048, Time=434692859
2173	113.752372	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8049, Time=434692859
2174	113.755185	192.168.1.119	192.168.1.231	RTP	563 PT=DynamicRTP-Type-96, SSRC=0xE85FFA9, Seq=5080, Time=231836703, Mark
2175	113.759601	192.168.1.119	192.168.1.231	RTP	81 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8050, Time=434692859, Mark
2176	113.760912	192.168.1.119	192.168.1.231	RTP	60 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8051, Time=434694359
2177	113.766322	192.168.1.119	192.168.1.231	RTP	1442 PT=DynamicRTP-Type-96, SSRC=0x68CBD177, Seq=8052, Time=434694359

> Frame 2154: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits) on interface \Device\NPF_{E4BF8B19-222E-4832-86E4-3E45A2217ABA}, id 0

> Ethernet II, Src: AsixElec_c3:6e:b3 (00:0e:c6:c3:6e:b3), Dst: LiteonTe_54:fc:9d (e0:0a:f6:54:fc:9d)

> Internet Protocol Version 4, Src: 192.168.1.119, Dst: 192.168.1.231

> User Datagram Protocol, Src Port: 59562, Dst Port: 58376

Source Port: 59562

Destination Port: 58376

Task 2: Phân tích hoạt động giao thức TCP

Câu 7: Tìm địa chỉ IP và TCP port của máy client

- IP address của client: 192.168.1.231
- Cổng port là : 50420

14126	33.856872	192.168.1.119	192.168.1.231	TCP	157 8080 → 50420 [RST, ACK] Seq=1 Ack=141 Win=1310
14151	33.911498	192.168.1.231	192.168.1.119	TCP	54 50420 → 8080 [ACK] Seq=141 Ack=104 Win=131072
14152	33.913151	192.168.1.119	192.168.1.231	TCP	450 8080 → 50420 [RST, ACK] Seq=104 Ack=141 Win=1310
14153	33.923412	13.107.138.9	192.168.1.231	TCP	1466 443 → 56756 [ACK] Seq=1809 Ack=3899 Win=16384
14156	33.923505	13.107.138.9	192.168.1.231	TLSv1.2	451 Application Data
14159	33.923541	192.168.1.231	13.107.138.9	TCP	54 56756 → 443 [ACK] Seq=3899 Ack=3618 Win=512 Le
14183	33.957174	192.168.1.231	192.168.1.119	TCP	54 50420 → 8080 [ACK] Seq=141 Ack=506 Win=130816
14202	34.400044	192.168.1.231	192.168.1.119	TLSv1.2	87 Application Data

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: TCP (6)

Header Checksum: 0x4e2f [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.231

Destination Address: 192.168.1.119

> Transmission Control Protocol, Src Port: 50420, Dst Port: 8080, Seq: 1

Source Port: 50420

Destination Port: 8080

[Stream index: 20]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 141 (relative sequence number)

Sequence Number (raw): 2520867610

[Next Sequence Number: 141 (relative sequence number)]

Acknowledgment Number: 104 (relative ack number)

Acknowledgment number (raw): 3292985013

0000 00 0e c6 c3 6e b3 e0 0a f6 54 fc 9d 08 00 45 00 ..

0010 00 28 67 f2 40 00 40 06 4e 2f c0 a8 01 e7 c0 a8 ..

0020 01 77 c4 f4 1f 90 96 41 63 1a c4 46 f6 b5 50 10 ..

0030 02 00 90 48 00 00 ..

Source Port (tcp.srcport), 2 bytes

Packets: 68880 · Displayed: 9280 (13.5%)

Profile: Default

Câu 8: Tìm địa chỉ của server? Kết nối TCP dùng để gửi và nhận các segments sử dụng port nào?

- Địa chỉ Ip của server: 192.168.1.119
- Sử dụng cổng port 8080 để nhận và gửi

Wireshark packet capture showing a TCP segment. The packet details pane highlights the source port 8080 and the sequence number 104. The packet is a TCP segment with sequence number 104, source port 8080, and destination port 50420. The packet is a PUSH (PSH) segment with the ACK flag set.

Câu 9: TCP SYN segment (gói tin TCP có cờ SYN) sử dụng sequence number nào để khởi tạo kết nối TCP giữa client và server? Thành phần nào trong segment cho ta biết segment đó là TCP SYN segment?

- TCP sử dụng sequence number 0 để khởi tạo kết nối TCP

Wireshark packet capture showing a TCP SYN segment. The packet details pane highlights the source port 50420 and the sequence number 0. The packet is a TCP SYN segment with sequence number 0, source port 50420, and destination port 8080. The packet is a SYN segment with the SYN flag set.

- Cờ SYN được bật lên 1 cho biết segment đó là TCP segment SYN

Wireshark packet capture showing the TCP flags field. The SYN flag is set to 1, indicating a SYN segment. The packet details pane shows the TCP flags field with the SYN flag set to 1.

Câu 10: Tìm sequence number của gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment? Tìm giá trị của Acknowledge trong SYN/ACK segment? Làm sao server có thể xác định giá trị đó? Thành phần nào trong segment cho ta biết đó là SYN/ ACKC segment

21540	51.4112...	192.168.1.231	192.168.1.119	TCP	66 50421 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
21542	51.4146...	192.168.1.119	192.168.1.231	TCP	66 8080 → 50421 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
21543	51.4146...	192.168.1.231	192.168.1.119	TCP	54 50421 → 8080 [ACK] Seq=1 Ack=1 Win=131328 Len=0
21544	51.4150...	192.168.1.231	192.168.1.119	HTTP	194 GET / HTTP/1.1
21562	51.4387...	192.168.1.119	192.168.1.231	TCP	157 8080 → 50421 [PSH, ACK] Seq=1 Ack=141 Win=131072 Len=103 [TCP segment of a reassembled PDU]
21581	51.4823...	192.168.1.231	192.168.1.119	TCP	54 50421 → 8080 [ACK] Seq=141 Ack=104 Win=131072 Len=0
21585	51.4861...	192.168.1.119	192.168.1.231	TCP	456 8080 → 50421 [PSH, ACK] Seq=104 Ack=141 Win=131072 Len=402 [TCP segment of a reassembled PDU]
21606	51.5276...	192.168.1.231	192.168.1.119	TCP	54 50421 → 8080 [ACK] Seq=141 Ack=506 Win=130816 Len=0
22291	53.6235...	192.168.1.231	162.159.128.235	TLSv1.2	140 Application Data
22309	53.6655...	162.159.128.235	192.168.1.231	TCP	54 443 → 51318 [ACK] Seq=229 Ack=2223 Win=8 Len=0

[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2770901143
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3979513008
1000 = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
000. = Reserved: Not set
...0 = Accurate ECN: Not set
...0 = Congestion Window Reduced: Not set
....0.. = ECN-Echo: Not set
....0. = Urgent: Not set
....1. = Acknowledgment: Set
....0... = Push: Not set
....0... = Reset: Not set
....1. = Syn: Set
....0... = Fin: Not set
[TCP Flags:A..S.]
Window: 65535

- Sequence number = 2770901143
- ACK number = 3979513008
- ACK number được xác định là số sequence number tiếp theo của TCP syn
 - o TCP syn sequence number = 3979513007

21540	51.4112...	192.168.1.231	192.168.1.119	TCP	66 50421 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
21542	51.4146...	192.168.1.119	192.168.1.231	TCP	66 8080 → 50421 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
21543	51.4146...	192.168.1.231	192.168.1.119	TCP	54 50421 → 8080 [ACK] Seq=1 Ack=1 Win=131328 Len=0
21544	51.4150...	192.168.1.231	192.168.1.119	HTTP	194 GET / HTTP/1.1
21562	51.4387...	192.168.1.119	192.168.1.231	TCP	157 8080 → 50421 [PSH, ACK] Seq=1 Ack=141 Win=131072 Len=103 [TCP segment of a reassembled PDU]
21581	51.4823...	192.168.1.231	192.168.1.119	TCP	54 50421 → 8080 [ACK] Seq=141 Ack=104 Win=131072 Len=0
21585	51.4861...	192.168.1.119	192.168.1.231	TCP	456 8080 → 50421 [PSH, ACK] Seq=104 Ack=141 Win=131072 Len=402 [TCP segment of a reassembled PDU]
21606	51.5276...	192.168.1.231	192.168.1.119	TCP	54 50421 → 8080 [ACK] Seq=141 Ack=506 Win=130816 Len=0
22291	53.6235...	192.168.1.231	162.159.128.235	TLSv1.2	140 Application Data
22309	53.6655...	162.159.128.235	192.168.1.231	TCP	54 443 → 51318 [ACK] Seq=229 Ack=2223 Win=8 Len=0

[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3979513007
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)

- TCP SYN ACK
 $ACK\ number = 3979513007 + 1 = 3975913008$

Sequence Number (raw): 2770901143
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 3979513008
 1000 = Header Length: 32 bytes (8)
 Flags: 0x012 (SYN, ACK)
 0000 = Reserved: Not set
 = Accurate ECN: Not set
 = Congestion Window Reduced: Not set
 = ECH-Echo: Not set
 = Urgent: Not set
 = Acknowledgment: Set
 = Push: Not set
 = Reset: Not set
 = Syn: Set
 = Fin: Not set
 [TCP Flags:A..S.]

- Cờ Syn và Acknowledge đều bật là 1