



BÁO CÁO LAB 3

Môn: Nhập môn mạng máy tính

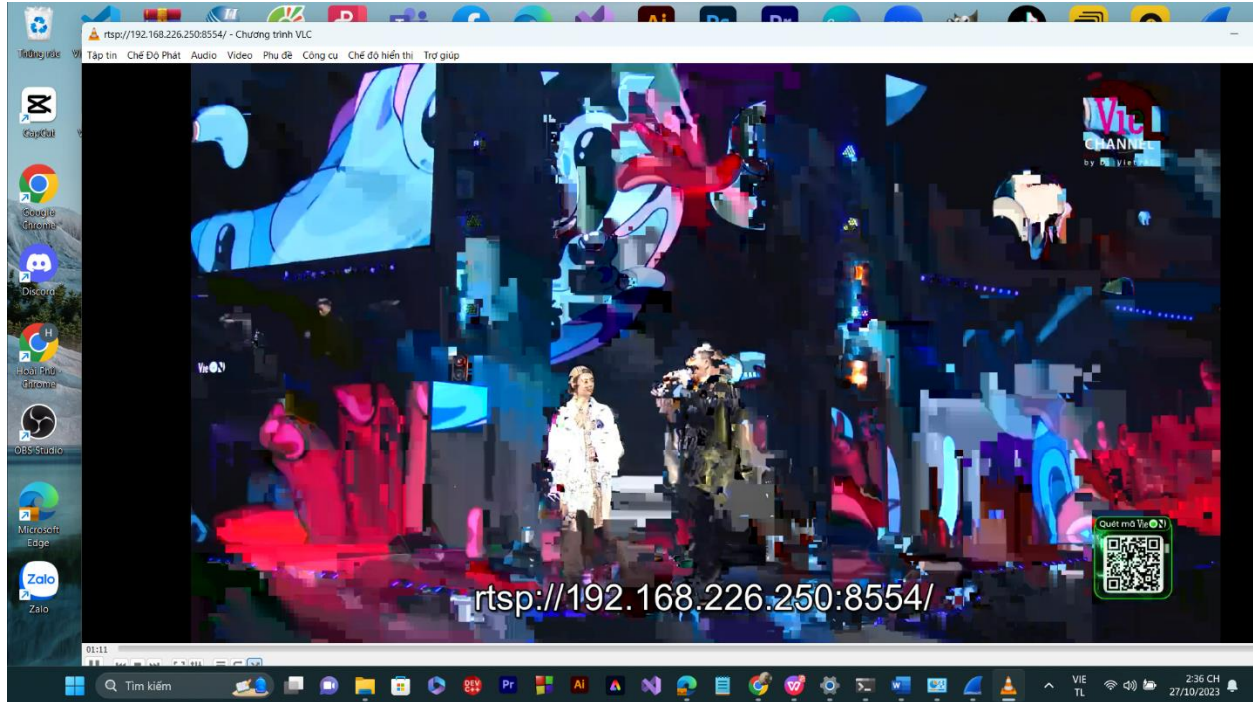
GVTH: Đỗ Thị Phương Uyên

Sinh viên thực hiện	Sinh viên 1 MSSV: 22521106 Họ tên: Trần Hoài Phú Sinh viên 2 MSSV: 22520776 Họ tên: Phạm Gia Linh
Lớp	IT005.O119.1
Tổng thời gian thực hiện Lab trung bình	3 tiếng
Phân chia công việc (nếu là nhóm)	[Sinh viên 1]: Làm task1 [Sinh viên 2]: Làm task 2
Link Video thực hiện (nếu có yêu cầu)	
Ý kiến (nếu có) + Khó khăn gặp phải + Đề xuất, góp ý...	
Điểm tự đánh giá (bắt buộc)	10 /10

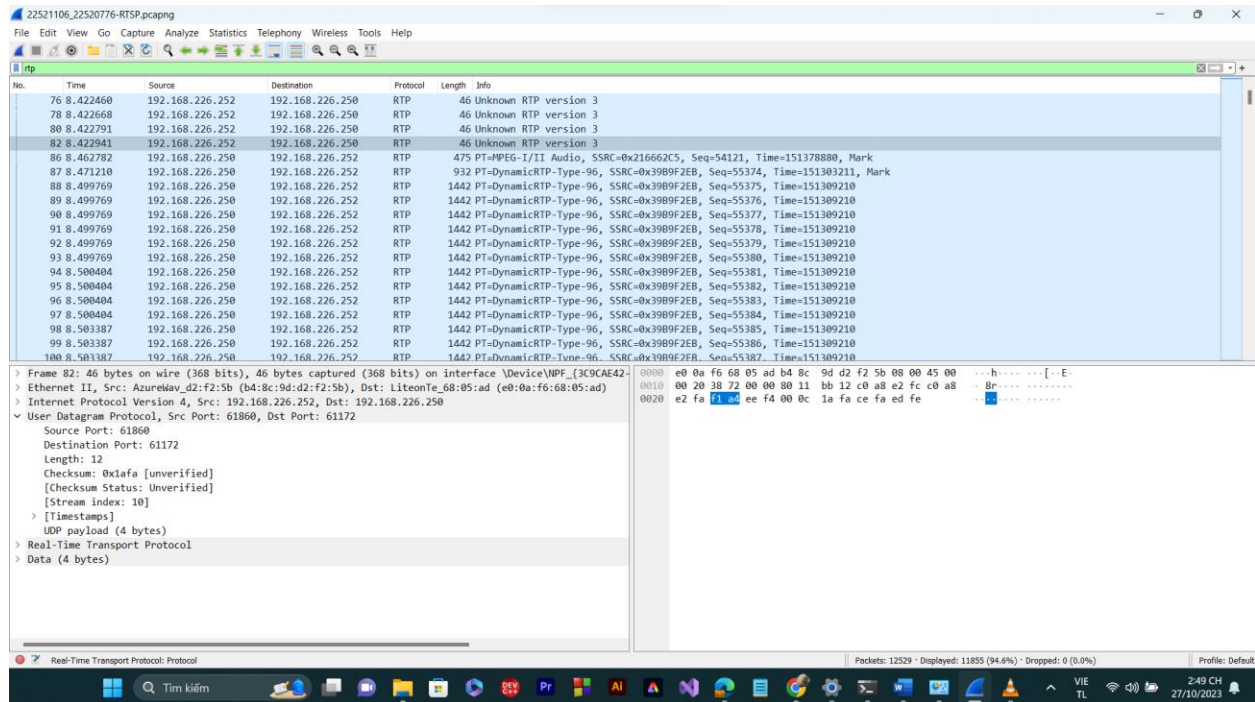


Task 1: Phân tích hoạt động giao thức UDP

Hình ảnh trong video máy Client bắt được:



1. Chọn một gói tin UDP, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó? Gợi ý: Xem tại phần User Datagram Protocol



Các trường (field) có trong UDP header bao gồm:

- **Source Port:** Trường này xác định cổng của người gửi thông tin và có ý nghĩa nếu muốn nhận thông tin phản hồi từ người nhận. Nếu không dùng đến thì đặt nó bằng 0.
- **Destination Port:** Trường xác định cổng nhận thông tin, và trường này là cần thiết.
- **Length:** Trường có độ dài 16 bit xác định chiều dài của toàn bộ datagram: phần header và dữ liệu. Chiều dài tối thiểu là 8 byte khi gói tin không có dữ liệu, chỉ có header.
- **Checksum:** Trường checksum 16 bit dùng cho việc kiểm tra lỗi của phần header và dữ liệu.

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



```
> Frame 82: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{3C9CAE42-...}
> Ethernet II, Src: AzureWav_d2:f2:5b (b4:8c:9d:d2:f2:5b), Dst: LiteonTe_68:05:ad (e0:0a:f6:68:05:ad)
> Internet Protocol Version 4, Src: 192.168.226.252, Dst: 192.168.226.250
> User Datagram Protocol, Src Port: 61860, Dst Port: 61172
  Source Port: 61860
  Destination Port: 61172
  Length: 12
  Checksum: 0x1afa [unverified]
  [Checksum Status: Unverified]
  [Stream index: 10]
  > [Timestamps]
    UDP payload (4 bytes)
> Real-Time Transport Protocol
> Data (4 bytes)
```

Source Port (udp.srcport), 2 byte(s)

- Destination Port: 2 bytes

```
> Frame 82: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{3C9CAE42-...}
> Ethernet II, Src: AzureWav_d2:f2:5b (b4:8c:9d:d2:f2:5b), Dst: LiteonTe_68:05:ad (e0:0a:f6:68:05:ad)
> Internet Protocol Version 4, Src: 192.168.226.252, Dst: 192.168.226.250
> User Datagram Protocol, Src Port: 61860, Dst Port: 61172
  Source Port: 61860
  Destination Port: 61172
  Length: 12
  Checksum: 0x1afa [unverified]
  [Checksum Status: Unverified]
  [Stream index: 10]
  > [Timestamps]
    UDP payload (4 bytes)
> Real-Time Transport Protocol
> Data (4 bytes)
```

Destination Port (udp.dstport), 2 byte(s)

- Datagram size (Length): 2 bytes

```
> Frame 82: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{3C9CAE42-...}
> Ethernet II, Src: AzureWav_d2:f2:5b (b4:8c:9d:d2:f2:5b), Dst: LiteonTe_68:05:ad (e0:0a:f6:68:05:ad)
> Internet Protocol Version 4, Src: 192.168.226.252, Dst: 192.168.226.250
> User Datagram Protocol, Src Port: 61860, Dst Port: 61172
  Source Port: 61860
  Destination Port: 61172
  Length: 12
  Checksum: 0x1afa [unverified]
  [Checksum Status: Unverified]
  [Stream index: 10]
  > [Timestamps]
    UDP payload (4 bytes)
> Real-Time Transport Protocol
> Data (4 bytes)
```

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

- Checksum: 2 bytes



```
> Frame 82: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{3C9CAE42-...}
> Ethernet II, Src: AzureWav_d2:f2:5b (b4:8c:9d:d2:f2:5b), Dst: LiteonTe_68:05:ad (e0:0a:f6:68:05:ad)
> Internet Protocol Version 4, Src: 192.168.226.252, Dst: 192.168.226.250
▼ User Datagram Protocol, Src Port: 61860, Dst Port: 61172
    Source Port: 61860
    Destination Port: 61172
    Length: 12
    Checksum: 0x1afa [unverified]
    [Checksum Status: Unverified]
    [Stream index: 10]
    > [Timestamps]
    UDP payload (4 bytes)
> Real-Time Transport Protocol
> Data (4 bytes)
```

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (udp.checksum), 2 byte(s)

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

- Trường Length xác định độ dài của toàn bộ datagram: header và data. Độ dài của trường Length trong trường hợp trên là 12 bytes.

```
▼ User Datagram Protocol, Src Port: 61860, Dst Port: 61172
    Source Port: 61860
    Destination Port: 61172
    Length: 12
    Checksum: 0x1afa [unverified]
    [Checksum Status: Unverified]
    [Stream index: 10]
    > [Timestamps]
    UDP payload (4 bytes)
> Real-Time Transport Protocol
> Data (4 bytes)
```

User Datagram Protocol (udp), 8 byte(s)

4. Số bytes lớn nhất mà payload (phần chứa dữ liệu gốc, không tính UDP header và IP header) của UDP có thể chứa? Gợi ý: Dựa vào kích thước của trường Length trong UDP header và giá trị lớn nhất có thể thể hiện.

- Số bytes lớn nhất mà payload (trừ đi 8 bytes của header) của UDP có thể chứa là $65535 - 8 = 65527$ bytes.



▼ User Datagram Protocol, Src Port: 61860, Dst Port: 61172

Source Port: 61860
Destination Port: 61172
Length: 12
Checksum: 0x1afa [unverified]
[Checksum Status: Unverified]
[Stream index: 10]
> [Timestamps]
UDP payload (4 bytes)

> Real-Time Transport Protocol
> Data (4 bytes)

User Datagram Protocol (udp), 8 byte(s)

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

- Giá trị lớn nhất có thể có của Source port: 65535.

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.

- Gói 82 và gói 87

Wireshark packet capture showing UDP traffic. The packet list shows two packets: packet 82 and packet 87. Packet 82 is a UDP packet from 192.168.226.252 to 224.0.0.251. Packet 87 is a response packet from 224.0.0.251 to 192.168.226.252. The packet details show the UDP payload and the Real-Time Transport Protocol (RTP) data.

Packet 82: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{3C9CAE42-...} Ethernet II, Src: Azure-Nic-800000000000, Dst: LiteonTe_68:05:ad (e0:0a:f6:68:05:ad)
> Internet Protocol Version 4, Src: 192.168.226.252, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 61860, Dst Port: 61172
> Real-Time Transport Protocol
> Data (4 bytes)

Packet 87: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{3C9CAE42-...} Ethernet II, Src: LiteonTe_68:05:ad (e0:0a:f6:68:05:ad), Dst: Azure-Nic-800000000000
> Internet Protocol Version 4, Src: 224.0.0.251, Dst: 192.168.226.252
> User Datagram Protocol, Src Port: 61172, Dst Port: 61860
> Real-Time Transport Protocol
> Data (4 bytes)

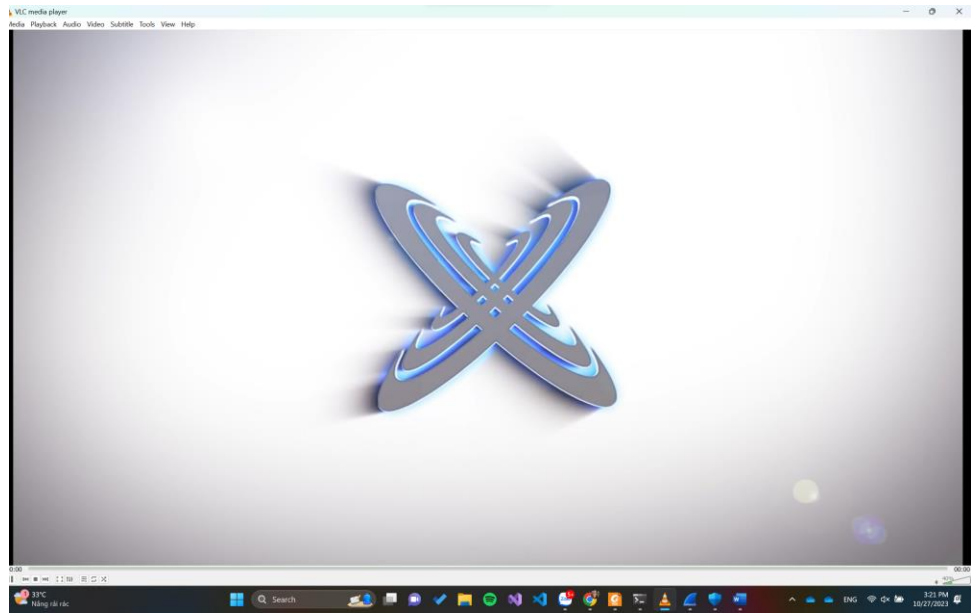


No.	Time	Source	Destination	Protocol	Length	Info
52	7.661700	192.168.226.252	224.0.0.251	MDNS	170	Standard query response 0x0000 AAAA 2401:d800:7b9d:cb60:be5a:6b9d:3a47:4a42 AAAA 2401:d800:7b9d:cb60:829:ab27:d681:c76 AAAA fe80::8620:49c0:dbd::ff02::1:3
53	7.661826	fe80::8620:49c0:dbd::ff02::1:3	ff02::1:3	MDNS	190	Standard query response 0x0000 AAAA 2401:d800:7b9d:cb60:be5a:6b9d:3a47:4a42 AAAA 2401:d800:7b9d:cb60:829:ab27:d681:c76 AAAA fe80::8620:49c0:dbd::ff02::1:3
54	7.661901	fe80::8620:49c0:dbd::ff02::1:3	ff02::1:3	LLMNR	90	Standard query 0xa5db ANY LAPTOP-PIO
55	7.662203	192.168.226.252	224.0.0.252	LLMNR	70	Standard query 0xa5db ANY LAPTOP-PIO
76	8.422460	192.168.226.252	192.168.226.250	RTP	46	Unknown RTP version 3
77	8.422637	192.168.226.252	192.168.226.250	RTCP	46	Unknown RTP version 3
78	8.422668	192.168.226.252	192.168.226.250	RTP	46	Unknown RTP version 3
79	8.422692	192.168.226.252	192.168.226.250	RTCP	46	Unknown RTP version 3
80	8.422791	192.168.226.252	192.168.226.250	RTP	46	Unknown RTP version 3
81	8.422904	192.168.226.252	192.168.226.250	RTCP	46	Unknown RTP version 3
82	8.422941	192.168.226.252	192.168.226.250	RTP	46	Unknown RTP version 3
83	8.423080	192.168.226.252	192.168.226.250	RTCP	46	Unknown RTP version 3
86	8.462782	192.168.226.250	192.168.226.252	RTP	475	PT=MPEG-T/II Audio, SSRC=0x216662C5, Seq=54121, Time=151378880, Mark
87	8.471210	192.168.226.250	192.168.226.252	RTP	932	PT=DynamicRTP-Type-96, SSRC=0x3989F2EB, Seq=55374, Time=151303211, Mark
88	8.499769	192.168.226.250	192.168.226.252	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x3989F2EB, Seq=55375, Time=151309210
89	8.499769	192.168.226.250	192.168.226.252	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x3989F2EB, Seq=55376, Time=151309210
90	8.499769	192.168.226.250	192.168.226.252	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x3989F2EB, Seq=55377, Time=151309210
91	8.499769	192.168.226.250	192.168.226.252	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x3989F2EB, Seq=55378, Time=151309210
92	8.499769	192.168.226.250	192.168.226.252	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x3989F2EB, Seq=55379, Time=151309210
93	8.499769	192.168.226.250	192.168.226.252	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x3989F2EB, Seq=55380, Time=151309210
94	8.500404	192.168.226.250	192.168.226.252	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x3989F2EB, Seq=55381, Time=151309210
95	8.500404	192.168.226.250	192.168.226.252	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x3989F2EB, Seq=55382, Time=151309210
96	8.500404	192.168.226.250	192.168.226.252	RTP	1442	PT=DynamicRTP-Type-96, SSRC=0x3989F2EB, Seq=55383, Time=151309210

> Frame 87: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface \Device\NPF{3C9C4...} Ethernet II, Src: LiteonTe_68:95:ad (e0:8a:f6:68:95:ad), Dst: AzureWav_d2:f2:5b (b4:8c:9d:d2:f2:5b)
> Internet Protocol Version 4, Src: 192.168.226.250, Dst: 192.168.226.252
> User Datagram Protocol, Src Port: 61172, Dst Port: 61860
> Real-Time Transport Protocol, SSRC: 0x3989F2EB, Seq: 55374, Time: 151303211, Mark

0020 e2 fc be f4 f1 ad 03 82 48 c2 80 e0 d8 4e 09 04 ...-baxosa-Ha...N...
0030 b4 2b 39 b9 f2 eb 01 9f cb 6a 42 7f f3 49 19 a5 ...+9...j8...I...
0040 d4 a9 0b 7a 4b f7 e6 e7 8b ab 82 d5 72 0c 31 e0 ...-zK...-...I...
0050 6f d1 8d 48 00 88 77 67 6b b3 d1 a7 4f 33 1b 6c ...o-H-wp k...03.1
0060 0f 51 3e 20 5f 54 da b7 3e 20 0a 21 6e b6 aa 75 ...Q>_T...>:In-u
0070 cd 6c 6c 3c a3 70 e4 f2 57 54 16 28 87 ca ae 85 ...l<g...WT(...
0080 e4 00 4a 50 f5 d9 14 d1 6c f8 75 2f 23 82 80 96 ...-JP...1u/#...
0090 c0 48 43 64 a5 ba f5 49 37 76 f1 50 a0 08 59 8b ...HcDE-I 7v P-Y...
00a0 57 58 93 25 eb 43 63 d2 38 da c4 68 cc ce f7 37 ...MX%Cc-8...7
00b0 e4 9f 85 96 3f 2c 3d 01 7d 3d 58 72 c6 7a 09 d2 ...-7...)=Xp-z...
...-7...)=Xp-z...
...-7...)=Xp-z...

Task 2: Phân tích hoạt động giao thức TCP





7. Tìm địa chỉ IP và TCP port của máy Client?

- Địa chỉ Ip của máy client: 192.168.226.250

- TCP port của máy client: 53090

22521106.22520776-TCP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
129	4.706059	2603:1063:2202:38::	2401:d800:7b9d:cb60::	TCP	2712	443 → 52928 [ACK] Seq=2865 Ack=5245 Win=16384 Len=2638 [TCP segment of a reassembled PDU]
130	4.706130	2401:d800:7b9d:cb60::	2603:1063:2202:38::	TCP	74	52928 → 443 [ACK] Seq=5245 Ack=5503 Win=515 Len=0
131	4.706714	2603:1063:2202:38::	2401:d800:7b9d:cb60::	TLSv1.2	300	Application Data
132	4.751995	2401:d800:7b9d:cb60::	2603:1063:2202:38::	TCP	74	52928 → 443 [ACK] Seq=5245 Ack=5729 Win=514 Len=0
133	4.904352	192.168.226.250	192.168.226.252	TCP	54	8080 → 58822 [FIN, ACK] Seq=1 Ack=1 Win=4100 Len=0
134	4.906481	192.168.226.250	192.168.226.252	TCP	66	53090 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
135	4.921388	192.168.226.252	192.168.226.250	TCP	54	58822 → 8080 [ACK] Seq=1 Ack=2 Win=511 Len=0
136	4.983554	192.168.226.252	192.168.226.250	TCP	54	58822 → 8080 [FIN, ACK] Seq=1 Ack=2 Win=511 Len=0
137	4.983599	192.168.226.250	192.168.226.252	TCP	54	8080 → 58822 [ACK] Seq=2 Ack=2 Win=4100 Len=0
138	5.919823	192.168.226.250	192.168.226.252	TCP	66	[TCP Retransmission] 53090 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
139	5.920480	2401:d800:7b9d:cb60::	2603:1046:1402:1::4	TLSv1.2	110	Application Data
140	5.929437	192.168.226.252	192.168.226.250	TCP	66	8080 → 53090 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
141	5.929545	192.168.226.250	192.168.226.252	TCP	54	53090 → 8080 [ACK] Seq=1 Ack=1 Win=131328 Len=0
142	5.929659	192.168.226.250	192.168.226.252	HTTP	192	GET / HTTP/1.1
143	5.961147	192.168.226.252	192.168.226.250	TCP	157	8080 → 53090 [PSH, ACK] Seq=1 Ack=139 Win=1049600 Len=103 [TCP segment of a reassembled PDU]
144	6.013149	192.168.226.250	192.168.226.252	TCP	54	53090 → 8080 [ACK] Seq=139 Ack=104 Win=131072 Len=0
145	6.023969	2603:1046:1402:1::4	2401:d800:7b9d:cb60::	TLSv1.2	106	Application Data
146	6.023969	192.168.226.252	192.168.226.250	TCP	454	8080 → 53090 [PSH, ACK] Seq=104 Ack=139 Win=1049600 Len=400 [TCP segment of a reassembled PDU]

> Frame 142: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface
> Ethernet II, Src: LiteonTe_68:05:ad (e0:0a:f6:68:05:ad), Dst: AzureWav_d2:f2:5b (b4:
> Internet Protocol Version 4, Src: 192.168.226.250, Dst: 192.168.226.252
v Transmission Control Protocol, Src Port: 53090, Dst Port: 8080, Seq: 1, Ack: 1, Len:
Source Port: 53090
Destination Port: 8080
[Stream index: 10]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 138]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3090996209
[Next Sequence Number: 139 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 708543260
0101 = Header Length: 20 bytes (5)

0000 b4 8c 9d d2 f2 5b e0 0a f6 68 05 ad 08 00 45 00[...h....E-
0010 00 b2 d5 be 40 00 80 06 dd 3e c0 a8 e2 fa c0 a8@...>.....
0020 e2 fc cf 62 1f 90 b8 3c db f1 2a 3b 83 1c 50 18b...<.*;...P-
0030 02 01 e4 f3 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e /1.1..Ho st: 192.
0050 31 36 38 2e 32 32 36 2e 32 35 32 3a 38 30 38 30 168.226. 252:8080
0060 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 ..Accept : /*.*.A
0070 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 ccept-La nguage:
0080 65 6e 5f 55 53 0d 0a 55 73 65 72 2d 41 67 65 6e en_US..U ser-Agen
0090 74 3a 20 56 4c 43 2f 33 2e 30 2e 31 39 20 4c 69 t: VLC/3 .0.19 Li
00a0 62 56 4c 43 2f 33 2e 30 2e 31 39 0d 0a 52 61 6e bVLC/3.0.19..Ran
00b0 67 65 3a 20 62 79 74 65 73 3d 30 2d 0d 0a 0d 0a ge: byte s=0-....

Transmission Control Protocol: Protocol

Packets: 7079 · Displayed: 6623 (93.6%) · Dropped: 0 (0.0%) Profile: Default

33°C
Nắng rải rác

Search

3:24 PM
10/27/2023



8. Tìm địa chỉ IP của Server? Kết nối TCP dùng để gửi và nhận các segments sử dụng port nào?

- Địa chỉ IP của server là: 192.168.226.252

- Kết nối TCP dùng để gửi và nhận các segments sử dụng port: 8080

Transmission Control Protocol, Src Port: 8080, Dst Port: 53090, Seq: 1, Ack: 139, Len: 103

Source Port: 8080
Destination Port: 53090
[Stream index: 10]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 103]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 708543260
[Next Sequence Number: 104 (relative sequence number)]
Acknowledgment Number: 139 (relative ack number)
Acknowledgment number (raw): 3090996347
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 4100
[Calculated window size: 1049600]

0000 e0 0a f6 68 05 ad b4 8c 9d d2 f2 5b 08 00 45 00 ...h... [E...
0010 00 8f 3a 25 40 00 80 06 78 fb c0 a8 e2 fc c0 a8 ...:x...
0020 e2 fa 1f 90 cf 62 2a 3b 83 1c b8 3c dc 7b 50 18 ...b*...<P...
0030 10 04 d4 f0 00 00 48 54 54 50 2f 31 2e 30 20 32 ...HT TP/1.0 2...
0040 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 74 ...OK...C ontent-t...
0050 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e ...ype: app lication...
0060 2f 6f 63 74 65 74 2d 73 74 72 65 61 6d 0d 0a 45 .../octet-s tream+G...
0070 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f ...ache-Con trol: no...
0080 2d 63 61 63 68 65 0d 0a 43 6f 6e 6e 65 63 74 69 ...-cache.. Connecti...
0090 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 0d 0a ...on: clos e....

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? Gợi ý: Quan sát trường Flags.

- TCP SYN segment (gói tin TCP có cờ SYN) sử dụng Sequence Number “0” nào để khởi tạo kết nối TCP giữa client và server.

- Thành phần Flag (cờ) SYN được bật lên để xác định đó là SYN Segment.



The image shows a Wireshark packet capture of a TCP segment. The packet list shows a packet with sequence number 0 and acknowledgment number 1. The packet details pane shows the following information:

- Sequence Number: 0 (relative sequence number)
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 3090996209
- 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
- Calculate window size: 65535

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 Acknowledgement trong SYN/ACK segment? Làm sao server có thể xác định giá trị đó? Thành phần nào trong segment cho ta biết segment đó là SYN/ACK segment?

- Sequence Number của gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment:

The image shows a Wireshark packet capture of a TCP segment. The packet list shows a packet with sequence number 0 and acknowledgment number 1. The packet details pane shows the following information:

- Sequence Number: 0 (relative sequence number)
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 3090996209
- 1000 = Header Length: 32 bytes (8)
- Flags: 0x012 (SYN, ACK)



- Giá trị của Acknowledgement trong SYN/ACK segment:

Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 708543259
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3090996209
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 = Reset: Not set
 > ...1 = **Syn: Set**
 ...0 = Fin: Not set
 [TCP Flags:A..S.]
Window: 65535
[Calculated window size: 65535]

- **Làm sao server có thể xác định giá trị đó:**
Bit cờ của trường ACK = 1 và bit cờ trường SYN = 1

Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 708543259
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3090996209
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
[Calculated window size: 65535]



11. Chỉ ra 6 segment đầu tiên mà server gửi cho Client (dựa vào Số thứ tự gói – No)

- Tìm sequence number của 6 segments đầu tiên đó?
- Xác định thời gian mà mỗi segment được gửi, thời gian ACK cho mỗi segment được nhận?
- Đưa ra sự khác nhau giữa thời gian mà mỗi segment được gửi và thời gian ACK cho mỗi segment được nhận bằng cách tính RTT (Round Trip Time) cho 6 segments này?
- Sequence number của 6 segments đầu tiên:

142	5.929659	192.168.226.250	192.168.226.252	HTTP	192 GET / HTTP/1.1
143	5.961147	192.168.226.252	192.168.226.250	TCP	1578080 → 53090 [PSH, ACK] Seq=1 Ack=139 Win=1049600 Len=103 [TCP segment of a reassembled PDU]
144	6.013149	192.168.226.250	192.168.226.252	TCP	54 53090 → 8080 [ACK] Seq=139 Ack=104 Win=131072 Len=0
145	6.023969	2603:1046:1402:1::4	2401:d800:7b9d:cb60::	TLSv1.2	106 Application Data
146	6.023969	192.168.226.252	192.168.226.250	TCP	454 8080 → 53090 [PSH, ACK] Seq=104 Ack=139 Win=1049600 Len=400 [TCP segment of a reassembled PDU]
147	6.067178	192.168.226.250	192.168.226.252	TCP	54 53090 → 8080 [ACK] Seq=139 Ack=504 Win=130816 Len=0
148	6.067178	2401:d800:7b9d:cb60::	2603:1046:1402:1::4	TCP	74 49880 → 443 [ACK] Seq=37 Ack=33 Win=511 Len=0
149	6.127910	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [ACK] Seq=504 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
150	6.148968	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [ACK] Seq=1964 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
151	6.148968	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [ACK] Seq=3424 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
152	6.148968	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [ACK] Seq=4884 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
153	6.148968	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [ACK] Seq=6344 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
154	6.148968	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [ACK] Seq=7804 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
155	6.148968	192.168.226.252	192.168.226.250	TCP	305 8080 → 53090 [PSH, ACK] Seq=9264 Ack=139 Win=1049600 Len=251 [TCP segment of a reassembled PDU]
156	6.149049	192.168.226.250	192.168.226.252	TCP	54 53090 → 8080 [ACK] Seq=139 Ack=9515 Win=131328 Len=0
157	6.149534	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [ACK] Seq=9515 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
158	6.149534	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [ACK] Seq=10975 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
159	6.149534	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [ACK] Seq=12435 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
160	6.149570	192.168.226.250	192.168.226.252	TCP	54 53090 → 8080 [ACK] Seq=139 Ack=13895 Win=131328 Len=0
161	6.154183	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [ACK] Seq=13895 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
162	6.168585	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [PSH, ACK] Seq=15355 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
163	6.168621	192.168.226.250	192.168.226.252	TCP	54 53090 → 8080 [ACK] Seq=139 Ack=16815 Win=131328 Len=0
164	6.170828	192.168.226.252	192.168.226.250	TCP	1514 8080 → 53090 [PSH, ACK] Seq=16815 Ack=139 Win=1049600 Len=1460 [TCP segment of a reassembled PDU]
165	6.171457	192.168.226.252	192.168.226.250	TCP	379 8080 → 53090 [PSH, ACK] Seq=18275 Ack=139 Win=1049600 Len=325 [TCP segment of a reassembled PDU]
166	6.171473	192.168.226.250	192.168.226.252	TCP	54 53090 → 8080 [ACK] Seq=139 Ack=18600 Win=131328 Len=0

STT	STT segments	Thời gian gửi	Thời gian nhận ACK	RTT (Round trip time)
1	143-144	5.961147	6.013149	0.052002
2	146-147	6.023969	6.067178	0.043209
3	155-156	6.148968	6.149049	0.000081
4	157-160	6.149534	6.149570	0.000036
5	161-163	6.154183	6.168621	0.014438
6	164-166	6.170828	6.171473	0.000645

12. Có segment nào được gửi lại hay không? Thông tin nào trong quá trình truyền tin cho chúng ta biết điều đó?

- Có segment gửi lại, dựa vào sequence number. Biểu đồ:

