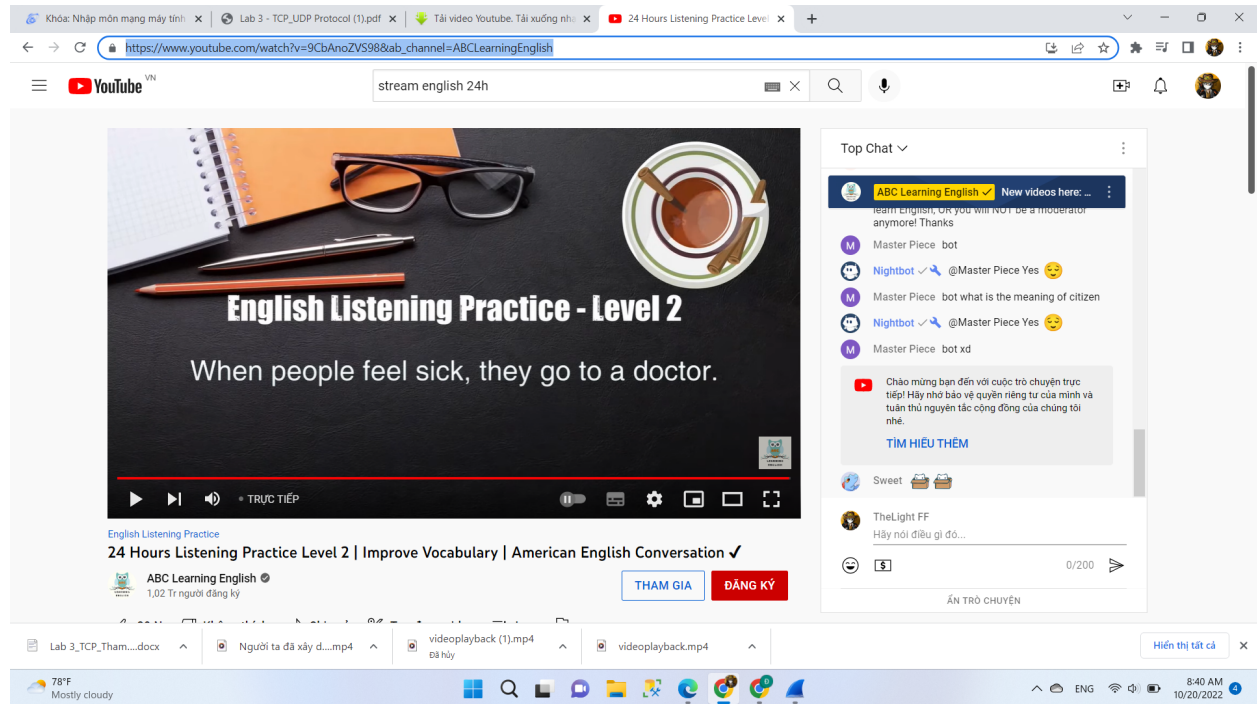


Tên: Nguyễn Thành Đăng
MSSV: 21520683
Lớp: IT005.N12

Phân tích hoạt động của giao thức TCP - UDP

Task 1. Phân tích hoạt động giao thức UDP



Vì không stream được VLC nên em bắt gói tin UDP từ youtube

Link: https://www.youtube.com/watch?v=9CbAnoZVS98&ab_channel=ABCLearningEnglish

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.

Có 4 trường field

Source Port: 443 Trường này xác định cổng của người gửi thông tin và có ý nghĩa nếu muốn nhận thông tin phản hồi từ người nhận. (Port nguồn)

Destination Port: 61005 Trường xác định cổng nhận thông tin, và trường này là cần thiết. (Port đích)

Length: 33 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: 0xbd7 Trường checksum 16 bit dùng cho việc kiểm tra lỗi của phần header và dữ liệu.

```
> Internet Protocol Version 4, Src: 172.217.24.238, Dst: 192.168.210.105
  User Datagram Protocol, Src Port: 443, Dst Port: 61005
    Source Port: 443
    Destination Port: 61005
    Length: 33
    Checksum: 0xabd7 [unverified]
    [Checksum Status: Unverified]
```



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

UDP gồm 4 trường, kích thước của mỗi trường:

- Source port number: 2 bytes
- Destination port number: 2 bytes
- Datagram size(Length) : 2 bytes
- Checksum : 2 bytes



- > Internet Protocol Version 4, Src: 172.217.24.238, Dst: 192.168.210.105
- Source Port: 443
 - Destination Port: 61005
 - Length: 33
 - Checksum: 0xabd7 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 0]
 - > [Timestamps]
 - UDP payload (25 bytes)
- > Data (25 bytes)

0000	94 e6 f7 12 fb 3d 18 66 da 02 cd 44 08 00 45 fc=f ...D..E.
0010	00 35 00 00 40 00 39 11 e7 e2 ac d9 18 ee c0 a8	.5..@.9.
0020	d2 69 01 bb ee 4d 00 21 ab d7 58 fc 9e 15 41 98	..i...M.! ..X...A.
0030	45 24 f3 cc 23 4c 4b c1 95 30 0c a5 d7 01 eb 21	E\$.-#LK- -0-....!
0040	af 4f 17	-O-

  Source Port (udp.srcport), 2 bytes

Source Port: 443
Destination Port: 61005
Length: 33
Checksum: 0xabd7 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
> [Timestamps]
UDP payload (25 bytes)
> Data (25 bytes)

0000	94 e6 f7 12 fb 3d 18 66 da 02 cd 44 08 00 45 fc=-f ...D..E.
0010	00 35 00 00 40 00 39 11 e7 e2 ac d9 18 ee c0 a8	-5..@-9-
0020	d2 69 01 bb ee 4d 00 21 ab d7 58 fc 9e 15 41 98	-i..M-! ..X...A.
0030	45 24 f3 cc 23 4c 4b c1 95 30 0c a5 d7 01 eb 21	E\$-#LK- .0-....!
0040	af 4f 17	-0-

  Destination Port (udp.dstport), 2 bytes

✓ User Datagram Protocol, Src Port: 443, Dst Port: 61005

Source Port: 443

Destination Port: 61005

Length: 33

Checksum: 0xabd7 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (25 bytes)

> Data (25 bytes)

0000	94 e6 f7 12 fb 3d 18 66	da 02 cd 44 08 00 45 fc=f...D..E.
0010	00 35 00 00 40 00 39 11	e7 e2 ac d9 18 ee c0 a8	-5-@.9.
0020	d2 69 01 bb ee 4d 00 21	ab d7 58 fc 9e 15 41 98	-i...M.!..X...A-
0030	45 24 f3 cc 23 4c 4b c1	95 30 0c a5 d7 01 eb 21	E\$.#LK-0....!
0040	af 4f 17		-O-



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

▼ User Datagram Protocol, Src Port: 443, Dst Port: 61005

Source Port: 443

Destination Port: 61005

Length: 33

Checksum: 0xabd7 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (25 bytes)

> Data (25 bytes)

```
0000  94 e6 f7 12 fb 3d 18 66 da 02 cd 44 08 00 45 fc  ....=f...D..E.
0010  00 35 00 00 40 00 39 11 e7 e2 ac d9 18 ee c0 a8  .5..@.9. ....
0020  d2 69 01 bb ee 4d 00 21 ab d7 58 fc 9e 15 41 98  .i..M.!..X...A.
0030  45 24 f3 cc 23 4c 4b c1 95 30 0c a5 d7 01 eb 21  E$.#LK..0....!
0040  af 4f 17                                     .O.
```

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

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

Giá trị trường Length trong UDP header là 8 bytes

Length = 33 bytes = 25 bytes (data) + 8 bytes (header)

▼ User Datagram Protocol, Src Port: 443, Dst Port: 61005

Source Port: 443

Destination Port: 61005

Length: 33

Checksum: 0xabd7 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (25 bytes)

> Data (25 bytes)

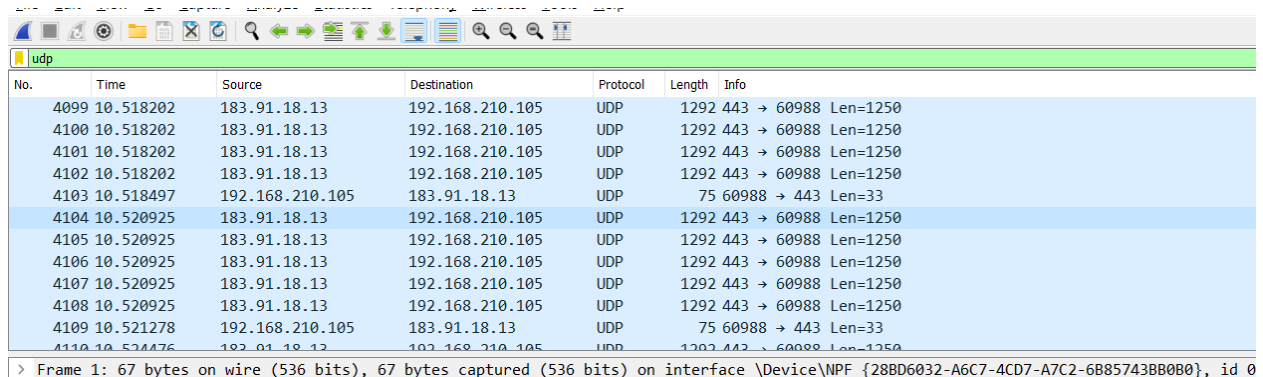
4. Số bytes lớn nhất mà payload (phần chứa dữ liệu gốc, không tính UDP header và IP header) của UDP có thể chứa? Gợi ý: Dựa vào kích thước của trường Length trong UDP header và giá trị lớn nhất có thể thể hiện.

Số bytes lớn nhất mà payload (trừ đi 8 bytes của header) của UDP có thể chứa là $65535 - 8 = 65527$ bytes. ($2^{16} - 1 = 65535$)

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

Giá trị lớn nhất có thể có của Source port: 65535 ($2^{16} - 1$)

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.
Trong quá trình gửi IP nguồn Request Packet sẽ trở thành Destination Port và Source Port sẽ trở thành Destination Port còn IP người gửi sẽ trở thành IP nguồn.



No.	Time	Source	Destination	Protocol	Length	Info
4099	10.518202	183.91.18.13	192.168.210.105	UDP	1292	443 → 60988 Len=1250
4100	10.518202	183.91.18.13	192.168.210.105	UDP	1292	443 → 60988 Len=1250
4101	10.518202	183.91.18.13	192.168.210.105	UDP	1292	443 → 60988 Len=1250
4102	10.518202	183.91.18.13	192.168.210.105	UDP	1292	443 → 60988 Len=1250
4103	10.518497	192.168.210.105	183.91.18.13	UDP	75	60988 → 443 Len=33
4104	10.520925	183.91.18.13	192.168.210.105	UDP	1292	443 → 60988 Len=1250
4105	10.520925	183.91.18.13	192.168.210.105	UDP	1292	443 → 60988 Len=1250
4106	10.520925	183.91.18.13	192.168.210.105	UDP	1292	443 → 60988 Len=1250
4107	10.520925	183.91.18.13	192.168.210.105	UDP	1292	443 → 60988 Len=1250
4108	10.520925	183.91.18.13	192.168.210.105	UDP	1292	443 → 60988 Len=1250
4109	10.521278	192.168.210.105	183.91.18.13	UDP	75	60988 → 443 Len=33
4110	10.524476	183.91.18.13	192.168.210.105	UDP	1292	443 → 60988 Len=1250

> Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{28BD6032-A6C7-4CD7-A7C2-6B85743BB0B0}, id 0

Task 2: Phân tích hoạt động giao thức TCP

Không bắt được stream, nên dùng web tham khảo của cô

21520683-Bai2_Lab3pcapng.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
33	0.676838	192.168.210.105	31.13.68.1	TLSv1.2	86	Application Data
35	0.721458	31.13.68.1	192.168.210.105	TCP	60	443 → 50152 [ACK] Seq=1 Ack=33 Win=524 Len=0
38	0.916203	31.13.68.1	192.168.210.105	TLSv1.2	82	Application Data
39	0.962272	192.168.210.105	31.13.68.1	TCP	54	50152 → 443 [ACK] Seq=33 Ack=29 Win=258 Len=0
43	1.713273	192.168.210.105	74.125.204.188	TCP	55	50162 → 5228 [ACK] Seq=1 Ack=1 Win=259 Len=1
44	1.774529	74.125.204.188	192.168.210.105	TCP	66	5228 → 50162 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
45	1.983901	192.168.210.105	74.125.204.188	TCP	55	50163 → 5228 [ACK] Seq=1 Ack=1 Win=258 Len=1
46	2.149524	74.125.204.188	192.168.210.105	TCP	66	5228 → 50163 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
53	3.152787	192.168.210.105	31.13.68.17	TLSv1.2	83	Application Data
54	3.153009	192.168.210.105	31.13.68.1	TLSv1.2	86	Application Data
62	3.227819	31.13.68.17	192.168.210.105	TCP	60	443 → 50674 [ACK] Seq=1 Ack=30 Win=486 Len=0
63	3.229429	31.13.68.1	192.168.210.105	TCP	60	443 → 50149 [ACK] Seq=1 Ack=33 Win=274 Len=0
73	3.404620	31.13.68.1	192.168.210.105	TLSv1.2	82	Application Data
74	3.409071	31.13.68.17	192.168.210.105	TLSv1.2	79	Application Data
75	3.450156	192.168.210.105	31.13.68.1	TCP	54	50149 → 443 [ACK] Seq=33 Ack=29 Win=258 Len=0
76	3.450174	192.168.210.105	31.13.68.17	TCP	54	50674 → 443 [ACK] Seq=30 Ack=26 Win=256 Len=0

> Frame 33: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{28BD6032-A6C7-4CD7-A7C2-6B85743B8080}, id 0

> Ethernet II, Src: IntelCor_12:fb:3d (94:e6:f7:12:fb:3d), Dst: Dell_02:cd:44 (18:66:da:02:cd:44)

> Internet Protocol Version 4, Src: 192.168.210.105, Dst: 31.13.68.1

> Transmission Control Protocol, Src Port: 50152, Dst Port: 443, Seq: 1, Ack: 1, Len: 32

> Transport Layer Security

```

0000  18 66 da 02 cd 44 94 e6 f7 12 fb 3d 08 00 45 00  .f...D...==.E.
0010  00 48 16 b0 40 00 80 06 00 00 c0 a8 d2 69 1f 0d  .H..@...==.i.
0020  44 01 c3 e8 01 bb 31 7b fc c2 46 83 d0 0d 50 18  D....1{...F}.P.
0030  01 02 f6 5a 00 00 17 03 03 00 1b 07 2c e5 0a 6b  ...Z.....,ck
0040  4e 24 2d cb ea 08 2e e5 4e ce 5d f1 61 18 8a 4c  N$-----N].a..L
0050  ba dc 9c 8f 3d 31                                ....=1

```

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

IP client: 192.168.210.105

TCP port client: 50751

76	3.450174	192.168.210.105	31.13.68.17	TCP	54	50674 → 443 [ACK] Seq=30 Ack=26 Win=256 Len=0
143	5.305676	192.168.210.105	128.119.245.12	TCP	66	50751 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
144	5.314493	192.168.210.105	128.119.245.12	TCP	66	50752 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
147	5.344994	192.168.210.105	40.90.184.82	TCP	66	50755 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

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

IP server: 128.119.245.12

TCP port gửi và nhận của server: 80

76	3.450174	192.168.210.105	31.13.68.17	TCP	54	50674 → 443 [ACK] Seq=30 Ack=26 Win=256 Len=0
143	5.305676	192.168.210.105	128.119.245.12	TCP	66	50751 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
144	5.314493	192.168.210.105	128.119.245.12	TCP	66	50752 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
147	5.344994	192.168.210.105	40.90.184.82	TCP	66	50755 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
148	5.408924	40.90.184.82	192.168.210.105	TCP	66	443 → 50755 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
149	5.409065	192.168.210.105	40.90.184.82	TCP	54	50755 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0

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 sử dụng **sequence number = 0** để tạo kết nối TCP giữa client và server.

Ở trường Flag, giá trị **SYN = 1** cho ta biết segment đó là TCP SYN segment

No.	Time	Source	Destination	Protocol	Length	Info
54	3.153009	192.168.210.105	31.13.68.1	TLSv1.2	86	Application Data
62	3.227819	31.13.68.17	192.168.210.105	TCP	60	443 → 50674 [ACK] Seq=1 Ack=30 Win=486 Len=0
63	3.229429	31.13.68.1	192.168.210.105	TCP	60	443 → 50149 [ACK] Seq=1 Ack=33 Win=274 Len=0
73	3.404620	31.13.68.1	192.168.210.105	TLSv1.2	82	Application Data
74	3.409071	31.13.68.17	192.168.210.105	TLSv1.2	79	Application Data
75	3.450156	192.168.210.105	31.13.68.1	TCP	54	50149 → 443 [ACK] Seq=33 Ack=29 Win=258 Len=0
76	3.450174	192.168.210.105	31.13.68.17	TCP	54	50674 → 443 [ACK] Seq=30 Ack=26 Win=256 Len=0
143	5.305676	192.168.210.105	128.119.245.12	TCP	66	50751 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
144	5.314493	192.168.210.105	128.119.245.12	TCP	66	50752 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
147	5.344994	192.168.210.105	40.90.184.82	TCP	66	50755 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
148	5.408924	40.90.184.82	192.168.210.105	TCP	66	443 → 50755 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
149	5.409065	192.168.210.105	40.90.184.82	TCP	54	50755 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
150	5.415845	192.168.210.105	40.90.184.82	TLSv1.2	571	Client Hello
151	5.441693	40.90.184.82	192.168.210.105	TCP	1506	443 → 50755 [ACK] Seq=1 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

1000 = Header Length: 32 bytes (8)

Flags: 0x002 (SYN)

000. = Reserved: Not set

...0 = Nonce: Not set

....0... = Congestion Window Reduced (CWR): Not set

....0... = ECN-Echo: Not set

....0... = Urgent: Not set

....0... = Acknowledgment: Not set

....0... = Push: Not set

....0... = Reset: Not set

...1... = Syn: Set

....0... = Fin: Not set

[TCP Flags:S.]

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?

No.	Time	Source	Destination	Protocol	Length	Info
54	3.153009	192.168.210.105	31.13.68.1	TLSv1.2	86	Application Data
62	3.227819	31.13.68.17	192.168.210.105	TCP	60	443 → 50674 [ACK] Seq=1 Ack=30 Win=486 Len=0
63	3.229429	31.13.68.1	192.168.210.105	TCP	60	443 → 50149 [ACK] Seq=1 Ack=33 Win=274 Len=0
73	3.404620	31.13.68.1	192.168.210.105	TLSv1.2	82	Application Data
74	3.409071	31.13.68.17	192.168.210.105	TLSv1.2	79	Application Data
75	3.450156	192.168.210.105	31.13.68.1	TCP	54	50149 → 443 [ACK] Seq=33 Ack=29 Win=258 Len=0
76	3.450174	192.168.210.105	31.13.68.17	TCP	54	50674 → 443 [ACK] Seq=30 Ack=26 Win=256 Len=0
143	5.305676	192.168.210.105	128.119.245.12	TCP	66	50751 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
144	5.314493	192.168.210.105	128.119.245.12	TCP	66	50752 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
147	5.344994	192.168.210.105	40.90.184.82	TCP	66	50755 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
148	5.408924	40.90.184.82	192.168.210.105	TCP	66	443 → 50755 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
149	5.409065	192.168.210.105	40.90.184.82	TCP	54	50755 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
150	5.415845	192.168.210.105	40.90.184.82	TLSv1.2	571	Client Hello
151	5.441693	40.90.184.82	192.168.210.105	TCP	1506	443 → 50755 [ACK] Seq=1 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]

Transmission Control Protocol, Src Port: 443, Dst Port: 50755, Seq: 0, Ack: 1, Len: 0

Source Port: 443

Destination Port: 50755

[Stream index: 7]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 510028631

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 3015447898

1000 = Header Length: 32 bytes (8)

Flags: 0x012 (SYN, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

....0... = Congestion Window Reduced (CWR): Not set

0000 94 e6 f7 12 fb 3d 18 66 da 02 cd 44 08 00 45 00f...D..E..

0010 00 34 03 11 40 00 71 06 92 f4 28 5a b8 52 c0 a8 ..4..@.q... (Z.R..

0020 d2 69 01 bb c6 43 1e 66 6b 57 b3 bc 15 5a 00 12 ..i...C.f.kW...Z..

0030 ff ff e0 82 00 00 02 04 05 a0 01 03 03 08 01 01

0040 04 02

Giá trị của Sequence number = 0.
 Giá trị của Acknowledgement = 1

No.	Time	Source	Destination	Protocol	Length	Info
54	3.153009	192.168.210.105	31.13.68.1	TLsv1.2	86	Application Data
62	3.227819	31.13.68.17	192.168.210.105	TCP	60	443 → 50674 [ACK] Seq=1 Ack=30 Win=486 Len=0
63	3.229429	31.13.68.1	192.168.210.105	TCP	60	443 → 50149 [ACK] Seq=1 Ack=33 Win=274 Len=0
73	3.404620	31.13.68.1	192.168.210.105	TLsv1.2	82	Application Data
74	3.409071	31.13.68.17	192.168.210.105	TLsv1.2	79	Application Data
75	3.450156	192.168.210.105	31.13.68.1	TCP	54	50149 → 443 [ACK] Seq=33 Ack=29 Win=258 Len=0
76	3.450174	192.168.210.105	31.13.68.17	TCP	54	50674 → 443 [ACK] Seq=30 Ack=26 Win=256 Len=0
143	5.305676	192.168.210.105	128.119.245.12	TCP	66	50751 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
144	5.314493	192.168.210.105	128.119.245.12	TCP	66	50752 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
147	5.344994	192.168.210.105	40.90.184.82	TCP	66	50755 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
148	5.408924	40.90.184.82	192.168.210.105	TCP	66	443 → 50755 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
149	5.409065	192.168.210.105	40.90.184.82	TCP	54	50755 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
150	5.415845	192.168.210.105	40.90.184.82	TLsv1.2	571	Client Hello
151	5.441693	40.90.184.82	192.168.210.105	TCP	1506	443 → 50755 [ACK] Seq=1 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled
Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 3015447898 1000 = Header Length: 32 bytes (8) ▾ Flags: 0x012 (SYN, ACK) 000. = Reserved: Not set ...0 = Nonce: Not set0... = Congestion Window Reduced (CWR): Not set0... = ECN-Echo: Not set0... = Urgent: Not set1... = Acknowledgment: Set0... = Push: Not set0... = Reset: Not set >1... = Syn: Set0... = Fin: Not set [TCP Flags:A..S.] Window: 65535						

Acknowledgment và Syn đều Set = 1

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?

6 segment gửi đầu tiên gửi và nhận

217	7.063910	192.168.210.105	128.119.245.12	TCP	10218	50751 → 80 [PSH, ACK] Seq=15235 Ack=1 Win=66560 Len=10164 [TCP segment of a reassembled PDU]
219	7.322905	128.119.245.12	192.168.210.105	TCP	60	80 → 50751 [ACK] Seq=1 Ack=16687 Win=62720 Len=0
220	7.322905	128.119.245.12	192.168.210.105	TCP	60	80 → 50751 [ACK] Seq=1 Ack=18139 Win=65664 Len=0
221	7.323035	192.168.210.105	128.119.245.12	TCP	2958	50751 → 80 [ACK] Seq=25399 Ack=1 Win=66560 Len=2904 [TCP segment of a reassembled PDU]
222	7.323840	128.119.245.12	192.168.210.105	TCP	60	80 → 50751 [ACK] Seq=1 Ack=19591 Win=68608 Len=0
223	7.323917	192.168.210.105	128.119.245.12	TCP	1506	50751 → 80 [ACK] Seq=28303 Ack=1 Win=66560 Len=1452 [TCP segment of a reassembled PDU]
224	7.325344	128.119.245.12	192.168.210.105	TCP	60	80 → 50751 [ACK] Seq=1 Ack=21043 Win=71552 Len=0
225	7.325414	192.168.210.105	128.119.245.12	TCP	2958	50751 → 80 [ACK] Seq=29755 Ack=1 Win=66560 Len=2904 [TCP segment of a reassembled PDU]
226	7.335002	128.119.245.12	192.168.210.105	TCP	60	80 → 50751 [ACK] Seq=1 Ack=22495 Win=74496 Len=0
227	7.335112	192.168.210.105	128.119.245.12	TCP	1506	50751 → 80 [PSH, ACK] Seq=32659 Ack=1 Win=66560 Len=1452 [TCP segment of a reassembled PDU]
228	7.335683	128.119.245.12	192.168.210.105	TCP	60	80 → 50751 [ACK] Seq=1 Ack=23947 Win=77440 Len=0
229	7.335759	192.168.210.105	128.119.245.12	TCP	1506	50751 → 80 [ACK] Seq=34111 Ack=1 Win=66560 Len=1452 [TCP segment of a reassembled PDU]

STT Packet	Thời gian gửi	Thời gian nhận TCK	RTT (Round trip time)
217	7.063910	7.322905	0.258995
221	7.323035	7.323840	0.000805
223	7.323917	7.325344	0.001427
225	7.325414	7.335002	0.009588
227	7.335112	7.335683	0.000571

229	7.335759	7.339145	0.003386
-----	----------	----------	----------

12. Có segment nào được gửi lại hay không? Thông tin nào trong quá trình truyền tin cho chúng ta biết điều đó? Gợi ý: Để kiểm tra lượng dữ liệu được truyền trong một đơn vị thời gian, thay vì phải tự tính toán trực tiếp từ dữ liệu của các gói tin, ta sử dụng một tính năng của Wireshark – Time – Sequence – Graph (Steven) Chọn một segment bất kỳ trong phần danh sách các gói tin. Chọn Statistics » TCP Stream Graph » Time-Sequence-Graph(Steven).

