



Lab 3

BÁO CÁO BÀI THỰC HÀNH SỐ 3 **Phân tích giao thức UDP và TCP** **UDP & TCP Protocol**

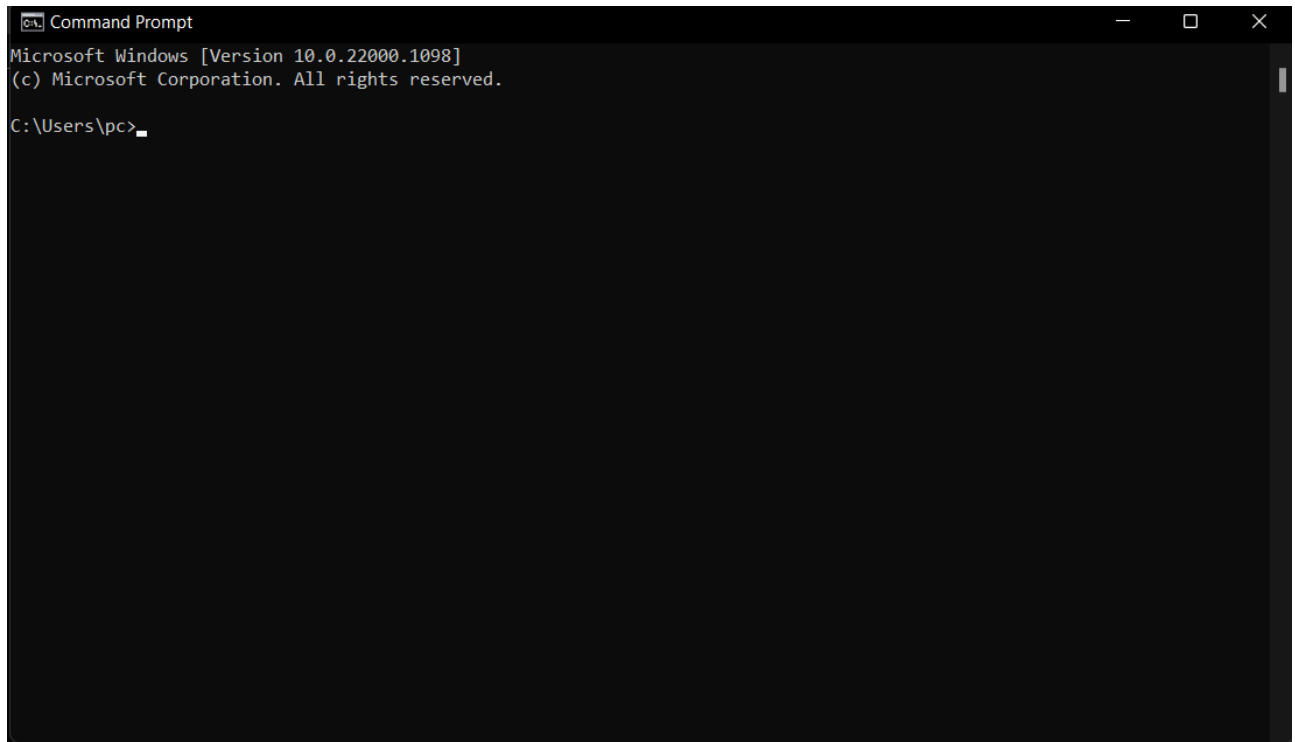
Môn học: Nhập môn Mạng máy tính

Giảng viên hướng dẫn	ThS. Đỗ Thị Hương Lan
Sinh viên thực hiện	Nguyễn Lê Quỳnh Hương (21520255)
Mức độ hoàn thành	Hoàn thành
Thời gian thực hiện	19/10/2022 – 19/10/2022
Tự chấm điểm	9/10

A. CÁC BƯỚC THỰC HÀNH

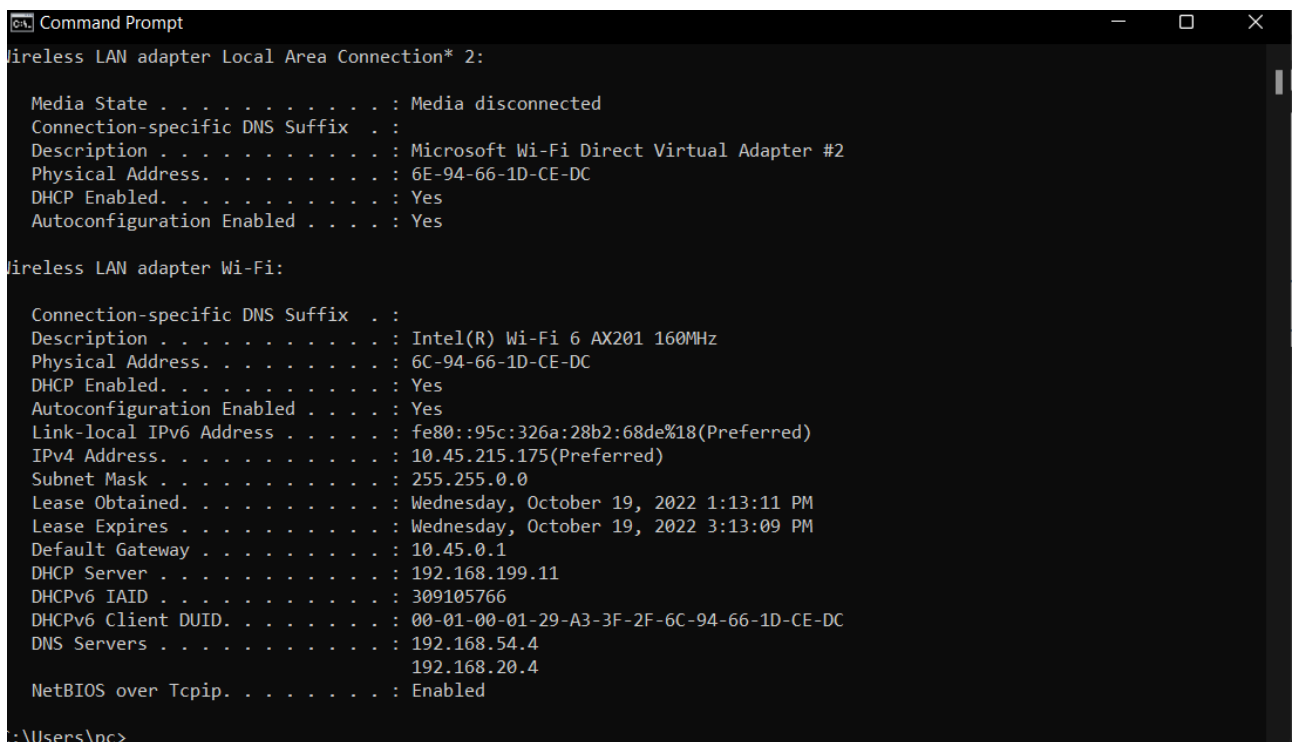
1. Bắt các gói tin truy vấn và phản hồi của DNS

Bước 1: Truy cập giao diện Command Prompt, sử dụng lệnh ipconfig /all



```
Command Prompt
Microsoft Windows [Version 10.0.22000.1098]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pc>
```



```
Command Prompt

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
    Physical Address. . . . . : 6E-94-66-1D-CE-DC
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

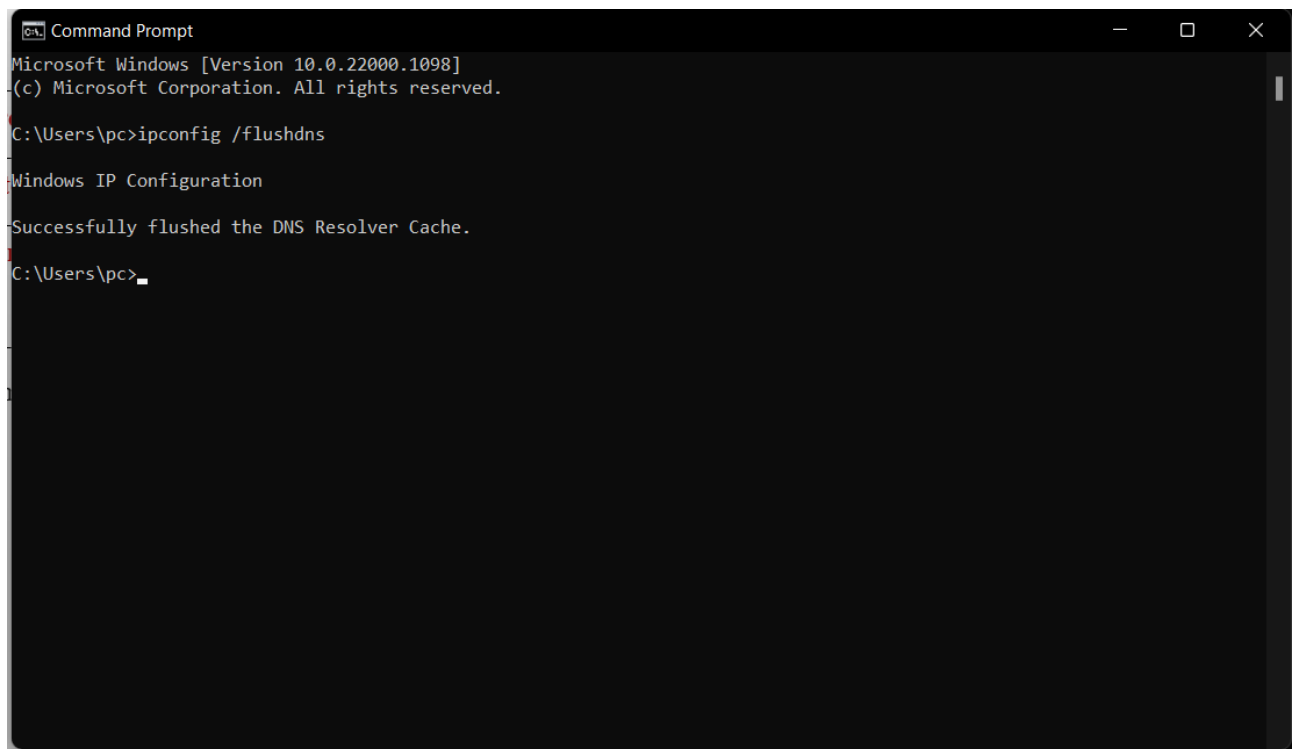
Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
    Physical Address. . . . . : 6C-94-66-1D-CE-DC
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::95c:326a:28b2:68de%18(Preferred)
    IPv4 Address. . . . . : 10.45.215.175(Preferred)
    Subnet Mask . . . . . : 255.255.0.0
    Lease Obtained. . . . . : Wednesday, October 19, 2022 1:13:11 PM
    Lease Expires . . . . . : Wednesday, October 19, 2022 3:13:09 PM
    Default Gateway . . . . . : 10.45.0.1
    DHCP Server . . . . . : 192.168.199.11
    DHCPv6 IAID . . . . . : 309105766
    DHCPv6 Client DUID. . . . . : 00-01-00-01-29-A3-3F-2F-6C-94-66-1D-CE-DC
    DNS Servers . . . . . : 192.168.54.4
                           192.168.20.4
    NetBIOS over Tcpip. . . . . : Enabled

C:\Users\pc>
```

IPv4, Link-local IPv6 address	10.45.215.175 fe80::95c:326a:28b2:68de%18
MAC address	6C-94-66-1D-CE-DC
Default gateway	10.45.0.1
DNS Servers	192.168.54.4 192.168.20.4

Bước 2 : Đảm bảo xóa DNS Cache bằng cách gõ lệnh ipconfig /flushdns



```
Command Prompt
Microsoft Windows [Version 10.0.22000.1098]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pc>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\pc>
```

Bước 3 : Khởi động phần mềm Wireshark. Chọn capture từ Interface đã ghi lại trong phần 1. Từ Command Line, gõ nslookup type=A uit.edu.vn

```
Command Prompt
Microsoft Windows [Version 10.0.22000.1098]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pc>ipconfig /flushdns

Windows IP Configuration

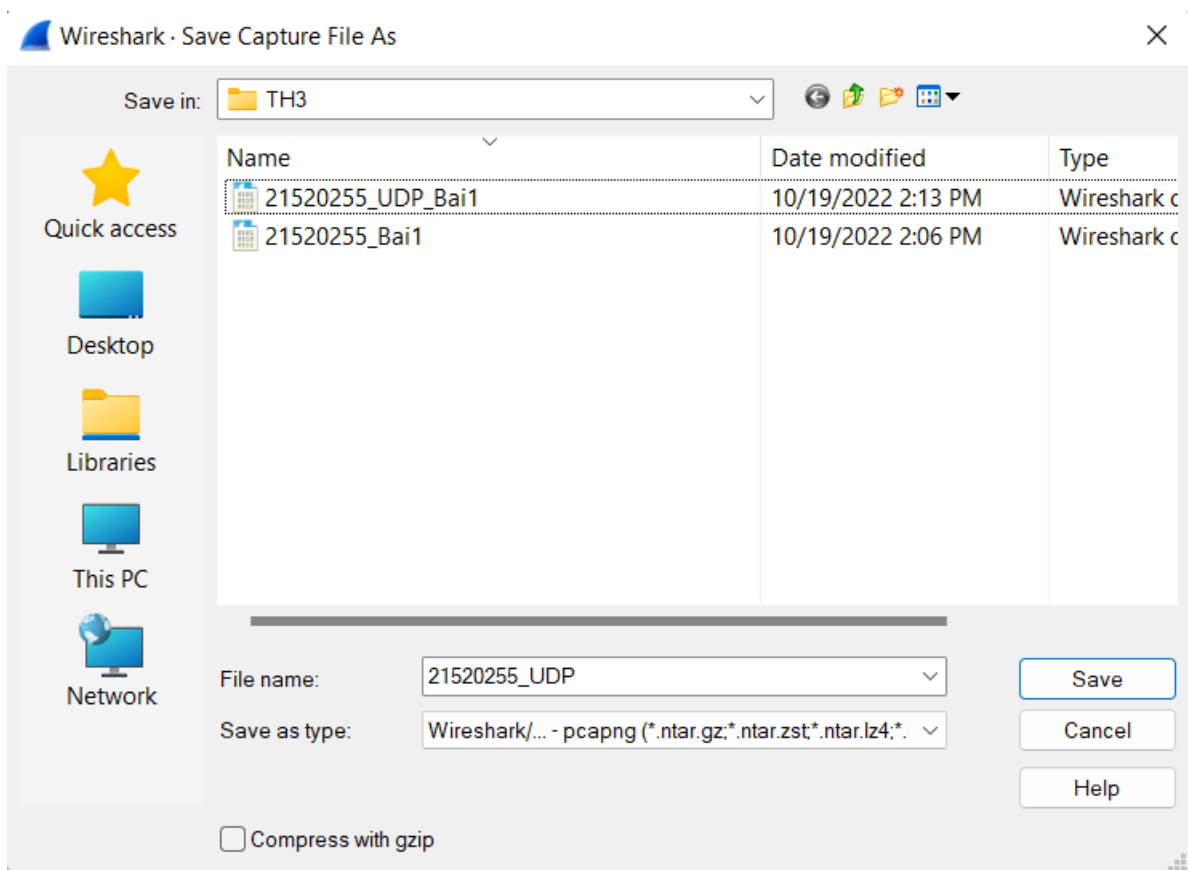
Successfully flushed the DNS Resolver Cache.

C:\Users\pc>nslookup type=A uit.edu.vn
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 192.168.20.23

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\pc>
```

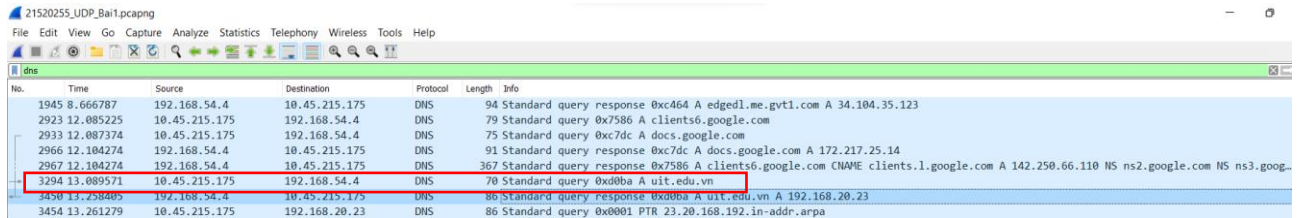
Bước 4: Dừng bắt gói tin và lưu lại dưới định dạng 21520255-UDP.pcapng



2. Phân tích các gói tin UDP

Câu 1 : Tại danh sách các gói tin bắt được, định vị gói tin truy vấn domain uit.edu.vn (hoặc domain tự chọn).

Gói tin số 3294 là gói tin truy vấn domain uit.edu.vn

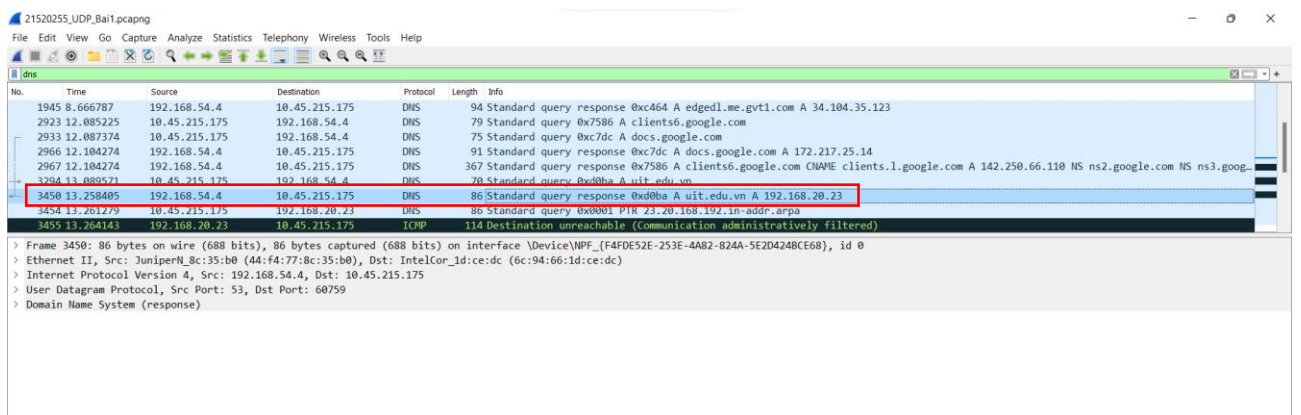


No.	Time	Source	Destination	Protocol	Length	Info
1945	8.666787	192.168.54.4	10.45.215.175	DNS	94	Standard query response 0xc464 A edgedl.me.gvt1.com A 34.104.35.123
2923	12.085225	10.45.215.175	192.168.54.4	DNS	79	Standard query 0x7586 A clients6.google.com
2933	12.087374	10.45.215.175	192.168.54.4	DNS	75	Standard query 0xc7dc A docs.google.com
2966	12.104274	192.168.54.4	10.45.215.175	DNS	91	Standard query response 0xc7dc A docs.google.com A 172.217.25.14
2967	12.104274	192.168.54.4	10.45.215.175	DNS	367	Standard query response 0x7586 A clients6.google.com CNAME clients.l.google.com A 142.250.66.110 NS ns2.google.com NS ns3.google.com
3294	13.080571	10.45.215.175	192.168.54.4	DNS	70	Standard query 0xd0ba A uit.edu.vn
3450	13.258405	192.168.54.4	10.45.215.175	DNS	86	Standard query response 0xd0ba A uit.edu.vn A 192.168.20.23
3454	13.261279	10.45.215.175	192.168.20.23	DNS	86	Standard query 0x0001 PTR 23.20.168.192.in-addr.arpa

Câu 2 : Xác định gói tin phản hồi của truy vấn trên? Từ thông điệp phản hồi, ghi lại địa chỉ IP của domain uit.edu.vn.

Gói tin phản hồi của truy vấn trên là gói tin số 3450.

Địa chỉ IP của domain uit.edu.vn là 192.168.54.4



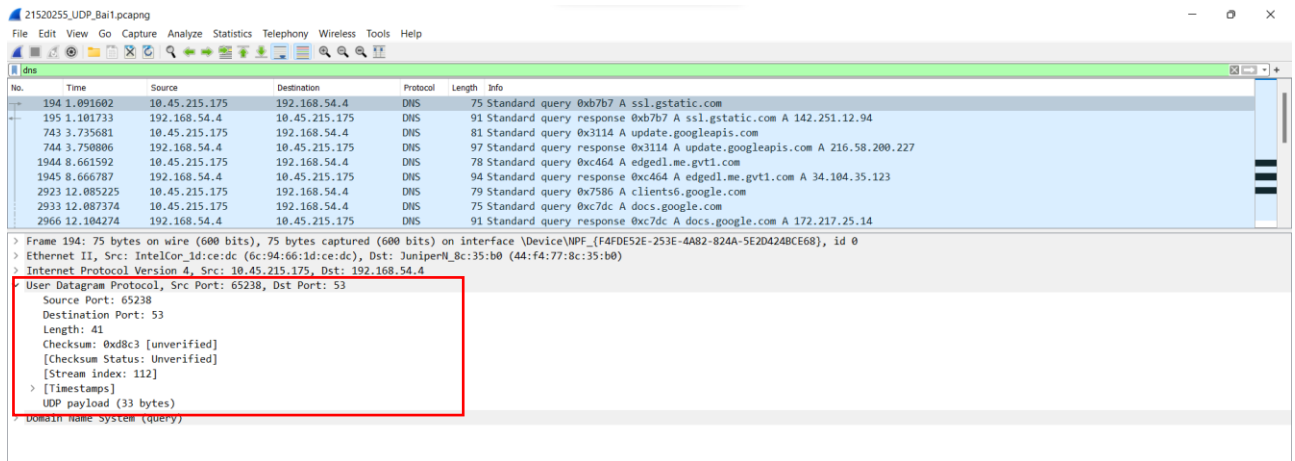
No.	Time	Source	Destination	Protocol	Length	Info
1945	8.666787	192.168.54.4	10.45.215.175	DNS	94	Standard query response 0xc464 A edgedl.me.gvt1.com A 34.104.35.123
2923	12.085225	10.45.215.175	192.168.54.4	DNS	79	Standard query 0x7586 A clients6.google.com
2933	12.087374	10.45.215.175	192.168.54.4	DNS	75	Standard query 0xc7dc A docs.google.com
2966	12.104274	192.168.54.4	10.45.215.175	DNS	91	Standard query response 0xc7dc A docs.google.com A 172.217.25.14
2967	12.104274	192.168.54.4	10.45.215.175	DNS	367	Standard query response 0x7586 A clients6.google.com CNAME clients.l.google.com A 142.250.66.110 NS ns2.google.com NS ns3.google.com
3294	13.080571	10.45.215.175	192.168.54.4	DNS	70	Standard query 0xd0ba A uit.edu.vn
3450	13.258405	192.168.54.4	10.45.215.175	DNS	86	Standard query response 0xd0ba A uit.edu.vn A 192.168.20.23
3454	13.261279	10.45.215.175	192.168.20.23	DNS	86	Standard query 0x0001 PTR 23.20.168.192.in-addr.arpa
3455	13.264143	192.168.20.23	10.45.215.175	TCP	114	Destination unreachable (communication administratively filtered)

> Frame 3450: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{F4FDE52E-253E-4A82-824A-5E2D424BC68}, id 0
 > Ethernet II, Src: Juniperl_8c:35:b0 (44:f4:77:8c:35:b0), Dst: IntelCor_id:ce:dc (6c:94:66:1d:ce:dc)
 > Internet Protocol Version 4, Src: 192.168.54.4, Dst: 10.45.215.175
 > User Datagram Protocol, Src Port: 53, Dst Port: 60759
 > Domain Name System (response)

Câu 3 : Chọn một gói tin DNS, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó?

- Source port : Số port nguồn 65238
- Destination Port : Số port đích 53
- Length : Độ dài được tính bằng byte của segment UDP, bao gồm cả header 41
- Checksum : dò tìm “các lỗi” (các bit cờ được bật) trong các segment đã được truyền 0xd8c3.
- UDP payload : Dữ liệu ứng dụng 33 bytes

Lab 3 : Phân tích giao thức UDP và TCP

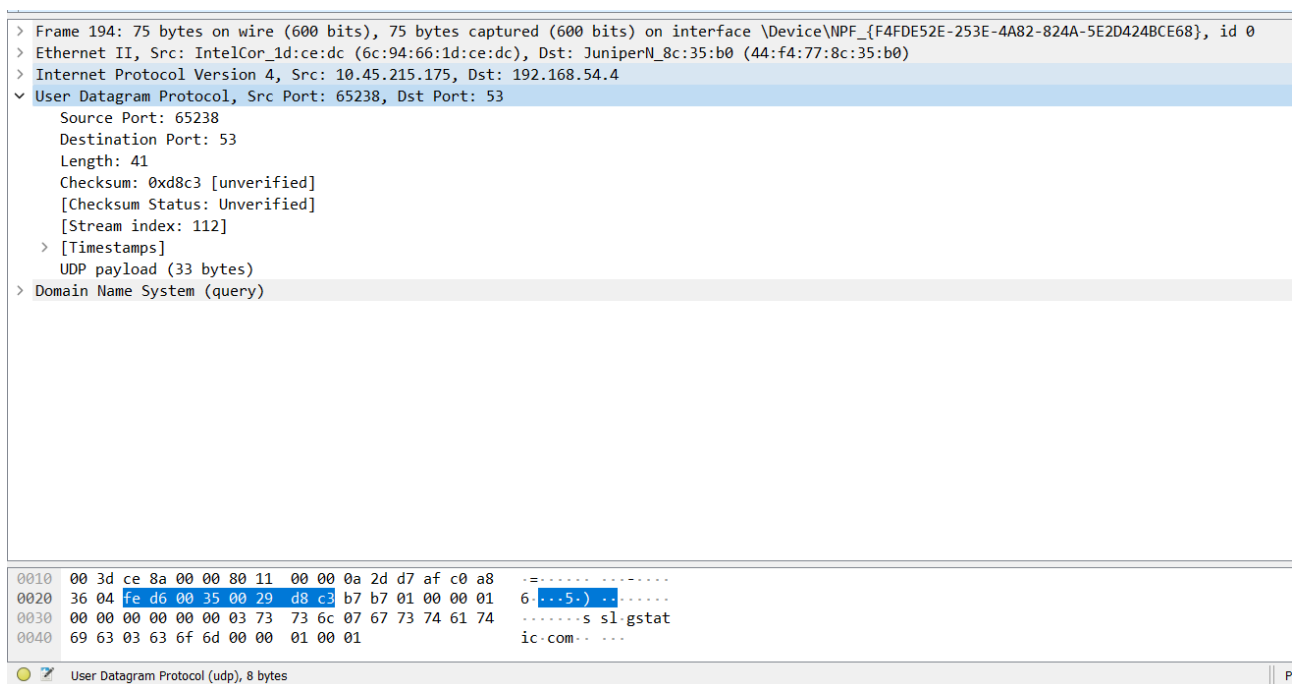


Câu 4 : Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?

- Source port có độ dài : 2 bytes
- Destination Port có độ dài : 2 bytes
- Length có độ dài : 2 bytes
- Checksum có độ dài : 2 bytes
- UDP payload có độ dài : 33 bytes

Câu 5 : Giá trị của trường Length trong UDP header là độ dài của gì? Chứng minh nhận định này bằng thông tin hiển thị của Wireshark?

Giá trị của trường Length trong UDP header là độ dài của segment UDP và UDP header
Chứng minh Length có độ dài là 41, gồm UDP payload : 33 và UDP header : 8



Câu 6 : Giá trị lớn nhất có thể có của port nguồn (Source port)?

Giá trị lớn nhất có thể có của port nguồn (Source port) là : 65535

Giải thích : Giá trị Source port chạy từ 0 đến 2 mũ 16, nên giá trị lớn nhất mà Source port có thể có là 2 mũ 16 trừ 1.

Câu 7 : Số bytes lớn nhất mà payload (phần chứa dữ liệu gốc, không tính UDP header và IP header) của UDP có thể chứa?

Số bytes lớn nhất mà payload của UDP có thể chứa là : $65535 - 8 = 65527$

Câu 8 : Quan sát 2 gói tin tìm được ở Câu 1 và 2, mô tả mối quan hệ giữa các địa chỉ IP và các port của 2 gói tin này.

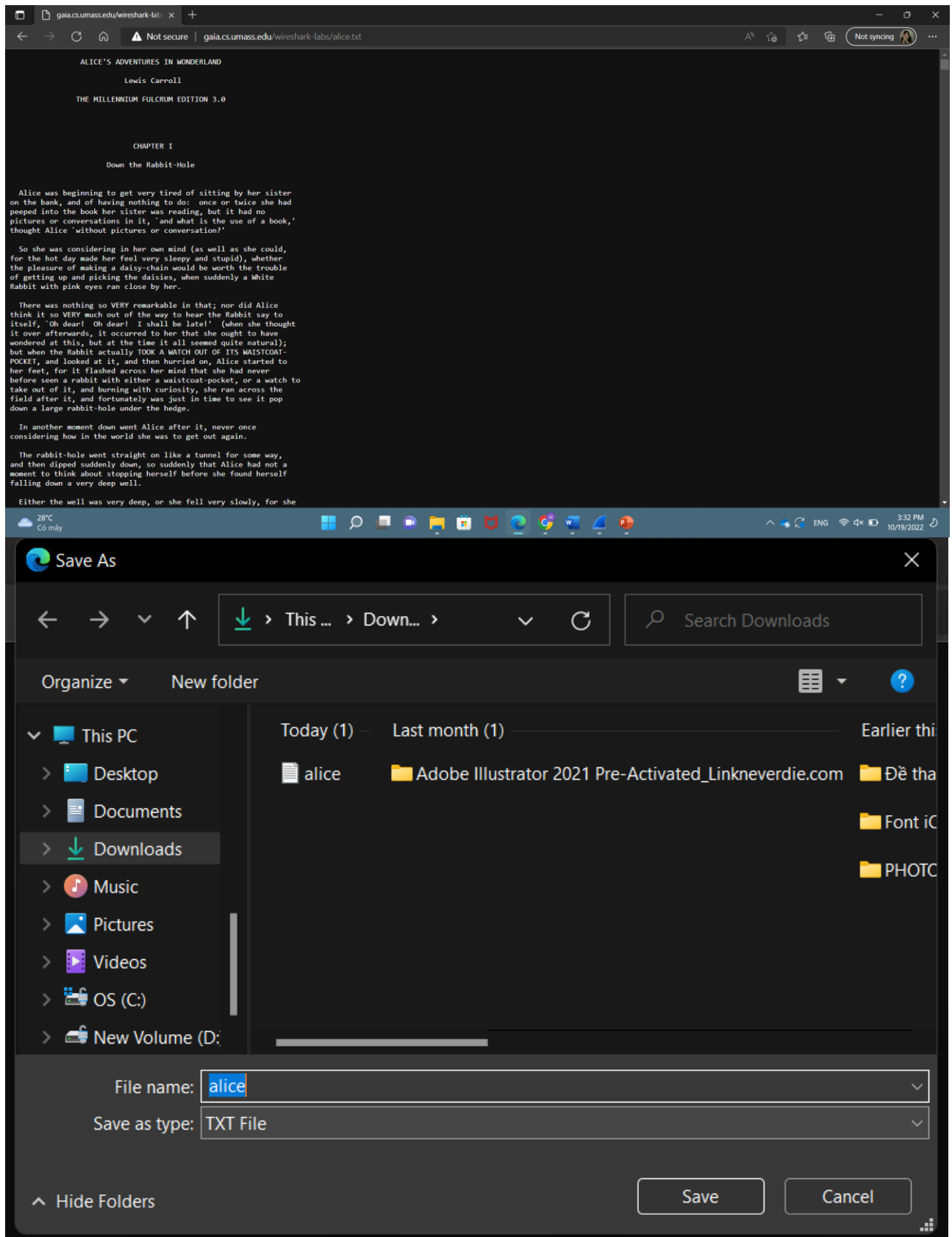
Gói tin ở câu 2 có phần Source port và Destination Port ngược lại so với gói tin ở câu 1. Quan sát phần Source (IP, Port) và Destination (IP, Port) của 2 gói tin.

The top screenshot shows a Wireshark capture of network traffic. The packet list shows a selected packet (No. 3294) with details: Source: 192.168.54.4, Destination: 10.45.215.175, Protocol: DNS, Length: 91. The details pane shows the packet structure: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (UDP). The UDP section shows Source Port: 60759, Destination Port: 53, Length: 36, and Checksum: 0xd8be [unverified].

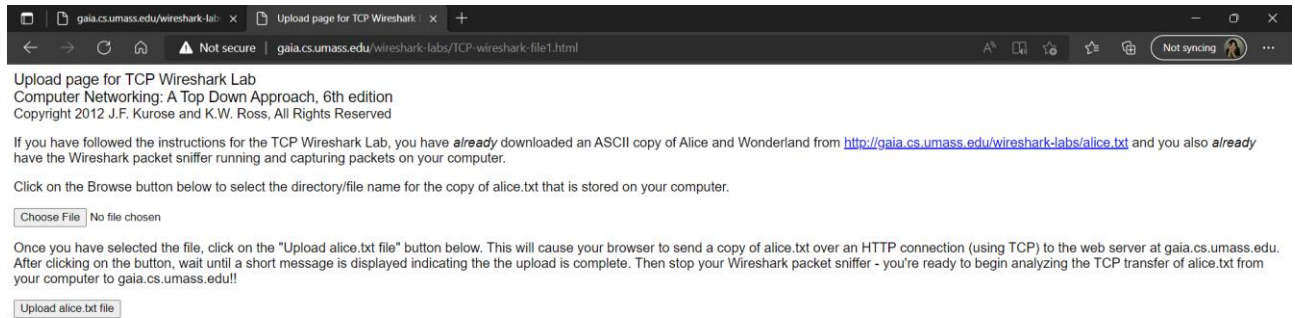
The bottom screenshot shows a similar Wireshark capture. The packet list shows a selected packet (No. 3450) with details: Source: 192.168.54.4, Destination: 10.45.215.175, Protocol: DNS, Length: 86. The details pane shows the packet structure: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (UDP). The UDP section shows Source Port: 53, Destination Port: 60759, Length: 52, and Checksum: 0xbdb0 [unverified].

3. Upload file thông qua Web Browser (HTTP) và bắt các gói tin TCP

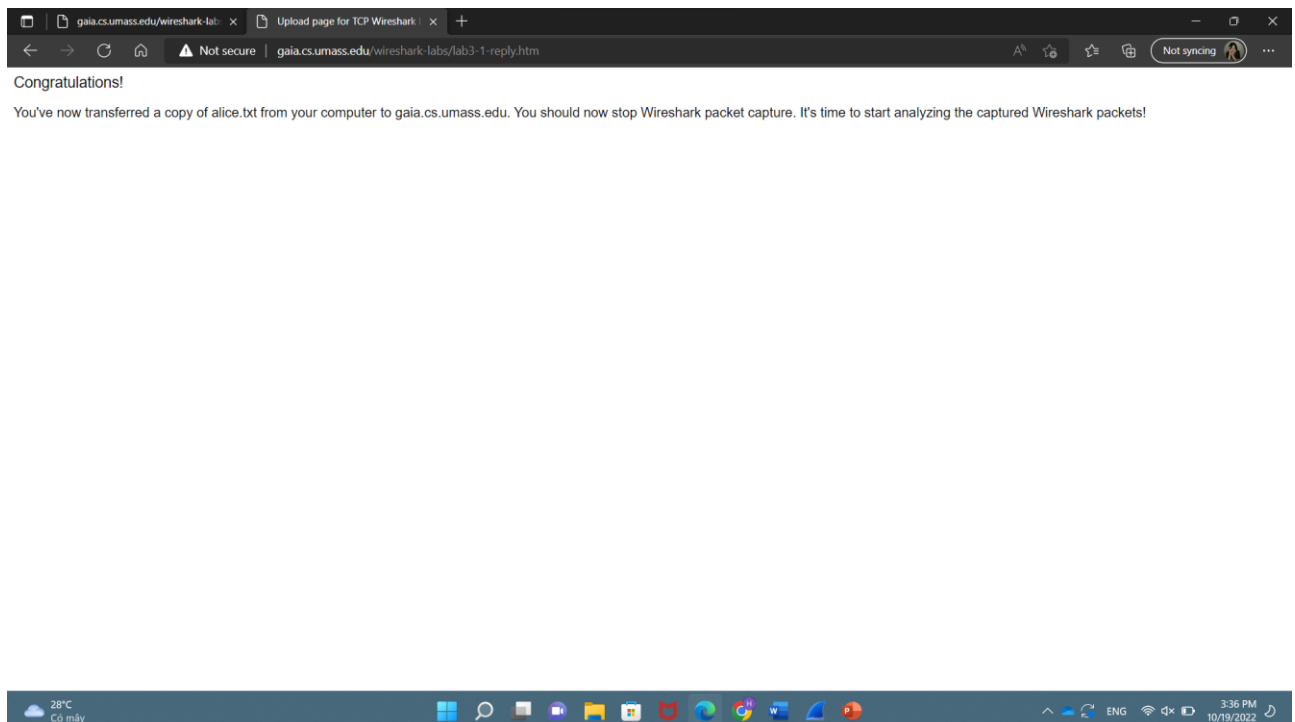
Bước 1 : Truy cập <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> và lấy bản sao ASCII của Alice in Wonderland. Lưu trữ tệp này trên máy tính của bạn



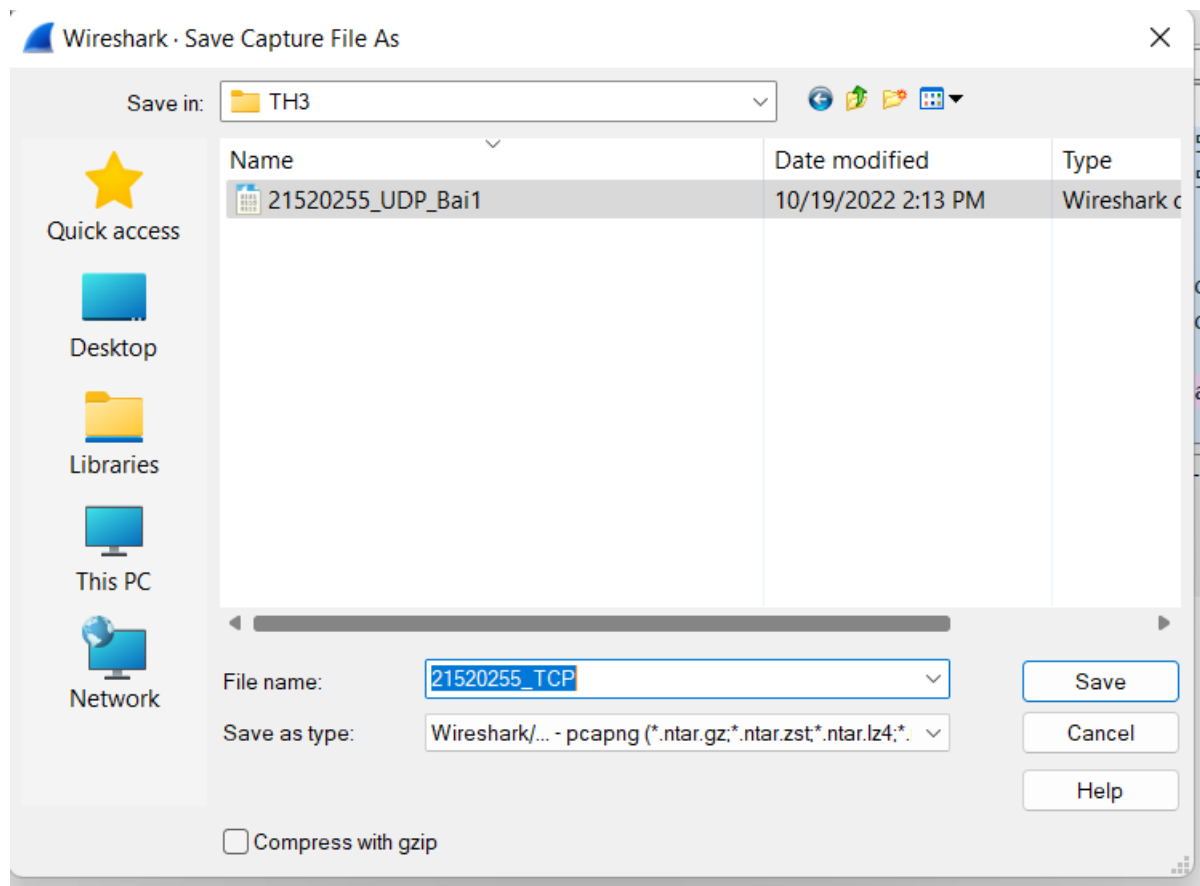
Bước 2 : Từ trình duyệt, truy cập đến địa chỉ sau: <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.



Bước 3 : Sử dụng nút Browse/Choose File trong trang web để chọn file alice.txt vừa download. Nhấn nút Upload alice.txt file để upload file lên server. Khi file đã được upload, một tin nhắn chúc mừng sẽ xuất hiện trên trình duyệt.



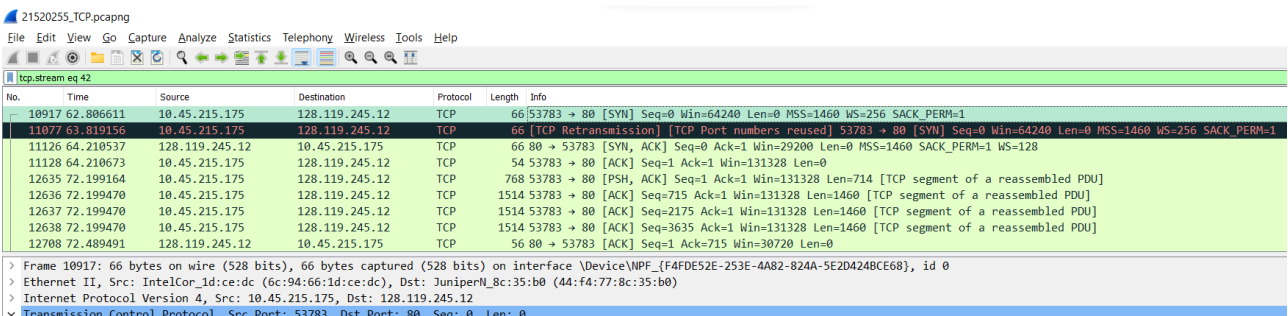
Bước 4: Dừng bắt gói tin và lưu lại dưới định dạng 21520255-TCP.pcapng



4. Phân tích các gói tin TCP

Câu 9 : Xác định Địa chỉ và cổng nguồn (Source Port) mà client sử dụng để chuyển tệp sang gaia.cs.umass.edu là gì?

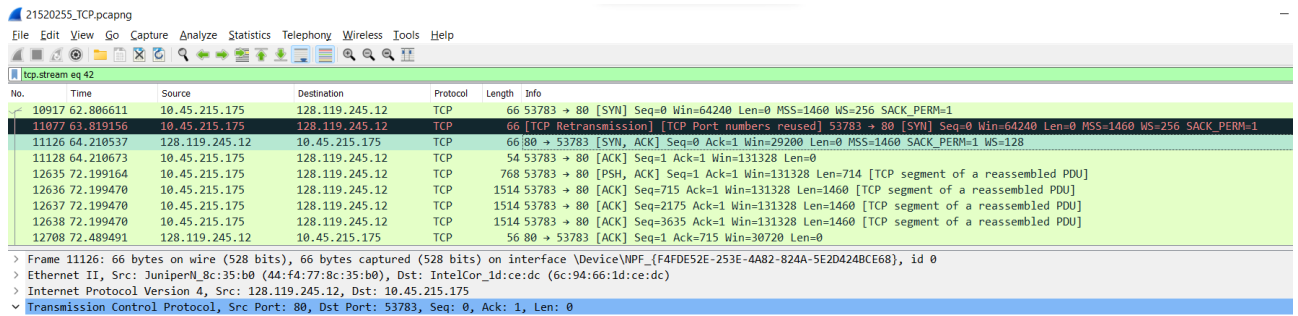
Địa chỉ IP của Client là 10.45.215.175 với Source Port là 53770.



Câu 10 : Địa chỉ IP của gaia.cs.umass.edu là gì? Trên số cổng nào nó nhận các dữ liệu của tệp alice.txt

IP của gaia.cs.umass.edu là : 128.119.245.12.
Trên số cổng 80 nó nhận các dữ liệu của tệp alice.txt

Lab 3 : Phân tích giao thức UDP và TCP



21520255.TCP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

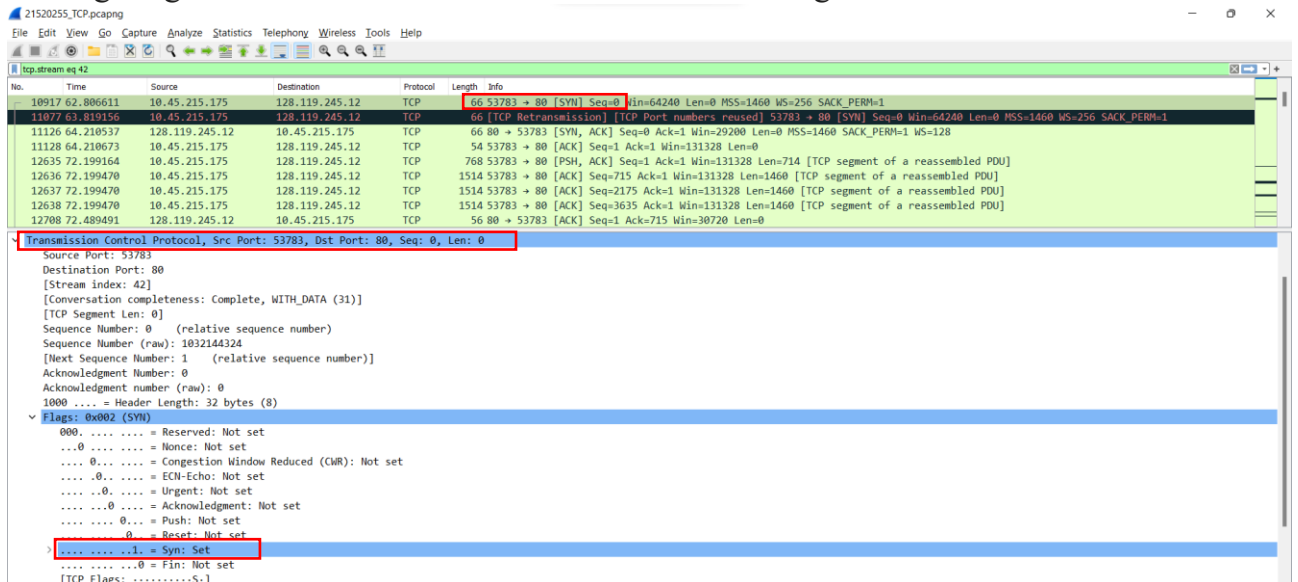
tcp.stream eq 42

No.	Time	Source	Destination	Protocol	Length	Info
10917	62.806611	10.45.215.175	128.119.245.12	TCP	66	53783 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11077	63.819156	10.45.215.175	128.119.245.12	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 53783 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11126	64.210537	128.119.245.12	10.45.215.175	TCP	66	80 → 53783 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
11128	64.210673	10.45.215.175	128.119.245.12	TCP	54	53783 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
12635	72.199164	10.45.215.175	128.119.245.12	TCP	768	53783 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=714 [TCP segment of a reassembled PDU]
12636	72.199470	10.45.215.175	128.119.245.12	TCP	1514	53783 → 80 [ACK] Seq=715 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
12637	72.199470	10.45.215.175	128.119.245.12	TCP	1514	53783 → 80 [ACK] Seq=2175 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
12638	72.199470	10.45.215.175	128.119.245.12	TCP	1514	53783 → 80 [ACK] Seq=3635 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
12708	72.489491	128.119.245.12	10.45.215.175	TCP	56	80 → 53783 [ACK] Seq=1 Ack=715 Win=30720 Len=0

Frame 11126: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{F4FDE52E-253E-4A82-824A-5E2D424BCE68}, id 0
Ethernet II, Src: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0), Dst: IntelCor_id:ce:dc (6c:94:66:1d:ce:dc)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.215.175
Transmission Control Protocol, Src Port: 80, Dst Port: 53783, Seq: 0, Ack: 1, Len: 0

Câu 11 : Định vị TCP SYN segment (gói tin TCP có cờ SYN) khởi tạo kết nối TCP giữa client và server? Thành phần nào trong segment cho ta biết segment đó là TCP SYN segment?

Trường Flags cờ SYN được set = 1 thì đó là TCP SYN segmen.



21520255.TCP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 42

No.	Time	Source	Destination	Protocol	Length	Info
10917	62.806611	10.45.215.175	128.119.245.12	TCP	66	53783 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11077	63.819156	10.45.215.175	128.119.245.12	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 53783 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11126	64.210537	128.119.245.12	10.45.215.175	TCP	66	80 → 53783 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
11128	64.210673	10.45.215.175	128.119.245.12	TCP	54	53783 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
12635	72.199164	10.45.215.175	128.119.245.12	TCP	768	53783 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=714 [TCP segment of a reassembled PDU]
12636	72.199470	10.45.215.175	128.119.245.12	TCP	1514	53783 → 80 [ACK] Seq=715 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
12637	72.199470	10.45.215.175	128.119.245.12	TCP	1514	53783 → 80 [ACK] Seq=2175 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
12638	72.199470	10.45.215.175	128.119.245.12	TCP	1514	53783 → 80 [ACK] Seq=3635 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
12708	72.489491	128.119.245.12	10.45.215.175	TCP	56	80 → 53783 [ACK] Seq=1 Ack=715 Win=30720 Len=0

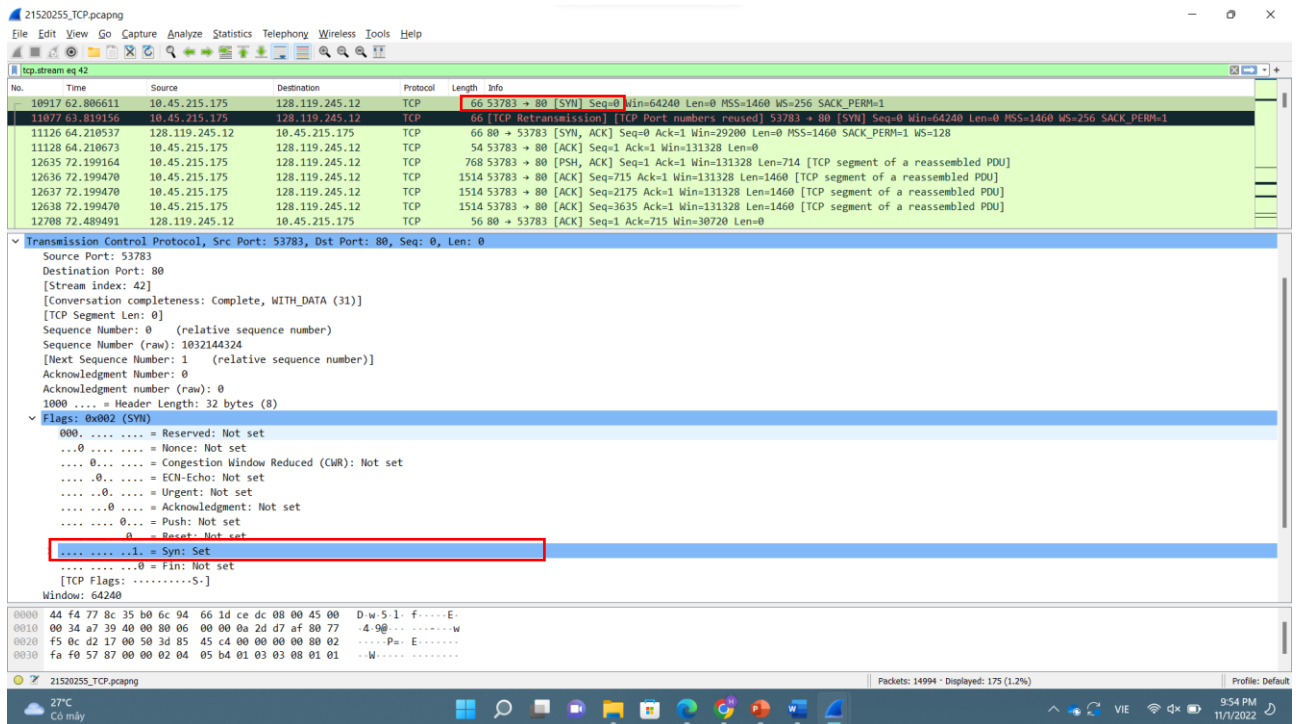
Transmission Control Protocol, Src Port: 53783, Dst Port: 80, Seq: 0, Len: 0

Source Port: 53783
Destination Port: 80
[Stream index: 42]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1032144324
[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.]

Câu 12 : TCP SYN segment ở trên có sequence number là bao nhiêu?

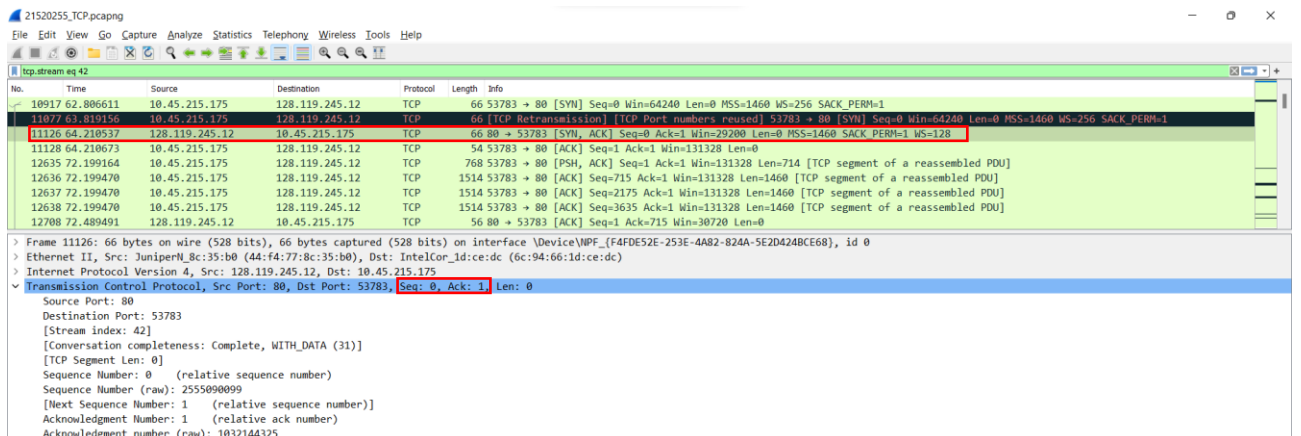
TCP SYN segment sử dụng sequence number bằng 0 để tạo kết nối TCP giữa client và server.

Lab 3 : Phân tích giao thức UDP và TCP



Câu 13 : Tìm sequence number của gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment ở trên?

Sequence number của SYN/ACK segment gửi từ sever đến client để trả lời cho SYN segment ở trên là 0.



**Câu 14 : 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?**

Giá trị của Acknowledgement trong SYN/ACK segment là 1.

Trường Flags trong Acknowledgement và SYN được set = 1 nên server có thể xác định được giá trị đó.

Lab 3 : Phân tích giao thức UDP và TCP

21520255_TCP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp stream eq 42

No.	Time	Source	Destination	Protocol	Length	Info
10917	62.806611	10.45.215.175	128.119.245.12	TCP	66	53783 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11077	63.819156	10.45.215.175	128.119.245.12	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 53783 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11126	64.210537	128.119.245.12	10.45.215.175	TCP	66	80 → 53783 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
11128	64.210673	10.45.215.175	128.119.245.12	TCP	54	53783 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
12635	72.199164	10.45.215.175	128.119.245.12	TCP	768	53783 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=714 [TCP segment of a reassembled PDU]
12636	72.199470	10.45.215.175	128.119.245.12	TCP	1514	53783 → 80 [ACK] Seq=715 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
12637	72.199470	10.45.215.175	128.119.245.12	TCP	1514	53783 → 80 [ACK] Seq=2175 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
12638	72.199470	10.45.215.175	128.119.245.12	TCP	1514	53783 → 80 [ACK] Seq=3635 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
12708	72.489491	128.119.245.12	10.45.215.175	TCP	56	80 → 53783 [ACK] Seq=1 Ack=715 Win=30720 Len=0

Transmission Control Protocol, Src Port: 80, Dst Port: 53783, Seq: 0, Ack: 1, Len: 0

Source Port: 80
Destination Port: 53783
[Stream index: 42]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 255090099
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1032144325
1000 = Header Length: 32 bytes (8)

Flags: 0x012 (SYN, ACK)
0000 = Reserved: Not set
...0 = Nonce: Not set
...0 = Congestion Window Reduced (CWR): 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: 29200

0000 6c 94 66 1d ce dc 44 f4 77 8c 35 b0 08 00 45 44 1-f...D...w...S...ED
0010 00 34 00 00 00 27 06 fc 1f 80 77 f5 0c 0a 2d 4-@...'....w...-
0020 d7 af 00 50 d2 17 00 00 00 00 3d 85 45 c5 80 12 --P...-E...-
0030 72 10 22 df 00 02 04 05 b4 01 01 04 02 01 03 m-.....

21520255_TCP.pcapng

Packets: 14994 - Displayed: 175 (1.2%)

Profile: Default

27°C
Có mây rải rác

Câu 15 : Chỉ ra 6 segment đầu tiên mà Client gửi cho Server (dựa vào Số thứ tự gói – No) và liệt kê vào bảng dưới đây :

- 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?
- Tính RTT (Round Trip Time) cho 6 segments này. Biết RTT là khoảng thời gian tính từ lúc máy tính bắt đầu gửi segment cho đến khi nó nhận được ACK trả về tương ứng.

○ Segment 1 (Frame 10916) sequence number: 0

21520255_TCP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
10913	62.789693	10.45.215.175	204.79.197.219	TCP	54	53757 → 443 [FIN, ACK] Seq=2 Ack=1 Win=516 Len=0
10914	62.789748	10.45.215.175	131.253.33.203	TCP	54	53737 → 443 [FIN, ACK] Seq=2 Ack=1 Win=515 Len=0
10915	62.789797	10.45.215.175	13.107.21.200	TCP	54	53749 → 443 [FIN, ACK] Seq=2 Ack=1 Win=515 Len=0
10916	62.790831	10.45.215.175	128.119.245.12	TCP	66	53782 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10917	62.806611	10.45.215.175	128.119.245.12	TCP	66	53783 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10919	62.817153	204.79.197.203	10.45.215.175	TCP	56	443 → 53725 [ACK] Seq=1 Ack=3 Win=16382 Len=0
10920	62.817153	204.79.197.219	10.45.215.175	TCP	56	443 → 53757 [ACK] Seq=1 Ack=3 Win=16382 Len=0
10921	62.817153	204.79.197.219	10.45.215.175	TCP	56	443 → 53757 [RST, ACK] Seq=1 Ack=3 Win=0 Len=0
10922	62.817153	204.79.197.203	10.45.215.175	TCP	56	443 → 53725 [RST, ACK] Seq=1 Ack=3 Win=0 Len=0

Transmission Control Protocol, Src Port: 53782, Dst Port: 80, Seq: 0, Len: 0

Source Port: 53782
Destination Port: 80
[Stream index: 41]
[Conversation completeness: Incomplete, ESTABLISHED (7)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1227676615
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)

Flags: 0x002 (SYN)
0000 = 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..]
Window: 64240

0010 00 34 a7 38 40 00 00 06 00 00 0a 2d d7 af 80 77 4-@...-...w...-
0020 f5 0c 52 16 00 50 49 2c db c7 00 00 00 00 80 02 --P...-E...-
0030 fa f0 57 87 00 00 02 04 05 b4 01 03 03 00 01 01 m-.....
0040 04 02

Transmission Control Protocol (tcp), 32 bytes

Packets: 14994 - Displayed: 689 (4.6%)

Profile: Default

26°C
Có mây rải rác

Lab 3 : Phân tích giao thức UDP và TCP

- Segment 2 (Frame 10917) sequence number: 0

The image shows a Wireshark packet capture of a TCP connection. The packet list on the left shows several packets, with packet 10917 (Frame 10917) selected. The packet details pane shows the Transmission Control Protocol (TCP) segment. The sequence number is 0, and the acknowledgment number is 0. The window size is 64240. The flags field shows the SYN flag set. The packet bytes pane shows the raw data of the packet.

Transmission Control Protocol, Src Port: 53783, Dst Port: 80, Seq: 0, Len: 0

Source Port: 53783
Destination Port: 80
[Stream index: 42]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1032144324
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
▼ Flags: 0x002 (SYN)
0000 = 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.]
Window: 64240

- Segment 3 (Frame 10982) sequence number: 0

The image shows a Wireshark packet capture of a TCP connection. The packet list on the left shows several packets, with packet 10982 (Frame 10982) selected. The packet details pane shows the Transmission Control Protocol (TCP) segment. The sequence number is 0, and the acknowledgment number is 0. The window size is 64240. The flags field shows the SYN flag set. The packet bytes pane shows the raw data of the packet.

Transmission Control Protocol, Src Port: 53787, Dst Port: 80, Seq: 0, Len: 0

Source Port: 53787
Destination Port: 80
[Stream index: 44]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1764852475
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
▼ Flags: 0x002 (SYN)
0000 = 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.]
Window: 64240

- Segment 4 (Frame 11024) sequence number: 1

Lab 3 : Phân tích giao thức UDP và TCP

The screenshot shows a Wireshark packet capture of a TCP connection. The packet list on the left shows several packets, with packet 5 (Frame 11075) selected. The packet details pane shows the following information:

- Source Port: 53787
- Destination Port: 80
- [Stream index: 44]
- [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 0]
- Sequence Number: 479 (relative sequence number)
- Sequence Number (raw): 1764852476
- [Next Sequence Number: 479 (relative sequence number)]
- Acknowledgment Number: 2195 (relative ack number)
- Acknowledgment number (raw): 304911856
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x010 (ACK)
- 0000 = Reserved: Not set
- ...0 = Nonce: Not set
- ...0 = Congestion Window Reduced (CWR): Not set
- ...0 = ECN-Echo: Not set
- ...0 = Urgent: Not set
- ...1 = Acknowledgment: Set
- ...0 = Push: Not set
- ...0 = Reset: Not set
- ...0 = Syn: Not set
- ...0 = Fin: Not set
- [TCP Flags:A....]
- Window: 513

The packet bytes pane shows the raw data of the packet, including the TCP header and the payload (HTTP/1.1 200 OK (text/html)).

o Segment 5 (Frame 11075) sequence number: 479

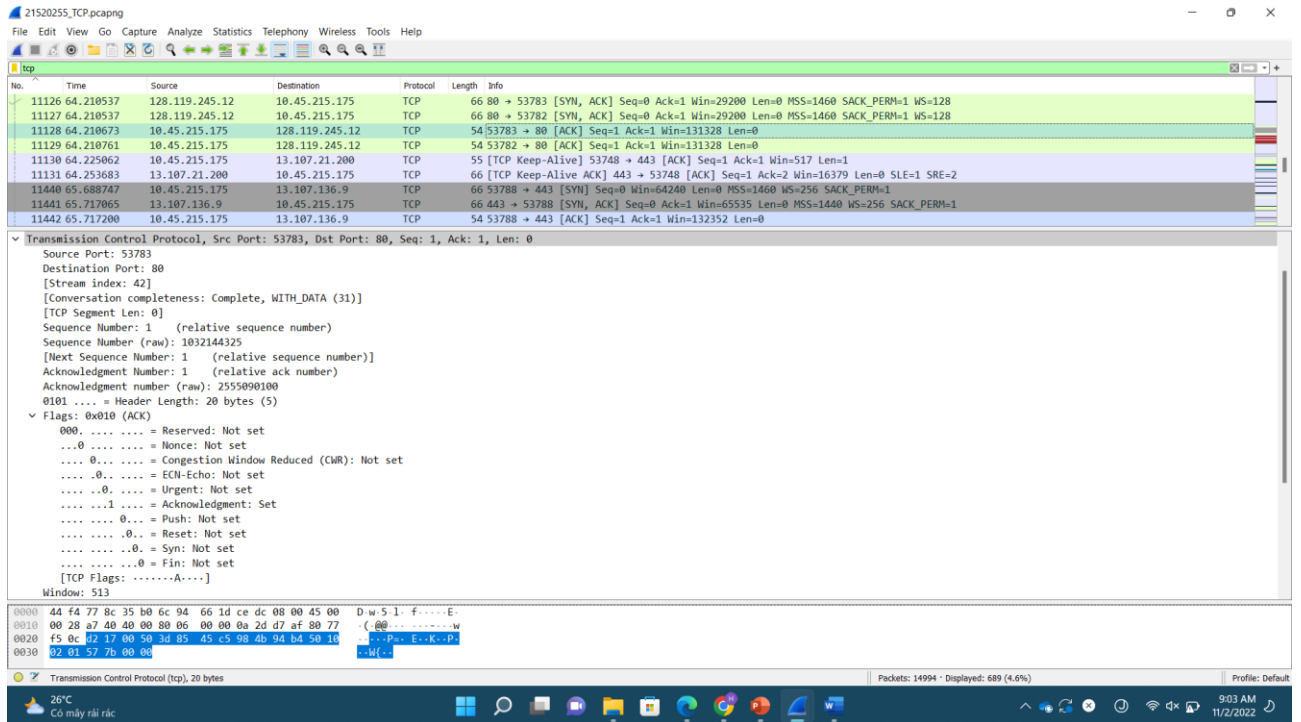
The screenshot shows a Wireshark packet capture of a TCP connection. The packet list on the left shows several packets, with packet 6 (Frame 11128) selected. The packet details pane shows the following information:

- Source Port: 53787
- Destination Port: 80
- [Stream index: 44]
- [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 0]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 1764852954
- [Next Sequence Number: 479 (relative sequence number)]
- Acknowledgment Number: 2195 (relative ack number)
- Acknowledgment number (raw): 304911856
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x010 (ACK)
- 0000 = Reserved: Not set
- ...0 = Nonce: Not set
- ...0 = Congestion Window Reduced (CWR): Not set
- ...0 = ECN-Echo: Not set
- ...0 = Urgent: Not set
- ...1 = Acknowledgment: Set
- ...0 = Push: Not set
- ...0 = Reset: Not set
- ...0 = Syn: Not set
- ...0 = Fin: Not set
- [TCP Flags:A....]
- Window: 513

The packet bytes pane shows the raw data of the packet, including the TCP header and the payload (HTTP/1.1 200 OK (text/html)).

o Segment 6 (Frame 11128) sequence number: 1

Lab 3 : Phân tích giao thức UDP và TCP



STT	Mốc thời gian gửi	Mốc thời gian nhận ACK	RTT (Round Trip Time)
1	62.790831	Không nhận được ACK	
2	62.806611	Không nhận được ACK	
3	63.054820	63.387116	0.332296000
4	63.387226	63.797489	0.409882000
5	63.797554	68.675072	4.877518000
6	64.210673	Không nhận được ACK	