3

Lab

**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 |

* 1. **CÁC BƯỚC THỰC HÀNH**

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

**Graphical user interface, text

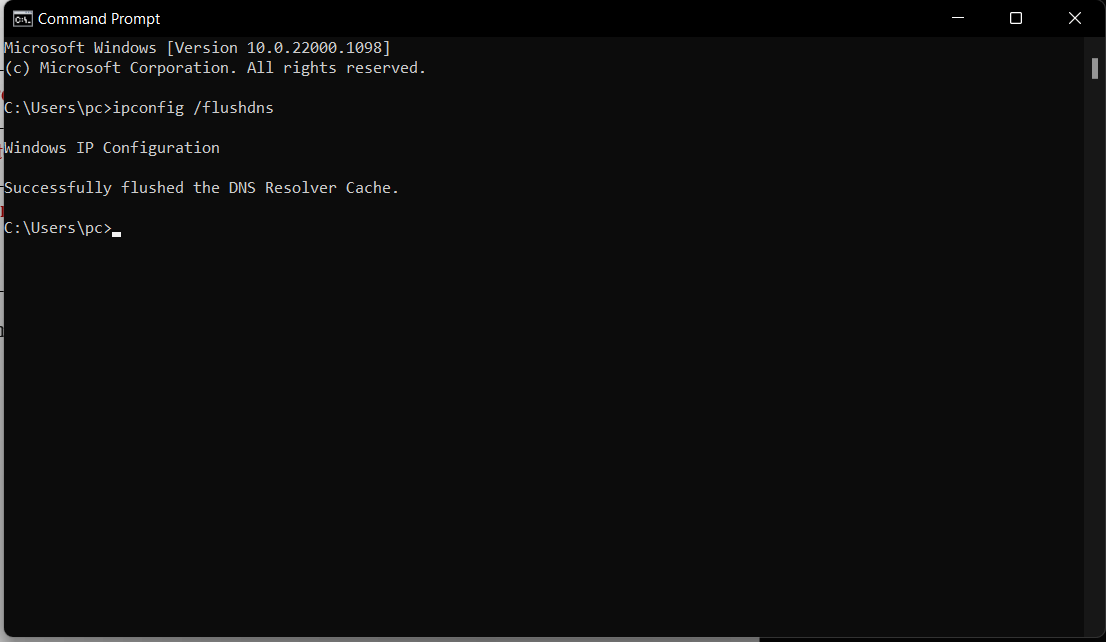
Description automatically generatedBước 1:** **Truy cập giao diện Command Promp, sử dụng lệnh ipconfig /all**

**Text

Description automatically generated**

|  |  |
| --- | --- |
| **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** |

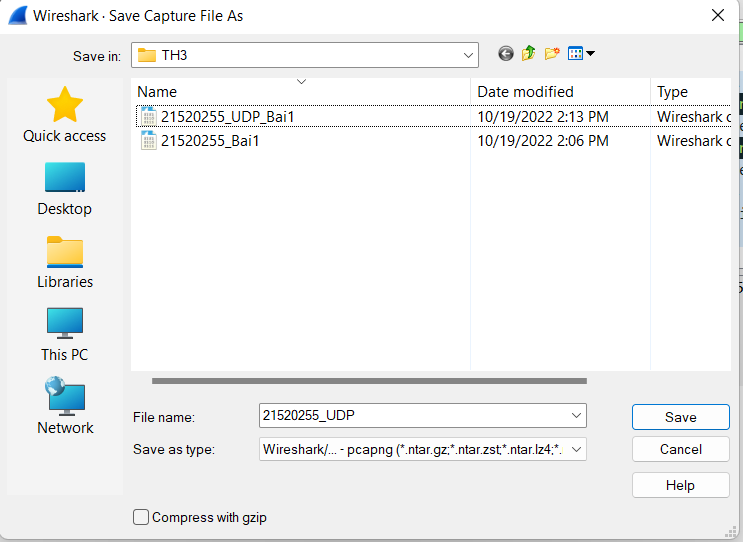
**Bước 2 : Đảm bảo xóa DNS Cache bằng cách gõ lệnh ipconfig /flushdns**



**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**

Text

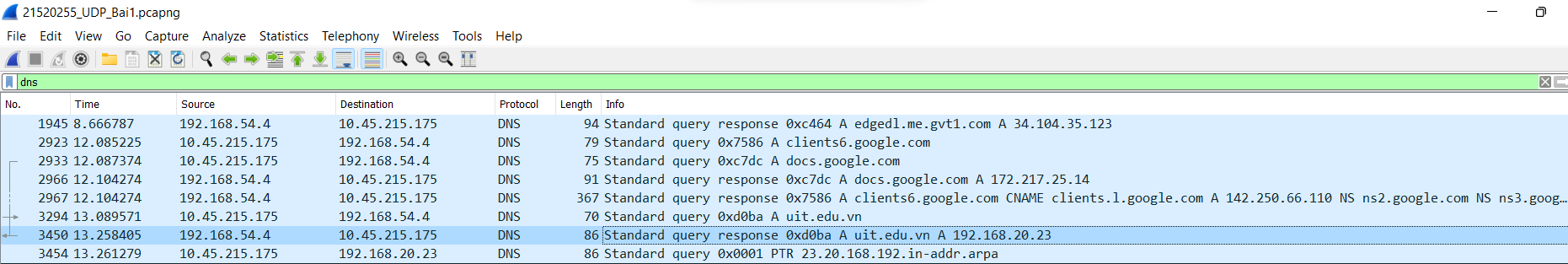
Description automatically generated

**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).**

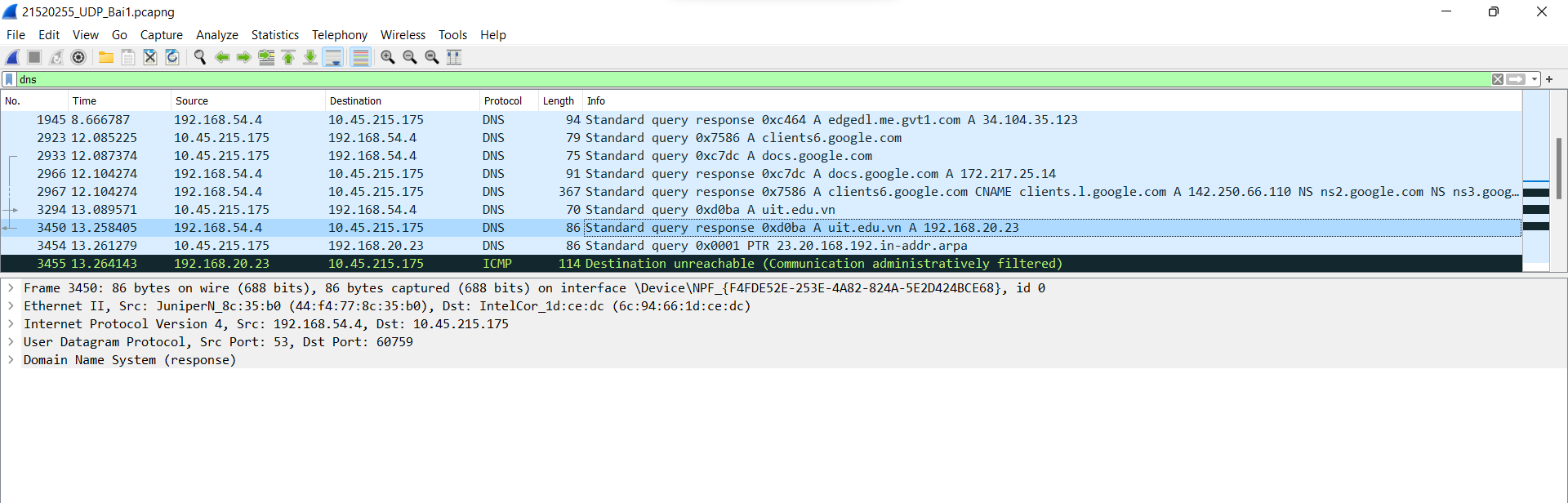
Gói tin số 3294 là gói tin truy vấn domain uit.edu.vn



**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.**

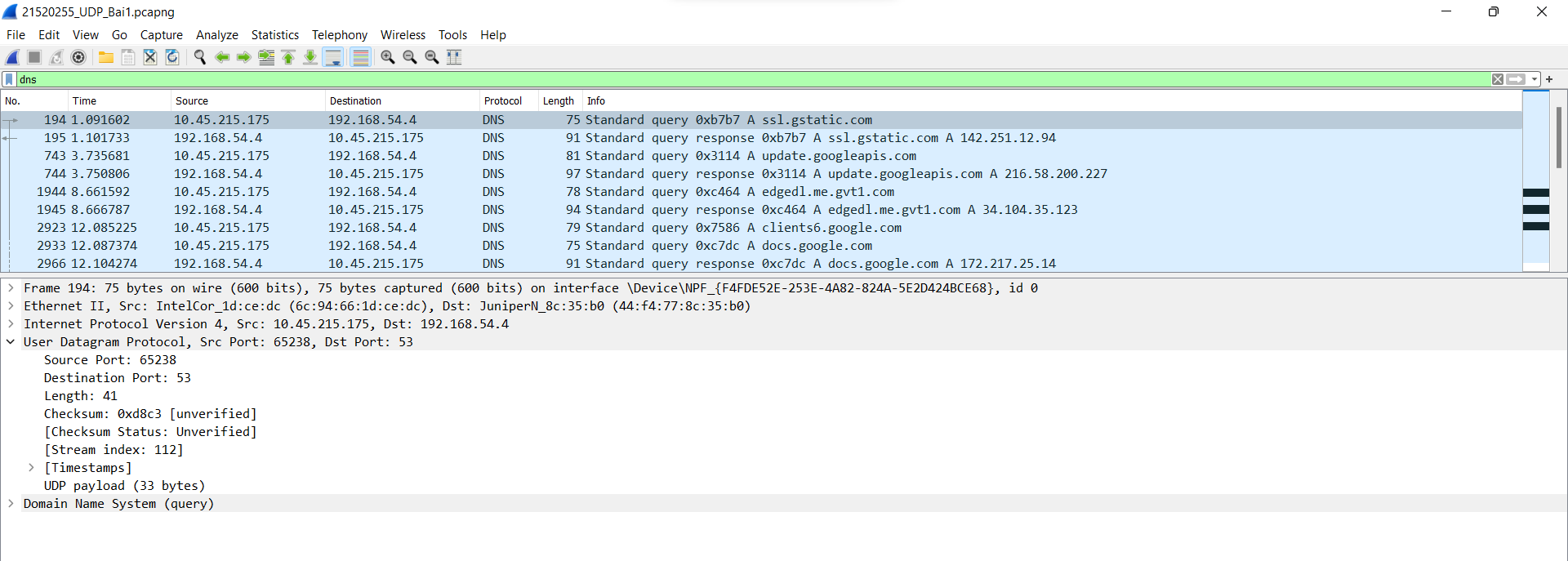
Gói tin phản hồi của truy vấn trên là gói tin số 3450.

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



**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



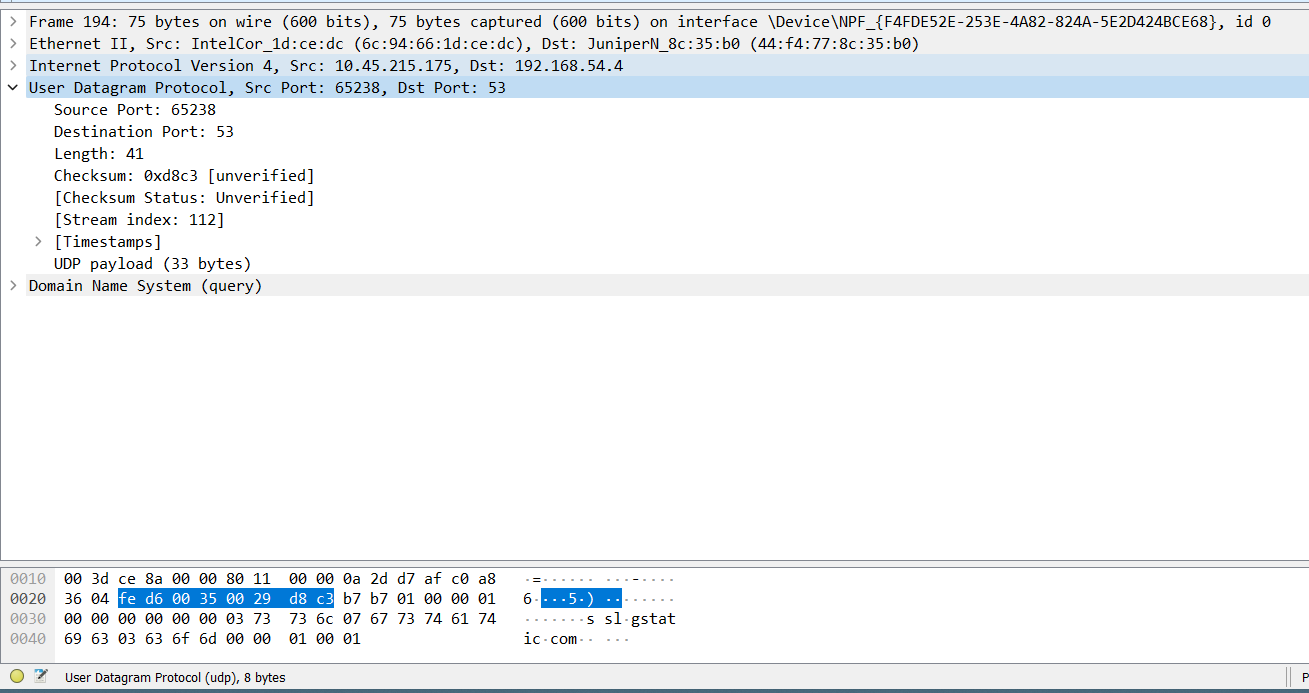
**Câu 4 : Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?**

* 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.

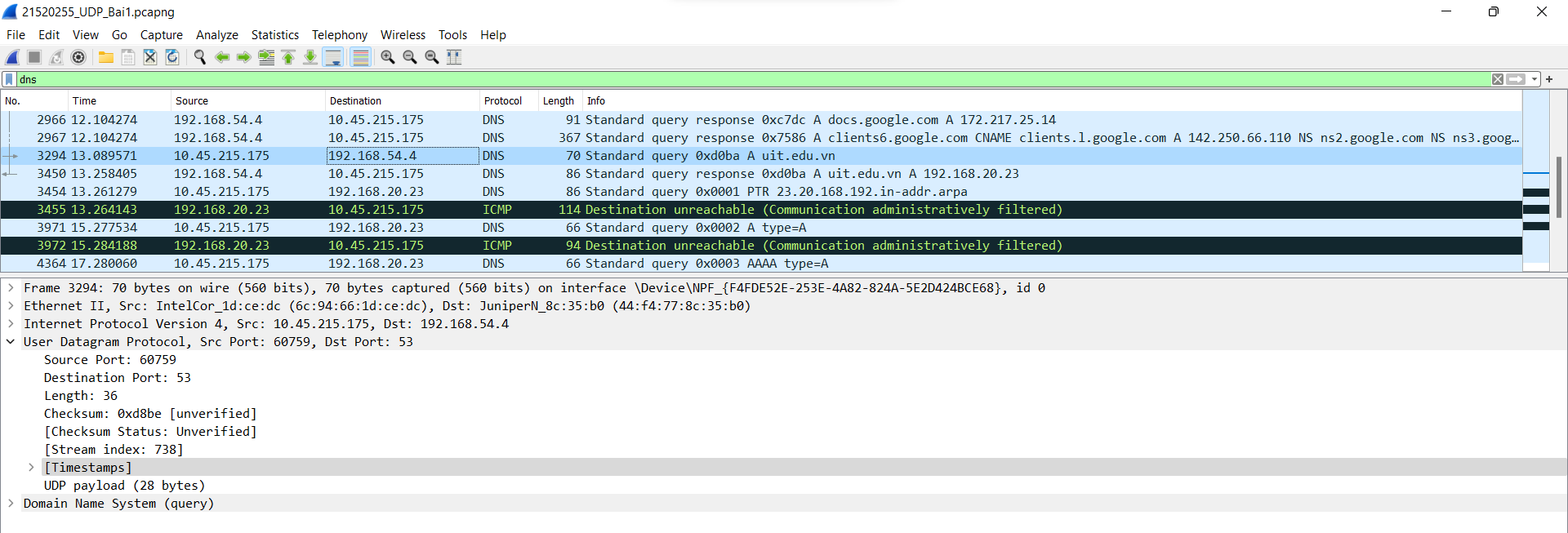
**Câu 7 : Số bytes lớn nhất mà payload (phần chứa dữ liệu gốc, không tính UDP header và IP header) của UDP có thể chứa?**

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.



Graphical user interface, application, Word

Description automatically generated

**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**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Bước 2 : Từ trình duyệt, truy cập đến địa chỉ sau:** [**http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html**](http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html).

Graphical user interface, text, application

Description automatically generated

**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.**

Graphical user interface, text, application, Word

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

**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?**

Text

Description automatically generated 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**

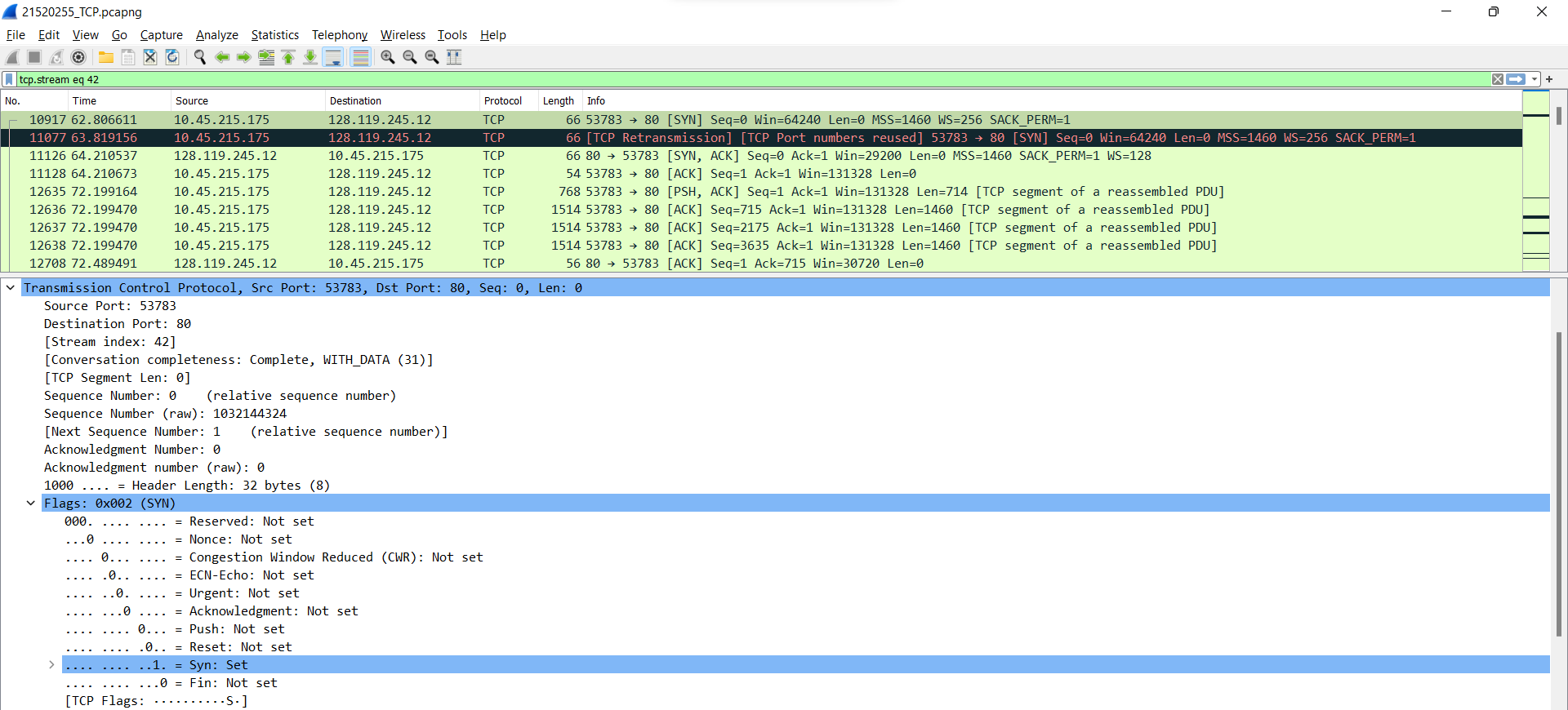
IP của gaia.cs.umass.edu là : 128.119.245.12.

Trên số cổng 80 nó nhận các dữ liệu của tệp alice.txt

Graphical user interface, text, application

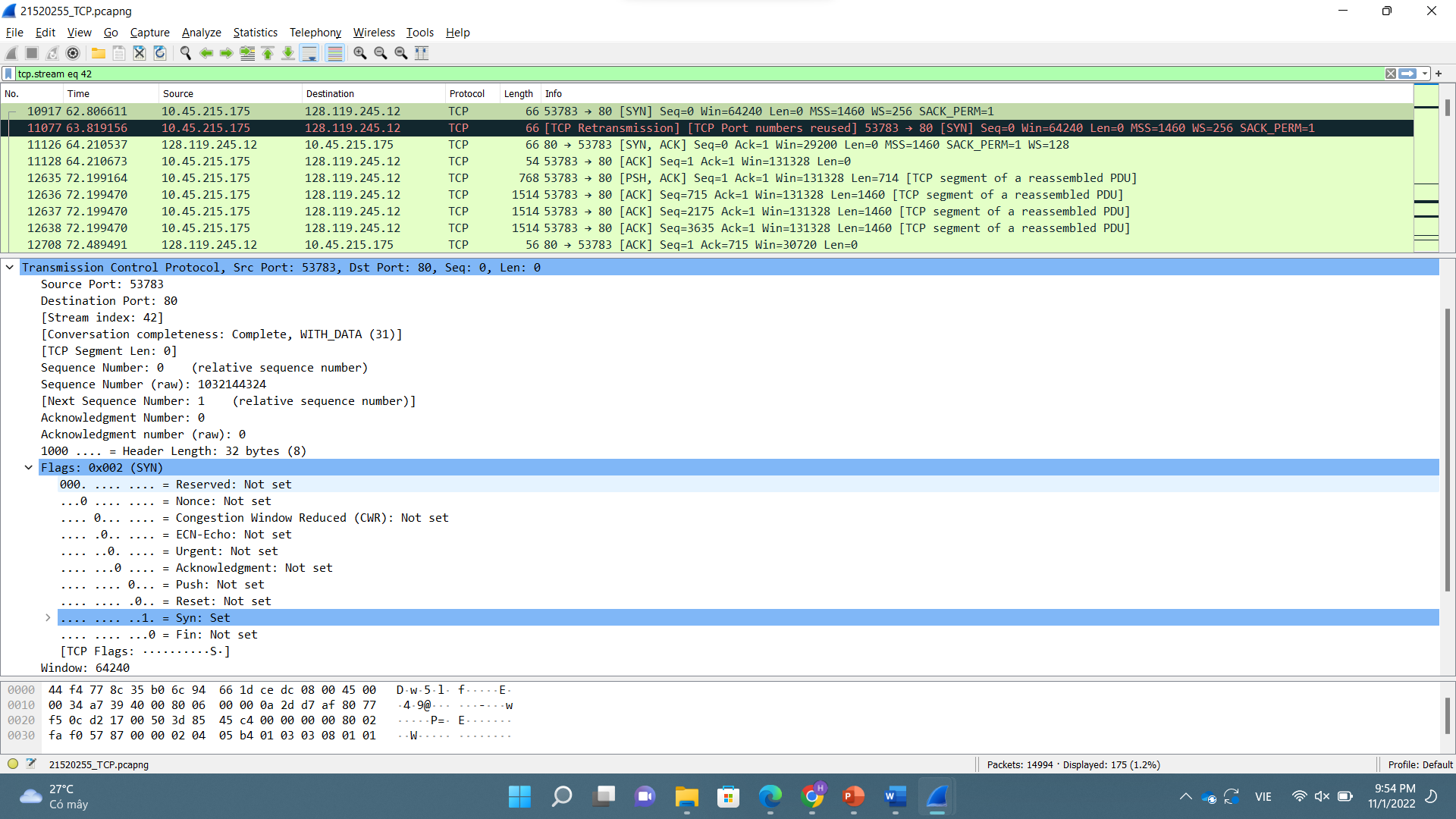
Description automatically generated

**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.

**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.



**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?**

Graphical user interface, application, Word

Description automatically generatedSequence 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.

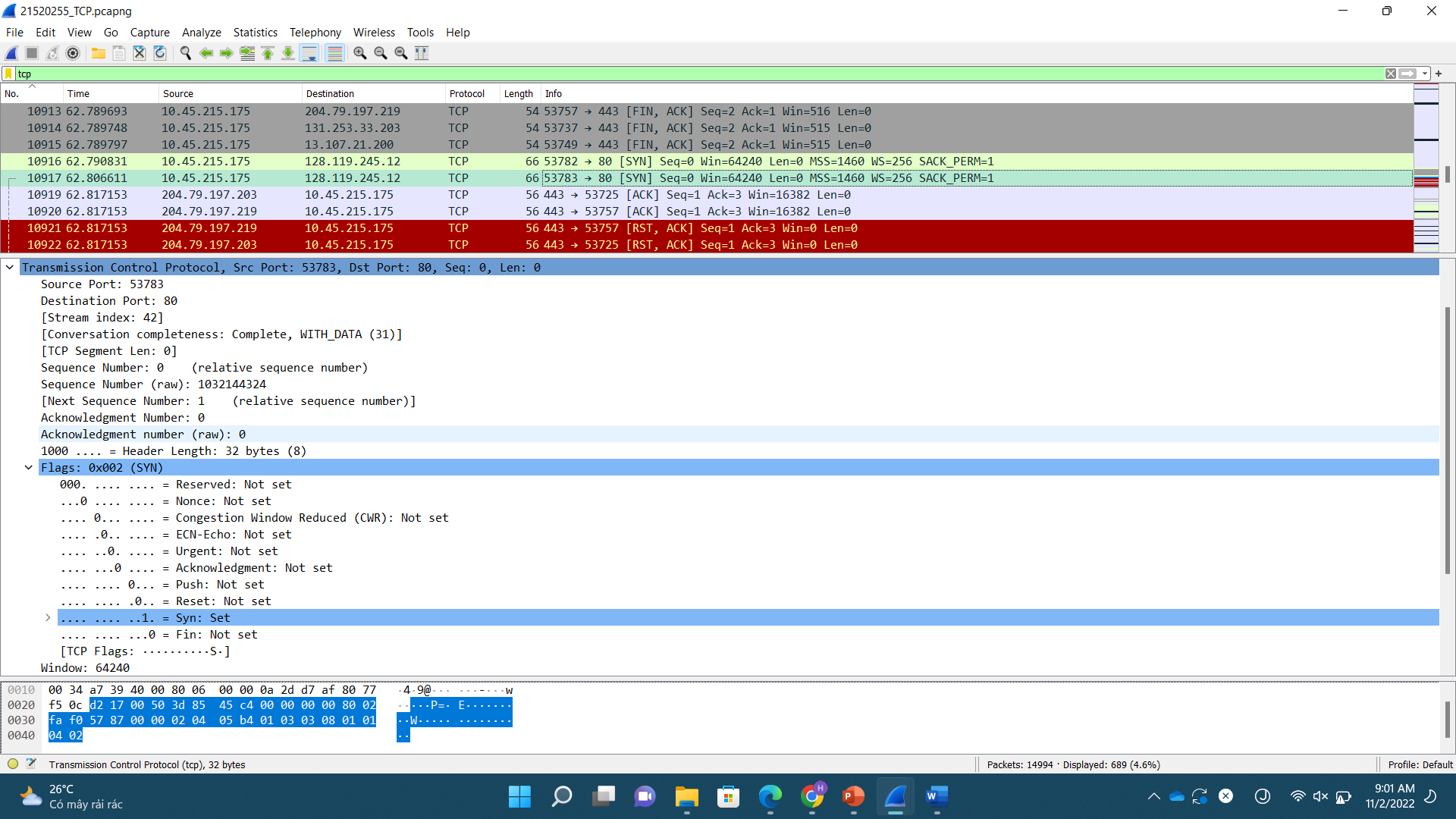
Graphical user interface, text, application

Description automatically generated

**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.
* Graphical user interface, application

  Description automatically generatedSegment 1 (Frame 10916) sequence number: 0
* Segment 2 (Frame 10917) sequence number: 0



* Graphical user interface, text, application, email

  Description automatically generatedSegment 3 (Frame 10982) sequence number: 0
* Segment 4 (Frame 11024) sequence number: 1

Graphical user interface, text, application

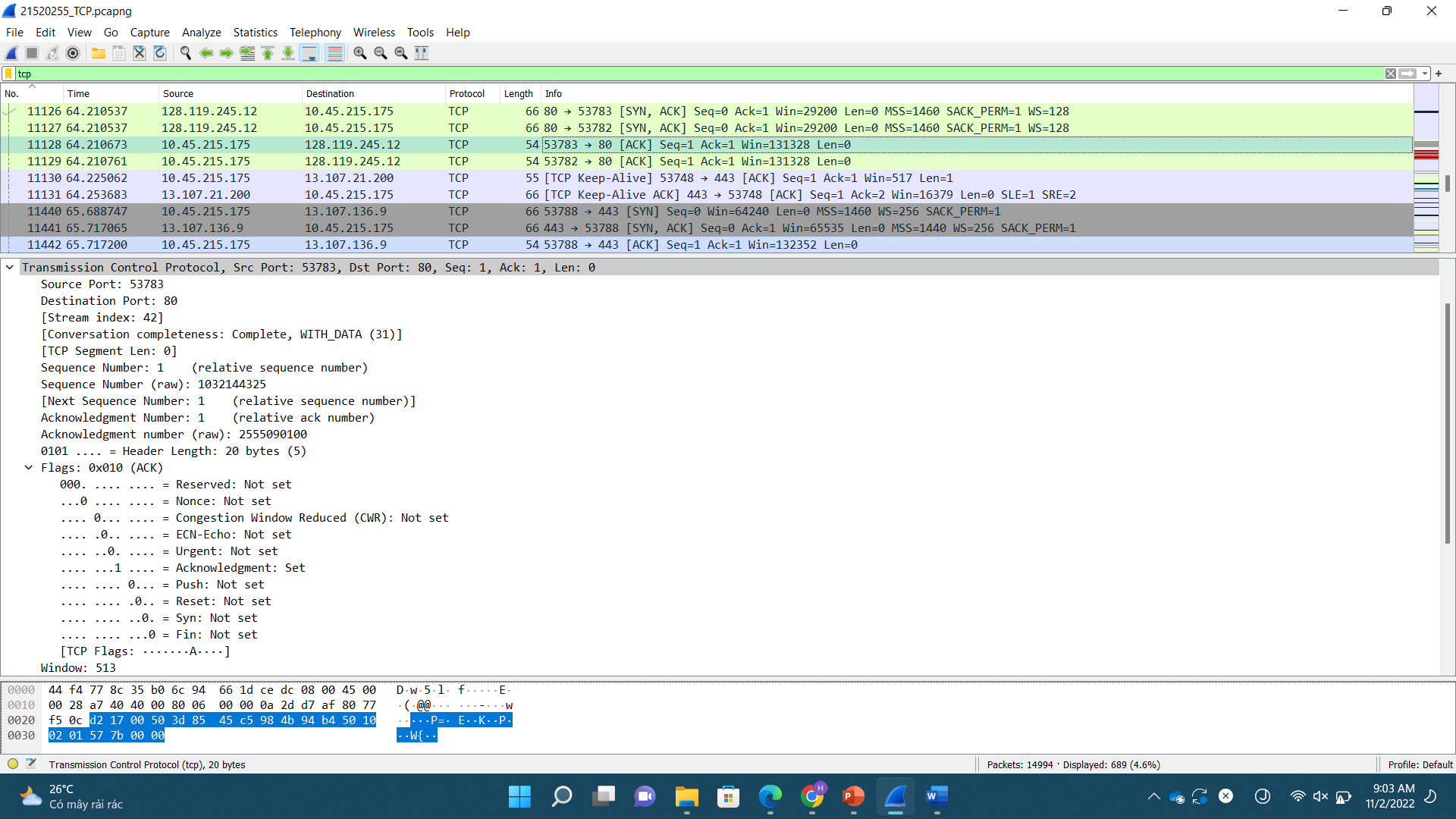
Description automatically generated

* Segment 5 (Frame 11075) sequence number: 479

Graphical user interface, text, application, Word

Description automatically generated

* Segment 6 (Frame 11128) sequence number: 1



|  |  |  |  |
| --- | --- | --- | --- |
| 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 |  |