**BÀI THỰC HÀNH 3**

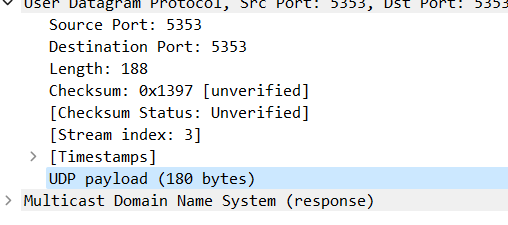
Họ tên: Nguyễn Trần Bảo Anh

MSSV: 22520066

***Bắt gói và phân tích UDP***

**1. Chọn một gói tin UDP, xác định các trường (field) trong UDP header?**

-Source port: Số hiệu cổng nơi đã gửi gói dữ liệu (datagram).  
-Destination port: Số hiệu cổng nơi datagram được chuyển tới.  
-Length: Độ dài tổng cộng kể cả phần header của gói UDP datagram.  
-Checksum: Trường checksum dùng cho việc kiểm tra lỗi của phần header và dữ liệu, nếu phát hiện lỗi thì UDP datagram sẽ bị loại bỏ mà không có thông báo trả về nơi gửi.



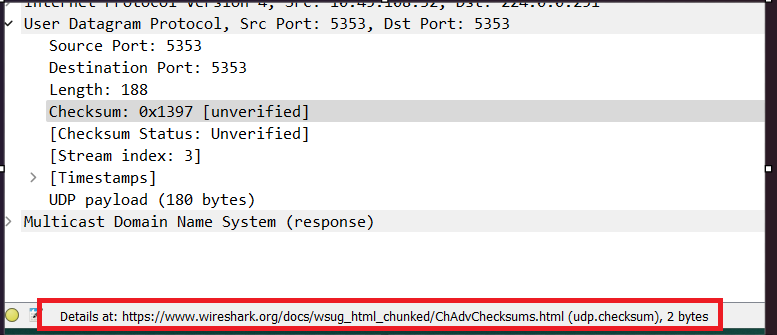
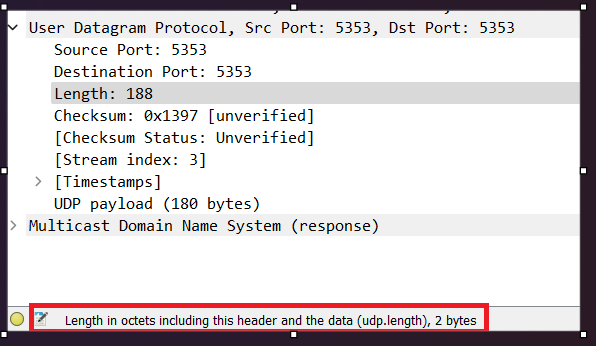
**2.Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?**

-Độ dài của mỗi trường trong UDP header là 2 bytes.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

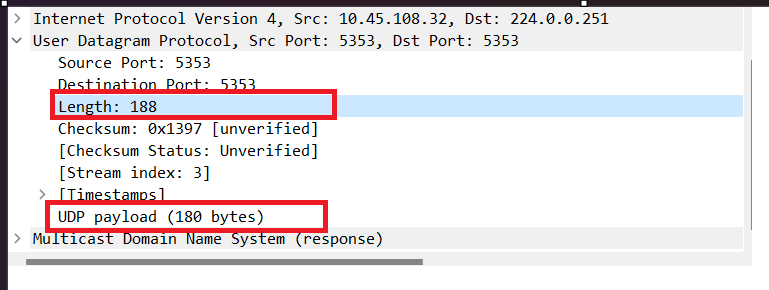
Description automatically generated

**3. Giá trị của trường Length là độ dài của cái gì? Chứng minh?**

Giá trị của trường Length trong UDP header là độ dài của 8 bytes UDP

header cộng với 180 bytes của data (UDP payload) tương đương với độ dài

188 bytes.



**4. Số bytes lớn nhất mà payload của UDP có thể chứa?**

Số bytes tối đa mà UDP payload có thể chứa là 2­16 – 1 trừ đi 8 bytes của header,

tức là 65535 – 8 = 65527 bytes

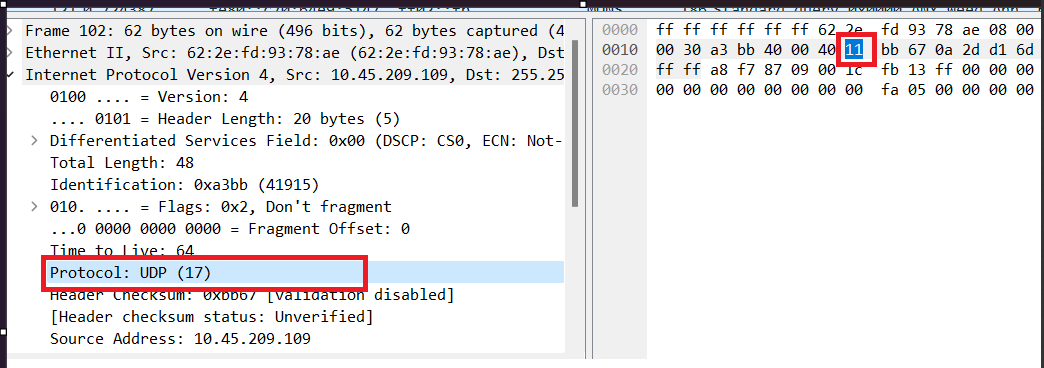
**5. Giá trị lớn nhất có thể có của port nguồn?**

Giá trị lớn nhất có thể có của port nguồn (Source port) là 216 – 1 = 65535

**6. Xác định protocol number của UDP (cả hệ 10 lẫn hệ 16)? Để trả lời câu hỏi này, chúng ta cần phải xem trường Protocol của IP header.**

Protocol number UDP hệ 10 là 17

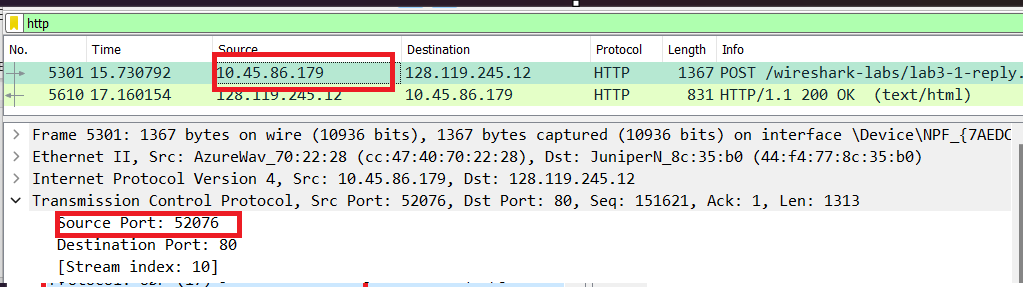
Protocol number UDP hệ 16 là 11

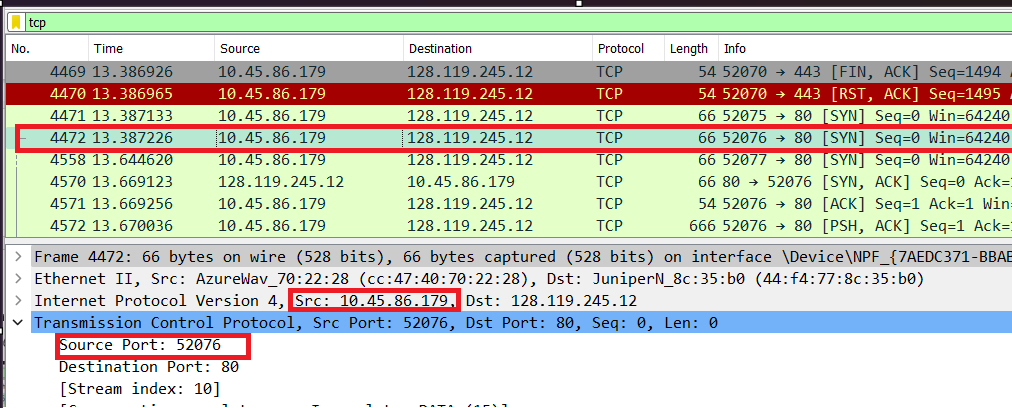


***Phân tích hành vi TCP***

**7. Tìm địa chỉ IP và TCP port của máy khách gửi file cho gaia.cs.umass.edu?**

Địa chỉ IP của máy client là 10.45.86.179 và TCP port là 52076

****

****

**8. Tìm địa chỉ IP của gaia.cs.umass.edu? Kết nối TCP dùng để gửi và nhận các segments sử dụng port nào?**

Địa chỉ IP server: 128.119.245.12 sử dụng port 80 để gửi và nhận các

segments.

**A screenshot of a computer

Description automatically generated**

**9. TCP SYN segment sử dụng sequence number nào để khởi tạo kết nối TCP giữa máy khách và gaia.cs.umass.edu? Thành phần nào trong segment cho ta biết segment đó là TCP SYN segment?**

TCP SYN segment sử dụng sequence number là 0 vì nó được sử dụng để

khởi tạo kết nối TCP giữa máy client và server.

Trong trường Flags, SYN flag được đặt thành 1 cho biết rằng segment này là một TCP SYN segment.

**A screenshot of a computer

Description automatically generated**

**10.Tìm sequence number của SYNACK segment được gửi bởi gaia.cs.umass.edu đến máy khách để trả lời cho SYN segment? Tìm giá trị của Acknowledgement trong SYNACK segment? Làm sao gaia.cs.umass.edu có thể xác định giá trị đó? Thành phần nào trong segment cho ta biết segment đó là SYNACK segment?**

Sequence number của gói tin SYN/ACK segment do server gửi đến máy

client để trả lời cho SYN segment là 0.

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

Một segment sẽ được xác định là SYN/ACK segment nếu cả giá trị SYN flag và Acknowledgement flag trong segment được đặt thành 1.

A screenshot of a computer

Description automatically generated

**11.Tìm sequence number của TCP segment có chứa lệnh HTTP POST?**

Sequence number của TCP segment có chứa lệnh HTTP POST: 1

**A screenshot of a computer

Description automatically generated**