ĐẠI HỌC KHOA HỌC TỰ NHIÊN
ĐẠI HỌC QUỐC GIA,
THÀNH PHỐ HỒ CHÍ MINH

Đồ Án

WIRESHARK

Lớp: 21CLC07
Môn học: Mạng Máy Tính

Thông tin thành viên:

	MSSV	Họ và Tên
1	21127175	Lê Anh Thư
2	21127294	Nguyễn Hi Hữu
3	21127693	Huỳnh Đức Thiện

MỤC LỤC

1 MỨC ĐỘ HOÀN THÀNH VÀ PHÂN CHIA CÔNG VIỆC

	Người thực hiện	Mức độ hoàn thành
Bài 1	Lê Anh Thư	100%
Bài 2	Nguyễn Hi Hữu	100%
Bài 3	Nội dung: Nguyễn Hi Hữu Hình ảnh: Lê Anh Thư	100%
Bài 4	Huỳnh Đức Thiện	100%
Viết báo cáo	Huỳnh Đức Thiện	

2 TRẢ LỜI CÂU HỎI

2.1 Bài 1

a. Giao thức ARP:

- Address Resolution Protocol (ARP) là giao thức mạng được dùng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn. Nó được sử dụng khi một thiết bị giao tiếp với các thiết bị khác dựa trên nền tảng local network.
- Hình minh họa:

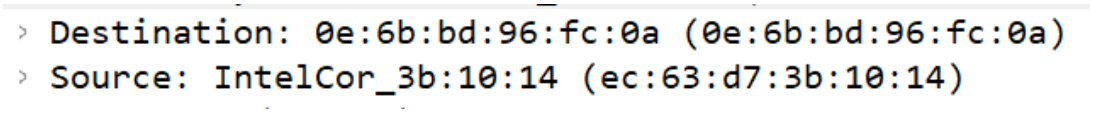
Hình 1: Các gói tin ARP bắt được.

b. Các địa chỉ nguồn và đích:

- Gói tin ARP request:

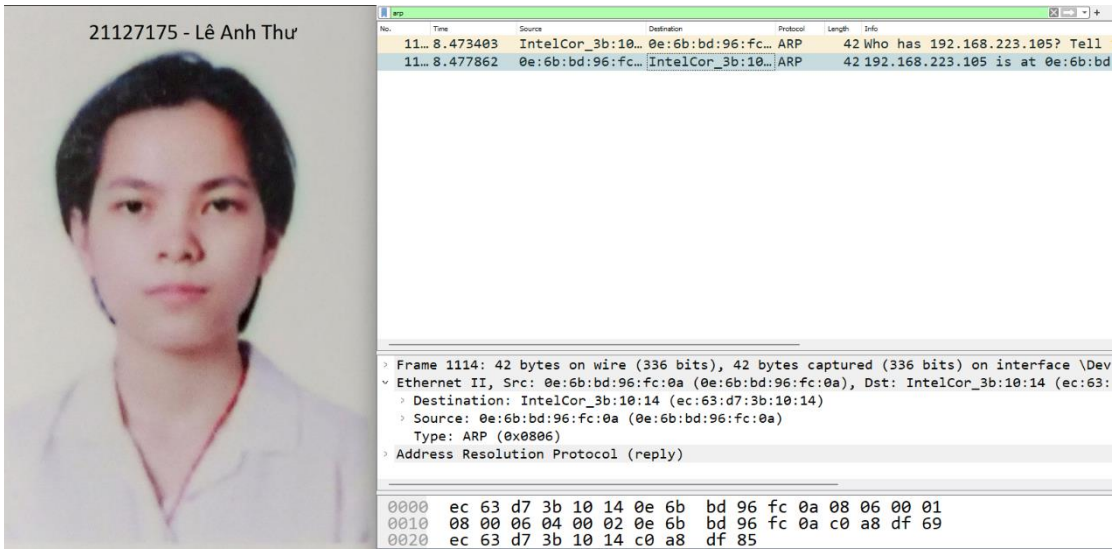
- Địa chỉ nguồn: ec:63:d7:3b:10:14
- Địa chỉ đích: 0e:6b:bd:96:fc:0a

Hình 2: Gói tin ARP request.

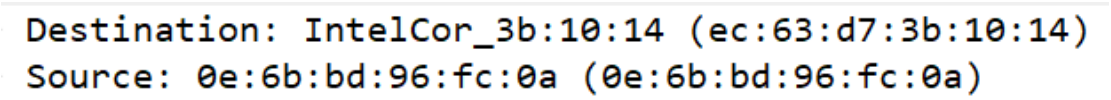


Hình 3: Địa chỉ port đích và port nguồn của gói tin ARP request.

- Gói tin ARP reply:
  - Địa chỉ nguồn: 0e:6b:bd:96:fc:0a
  - Địa chỉ đích: ec:63:d7:3b:10:14



Hình 4: Gói tin ARP reply.



Hình 5. Địa chỉ port nguồn và port đích của gói tin ARP reply.

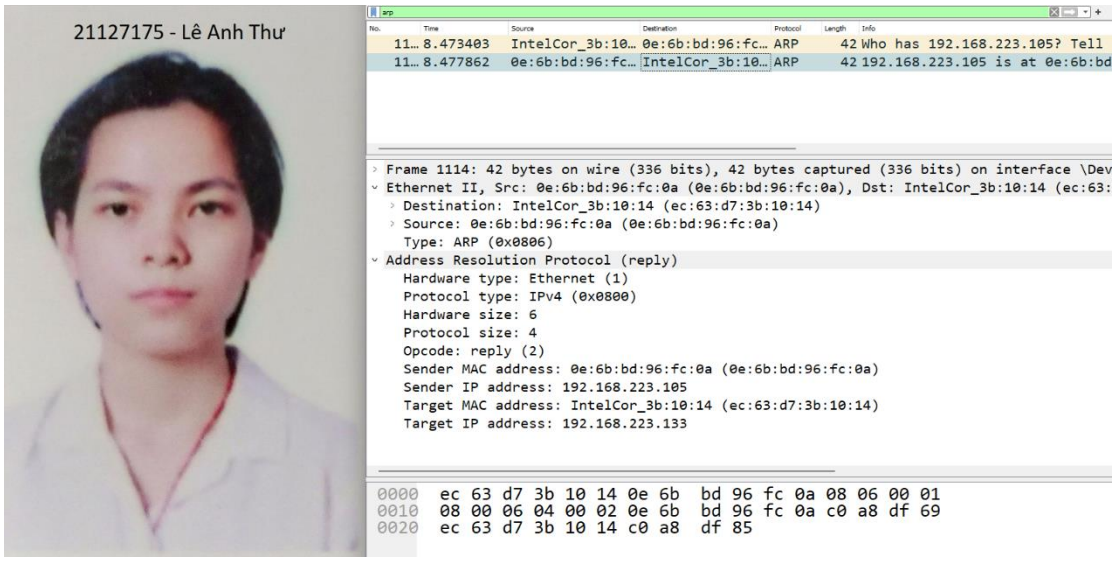
c. Giá trị và ý nghĩa:
   - Giá trị trường type: 0x0806
   - Ý nghĩa: Cho biết protocol được đóng gói bên trong payload của frame, trong trường hợp này, theo tiêu chuẩn IEEE thì protocol được sử dụng là ARP tương ứng với giá trị 0x0806.

Hình 6: Trường type trong Ethernet frame của gói ARP request.

d. Các trường thông tin trong phần ARP payload (reply):
   - Hardware type:
     - Kích thước: 2 bytes
     - Giá trị: 1 (Ethernet)
   - Protocol type:
     - Kích thước: 2 bytes
     - Giá trị: 0x0800 (IPv4)
   - Hardware size:
     - Kích thước: 1 byte
     - Giá trị: 6
   - Protocol size:
     - Kích thước: 1 byte
     - Giá trị: 4
   - Opcode:
     - Kích thước: 2 bytes
     - Giá trị: 2 (reply)
   - Sender MAC address:
     - Kích thước: 6 bytes
     - Giá trị: 0e:6b:bd:96:fc:0a
   - Sender IP address:
     - Kích thước: 4 bytes
     - Giá trị:192.168.223.105
   - Target MAC address:

- Kích thước: 6 bytes
- Giá trị: ec:63:d7:3b:10:14

- Target IP address:
  - Kích thước: 4 bytes
  - Giá trị: 192.168.223.133

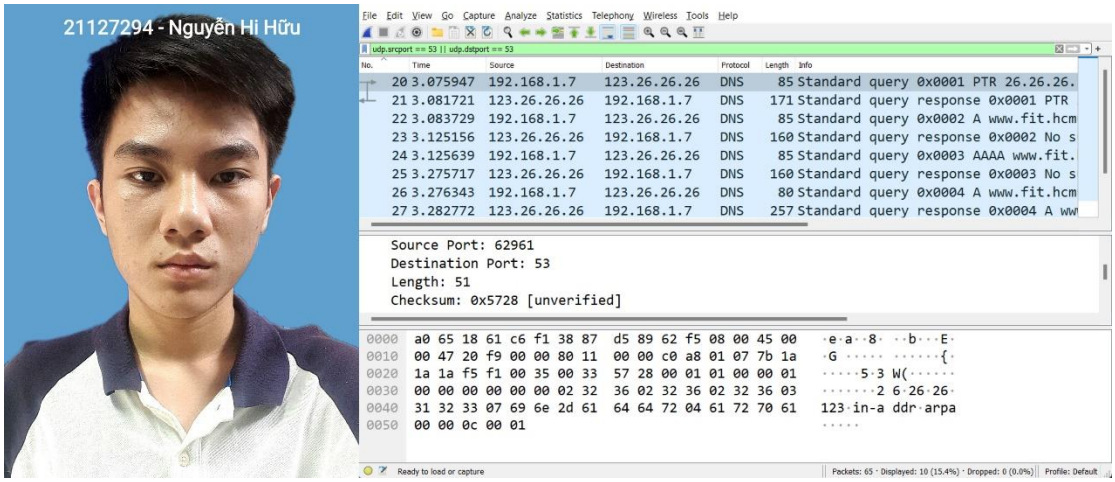


Hình 7: Các trường thông tin trong ARP payload (reply).

2.2 Bài 2

a. Ý nghĩa câu lệnh “nslookup www.fit.hcmus.edu.vn”:
Lệnh nslookup được sử dụng để truy vấn bản ghi DNS thông qua việc lấy tên miền đã nhập vào từ đó trả về các thông tin như địa chỉ IP, tên server,…

b. Các trường thông tin trong header của gói tin UDP:
- Source port: 2 bytes.
- Destination port: 2 bytes.
- Length: 2 bytes.
- Checksum: 2 bytes.



Hình 8: Các trường thông tin trong header của gói tin UDP.

c. Trường Length:
   - Giá trị: 51
   - Đơn vị: byte
   - Trường này nói đến chiều dài của datagram bao gồm cả header và data.

d. Protocol number của UDP:
   - Hexadecimal: 0x011
   - Decimal: 17

e. Lượng dữ liệu tối đa có thể đưa vào UDP payload:
   - IPv6: 65 527 bytes
   - IPv4: 65 507 bytes

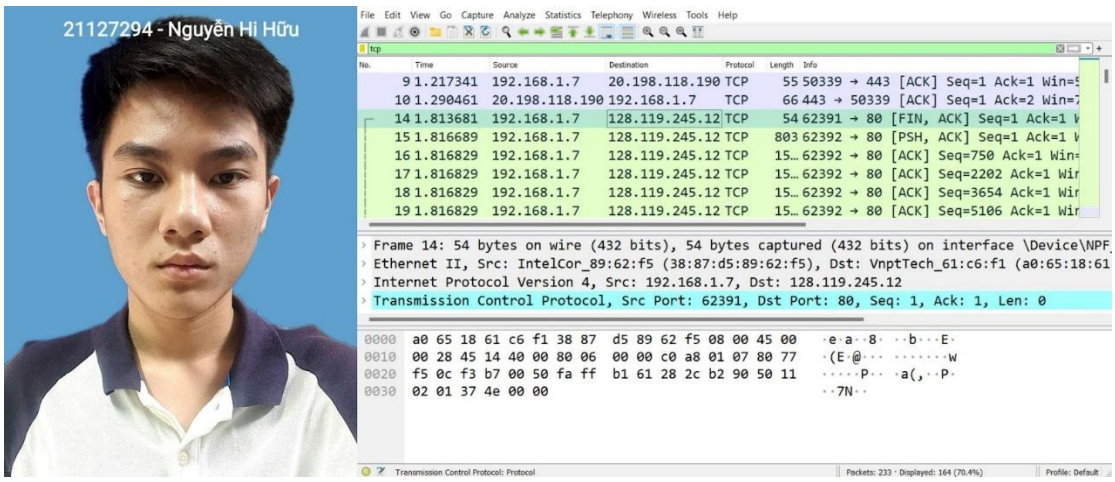
f. Quan hệ giữa các port number trong những gói tin lọc được: Hoặc source port là 53 hoặc destination port là 53.

2.3 Bài 3

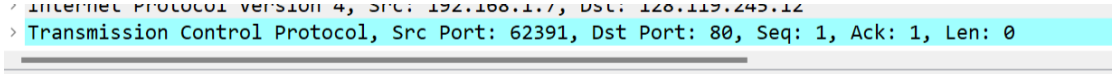
a. Máy chủ gaia.cs.umass.edu:
   - Địa chỉ IP: 128.119.145.12
   - Port dịch vụ được sử dụng để nhận và gửi các gói tin: 80

b. Kích thước 3 gói tin đầu tiên bắt được:
   - Packet 1:
     - SEQ: 1

- ACK: 1
- Len: 0

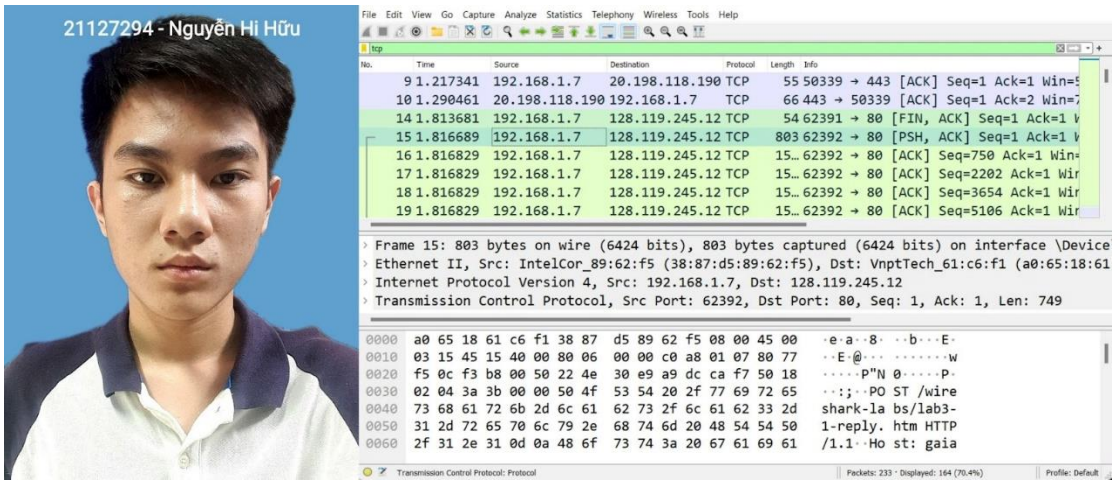


Hình 9: Gói tin thứ nhất.

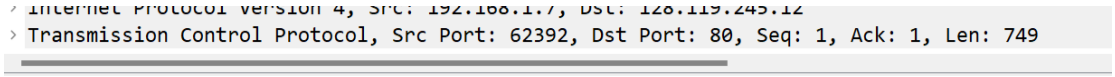


Hình 10: Các thông tin của gói tin thứ nhất.

- Packet 2:
  - SEQ: 1
  - ACK: 1
  - Len: 749

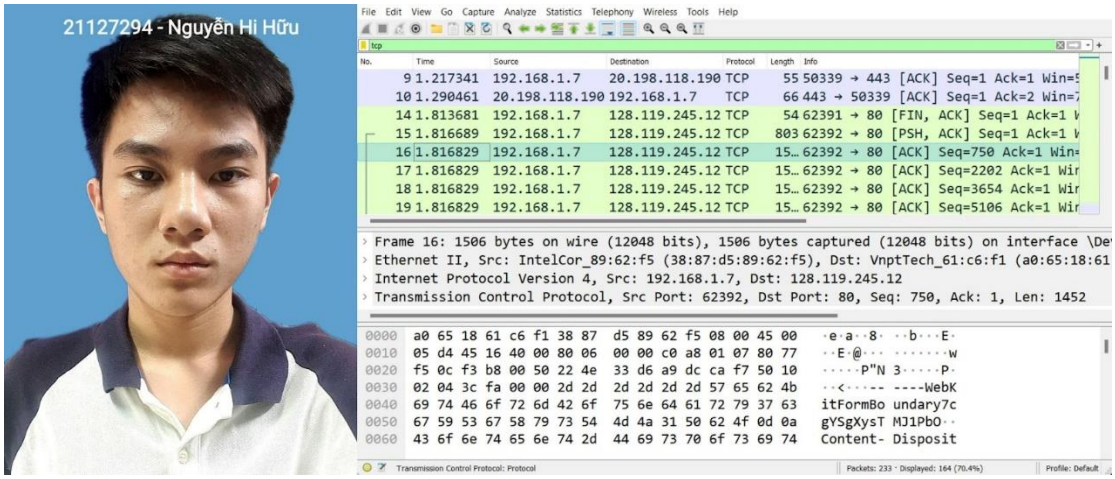


Hình 11: Gói tin thứ hai.

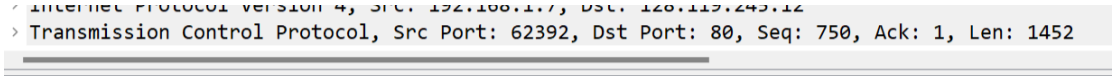


Hình 12: Các thông tin của gói tin thứ hai.

- Packet 3:
    - SEQ: 750
    - ACK: 1
    - Len: 1452

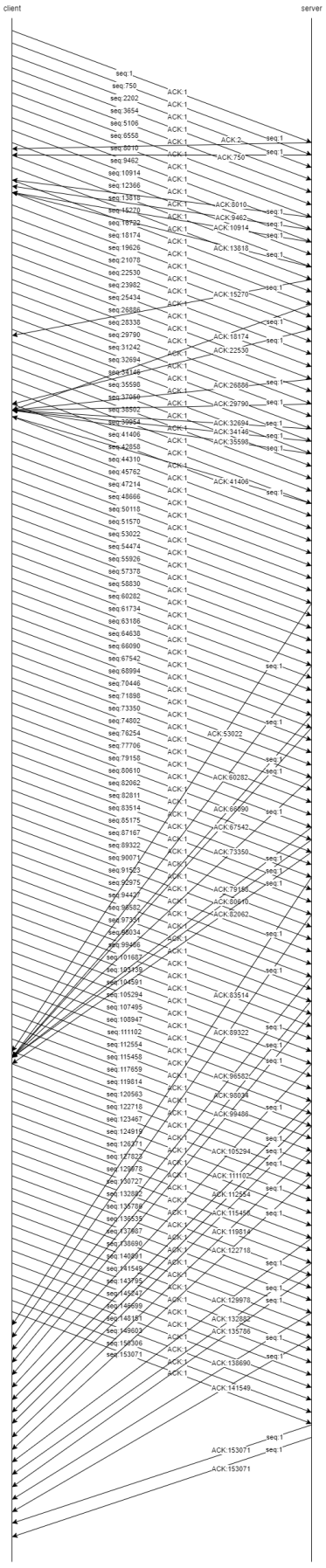


Hình 13: Gói tin thứ ba.



Hình 14: Các thông tin của gói tin thứ ba.

c. Quá trình trao đổi gói tin từ lúc khởi tạo đến lúc đóng kết nối TCP:

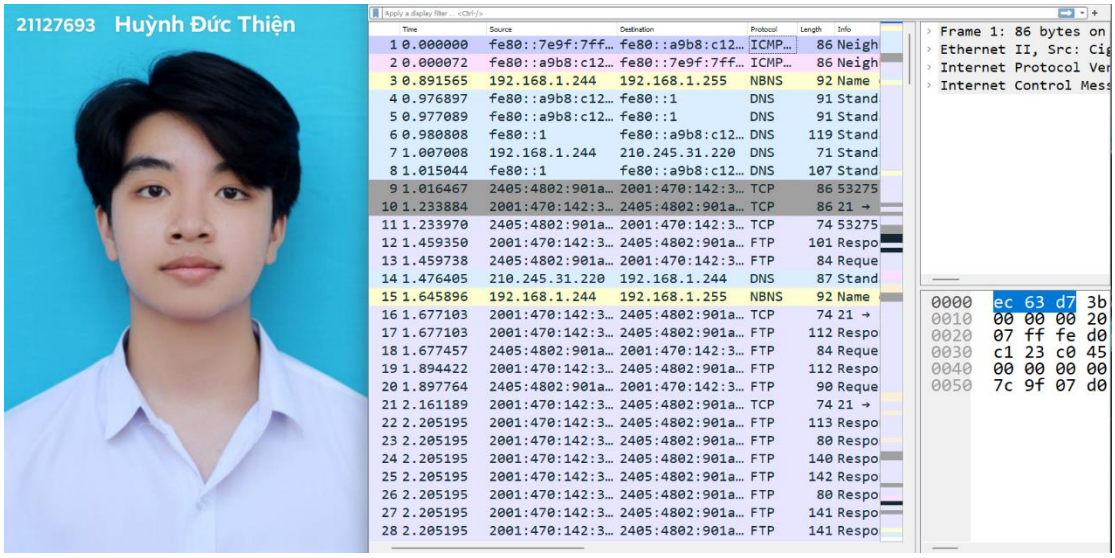


Hình 15: Quá trình trao đổi gói tin.

d. Cách máy chủ gaia.cs.umass.edu xác định ACK number trong TCP SYNACK segment:
Giá trị của tường Acknowledgement trong gói SYN/ACK được xác định bởi server gaia.cs.umass.edu. Server sẽ khởi tạo số Sequence đầu tiên (Initial Sequence Numer – ISN) SYN segment từ client là 0. Do đó giá trị của trường Acknowledgement trong gói SYN/ACK là 1. Một segment sẽ là một SYN/ACK segment nếu có cả cờ SYN và cờ ACK đều set là 1.

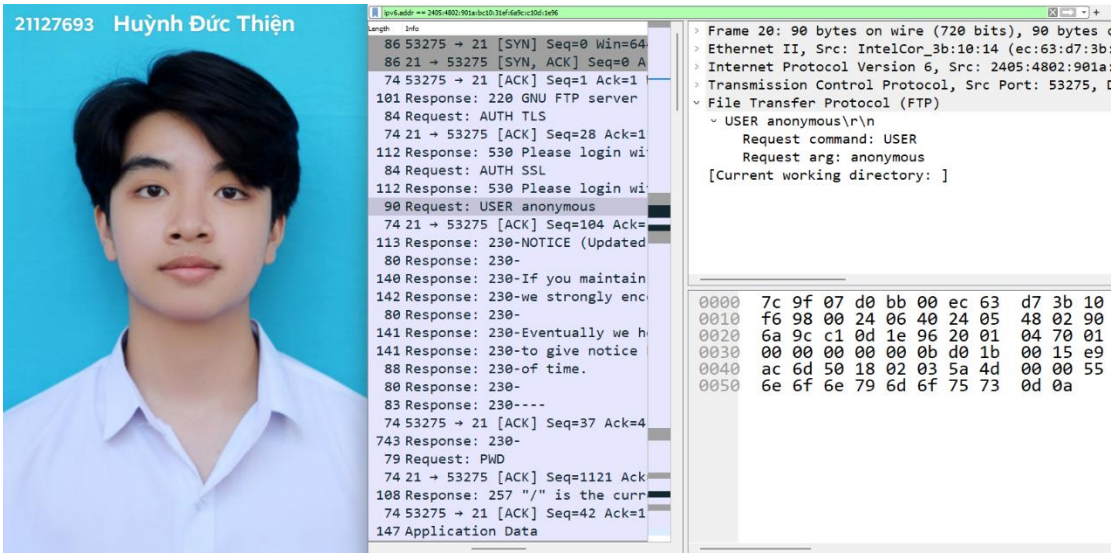
2.4 Bài 4

a. Hình ảnh:

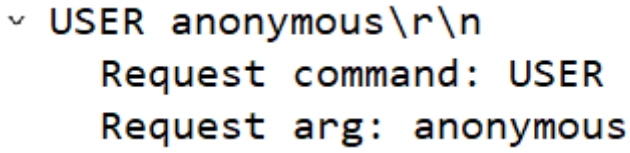


Hình 16 : Các gói tin bắt được sau khi kết nối đến server ftp.gnu.org.

b. Username được dùng để login vào server: anonymous



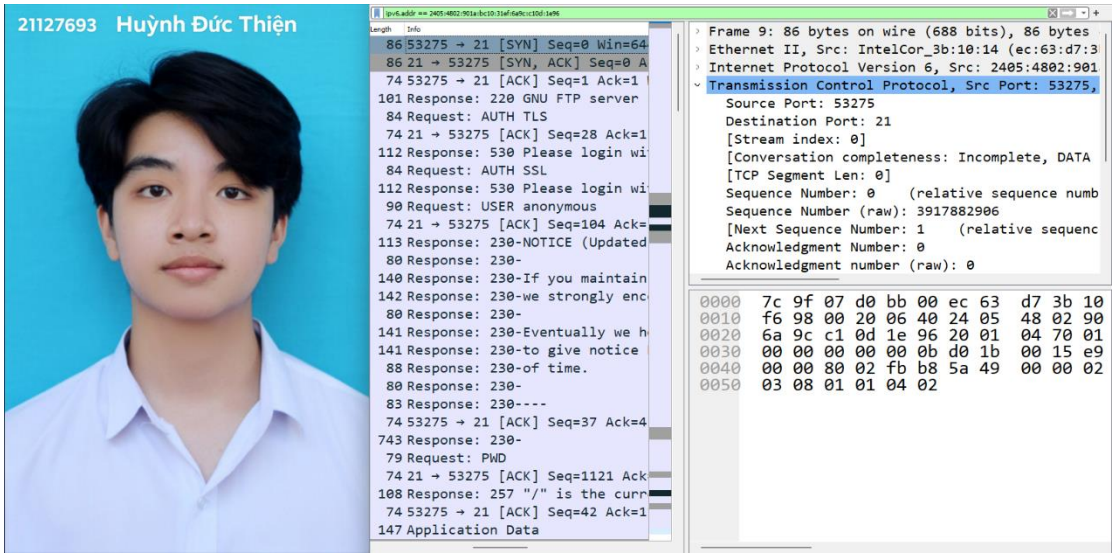
Hình 17 : Gói tin chứa Username.



Hình 18 : Username được sử dụng để login vào server.

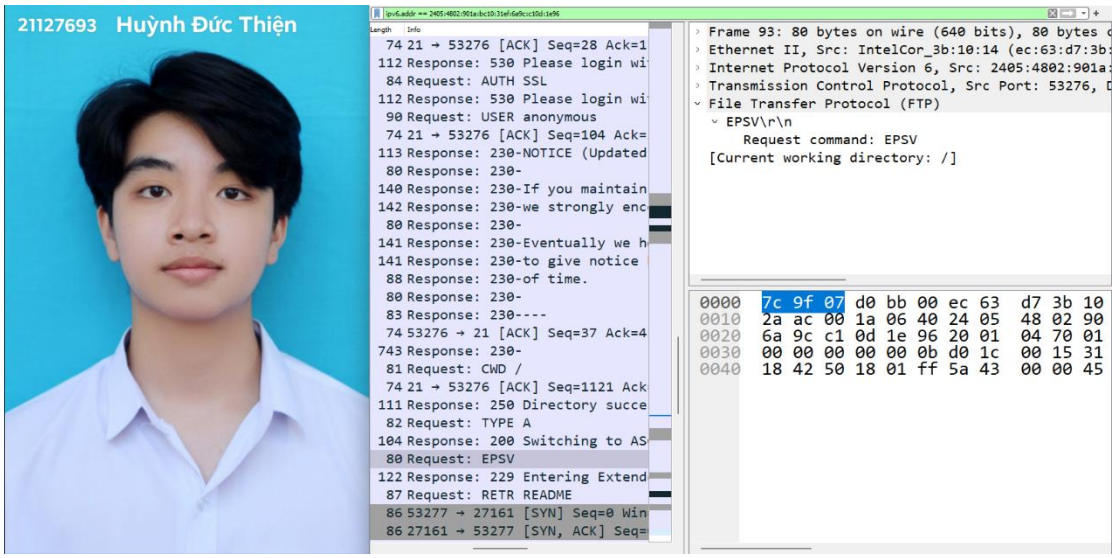
c. Port client và server dùng để truyền lệnh:

- Client: 53275
- Server: 21

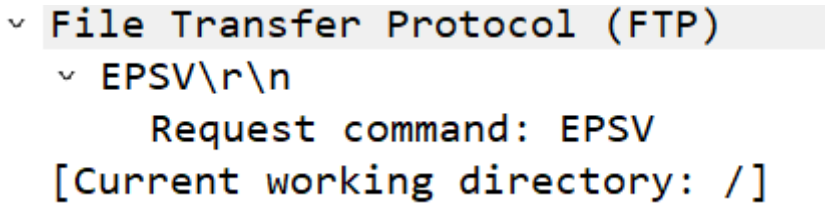


Hình 19 : Port của client và server được dùng để truyền lệnh.

d. Mode data và ý nghĩa:
   - Mode data: Extended Passive Mode – ESPV.
   - Ý nghĩa: EPSV là phương thức

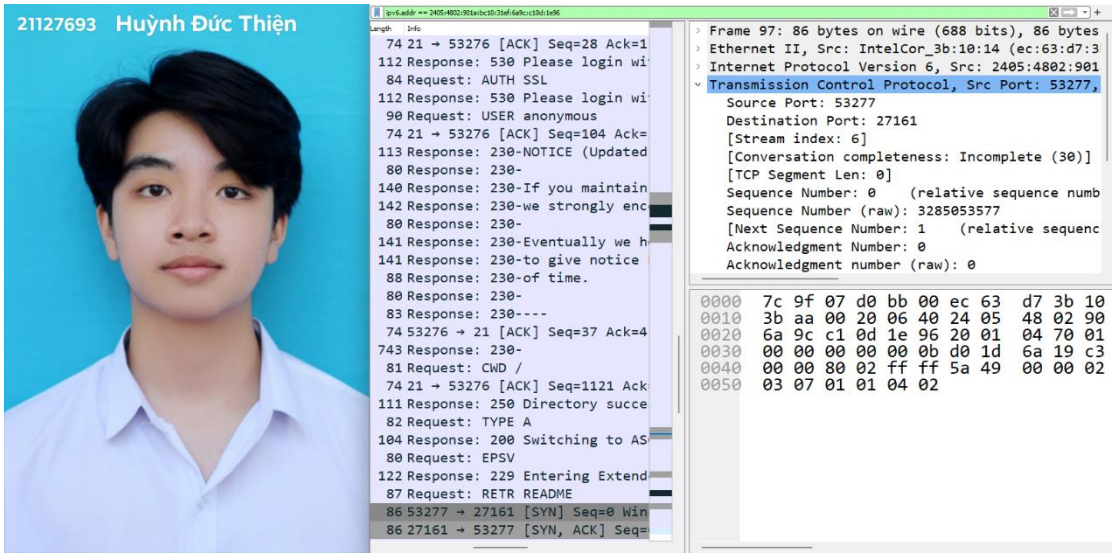


Hình 20 : Gói tin xác định mode truyền data.

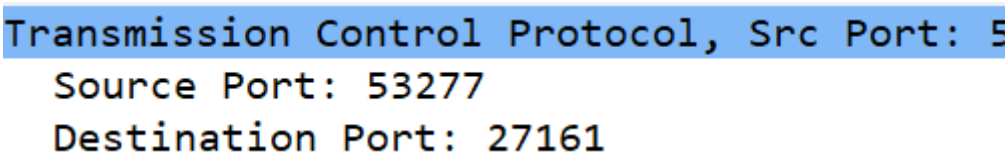


Hình 21 : Mode data được sử dụng.

e. Port client và server dùng để truyền – nhận danh sách folder và file:
   - Client: 53277
   - Server: 27161



Hình 22 : Gói tin data.



Hình 23 : Các port client và server được dùng để truyền – nhận danh sách file và folder.

3 TÀI LIỆU THAM KHẢO

- Các hình ảnh chi tiết có trong báo cáo: https://drive.google.com/drive/folders/1-L1GV21eKhkdzy1cUWKo0M_7VQHEYQM8?usp=sharing
- Computer Networking: A Top-Down Approach, sixth edition, James F.Kurose, Keith W.Ross.
- Slide bài giảng, tài liệu thực hành bộ môn Mạng Máy Tính – trường Đại học Khoa Học Tự Nhiên.
- ARP: What Is Address Resolution Protocol (ARP) | Fortinet
- WireShark turtorial: [Wireshark Là Gì] Hướng dẫn sử dụng Wireshark chi tiết | Vietnix
- FTP: Active vs. Passive FTP Simplified: Understanding FTP Ports | JSCAPE

-Hết-