

ĐẠI HỌC QUỐC GIA  
THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN  
KHOA CÔNG NGHỆ THÔNG TIN



CSC10008 - Mạng máy tính

BÁO CÁO ĐỒ ÁN  
Phân tích gói tin với Wireshark

Họ tên	MSSV
Bùi Minh Duy	23127040
Nguyễn Thị Khánh Linh	23127082
Nguyễn Lê Hồ Anh Khoa	23127211

Giảng viên hướng dẫn

Lê Hà Minh

Thành phố Hồ Chí Minh, 15/08/2024

## Mục lục

1	Thông tin giới thiệu	2
2	Dánh giá mức độ hoàn thành	2
3	Bài 1: Traceroute	3
4	Bài 2: DHCP	5
5	Bài 3: TCP	9
6	Bảng phân công công việc	15
7	Nguồn tài liệu tham khảo	15

## 1 Thông tin giới thiệu

- Tên học phần: Mạng máy tính
- Giảng viên hướng dẫn: Lê Hà Minh
- Đề án thực hiện: Phân tích gói tin với Wireshark
- Thời gian thực hiện: 05/08/2024 - 17/08/2024
- Danh sách thành viên:

STT	MSSV	HỌ VÀ TÊN	EMAIL	VAI TRÒ
01	23127040	Bùi Minh Duy	bmduy23@clc.fitus.edu.vn	Thành viên
02	23127082	Nguyễn Thị Khánh Linh	ntklinh23@clc.fitus.edu.vn	Nhóm trưởng
03	23127211	Nguyễn Lê Hồ Anh Khoa	nlhakhoa23@clc.fitus.edu.vn	Thành viên

Bảng 1: Danh sách thành viên

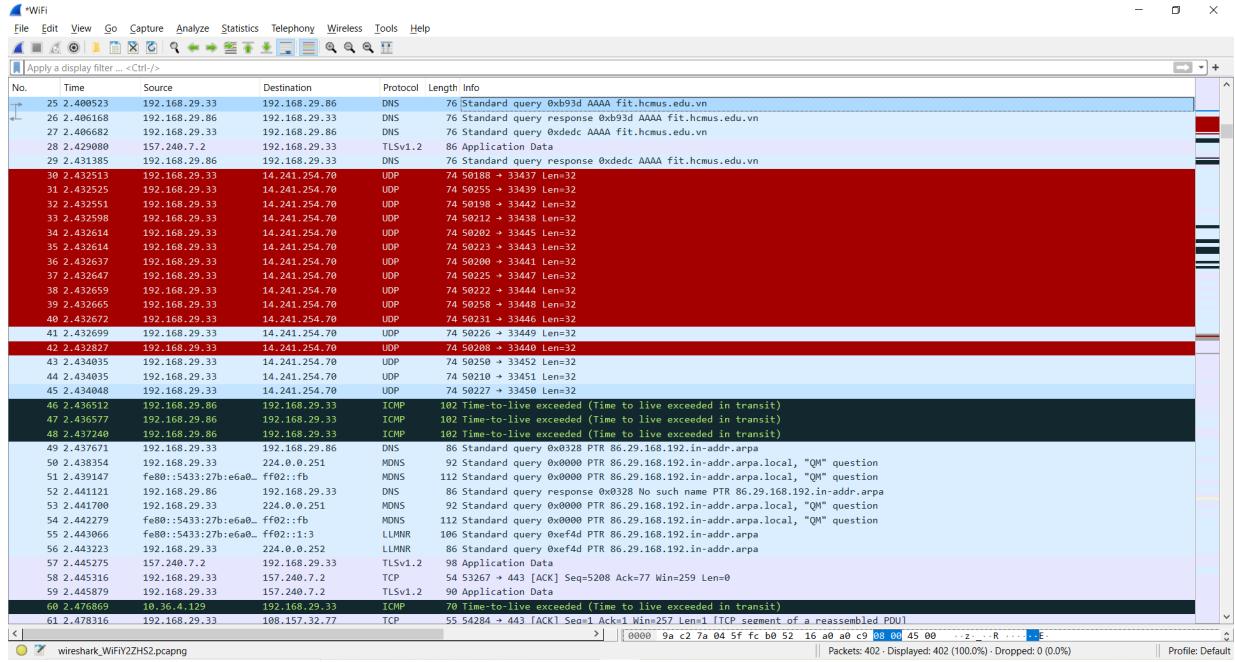
## 2 Đánh giá mức độ hoàn thành

STT	NỘI DUNG	MỨC ĐỘ HOÀN THÀNH
01	Bài 1	100%
02	Bài 2	100%
03	Bài 3	100%

Bảng 2: Đánh giá mức độ hoàn thành

### 3 Bài 1: Traceroute

#### 1. Kết quả bắt gói tin sau khi Traceroute.



Hình 1: Kết quả bắt gói tin sau khi Traceroute

#### 2. Cho biết chức năng của lệnh Traceroute

**Trả lời:** Lệnh traceroute dùng để xác định đường đi của các gói tin từ máy nguồn đến máy đích. Nó cho phép hiển thị tất cả các router trung gian mà gói tin đi qua, cùng với thời gian di chuyển giữa các bước nhảy

#### 3. Cho biết địa chỉ IP của máy gửi request ?

**Trả lời:** 192.168.29.33

#### 4. Quan sát và chỉ rõ những gói tin dùng xác định địa chỉ IP của FIT từ tên miền trong danh sách các gói tin bắt được. Cho biết các gói tin này dùng giao thức gì tại tầng ứng dụng trong mô hình TCP/IP

Quan sát hình ảnh Wireshark và kết quả thực hiện lệnh traceroute, có thể thấy rằng các gói tin dùng để xác định địa chỉ IP của FIT (fit.hcmus.edu.vn) trong danh sách các gói tin bắt được bao gồm các gói tin với giao thức UDP và ICMP. Cụ thể:

- Các gói tin UDP được đánh dấu màu đỏ, có địa chỉ đích là 14.241.254.70, được dùng trong quá trình thực hiện lệnh traceroute để gửi các yêu cầu đến máy chủ.

- Khi các gói tin UDP này hết thời gian sống (TTL = 0), chúng sẽ gây ra việc tạo ra các gói tin ICMP với thông báo "Time-to-live exceeded", đánh dấu bằng màu xanh đậm, được gửi ngược lại từ các router đến máy tính nguồn.
- Tại tầng ứng dụng trong mô hình TCP/IP, các gói tin UDP này thường không được gán trực tiếp với một giao thức ứng dụng cụ thể, mà được sử dụng để thực hiện các thao tác như kiểm tra đường đi của gói tin (traceroute).

## 5. Sau khi xác định được IP của www.fit.hcmus.edu.vn, máy sẽ bắt đầu gửi gói tin:

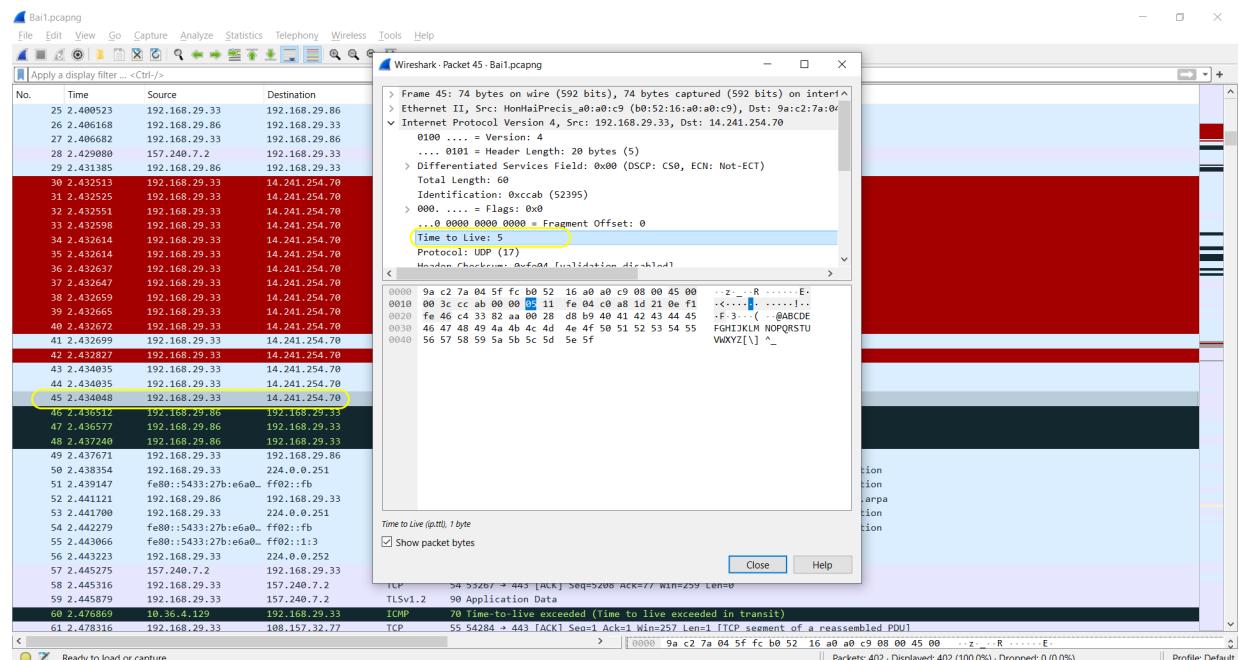
### a. Protocol được sử dụng của những gói tin sau đó là gì?

**Trả lời:** Sau khi xác định được IP của www.fit.hcmus.edu.vn, các gói tin gửi đi tiếp tục sử dụng giao thức UDP (User Datagram Protocol) cho việc gửi các yêu cầu traceroute.

### b. Có bao nhiêu gói tin được gửi đi (request) trước khi nhận được response đầu tiên trả lời cho những request? (Hay nói một cách khác là: lệnh trace\* sẽ gửi request message đi, và nhận về response. Vậy có bao nhiêu gói tin request đã gửi đi đến khi nhận được gói tin response đầu tiên?)

**Trả lời:** Có tổng cộng 16 gói tin request (từ gói thứ 30 đến gói thứ 45) được gửi đi trước khi nhận được gói tin response đầu tiên, đây là hành vi mặc định của lệnh traceroute.

### c. Cho biết TTL của gói tin cuối cùng được gửi trước khi nhận được gói tin response đầu tiên trả lời cho những gói tin request?



Hình 2: TTL của gói tin cuối cùng được gửi trước khi nhận được gói tin response đầu tiên là 5

d. Bạn có thấy thông tin port trong các gói tin gửi đi? Nếu có bạn nhận thấy port nguồn/dích của gói tin có gì đặc biệt? Nếu không thấy thông tin port, hãy giải thích nguyên nhân?

**Trả lời:** Có, các gói tin gửi đi có thông tin về port nguồn và port đích. Các cổng này có giá trị ngẫu nhiên nhưng vẫn thuộc dải cao ( $>= 33434$ ) để tránh trùng lặp với các cổng thường dùng bởi các giao thức khác.

e. Gói tin response đầu tiên là trả lời cho gói tin request thứ mấy?

25	2.400523	192.168.29.33	192.168.29.86	DNS	76 Standard query 0xb93d AAAA fit.hcmus.edu.vn
26	2.406168	192.168.29.86	192.168.29.33	DNS	76 Standard query response 0xb93d AAAA fit.hcmus.edu.vn
27	2.406682	192.168.29.33	192.168.29.86	DNS	76 Standard query 0xdedc AAAA fit.hcmus.edu.vn
28	2.429080	157.240.7.2	192.168.29.33	TLSv1.2	86 Application Data
29	2.431385	192.168.29.86	192.168.29.33	DNS	76 Standard query response 0xdedc AAAA fit.hcmus.edu.vn
30	2.432513	192.168.29.33	14.241.254.70	UDP	74 50188 → 33437 Len=32
31	2.432525	192.168.29.33	14.241.254.70	UDP	74 50255 → 33439 Len=32
32	2.432551	192.168.29.33	14.241.254.70	UDP	74 50198 → 33442 Len=32
33	2.432598	192.168.29.33	14.241.254.70	UDP	74 50212 → 33438 Len=32
34	2.432614	192.168.29.33	14.241.254.70	UDP	74 50202 → 33445 Len=32
35	2.432614	192.168.29.33	14.241.254.70	UDP	74 50223 → 33443 Len=32
36	2.432637	192.168.29.33	14.241.254.70	UDP	74 50200 → 33441 Len=32
37	2.432647	192.168.29.33	14.241.254.70	UDP	74 50225 → 33447 Len=32
38	2.432659	192.168.29.33	14.241.254.70	UDP	74 50222 → 33444 Len=32
39	2.432665	192.168.29.33	14.241.254.70	UDP	74 50258 → 33448 Len=32
40	2.432672	192.168.29.33	14.241.254.70	UDP	74 50231 → 33446 Len=32
41	2.432699	192.168.29.33	14.241.254.70	UDP	74 50226 → 33449 Len=32
42	2.432827	192.168.29.33	14.241.254.70	UDP	74 50208 → 33440 Len=32
43	2.434035	192.168.29.33	14.241.254.70	UDP	74 50250 → 33452 Len=32
44	2.434035	192.168.29.33	14.241.254.70	UDP	74 50210 → 33451 Len=32
45	2.434048	192.168.29.33	14.241.254.70	UDP	74 50227 → 33450 Len=32
46	2.436512	192.168.29.86	192.168.29.33	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
47	2.436577	192.168.29.86	192.168.29.33	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
48	2.437240	192.168.29.86	192.168.29.33	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)

Hình 3: Gói tin response đầu tiên là trả lời cho gói tin request thứ nhất

## 4 Bài 2: DHCP

### 1. Lọc các gói tin theo giao thức DHCP

No.	Time	Source	Destination	Protocol	Lengt	Info
184	4.436360	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x32b41237
185	4.440413	10.124.0.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x32b41237
186	4.441908	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x32b41237
194	4.608620	10.124.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x32b41237
941	10.303724	10.124.9.182	10.124.0.1	DHCP	342	DHCP Release - Transaction ID 0xd602e58a
1098	14.457990	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe8ee2265
1099	14.461351	10.124.0.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xe8ee2265
1100	14.462557	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0xe8ee2265
1129	15.360923	10.124.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe8ee2265

Hình 4: Lọc các gói tin theo giao thức DHCP

### 2. Giao thức được gói tin DHCP sử dụng tại tầng transport:

Giao thức UDP (User Datagram Protocol)

### 3. Địa chỉ tại tầng link của host được cấp IP là:

3c:21:9c:84:2d:71

```

▼ Ethernet II, Src: Intel_84:2d:71 (3c:21:9c:84:2d:71), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Intel_84:2d:71 (3c:21:9c:84:2d:71)
  Type: IPv4 (0x0800)

```

Hình 5: Client MAC Address

#### 4. IP nguồn, Port nguồn và IP đích, Port đích của 4 gói tin Discover/Offer/Request/ACK trong đợt xin cấp IP đầu tiên:

- **DHCP Discover:**

- IP nguồn: 0.0.0.0
- Port nguồn: 68
- IP đích: 255.255.255.255
- Port đích: 67

- **DHCP Offer:**

- IP nguồn: 10.124.0.1
- Port nguồn: 67
- IP đích: 255.255.255.255
- Port đích: 68

- **DHCP Request:**

- IP nguồn: 0.0.0.0
- Port nguồn: 68
- IP đích: 255.255.255.255
- Port đích: 67

- **DHCP ACK:**

- IP nguồn: 10.124.0.1
- Port nguồn: 67
- IP đích: 255.255.255.255
- Port đích: 68

## 5. Điểm khác biệt giữa các giá trị trong gói tin DHCP Discover và DHCP Request

(a) DHCP Discover

```

User Datagram Protocol, Src Port: 68, Dst Port: 67
Source Port: 68
Destination Port: 67
Length: 308
Checksum: 0xe1cb [unverified]
[Checksum Status: Unverified]
[Stream index: 66]
> [Timestamps]
    UDP payload (300 bytes)
Dynamic Host Configuration Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x32b41237
Seconds elapsed: 0
> Boot flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Intel_84:2d:71 (3c:21:9c:84:2d:71)
Client hardware address padding: 000000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
    Length: 1
        DHCP: Discover (1)
Option: (61) Client identifier
    Length: 7
        Hardware type: Ethernet (0x01)
        Client MAC address: Intel_84:2d:71 (3c:21:9c:84:2d:71)
Option: (50) Requested IP Address (10.124.9.182)
    Length: 4
        Requested IP Address: 10.124.9.182
Option: (12) Host Name
    Length: 3
        Host Name: Zuy
Option: (60) Vendor class identifier
    Length: 8
        Vendor class identifier: MSFT 5.0
Option: (55) Parameter Request List
Option: (255) End
    Option End: 255
    Padding: 000000000000000000000000

```

(b) DHCP Request

```

User Datagram Protocol, Src Port: 68, Dst Port: 67
Source Port: 68
Destination Port: 67
Length: 312
Checksum: 0xc57b [unverified]
[Checksum Status: Unverified]
[Stream index: 66]
> [Timestamps]
    UDP payload (304 bytes)
Dynamic Host Configuration Protocol (Request)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x32b41237
Seconds elapsed: 0
> Boot flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Intel_84:2d:71 (3c:21:9c:84:2d:71)
Client hardware address padding: 000000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Request)
    Length: 1
        DHCP: Request (3)
Option: (61) Client identifier
    Length: 7
        Hardware type: Ethernet (0x01)
        Client MAC address: Intel_84:2d:71 (3c:21:9c:84:2d:71)
Option: (50) Requested IP Address (10.124.9.182)
    Length: 4
        Requested IP Address: 10.124.9.182
Option: (54) DHCP Server Identifier (10.124.0.1)
    Length: 4
        DHCP Server Identifier: 10.124.0.1
Option: (12) Host Name
    Length: 3
        Host Name: Zuy
Option: (81) Client Fully Qualified Domain Name
    Length: 6
        > Flags: 0x00
        A-RR result: 0
        PTR-RR result: 0
        Client name: Zuy
Option: (60) Vendor class identifier
    Length: 8
        Vendor class identifier: MSFT 5.0
Option: (55) Parameter Request List
Option: (255) End
    Option End: 255

```

Hình 6

### Điểm khác nhau giữa các giá trị:

	Discover	Request
<b>Length</b>	308	312
<b>Checksum</b>	0xe1cb	0xc57b
<b>UDP payload</b>	300 bytes	304 bytes
<b>DHCP Message Type</b>	Discover	Request
<b>DHCP Server Identifier</b>	none	10.124.0.1
<b>Client Fully Qualified Domain Name</b>	none	yes

**6. Transaction-ID của 4 gói tin Discover/Offer/Request/ACK trong đợt xin cấp IP đầu tiên và Transaction-ID của 2 gói tin Request/ACK trong đợt xin cấp IP lần hai:**

**Đợt xin cấp IP đầu tiên:**

- **Discover:** 0x32b41237
- **Offer:** 0x32b41237
- **Request:** 0x32b41237
- **ACK:** 0x32b41237

**Đợt xin cấp IP lần hai:**

- **Request:** 0xe8ee2265
- **ACK:** 0xe8ee2265

**7. Ý nghĩa trường thông tin lease-time và giá trị của trường này trong gói tin bắt được:**

- **Lease Time:** Là khoảng thời gian máy khách được quyền sử dụng địa chỉ IP cấp phát bởi DHCP server.
- **Giá trị:** 1 giờ (3600s)

**\* Option: (51) IP Address Lease Time**

**Length: 4**

**IP Address Lease Time: 1 hour (3600)**

Hình 7: IP Address Lease Time

**8. Trường giá trị cho biết có thông tin DHCP relay agent hay không và IP của DHCP relay agent nếu có:**

- Thông tin về DHCP relay agent được cung cấp trong tùy chọn thông tin Relay Agent (option 82) của gói tin DHCP. Tùy chọn này sẽ xuất hiện nếu một relay agent tham gia vào việc chuyển tiếp các thông điệp DHCP giữa máy khách và máy chủ.
- Nếu không có tùy chọn thông tin Relay Agent (Option 82) xuất hiện, điều này có nghĩa là các gói tin DHCP được gửi trực tiếp giữa máy khách và máy chủ mà không có sự tham gia của relay agent. Khi đó, IP của relay agent là 0.0.0.0

Client IP address: 0.0.0.0  
 Your (client) IP address: 10.124.9.182  
 Next server IP address: 0.0.0.0  
**Relay agent IP address: 0.0.0.0**  
 Client MAC address: Intel\_84:2d:71 (3c:21:9c:84:2d:71)

Hình 8: Relay agent IP address

## 5 Bài 3: TCP

### 1. Lọc các gói tin HTTP bắt được trong quá trình upload file alice.txt

http						
No.	Time	Source	Destination	Protocol	Length	Info
60	5.268352	192.168.29.124	128.119.245.12	HTTP	20455	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
90	5.932786	128.119.245.12	192.168.29.124	HTTP	831	HTTP/1.1 200 OK (text/html)

Hình 9: Lọc các gói tin HTTP

### 2. Xác định IP của gaia.cs.umass.edu (máy chủ HTTP)

Trả lời: 128.119.245.12

### 3. Lọc các gói tin TCP

tcp						
No.	Time	Source	Destination	Protocol	Length	Info
3	1.973621	192.168.29.124	184.73.239.182	TCP	55	63803 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
4	2.387208	184.73.239.182	192.168.29.124	TCP	66	443 → 63803 [ACK] Seq=1 Ack=2 Win=425 Len=0 SLE=1 SRE=2
5	3.386967	192.168.29.124	128.119.245.12	TCP	54	63843 → 88 [FIN, ACK] Seq=1 Ack=1 Win=259 Len=0
6	3.388243	192.168.29.124	128.119.245.12	TCP	66	63847 → 88 [SYN] Seq=0 Win=4240 Len=0 MSS=1460 WS=256 SACK_PERM
7	3.390778	192.168.29.124	128.119.245.12	TCP	803	63845 → 88 [PSH, ACK] Seq=1 Ack=1 Win=260 Len=749 [TCP segment of a reassembled PDU]
8	3.391071	192.168.29.124	128.119.245.12	TCP	12294	63845 → 88 [ACK] Seq=759 Ack=1 Win=268 Len=12249 [TCP segment of a reassembled PDU]
9	4.026468	128.119.245.12	192.168.29.124	TCP	54	80 → 63843 [ACK] Seq=1 Ack=2 Win=233 Len=0
10	4.026468	128.119.245.12	192.168.29.124	TCP	66	63847 [SYN, ACK] Seq=0 Ack=1 Win=29208 Len=0 MSS=1360 SACK_PERM WS=128
11	4.026468	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=750 Win=240 Len=0
12	4.026468	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=1109 Win=263 Len=0
13	4.026468	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=0 Win=9190 Win=363 Len=0
14	4.026468	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=12999 Win=433 Len=0
15	4.026625	192.168.29.124	128.119.245.12	TCP	54	63847 → 88 [ACK] Seq=1 Ack=1 Win=66568 Len=0
16	4.026697	192.168.29.124	128.119.245.12	TCP	25894	63845 → 88 [PSH, ACK] Seq=12999 Ack=1 Win=260 Len=25840 [TCP segment of a reassembled PDU]
17	4.546907	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=14358 Win=456 Len=0
18	4.546907	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=15710 Win=479 Len=0
19	4.546907	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=17070 Win=502 Len=0
20	4.546907	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=19790 Win=544 Len=0
21	4.546907	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=21158 Win=567 Len=0
22	4.546907	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=22510 Win=599 Len=0
23	4.546907	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=25230 Win=632 Len=0
24	4.546907	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=26599 Win=655 Len=0
25	4.546907	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=27959 Win=678 Len=0
26	4.547819	192.168.29.124	128.119.245.12	TCP	29974	63845 → 88 [PSH, ACK] Seq=38830 Ack=1 Win=260 Len=29920 [TCP segment of a reassembled PDU]
27	4.551348	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=29310 Win=701 Len=0
28	4.551348	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=30670 Win=723 Len=0
29	4.551410	192.168.29.124	128.119.245.12	TCP	5494	63845 → 88 [ACK] Seq=68750 Ack=1 Win=260 Len=5440 [TCP segment of a reassembled PDU]
30	4.556244	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=32030 Win=746 Len=0
31	4.556293	192.168.29.124	128.119.245.12	TCP	2774	63845 → 88 [ACK] Seq=74190 Ack=1 Win=260 Len=2720 [TCP segment of a reassembled PDU]
32	4.582196	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=37470 Win=831 Len=0
33	4.582196	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=1 Ack=38830 Win=854 Len=0
34	4.582293	192.168.29.124	128.119.245.12	TCP	13654	63845 → 88 [PSH, ACK] Seq=76910 Ack=1 Win=260 Len=13600 [TCP segment of a reassembled PDU]
35	5.261392	128.119.245.12	192.168.29.124	TCP	54	80 → 63845 [ACK] Seq=48190 Win=877 Len=0

Hình 10: Lọc các gói tin TCP - 1

No.	Time	Source	Destination	Protocol	Length	Info
35	5.261392	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=4 Ack=60190 Win=877 Len=0	
39	5.261392	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=4 Ack=15150 Win=900 Len=0	
37	5.261392	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=4 Ack=6599 Win=985 Len=0	
31	5.261392	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=4 Ack=8359 Win=1008 Len=0	
39	5.261392	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=49710 Win=1039 Len=0	
40	5.261392	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=53798 Win=1094 Len=0	
41	5.261392	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=65510 Win=1137 Len=0	
42	5.261392	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=57878 Win=1159 Len=0	
43	5.261392	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=59238 Win=1182 Len=0	
44	5.261392	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=60590 Win=1205 Len=0	
45	5.261479	192.168.29.124	128.119.245.12	TCP	42214 63845 → 80 [PSH, ACK] Seq=1 Ack=1 Win=260 Len=42160 [TCP segment of a reassembled PDU]	
46	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=63310 Win=1241 Len=0	
47	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=64678 Win=1278 Len=0	
48	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=66038 Win=1293 Len=0	
49	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=67398 Win=1316 Len=0	
50	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=68758 Win=1338 Len=0	
51	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=71478 Win=1381 Len=0	
52	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=72838 Win=1404 Len=0	
53	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=75558 Win=1422 Len=0	
64	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=78278 Win=1426 Len=0	
55	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=79638 Win=1432 Len=0	
56	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=82358 Win=1426 Len=0	
57	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=85078 Win=1426 Len=0	
58	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=87798 Win=1426 Len=0	
59	5.268269	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=90518 Win=1426 Len=0	
60	5.268352	192.168.29.124	128.119.245.12	HTTP	20455 POST /wireshark-labs/lab3\1-reply.htm HTTP/1.1 (text/plain)	
61	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=45090 Win=1419 Len=0	
62	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=97310 Win=1474 Len=0	
63	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=98679 Win=1497 Len=0	
64	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=100930 Win=1520 Len=0	
65	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=101390 Win=1543 Len=0	
66	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=105470 Win=1608 Len=0	
67	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=108198 Win=1649 Len=0	

Hình 11: Lọc các gói tin TCP - 2

No.	Time	Source	Destination	Protocol	Length	Info
66	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=105470 Win=1606 Len=0	
67	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=108198 Win=1649 Len=0	
68	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=110910 Win=1651 Len=0	
69	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=113639 Win=1734 Len=0	
70	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=114998 Win=1757 Len=0	
71	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=116358 Win=1779 Len=0	
72	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=117710 Win=1802 Len=0	
73	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=121790 Win=1889 Len=0	
74	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=123159 Win=1889 Len=0	
75	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=124510 Win=1912 Len=0	
76	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=125878 Win=1934 Len=0	
77	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=132678 Win=2041 Len=0	
78	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=134030 Win=2063 Len=0	
79	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=135398 Win=2086 Len=0	
80	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=138110 Win=2129 Len=0	
81	5.871861	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=139478 Win=2152 Len=0	
92	5.875810	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=142198 Win=2194 Len=0	
93	5.875810	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=143550 Win=2171 Len=0	
84	5.884669	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=144010 Win=2240 Len=0	
85	5.886089	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=148990 Win=2383 Len=0	
86	5.900604	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=150358 Win=2326 Len=0	
87	5.919179	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=151700 Win=2349 Len=0	
88	5.932692	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=153070 Win=2363 Len=0	
89	5.932692	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=1 Ack=153071 Win=2363 Len=0	
90	5.932786	128.119.245.12	192.168.29.124	HTTP	831 HTTP/1.1 200 OK (text/html)	
91	5.932786	192.168.29.124	128.119.245.12	TCP	54 63845 → 80 [ACK] Seq=153071 Ack=778 Win=257 Len=0	
92	6.218460	192.168.29.124	184.18.32.47	TCP	55 63840 → 443 [ACK] Seq=1 Ack=1 Win=260 Len=1 [TCP segment of a reassembled PDU]	
93	6.382835	184.18.32.47	192.168.29.124	TCP	66 443 → 63840 [ACK] Seq=1 Ack=1 Len=0 SLE=1 SRE=2	
94	6.382835	192.168.29.124	34.196.223.149	TCP	55 63841 → 443 [ACK] Seq=1 Ack=1 Win=259 Len=1 [TCP segment of a reassembled PDU]	
95	6.397029	192.168.29.124	44.199.104.227	TCP	55 63842 → 443 [ACK] Seq=1 Ack=1 Win=259 Len=1 [TCP segment of a reassembled PDU]	
96	6.397029	192.168.29.124	44.199.104.227	TCP	55 63839 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]	
97	7.001568	192.168.29.124	44.199.104.227	TCP	55 63839 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]	
97	7.001703	192.168.29.124	44.199.104.227	TCP	55 63838 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]	
98	7.001703	192.168.29.124	44.199.104.227	TCP	66 443 → 63839 [ACK] Seq=1 Ack=2 Win=214 Len=0 SLE=1 SRE=2	
99	7.486566	44.199.104.227	192.168.29.124	TCP	55 63845 → 443 [ACK] Seq=1 Ack=2 Win=186 Len=0 SLE=1 SRE=2	
100	7.486566	44.199.104.227	192.168.29.124	TCP	66 443 → 63842 [ACK] Seq=1 Ack=2 Win=127 Len=0 SLE=1 SRE=2	
101	7.486566	44.199.104.227	192.168.29.124	TCP	66 443 → 63838 [ACK] Seq=1 Ack=2 Win=347 Len=0 SLE=1 SRE=2	
115	11.193656	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [FIN, ACK] Seq=778 Ack=153071 Win=2363 Len=0	
116	11.193716	128.119.245.12	128.119.245.12	TCP	54 63845 → 80 [ACK] Seq=153071 Ack=779 Win=257 Len=0	
123	12.502547	192.168.29.124	128.119.245.12	TCP	54 63845 → 80 [FIN, ACK] Seq=153071 Ack=779 Win=257 Len=0	
124	12.502962	192.168.29.124	115.79.4.48	TCP	66 63843 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
125	12.532880	115.79.4.48	192.168.29.124	TCP	66 443 → 63848 [SYN, ACK] Seq=0 Ack=1 Win=7308 Len=0 MSS=1360 SACK_PERM WS=1024	
126	12.53415	192.168.29.124	115.79.4.48	TCP	54 63848 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0	
127	12.534502	192.168.29.124	115.79.4.48	TLSV1.2	1997 Client Hello (SNI=courses.ctda.hcmus.edu.vn)	
128	12.580744	115.79.4.48	192.168.29.124	TCP	54 443 → 63848 [ACK] Seq=1 Ack=1944 Win=168 Len=0	
129	12.580744	115.79.4.48	192.168.29.124	TLSV1.2	195 Server Hello, Change Cipher Spec, Encrypted Handshake Message	
130	12.585029	192.168.29.124	115.79.4.48	TLSV1.2	105 Change Cipher Spec, Encrypted Handshake Message	
131	12.729931	115.79.4.48	192.168.29.124	TCP	54 443 → 63848 [ACK] Seq=142 Ack=1995 Win=168 Len=0	
133	12.988087	128.119.245.12	192.168.29.124	TCP	54 80 → 63845 [ACK] Seq=779 Ack=153072 Win=2363 Len=0	
162	14.780488	192.168.29.124	74.125.200.188	TCP	55 63727 → 5228 [ACK] Seq=1 Ack=1 Win=257 Len=1	
163	14.855963	74.125.200.188	192.168.29.124	TCP	66 5228 → 63727 [ACK] Seq=1 Ack=2 Win=289 Len=0 SLE=1 SRE=2	

Hình 13: Lọc các gói tin TCP - 4

- Sequence number của TCP SYN segment: **0** (raw sequence number: **3974004991**)
- Gói tin dùng để tạo kết nối giữa client và máy chủ HTTP: Gói tin đầu tiên có flag [SYN] trong cột Info. Đây là gói tin đầu tiên trong quá trình bắt tay TCP.
- Giá trị SYN flag trong gói tin sẽ là 1, điều này xác định đây là một SYN segment.

```
> Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{4F41E6B6-045C-45C5-B719-DDA411BAA5B7}, id 0
> Ethernet II, Src: Intel_0b:90:19 (28:6b:35:0b:90:19), Dst: 9a:c2:7a:04:5f:fc (9a:c2:7a:04:5f:fc)
> Internet Protocol Version 4, Src: 192.168.29.124, Dst: 128.119.245.12
└ Transmission Control Protocol, Src Port: 63847, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 63847
  Destination Port: 80
  [Stream index: 2]
  > [Conversation completeness: Incomplete, ESTABLISHED (7)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 3974004991
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
```

Hình 14: Chi tiết gói tin có flag [SYN] đầu tiên

```
Flags: 0x012 (SYN, ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Accurate ECN: Not set
  .... 0.... .... = Congestion Window Reduced: 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
```

Hình 15: Chi tiết trường Flags trong gói tin có flag [SYN] đầu tiên

#### 4. Xác định sequence number của TCP SYNACK segment và giá trị trường Acknowledgement

- Gói tin tiếp theo trong danh sách có flag [SYN, ACK] trong cột Info. Đây là gói tin phản hồi từ máy chủ HTTP.
- Gói tin này có sequence number: **0** (raw sequence number: **3974004991**)
- Giá trị trường Acknowledgement: **1**
- Giá trị ACK: **1** (raw ACK number: **3974004992**)
- Máy chủ HTTP xác định giá trị Acknowledgement bằng cách cộng 1 vào sequence number của gói tin SYN từ client.

```

> Frame 10: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{4F41E6B6-045C-45C5-B719-DDA411BAA5B7}, id 0
> Ethernet II, Src: 9a:c2:7a:04:5f:fc (9a:c2:7a:04:5f:fc), Dst: Intel_0b:90:19 (28:6b:35:0b:90:19)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.29.124
< Transmission Control Protocol, Src Port: 80, Dst Port: 63847, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 63847
    [Stream index: 2]
    > [Conversation completeness: Incomplete, ESTABLISHED (7)]
        [TCP Segment Len: 0]
        Sequence Number: 0 (relative sequence number)
        Sequence Number (raw): 1556213537
        [Next Sequence Number: 1 (relative sequence number)]
        Acknowledgment Number: 1 (relative ack number)
        Acknowledgment number (raw): 3974004992

```

Hình 16: Chi tiết gói tin có flag [SYN, ACK] đầu tiên

```

Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0.... .... = Congestion Window Reduced: 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

```

Hình 17: Chi tiết trường Flags trong gói tin có flag [SYN, ACK] đầu tiên

## 5. Xác định sequence number trong gói tin chứa HTTP POST command

- Sequence number: **132670** (raw sequence number: **4226641008**)

```

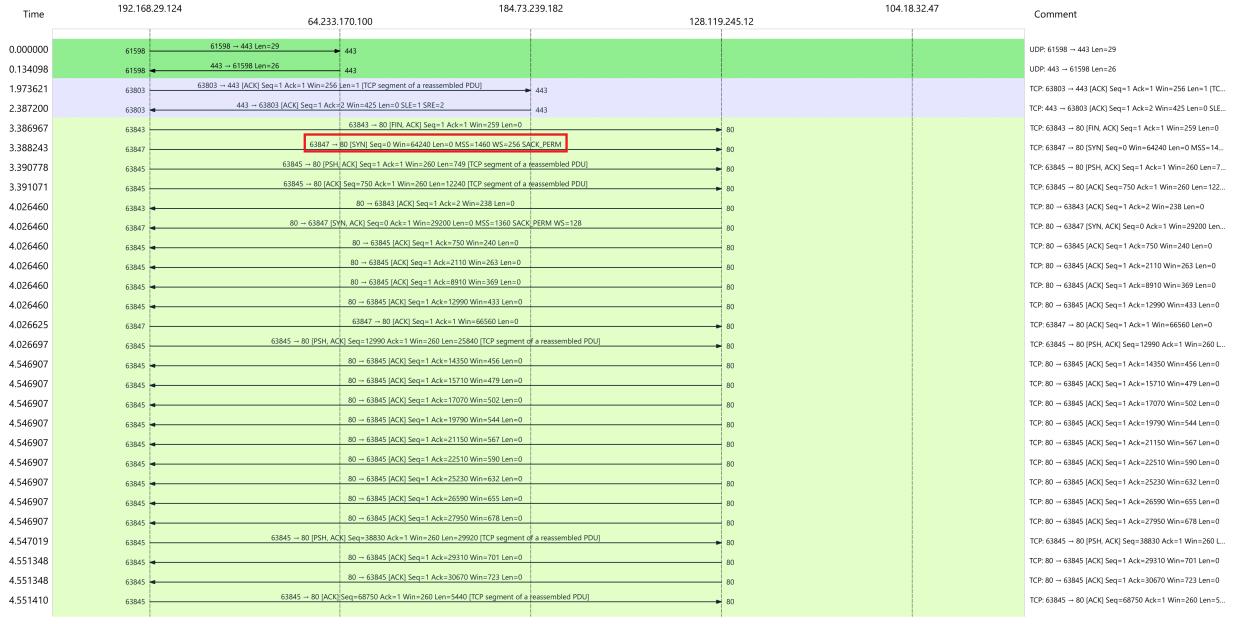
> Frame 60: 20455 bytes on wire (163640 bits), 20455 bytes captured (163640 bits) on interface \Device\NPF_{4F41E6B6-045C-45C5-B719-DDA411BAA5B7}, id 0
> Ethernet II, Src: Intel_0b:90:19 (28:6b:35:0b:90:19), Dst: 9a:c2:7a:04:5f:fc (9a:c2:7a:04:5f:fc)
> Internet Protocol Version 4, Src: 192.168.29.124, Dst: 128.119.245.12
< Transmission Control Protocol, Src Port: 63845, Dst Port: 80, Seq: 132670, Ack: 1, Len: 20401
    Source Port: 63845
    Destination Port: 80
    [Stream index: 3]
    > [Conversation completeness: Incomplete (28)]
        [TCP Segment Len: 20401]
        Sequence Number: 132670 (relative sequence number)
        Sequence Number (raw): 4226641008
        [Next Sequence Number: 153071 (relative sequence number)]
        Acknowledgment Number: 1 (relative ack number)
        Acknowledgment number (raw): 2308719039

```

Hình 18: Chi tiết gói tin chứa HTTP POST command

## 6. Vẽ quá trình trao đổi gói tin TCP

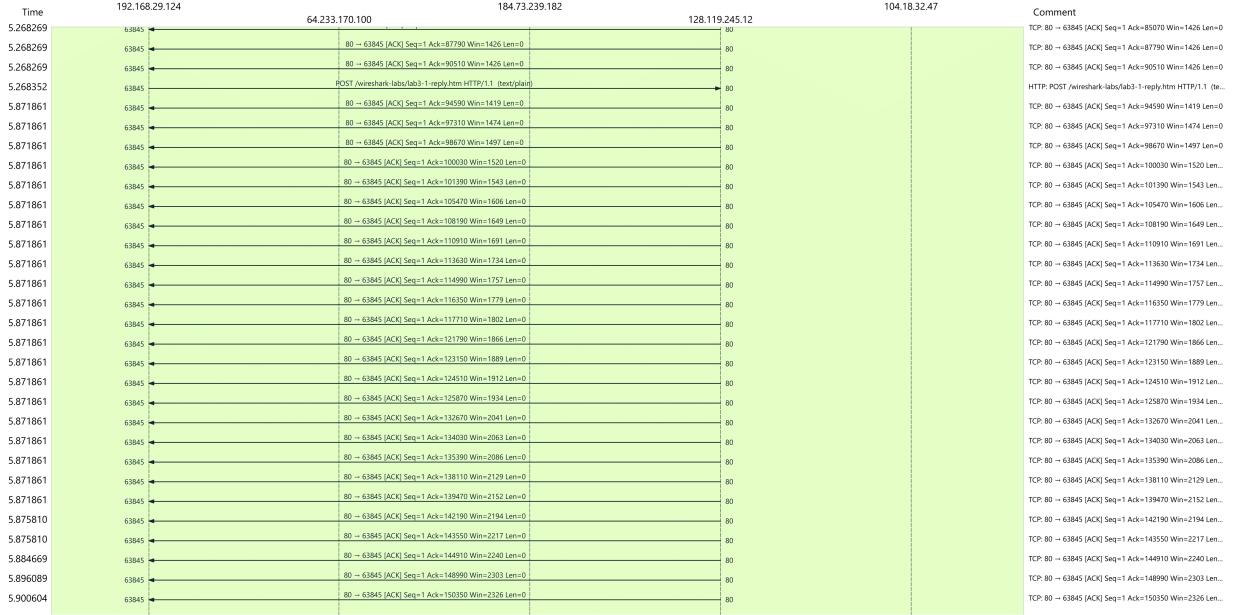
- Quá trình trao đổi gói tin TCP được vẽ sử dụng chức năng Statistics/Flow Graph của Wireshark.



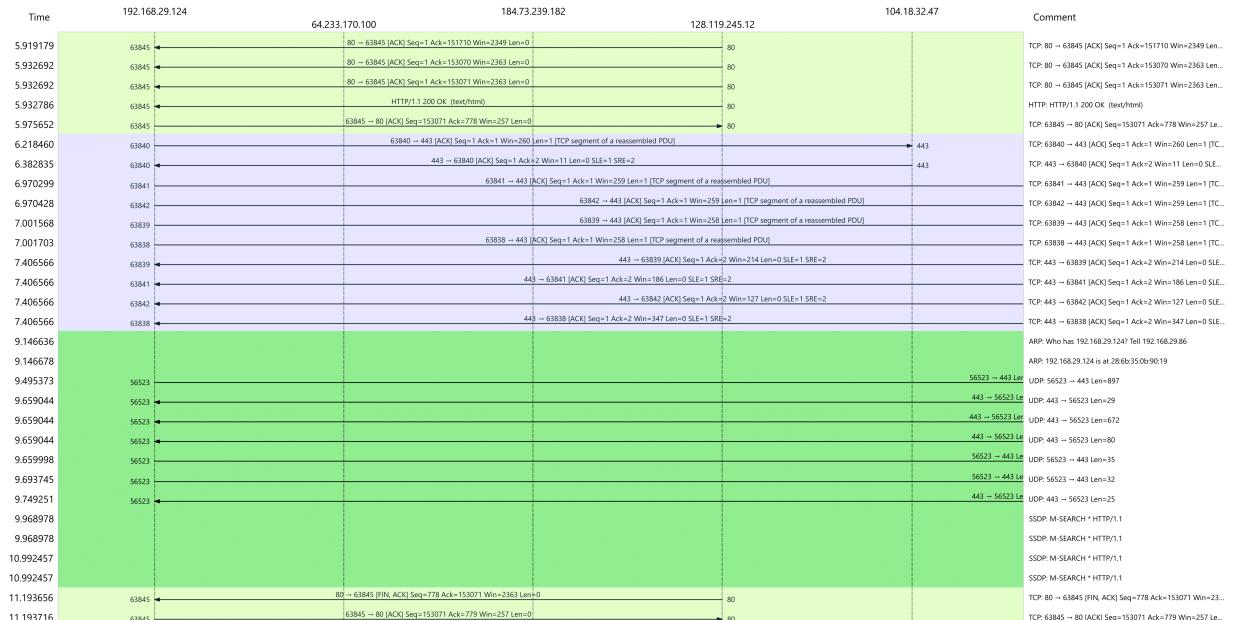
Hình 19: Quá trình trao đổi gói tin TCP - 1  
Bắt đầu từ gói tin chứa flag [SYN] đầu tiên



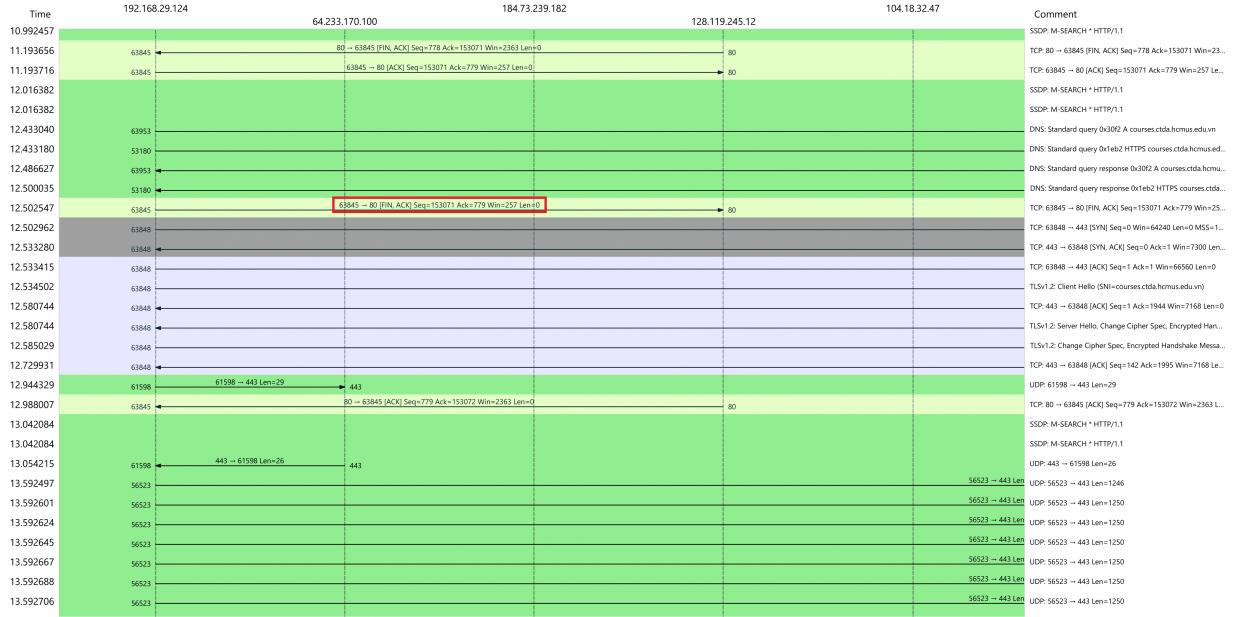
Hình 20: Quá trình trao đổi gói tin TCP - 2



Hình 21: Quá trình trao đổi gói tin TCP - 3



Hình 22: Quá trình trao đổi gói tin TCP - 4



Hình 23: Quá trình trao đổi gói tin TCP - 5  
Kết thúc bằng gói tin chứa flag FIN

## 6 Bảng phân công công việc

STT	MSSV	HỌ VÀ TÊN	PHÂN CÔNG CÔNG VIỆC
01	23127040	Bùi Minh Duy	Bài 2
02	23127082	Nguyễn Thị Khánh Linh	Bài 3
03	23127211	Nguyễn Lê Hồ Anh Khoa	Bài 1

Bảng 3: Bảng phân công công việc

## 7 Nguồn tài liệu tham khảo

- **Wireshark User's Guide**