

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



ĐỒ ÁN MẠNG MÁY TÍNH:
WIRESHARK

Lớp: 20CTT2

Thông tin nhóm: - Lê Trần Thiện Thắng – 20120188

- Nguyễn Huỳnh Phú Thịnh - 20120197

- Trần Minh Toàn - 20120215

Thành phố Hồ Chí Minh - 2021

- Bảng phân công công việc:

Tên	Lê Trần Thiện Thắng	Nguyễn Huỳnh Phú Thịnh	Trần Minh Toàn
Công việc	<ul style="list-style-type: none"> - Bài 2: HTTP Dùng wireshark để bắt gói tin khi truy cập vào trang web: http://example.com và trả lời các câu hỏi - Bài 4: câu 4 	<ul style="list-style-type: none"> - Bài 3: <ul style="list-style-type: none"> + Sử dụng Wireshark bắt gói tin và sử dụng lệnh tracert www.fit.hcmus.edu.vn ở command prompt để tìm kiếm đường đi của các gói tin. + Chụp màn hình kết quả và trả lời câu hỏi. - Bài 4: <ul style="list-style-type: none"> + Dùng Wireshark bắt gói tin DHCP. + Chụp màn hình kết quả và trả lời câu hỏi 1 và câu hỏi 2. 	<ul style="list-style-type: none"> - Bài 1: Sử dụng file ping.pcang để trả lời câu hỏi và chụp hình minh họa cho câu trả lời. - Bài 4: Câu 3

- Mức độ hoàn thành:

Mức độ	Đã hoàn thành	Chưa hoàn thành
Câu 1	100%	
Câu 2	100%	
Câu 3	100%	
Câu 4	100%	

BÀI LÀM

Bài 01: Ping

Ping

1. Địa chỉ IP của host ping: 192.168.0.105

Địa chỉ IP của host được ping: 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
T+	3 0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request id=0x000d, seq=1/256, ttl=64 (rep)

2. Không có port được sử dụng do giao thức ICMP thuộc tầng Internet còn port nằm trong giao thức TCP/UDP thuộc tầng Transport.

3.

48 bytes	16 bytes	20 bytes	14 bytes
ICMP data	ICMP header	IP header	Ethernet header

+ **ICMP data:** 48 bytes.

Data (48 bytes)

Data: b1af09000000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b...
[Length: 48]

- + **ICMP header:** 16 bytes bao gồm: Type (1 byte), Code (1 byte), Checksum (2 bytes), Identifier (2 byte), Sequence Number (2 byte), Timestamp From ICMP Data (8 bytes).

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x0cce [correct]
[Checksum Status: Good]
Identifier (BE): 13 (0x000d)
Identifier (LE): 3328 (0xd00d)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
[Response frame: 4]
Timestamp from icmp data: Apr  1, 2021 10:42:04.000000000 SE Asia Standard Time
[Timestamp from icmp data (relative): 0.636662804 seconds]
```

- + IP header: 20 bytes.

Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.1.1
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)

- + Ethernet header: 14 bytes

4. Có 2 gói tin ARP vì nguyên lý hoạt động của nghi thức ARP bao gồm ARP request và ARP reply

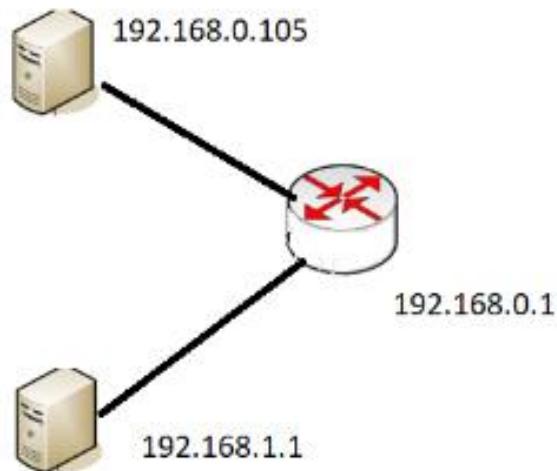
- ARP Request:
 - + Nội dung: Tìm địa chỉ MAC của một địa chỉ IP
 - + Source MAC là MAC của máy gửi, Destination MAC là broadcast

1 0.000000000 IntelCor_3c:ac:58 Broadcast ARP 42 Who has 192.168.0.1? Tell 192.168.0.105

- ARP Reply:
 - + Nội dung: Thông tin của địa chỉ MAC của địa chỉ IP tương ứng
 - + Gửi gói tin Unicast đến địa chỉ IP đã request đến

```
2 0.001828232 Tp-LinkT_fc:53:7e IntelCor_3c:ac:58 ARP 42 192.168.0.1 is at 18:d6:c7:fc:53:7e
```

5.



Mạng máy tính

Bài 02: HTTP

1. Kết quả:

- Bắt đầu DNS:

No.	Time	Source	Destination	Protocol	Length	Info
5 0 . 418249	192.168.1.4		52.111.240.14	TLSv1.2	89	Application Data
6 0 . 513294	52.111.240.14		192.168.1.4	TCP	54	443 → 58661 [ACK] Seq=1 Ack=36 Win=2045 Len=0
7 1 . 739741	192.168.1.1		224.0.0.1	IGMPv2	46	Membership Query, general
8 1 . 742976	fe80::6f64:2cff:febe:3cca		ff02::1	ICMPv6	90	Multicast Listener Query
9 1 . 743090	fe80::9466:9dcd:483a:d8b9		ff02::16	ICMPv6	170	Multicast Listener Report Message v2
10 1 . 847433	192.168.1.3		239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
11 1 . 940064	192.168.1.4		224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
12 1 . 940134	192.168.1.4		224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
13 2 . 2726815	192.168.1.4		123.26.26.26	DNS	71	Standard query 0x822d A example.com
14 2 . 2727841	192.168.1.4		123.26.26.26	DNS	71	Standard query 0x8e61 AAAA example.com
15 2 . 2729162	192.168.1.4		123.26.26.26	DNS	69	Standard query 0x7ef4 A wpad.Home
16 2 . 2729277	192.168.1.4		123.26.26.26	DNS	69	Standard query 0x8da7 AAAA wpad.Home
17 2 . 2731873	123.26.26.26		192.168.1.4	DNS	99	Standard query response 0xe861 AAAA example.com AAAA 2606:2800:220:1:248:1893:25c8:1946
18 2 . 732659	123.26.26.26		192.168.1.4	DNS	87	Standard query response 0x822d A example.com A 93.184.216.34
19 2 . 733027	2001:e0:56ba:16c0:10a4:a591:66da:6b7e		2606:2800:220:1:248:1893:25c8:1946	TCP	86	50707 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
20 2 . 734622	123.26.26.26		192.168.1.4	DNS	144	Standard query response 0x8da7 No such name AAAA wpad.Home SOA a.root-servers.net
21 2 . 735167	123.26.26.26		192.168.1.4	DNS	144	Standard query response 0x7ef4 A wpad.Home No such name AAAA wpad.Home SOA a.root-servers.net
22 2 . 762611	192.168.1.4		123.26.26.26	DNS	79	Standard query 0xb621 A x.urs.microsoft.com
23 2 . 762611	192.168.1.4		123.26.26.26	DNS	89	Standard query 0xacb2 A nav.smartscreen.microsoft.com
24 2 . 762730	192.168.1.4		123.26.26.26	DNS	79	Standard query 0x698f AAAA x.urs.microsoft.com
25 2 . 762778	192.168.1.4		123.26.26.26	DNS	89	Standard query 0x5df6 AAAA nav.smartscreen.microsoft.com
26 2 . 767544	123.26.26.26		192.168.1.4	DNS	210	Standard query response 0xb621 A x.urs.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAM
27 2 . 769070	123.26.26.26		192.168.1.4	DNS	220	Standard query response 0xacb2 A nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficman
28 2 . 769569	123.26.26.26		192.168.1.4	DNS	264	Standard query response 0x5df6 AAAA nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficman
29 2 . 769875	192.168.1.4		20.212.96.199	TCP	66	50708 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
30 2 . 793356	20.212.96.199		192.168.1.4	TCP	66	443 → 50708 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
31 2 . 793415	192.168.1.4		20.212.96.199	TCP	54	50708 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
32 2 . 793753	192.168.1.4		20.212.96.199	TLSv1.2	250	Client Hello
33 2 . 818589	20.212.96.199		192.168.1.4	TCP	1506	443 → 50708 [ACK] Seq=1 Ack=197 Win=525312 Len=1452 [TCP segment of a reassembled PDU]
34 2 . 819540	20.212.96.199		192.168.1.4	TCP	4410	443 → 50708 [ACK] Seq=1453 Ack=197 Win=525312 Len=4356 [TCP segment of a reassembled PDU]
35 2 . 819540	20.212.96.199		192.168.1.4	TLSv1.2	1480	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
36 2 . 819556	192.168.1.4		20.212.96.199	TCP	54	50708 → 443 [ACK] Seq=197 Ack=7235 Win=132352 Len=0
37 2 . 821441	192.168.1.4		20.212.96.199	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
38 2 . 845913	20.212.96.199		192.168.1.4	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
39 2 . 846553	192.168.1.4		20.212.96.199	TLSv1.2	463	Application Data
40 2 . 846611	192.168.1.4		20.212.96.199	TLSv1.2	1791	Application Data
41 2 . 871721	20.212.96.199		192.168.1.4	TCP	54	443 → 50708 [ACK] Seq=7286 Ack=2501 Win=525568 Len=0
42 2 . 874482	20.212.96.199		192.168.1.4	TLSv1.2	1375	Application Data
43 2 . 874542	192.168.1.4		20.212.96.199	TCP	54	50708 → 443 [ACK] Seq=2501 Ack=8608 Win=131072 Len=0
44 2 . 874634	192.168.1.4		20.212.96.199	TLSv1.2	85	Encrypted Alert
45 2 . 874662	192.168.1.4		20.212.96.199	TCP	54	50708 → 443 [FIN, ACK] Seq=2532 Ack=8608 Win=131072 Len=0

> Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{CA9FR89C-F419-4F4C-96F0-FD6042D55669}... id: 0	Packets: 259 · Displayed: 259 (100.0%)	Profile: Default
---	--	------------------

bai2.pcapng	801 CH	17/12/2021
-------------	--------	------------

- Bắt đầu gửi HTTP request

No.	Time	Source	Destination	Protocol	Length	Info
46 2 . 897724	20.212.96.199		192.168.1.4	TCP	54	443 → 50708 [ACK] Seq=8608 Ack=2533 Win=525568 Len=0
47 2 . 925318	2606:2800:220:1:248:1893:25c8:1946	2001:e0:56ba:16c0:10a4:a591:66da:6b7e		TCP	86	80 → 50707 [SYN, ACK] Seq=0 Ack=8608 Win=65535 Len=0 MSS=1220 SACK_PERM=1 WS=512
48 2 . 925365	2001:e0:56ba:16c0:10a4:a591:66da:6b7e	2606:2800:220:1:248:1893:25c8:1946		TCP	54	50707 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
49 2 . 925675	2001:e0:56ba:16c0:10a4:a591:66da:6b7e	2606:2800:220:1:248:1893:25c8:1946		HTTP	518	GET / HTTP/1.1
50 3 . 113823	2606:2800:220:1:248:1893:25c8:1946	2001:e0:56ba:16c0:10a4:a591:66da:6b7e		TCP	74	80 → 50707 [ACK] Seq=1 Ack=45 Win=67072 Len=0
51 3 . 173659	192.168.1.3		192.168.1.255	UDP	77	59014 → 15600 Len=35
52 3 . 186277	2606:2800:220:1:248:1893:25c8:1946	2001:e0:56ba:16c0:10a4:a591:66da:6b7e		HTTP	1079	HTTP/1.1 200 OK (text/html)
53 3 . 235817	2001:e0:56ba:16c0:10a4:a591:66da:6b7e	2606:2800:220:1:248:1893:25c8:1946		TCP	74	50707 → 80 [ACK] Seq=445 Ack=1006 Win=130560 Len=0
54 3 . 775784	192.168.1.4		123.23.23.23	DNS	79	Standard query 0x698f AAAA x.urs.microsoft.com
55 3 . 778129	123.23.23.23		192.168.1.4	DNS	254	Standard query response 0x698f AAAA x.urs.microsoft.com CNAME wd-prod-ss.trafficmanager.net ...
56 3 . 783641	192.168.1.4		20.212.96.199	TCP	66	50709 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
57 3 . 809291	20.212.96.199		192.168.1.4	TCP	66	443 → 50709 [ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
58 3 . 809386	192.168.1.4		20.212.96.199	TLSv1.2	54	50709 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
59 3 . 809650	192.168.1.4		20.212.96.199	TLSv1.2	240	Client Hello
60 3 . 838673	20.212.96.199		192.168.1.4	TCP	1506	443 → 50708 [ACK] Seq=1 Ack=187 Win=525312 Len=1452 [TCP segment of a reassembled PDU]
61 3 . 839832	20.212.96.199		192.168.1.4	TCP	4410	443 → 50708 [ACK] Seq=1453 Ack=187 Win=525312 Len=4356 [TCP segment of a reassembled PDU]
62 3 . 839832	20.212.96.199		192.168.1.4	TLSv1.2	1480	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
63 3 . 839848	192.168.1.4		20.212.96.199	TCP	54	50709 → 443 [ACK] Seq=187 Ack=7235 Win=132352 Len=0
64 3 . 841660	192.168.1.4		20.212.96.199	TLSv1.2	1056	443 → 50709 [ACK] Seq=1 Ack=187 Win=525312 Len=1452 [TCP segment of a reassembled PDU]
65 3 . 869118	20.212.96.199		192.168.1.4	TLSv1.2	4410	443 → 50708 [ACK] Seq=1453 Ack=187 Win=525312 Len=4356 [TCP segment of a reassembled PDU]
66 3 . 869705	192.168.1.4		20.212.96.199	TLSv1.2	361	Application Data
67 3 . 869760	192.168.1.4		20.212.96.199	TLSv1.2	350	Application Data
68 3 . 899201	20.212.96.199		192.168.1.4	TCP	54	443 → 50709 [ACK] Seq=7286 Ack=948 Win=524544 Len=0
69 3 . 901638	20.212.96.199		192.168.1.4	TLSv1.2	570	Application Data
70 3 . 901656	192.168.1.4		20.212.96.199	TCP	54	50709 → 441 [ACK] Seq=948 Ack=980 Win=131840 Len=0
71 3 . 901758	192.168.1.4		20.212.96.199	TLSv1.2	54	50709 → 441 [ACK] Seq=979 Ack=980 Win=131840 Len=0
72 3 . 991787	192.168.1.4		20.212.96.199	TCP	54	50709 → 443 [FIN, ACK] Seq=979 Ack=980 Win=131840 Len=0
73 3 . 927096	20.212.96.199		192.168.1.4	TCP	54	443 → 50709 [ACK] Seq=980 Ack=980 Win=524544 Len=0
74 3 . 935047	2001:e0:56ba:16c0:10a4:a591:66da:6b7e	2606:2800:220:1:248:1893:25c8:1946		HTTP	4508	HTTP/1.1 favicon.ico HTTP/1.1
75 4 . 163696	2606:2800:220:1:248:1893:25c8:1946	2001:e0:56ba:16c0:10a4:a591:66da:6b7e		TCP	74	80 → 50709 [ACK] Seq=1 Ack=820 Win=68096 Len=0
76 4 . 151613	2606:2800:220:1:248:1893:25c8:1946	2001:e0:56ba:16c0:10a4:a591:66da:6b7e		HTTP	1087	HTTP/1.1 404 Not Found (text/html)
77 4 . 199175	2001:e0:56ba:16c0:10a4:a591:66da:6b7e	2606:2800:220:1:248:1893:25c8:1946		TCP	74	50707 → 80 [ACK] Seq=829 Ack=2019 Win=131584 Len=0
78 4 . 414566	192.168.1.4		183.81.86.29	TCP	55	50809 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1 [TCP segment of a reassembled PDU]
79 4 . 443209	192.168.1.4		192.168.1.4	TCP	66	443 → 50809 [ACK] Seq=1 Ack=2 Win=237 Len=0 SLE=1 SRE=2
80 5 . 216521	2001:e0:56ba:16c0:10a4:a591:66da:6b7e	2404:6800:4005:80a::2002		TCP	75	50809 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
81 5 . 216542	192.168.1.4		216.58.200.66	TCP	55	50809 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
82 5 . 291195	2404:6800:4005:80a::2002	2001:e0:56ba:16c0:10a4:a591:66da:6b7e		TCP	86	443 → 50809 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
83 5 . 305131	216.58.200.66		192.168.1.4	TCP	66	443 → 50809 [ACK] Seq=1 Ack=1 Win=261 Len=0 SLE=0 SLE=1 SRE=2
84 6 . 143148	192.168.1.3		239.255.255.250	UDP	77	47465 → 15600 Len=35
85 6 . 367462	2001:e0:56ba:16c0:10a4:a591:66da:6b7e	2606:2800:220:1:248:1893:25c8:1946		TCP	74	50707 → 80 [FIN, ACK] Seq=829 Ack=2019 Win=131584 Len=0
86 6 . 424997	192.168.1.4		13.225.99.36	TCP	54	50809 → 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0

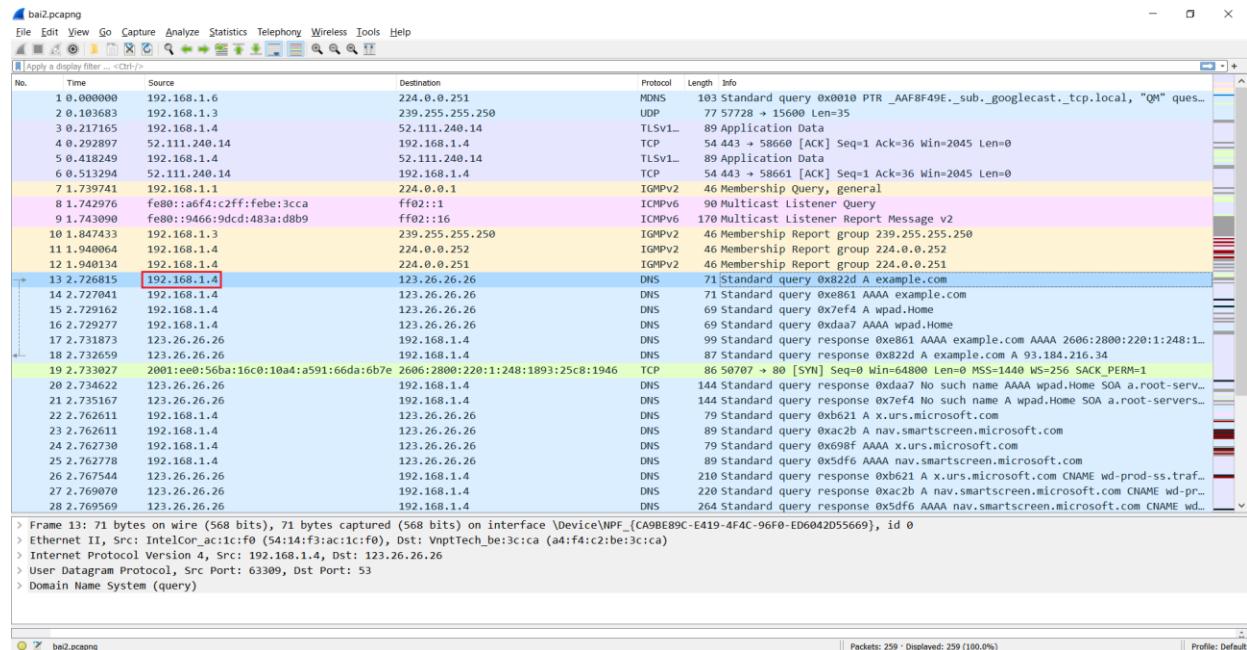
> Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{CA9FR89C-F419-4F4C-96F0-FD6042D55669}... id: 0	Packets: 259 · Displayed: 259 (100.0%)	Profile: Default
---	--	------------------

bai2.pcapng	802 CH	17/12/2021
-------------	--------	------------

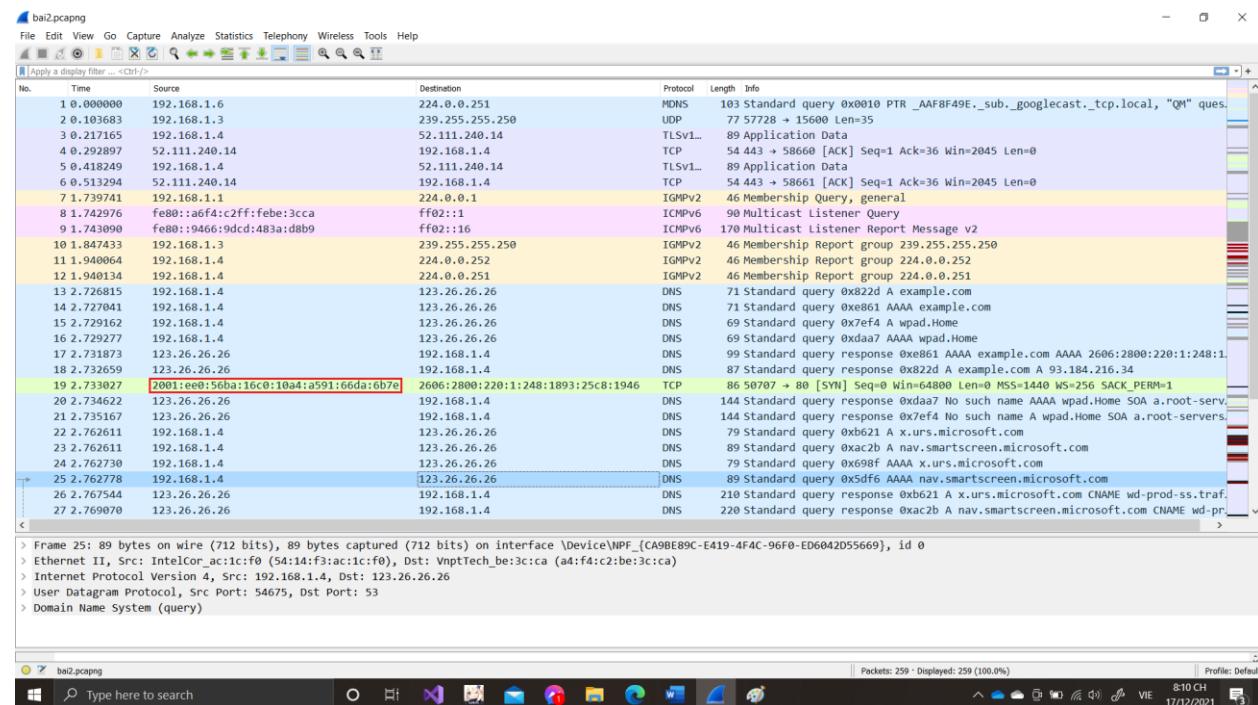
Mạng máy tính

2. IP của host:

- IPv4: 192.168.1.4

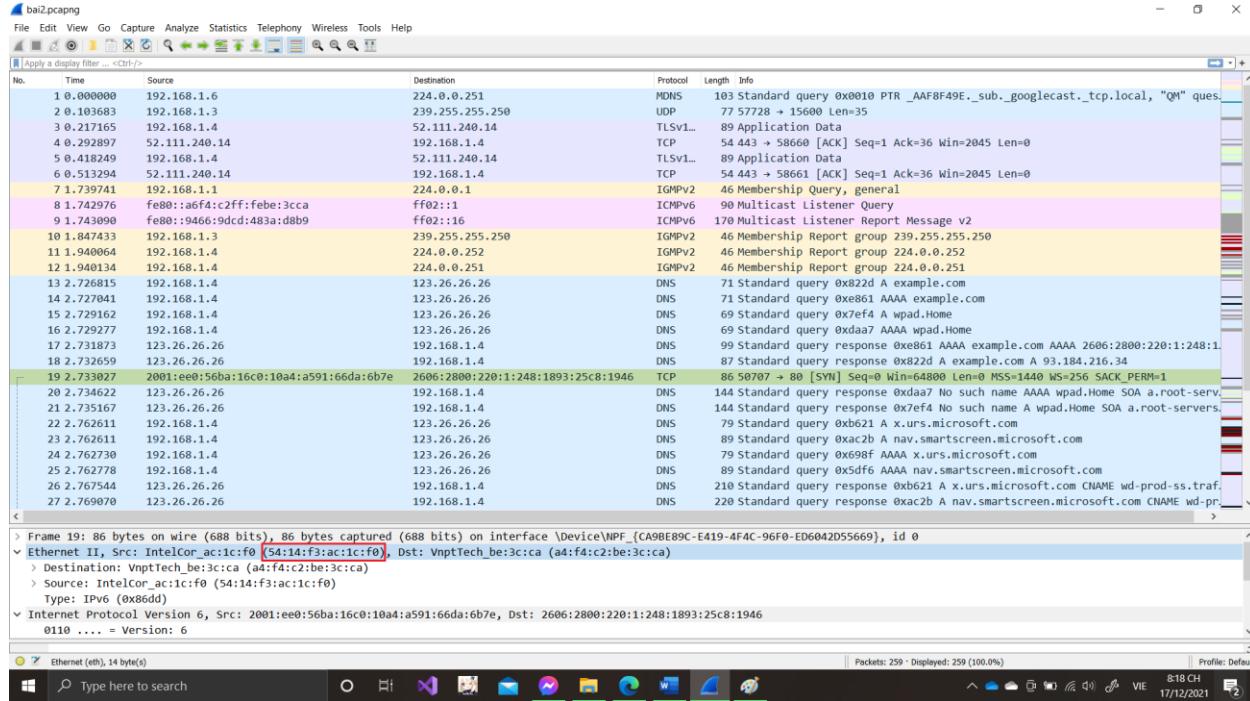


- IPv6: 2001:ee0:56ba:16c0:10a4:a591:66da:6b7e

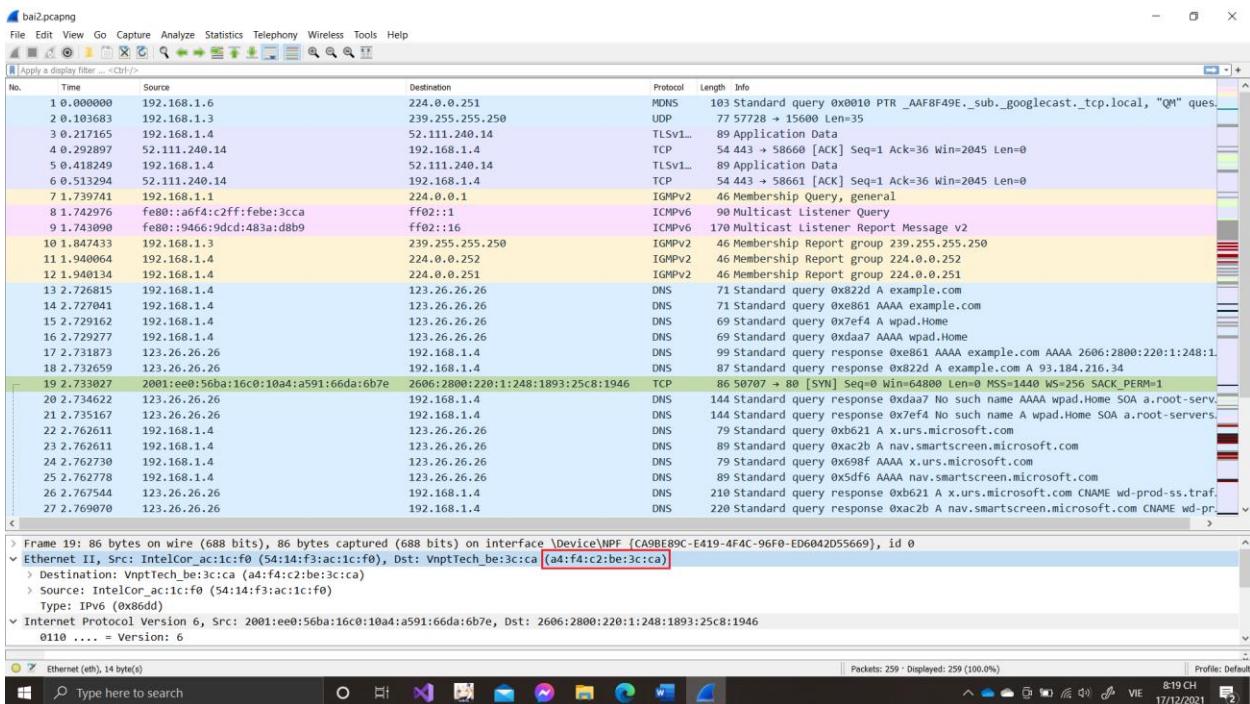


3. Không có IP của router vì: trong giao thức của các tầng đều không cần địa chỉ IP của router

4. Địa chỉ MAC của host: 54:14:f3:ac:1c:f0

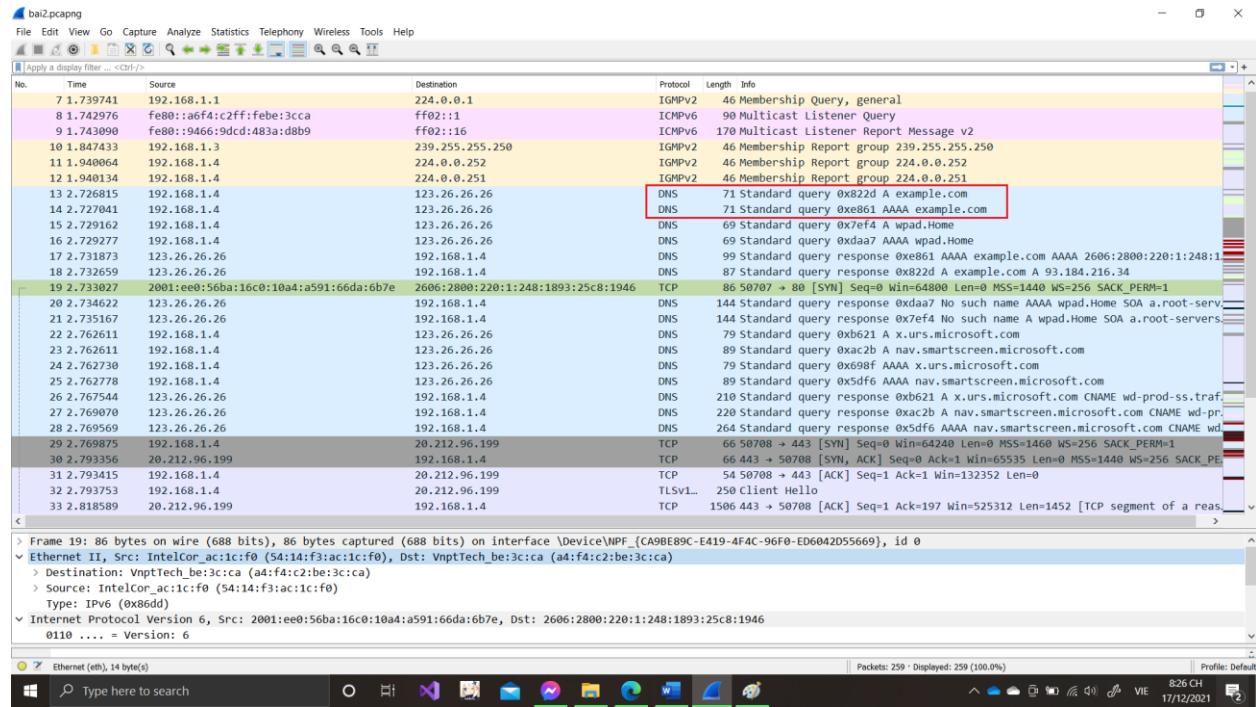


5. Địa chỉ MAC của router: a4:f4:c2:be:3c:ca

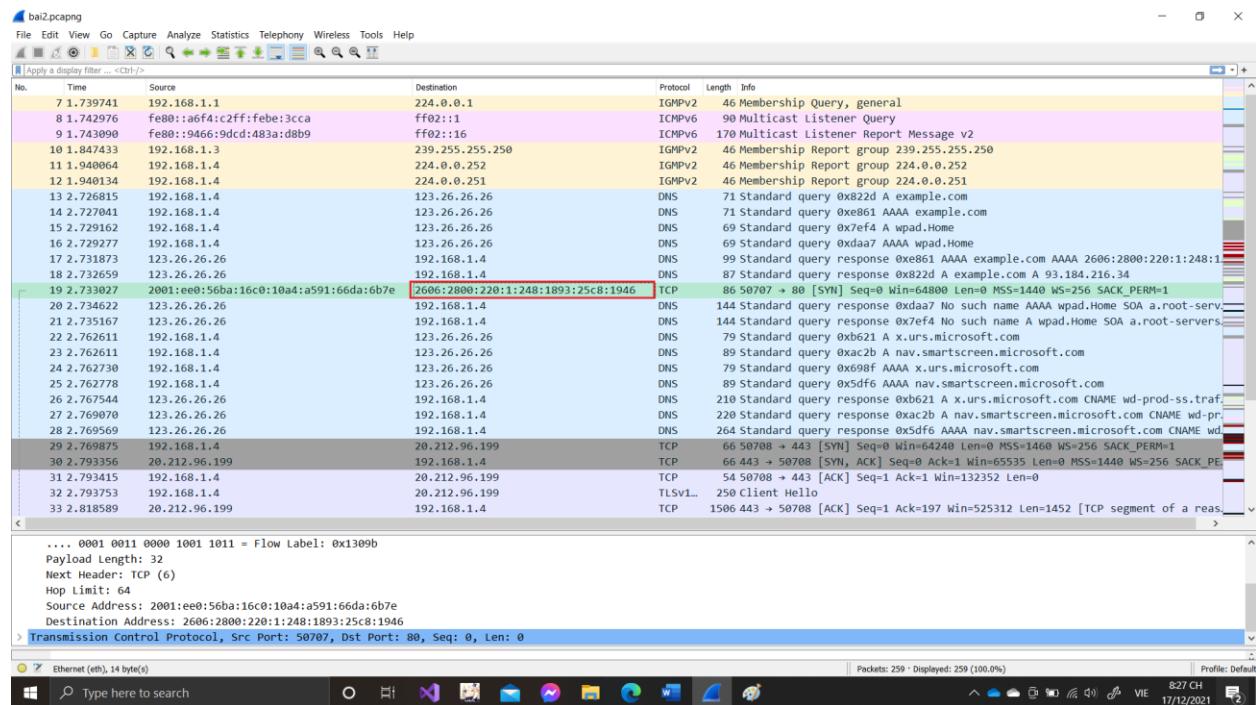


Mạng máy tính

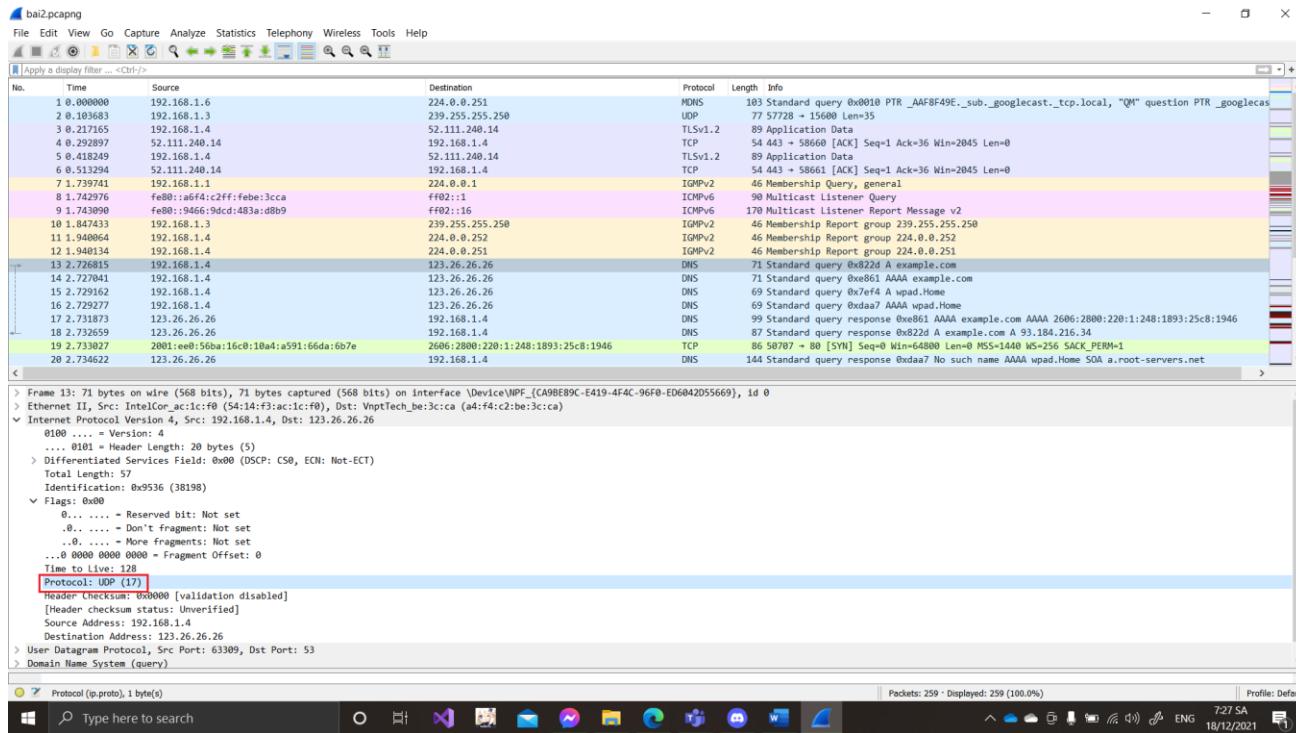
6. Protocol được sử dụng để phân giải tên miền của trang web: DNS



7. IP của HTTP server: 2606:2800:220:1:248:1893:25c8:1946

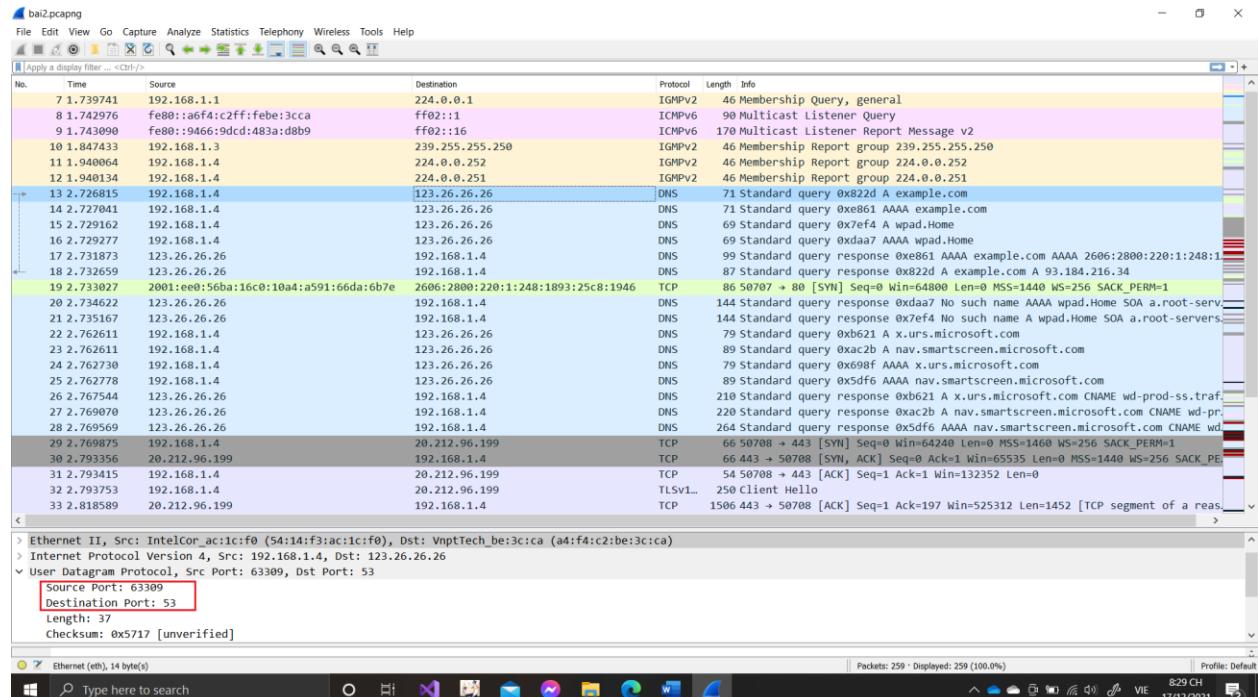


8. Protocol của tầng Transport được sử dụng bởi DNS: UDP

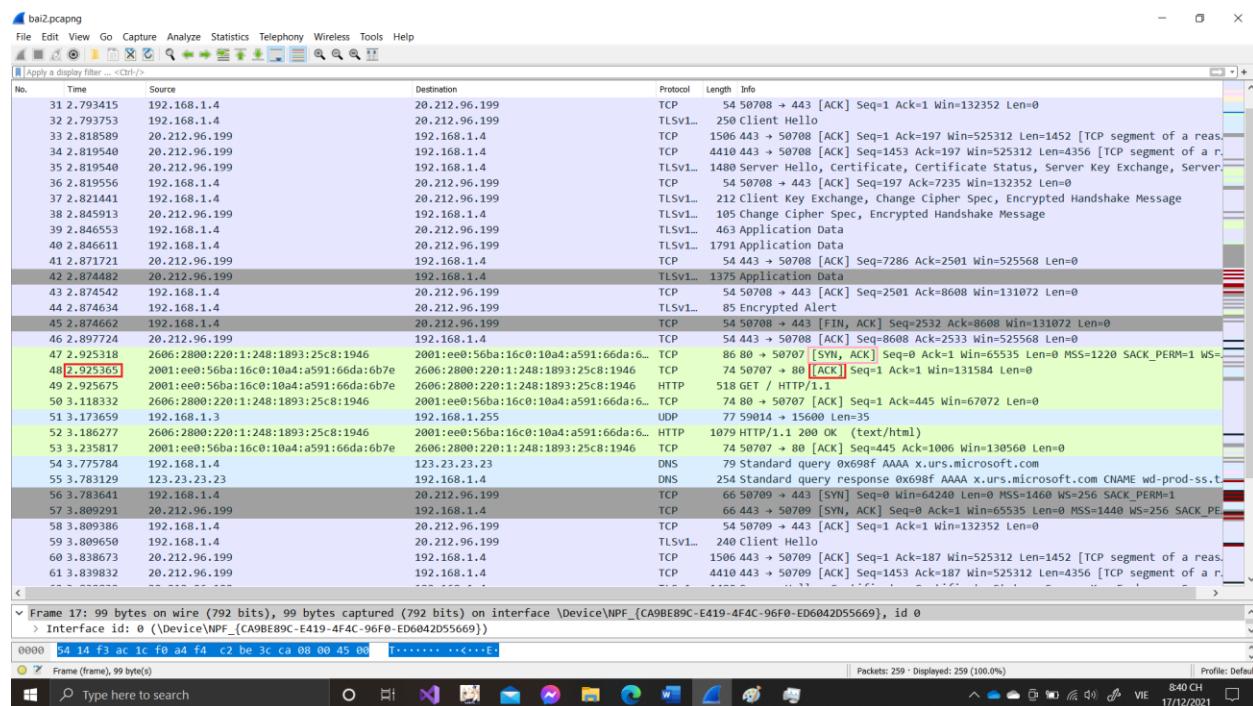
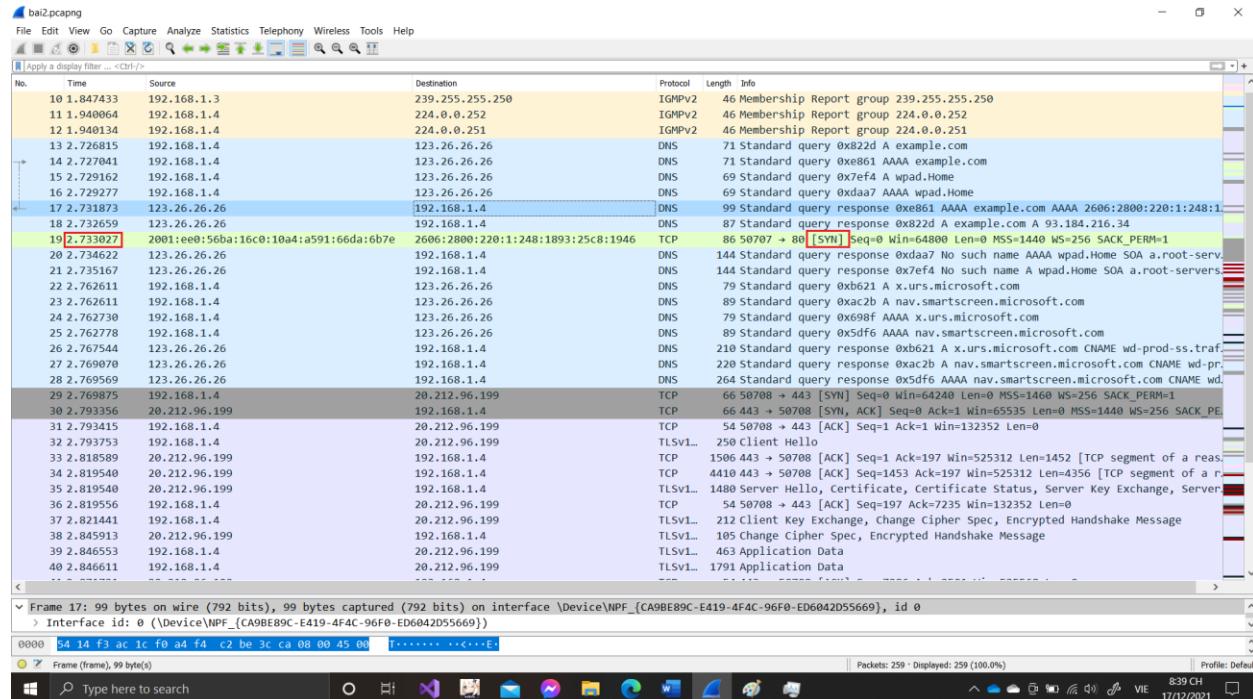


9. Port sử dụng khi truy vấn DNS server:

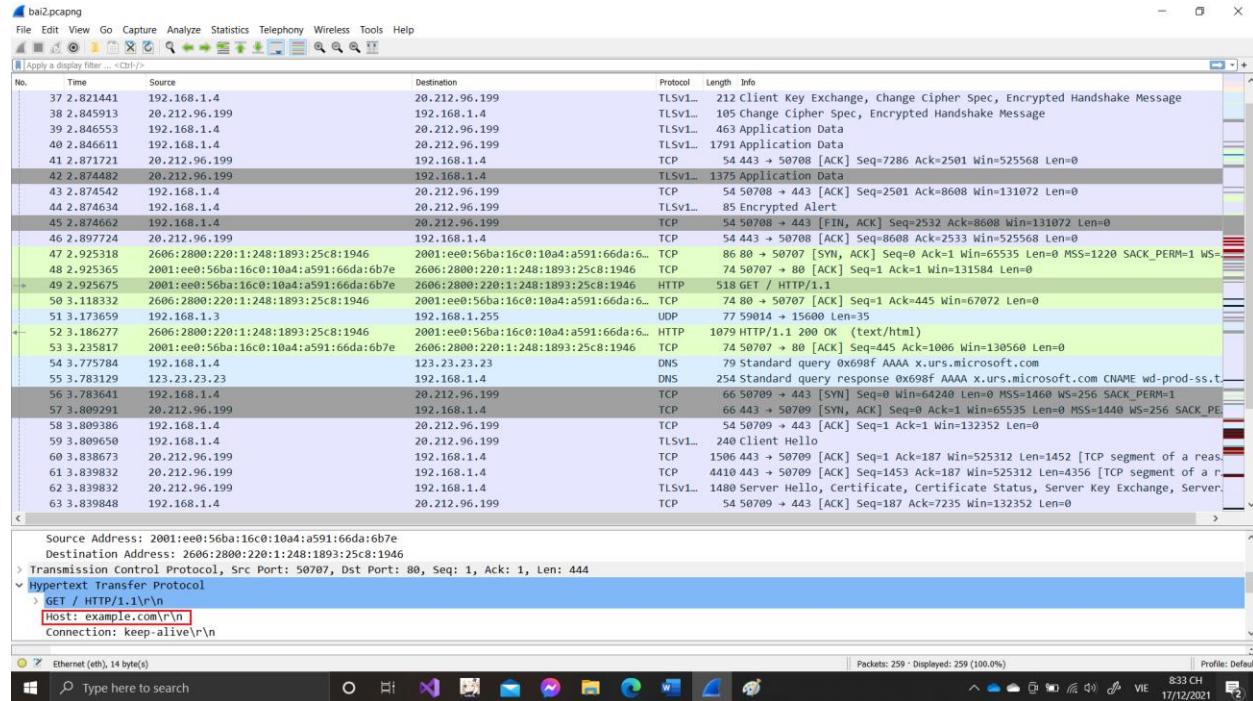
- Port của host: 63309
- Port của DNS server: 53



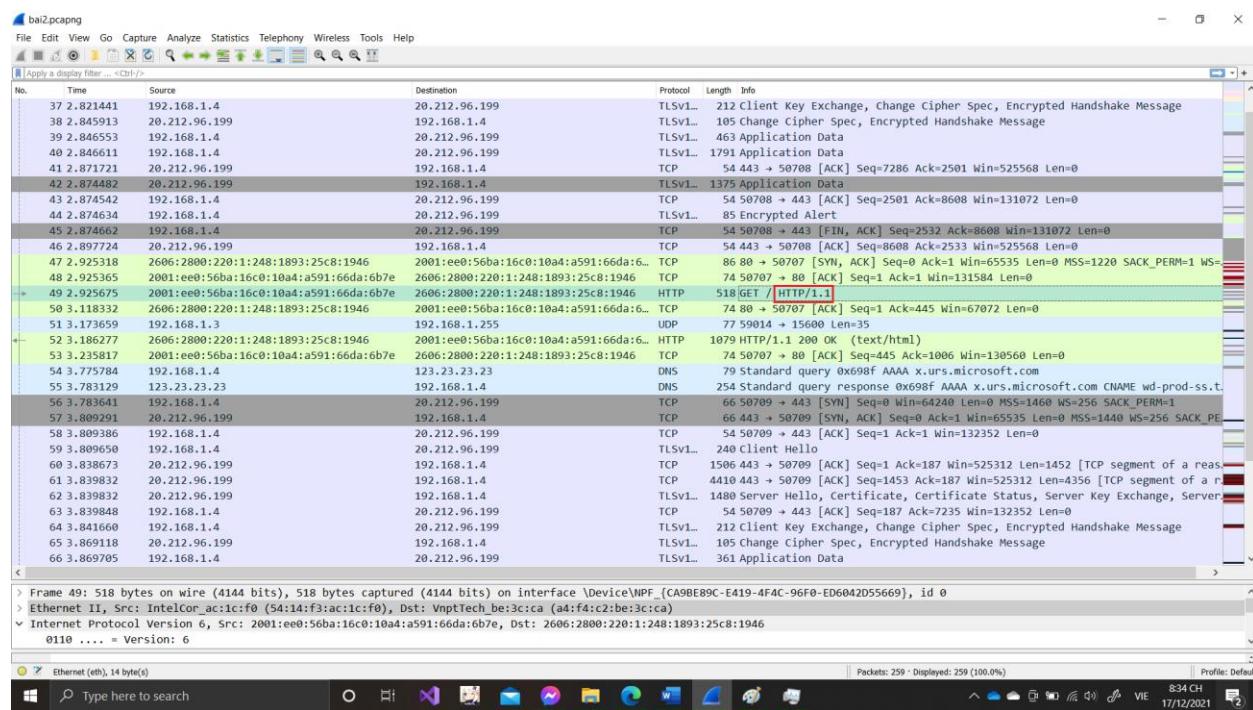
10. Quá trình bắt tay 3 bước (3-way handshake) hoàn thành trong: 0.192338 giây



11. Host machine của website: example.com\r\n

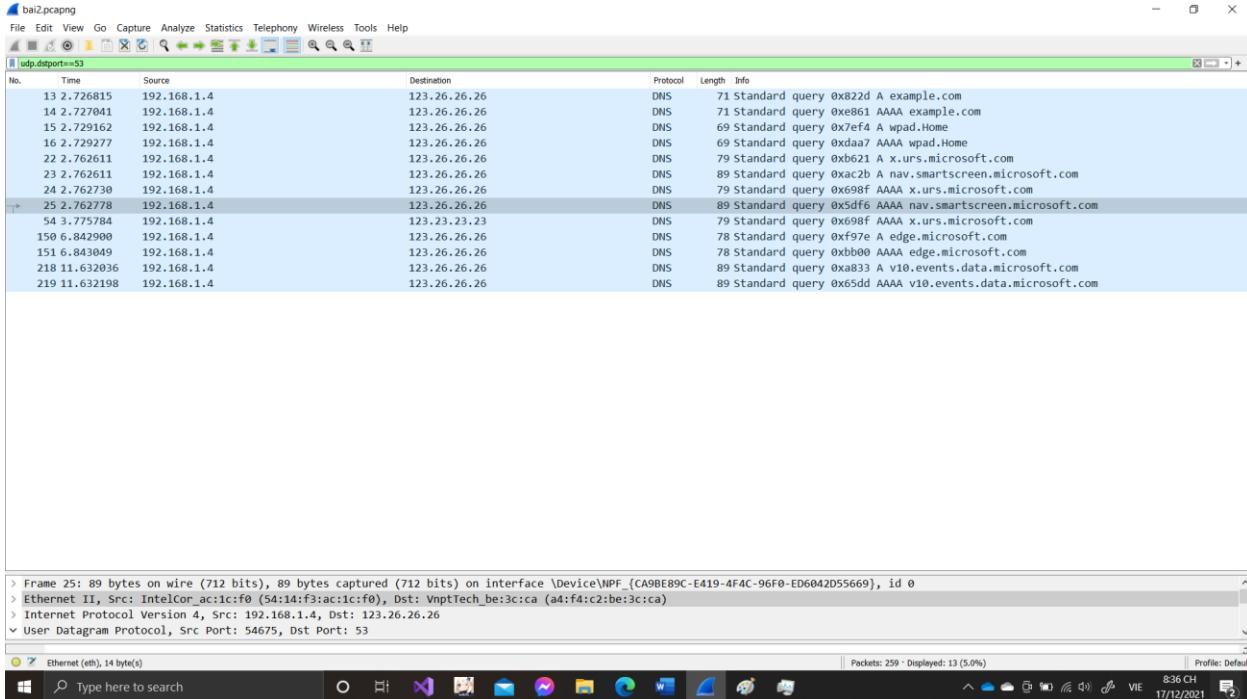


12. Version HTTP mà trình duyệt web (bowser) đang sử dụng: HTTP/1.1



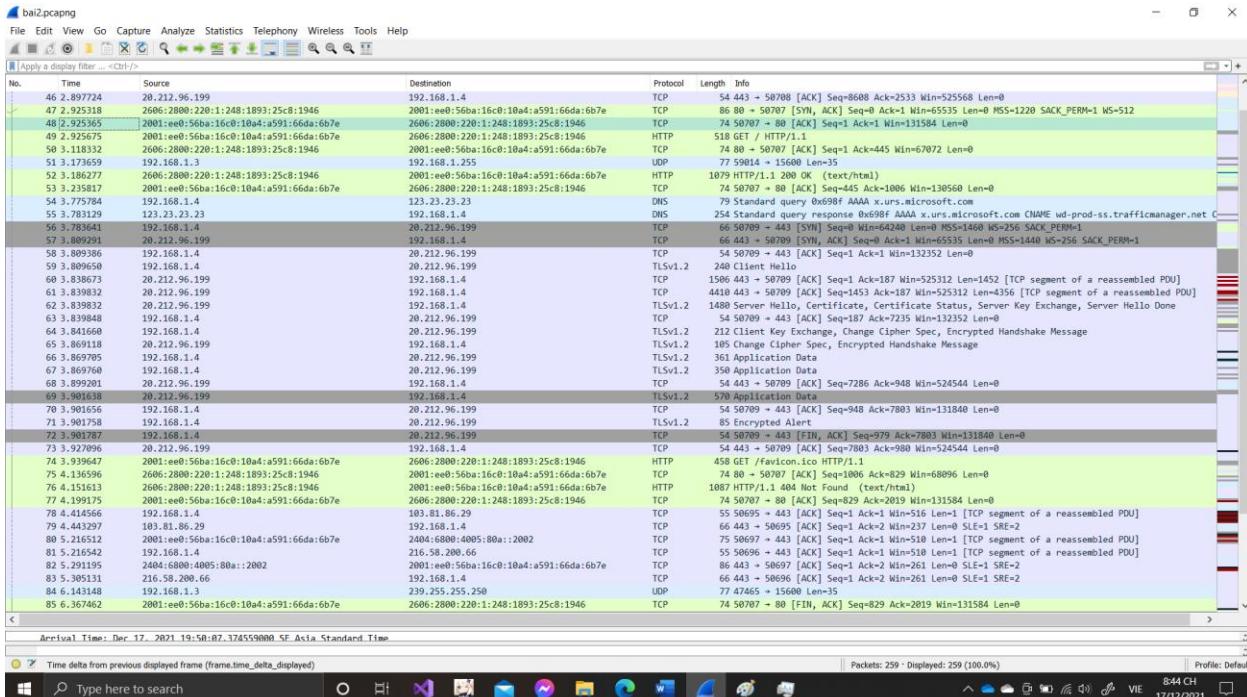
Mạng máy tính

13. **Chức năng của câu query udp.dstport==53:** lọc các gói tin UDP có port đích bằng 53

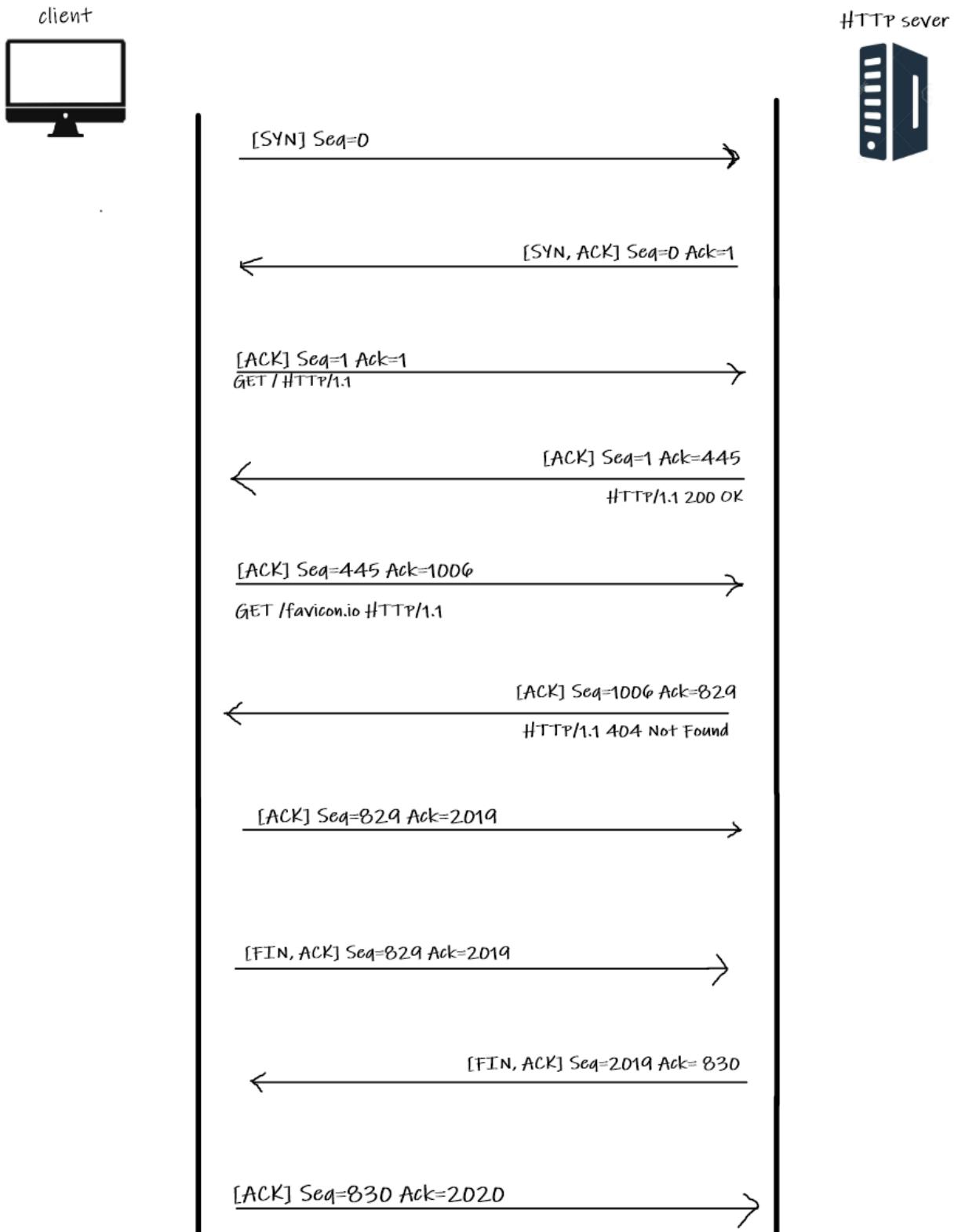


14. Quá trình gửi ACK:

- Quá trình gửi ACK trong wireshark:

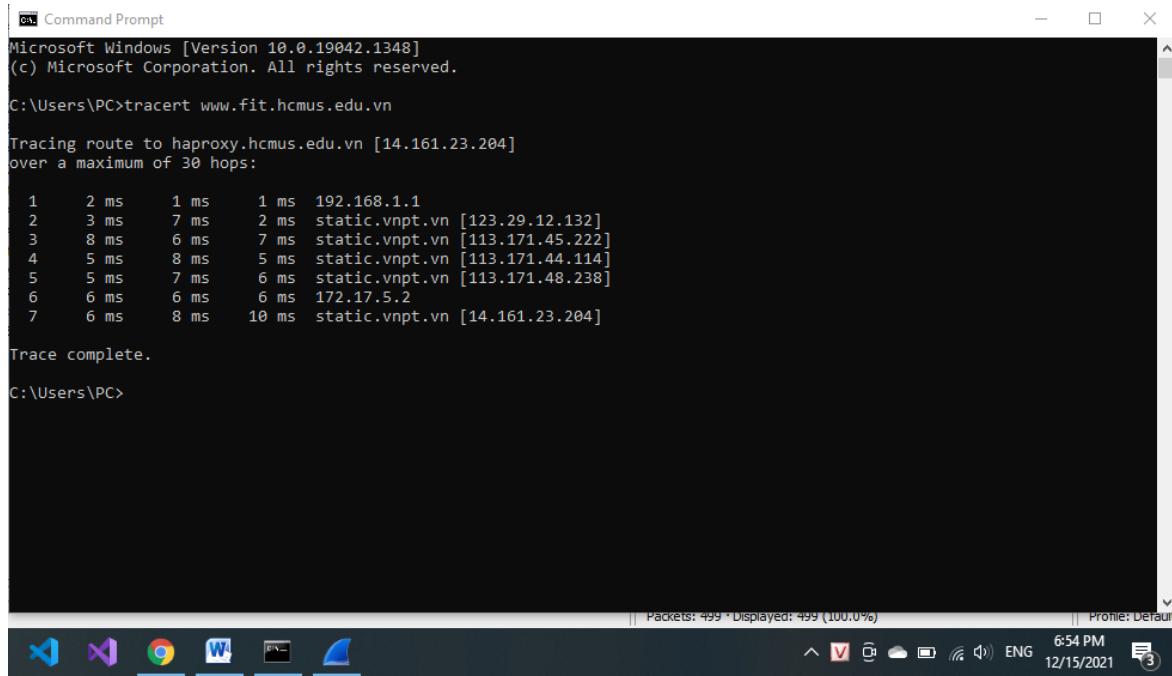


- Sơ đồ:



Bài 03: Traceroute

Câu 1: Hình chụp kết quả bắt gói tin sau khi dùng lệnh tracert trên Windows:



```
Command Prompt
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PC>tracert www.fit.hcmus.edu.vn

Tracing route to haproxy.hcmus.edu.vn [14.161.23.204]
over a maximum of 30 hops:

  1   2 ms    1 ms    1 ms  192.168.1.1
  2   3 ms    7 ms    2 ms  static.vnpt.vn [123.29.12.132]
  3   8 ms    6 ms    7 ms  static.vnpt.vn [113.171.45.222]
  4   5 ms    8 ms    5 ms  static.vnpt.vn [113.171.44.114]
  5   5 ms    7 ms    6 ms  static.vnpt.vn [113.171.48.238]
  6   6 ms    6 ms    6 ms  172.17.5.2
  7   6 ms    8 ms   10 ms  static.vnpt.vn [14.161.23.204]

Trace complete.

C:\Users\PC>
```

No.	Time	Source	Destination	Protocol	Length	Info
90	9.741662	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=20/5120, ttl=1 (no response found!)
91	9.743514	192.168.1.1	192.168.1.7	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
92	9.744324	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=21/5376, ttl=1 (no response found!)
93	9.74589	192.168.1.1	192.168.1.7	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
94	9.746313	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=22/5632, ttl=1 (no response found!)
95	9.747585	192.168.1.1	192.168.1.7	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
101	9.762692	192.168.1.1	192.168.1.7	ICMP	128	Destination unreachable (Port unreachable)
129	11.278031	192.168.1.1	192.168.1.7	ICMP	128	Destination unreachable (Port unreachable)
159	12.787997	192.168.1.1	192.168.1.7	ICMP	128	Destination unreachable (Port unreachable)
256	15.308823	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=23/5888, ttl=2 (no response found!)
257	15.311219	192.29.12.132	192.168.1.7	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
258	15.312213	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=24/6144, ttl=2 (no response found!)
259	15.319234	123.29.12.132	192.168.1.7	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
260	15.328347	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=25/6400, ttl=2 (no response found!)
261	15.32273	123.29.12.132	192.168.1.7	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
274	16.337981	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=26/6656, ttl=3 (no response found!)
275	16.345997	113.171.45.222	192.168.1.7	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
276	16.347087	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=3 (no response found!)
277	16.353486	113.171.45.222	192.168.1.7	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
278	16.354696	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=28/7168, ttl=3 (no response found!)
279	16.361927	113.171.45.222	192.168.1.7	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
337	17.379414	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=4 (no response found!)
338	17.384606	113.171.44.114	192.168.1.7	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
339	17.386156	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=4 (no response found!)
340	17.394673	113.171.44.114	192.168.1.7	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
341	17.396454	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=4 (no response found!)
342	17.401723	113.171.44.114	192.168.1.7	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
349	18.421724	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=5 (no response found!)
350	18.426952	113.171.48.238	192.168.1.7	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
351	18.428767	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=33/8448, ttl=5 (no response found!)

Câu 2: Công dụng của lệnh tracert: dùng để xác định đường đi từ nguồn tới đích của một gói Giao thức mạng Internet (IP - Internet Protocol).

Câu 3: Địa chỉ IP của máy gửi request: 192.168.1.7

No.	Time	Source	Destination	Protocol	Length	Info
90	9.741662	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=20/5120, ttl=1 (no response found!)
91	9.743514	192.168.1.1	192.168.1.7	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
92	9.744324	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=21/5376, ttl=1 (no response found!)
93	9.745589	192.168.1.1	192.168.1.7	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
94	9.746313	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=22/5632, ttl=1 (no response found!)
95	9.747583	192.168.1.1	192.168.1.7	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
101	9.762032	192.168.1.1	192.168.1.7	ICMP	120	Destination unreachable (Port unreachable)
129	11.278631	192.168.1.1	192.168.1.7	ICMP	120	Destination unreachable (Port unreachable)
159	12.787997	192.168.1.1	192.168.1.7	ICMP	120	Destination unreachable (Port unreachable)
256	15.308233	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=23/5888, ttl=2 (no response found!)

Câu 4: Cách máy tính xác định địa chỉ IP của FIT: sau khi máy tính dùng lệnh tracert thì tracert sẽ tìm đường tới đích bằng cách gửi các thông báo Echo Request (yêu cầu báo hiệu lại) Internet Control Message Protocol (ICMP) tới từng đích. Sau mỗi lần gặp một đích, giá trị Time to Live (TTL), tức thời gian cần để gửi đi sẽ được tăng lên cho tới khi gặp đúng đích cần đến.

Câu 5:

- a. Protocol được sử dụng của những gói tin sau đó là: ICMP.
- b. Số gói tin request đã gửi đi đến khi nhận được gói response đầu tiên là: 19 (gồm 18 gói không được response cộng với gói request nhận response đầu tiên).

No.	Time	Source	Destination	Protocol	Length	Info
90	9.741662	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=20/5120, ttl=1 (no response found!)
92	9.744324	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=21/5376, ttl=1 (no response found!)
94	9.746313	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=22/5632, ttl=1 (no response found!)
256	15.308233	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=23/5888, ttl=2 (no response found!)
258	15.312213	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=24/6400, ttl=2 (no response found!)
260	15.320347	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=25/6400, ttl=2 (no response found!)
274	16.337981	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=26/6656, ttl=3 (no response found!)
276	16.347037	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=3 (no response found!)
278	16.354699	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=28/7168, ttl=3 (no response found!)
337	17.379414	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=4 (no response found!)
339	17.386156	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=4 (no response found!)
341	17.396454	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=4 (no response found!)
349	18.421724	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=5 (no response found!)
351	18.428707	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=33/8448, ttl=5 (no response found!)
353	18.437393	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=34/8704, ttl=5 (no response found!)
366	19.467482	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=35/8960, ttl=6 (no response found!)
368	19.475246	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=36/9216, ttl=6 (no response found!)
370	19.483884	192.168.1.7	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=6 (no response found!)

Mạng máy tính

- c. TTL của gói tin cuối cùng được gửi trước khi nhận được gói tin response đầu tiên: 7

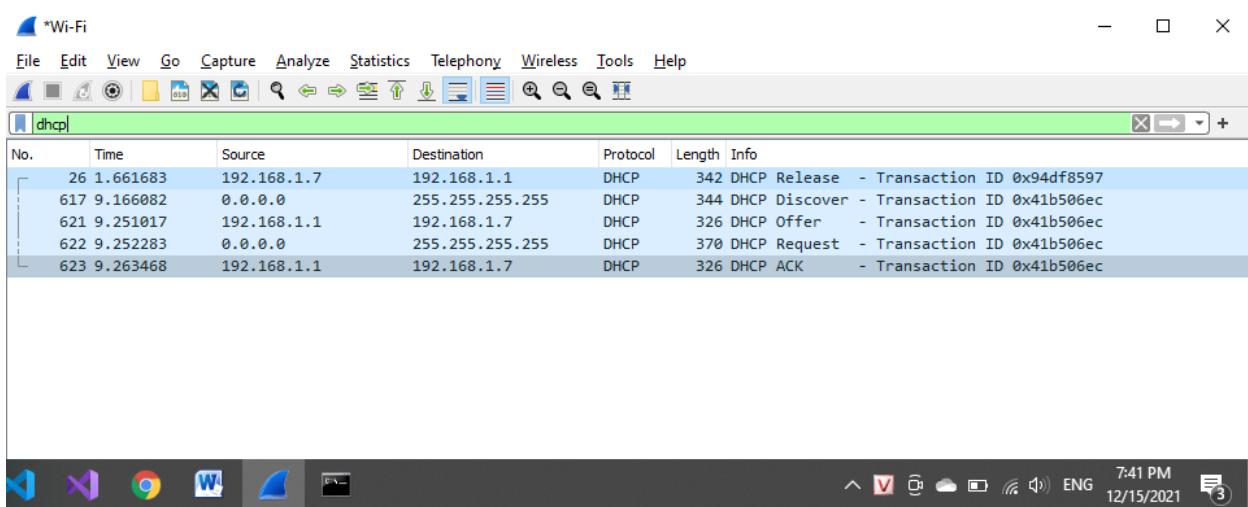
369 19.481798	172.17.5.2	192.168.1.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
370 19.483884	192.168.1.7	14.161.23.204	ICMP	106 Echo (ping) request id=0x0001, seq=37/9472, ttl=6 (no response found)
371 19.490624	172.17.5.2	192.168.1.7	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
476 25.028093	192.168.1.7	14.161.23.204	ICMP	106 Echo (ping) request id=0x0001, seq=38/9728, ttl=7 (reply in 477)
477 25.034320	14.161.23.204	192.168.1.7	ICMP	106 Echo (ping) reply id=0x0001, seq=38/9728, ttl=58 (request in 476)
478 25.035894	192.168.1.7	14.161.23.204	ICMP	106 Echo (ping) request id=0x0001, seq=39/9984, ttl=7 (reply in 479)
479 25.043721	14.161.23.204	192.168.1.7	ICMP	106 Echo (ping) reply id=0x0001, seq=39/9984, ttl=58 (request in 478)
480 25.045319	192.168.1.7	14.161.23.204	ICMP	106 Echo (ping) request id=0x0001, seq=40/10240, ttl=7 (reply in 481)
481 25.055531	14.161.23.204	192.168.1.7	ICMP	106 Echo (ping) reply id=0x0001, seq=40/10240, ttl=58 (request in 480)

- d. Không thấy thông tin port, vì: lệnh tracert sử dụng giao thức ICMP ở tầng Network trong khi địa chỉ port có ở tầng Transport.

- e. Gói tin response đầu tiên trả lời cho gói tin request thứ: 19

Bài 04: DHCP

Câu 1: Hình chụp kết quả sau khi bắt được gói tin DHCP trong quá trình release và renew:



Câu 2: DHCP sử dụng giao thức UDP tại tầng Transport vì:

- UDP nhanh do không phải thiết lập kết nối.
- Hai trong số DHCP messages sử dụng kiểu truyền broadcast (DISCOVER và REQUEST) mà TCP không hỗ trợ kiểu truyền này.
- Các yêu cầu của DHCP khá nhỏ, phù hợp với giao thức đơn giản như UDP.

- Tuy UDP truyền kiểu không tin cậy nhưng lỗi có thể được phát hiện và khắc phục ở tầng Application.

Câu 3:

- Mục đích của DHCP Release Message: DHCP Client DHCP Release Message lên DHCP Server để hủy thông tin IP mà DHCP Server cấp cho nó. Sau khi DHCP nhận được DHCP Release Message thì DHCP Server có thể cấp IP bị hủy đó cho Client khác.
- DHCP client không đảm bảo lúc nào cũng nhận được ACK message từ Server, vì ACK message là tín hiệu được gửi từ bên nhận tới bên gửi để biết được khối dữ liệu có gửi đến thành công không. DHCP client sẽ không nhận được ACK message từ Server khi khôi dữ liệu gửi từ DHCP client tới DHCP Server xảy ra lỗi.
- Nếu DHCP release message bị mất thì client gửi DHCP release message vẫn hủy được địa chỉ IP nhưng Server sẽ không biết IP đó đã được hủy và sẽ không gán địa chỉ IP này cho client khác.

Câu 4:

- a. Vì khách thứ 92 không thể truy cập được Internet vì:

DHCP server chỉ cấp được tối đa 91 IP với range IP từ 192.168.1.10 đến 192.168.1.100 trong vòng 8 tiếng.

Vì khách thứ 92 vào quán lúc 11:00 AM thì đã đạt giới hạn số IP và chỉ mới trôi qua 4 tiếng, chưa đủ thời gian để cấp lại IP

- b. Những vị khách tiếp theo (93, 94,...) không thể truy cập được và có thể truy cập được vào lúc 15:00 giờ
- c. Chủ quán nên reset modem để vị khách thứ 92 có thể truy cập được internet

=> Hướng giải quyết để khắc phục tình trạng này về sau: giảm thời gian cấp IP hoặc tăng range IP

Tài liệu tham khảo

- Tài liệu tham khảo trên moodle
- ICMP Header Size: <https://youtu.be/lJnU8w4ALY0>
- Ethernet Header Size: <https://osqa-ask.wireshark.org/questions/1846/wireshark-capture-of-ethernet-frame-size-shows-as-43-bytes/>
- ARP: <https://youtu.be/AoYa0JvSFIg>
- Lệnh tracert: <https://wiki.tino.org/lenh-tracert-trong-cmd-dung-de-lam-gi/>
- DHCP: https://is5com.com/documentation/DHCP-Configuration/CM-DHCP-iBiome-1.8.07-EN/iMX_Common/Configuration_Guides/DITA_Topics/DHCP/3_Intro.html

