ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN

----------o0o----------

BÁO CÁO ĐỒ ÁN

"PHÂN TÍCH GÓI TIN"

Bộ môn: MẠNG MÁY TÍNH

Giáo viên hướng dẫn: HUỲNH THỤY BẢO TRÂN

CHUNG THÙY LINH

Mục Lục

Phần I: Giới thiệu

- **Môn học**: Mạng máy tính

- **Phần mềm sử dụng**: Wireshark 64bit

- **Các thành viên trong nhóm:**
  - Trần Xuân Quang. MSSV: 20127608
  - Đặng Ngọc Tiến. MSSV: 20127641

- **Về phần mềm wireshark**: Wireshark là một chương trình phần mềm phân tích giao thức mạng nguồn mở do Gerald Combs khởi xướng từ năm 1998, nó là công cụ phân tích giao thức mạng phổ biến nhất thế giới. Wireshark cho phép ta xem lưu lượng truy cập và phân tích những gì đang diễn ra trong mạng, nó nắm bắt lưu lượng mạng trên mạng cục bộ và lưu trữ dữ liệu đó để phân tích ngoại tuyến. Wireshark nắm bắt lưu lượng mạng từ Ethernet, Bluetooth, Wireless (IEEE.802.11), v.v.

Phần II: Báo cáo tiến độ.

***Mức độ hoàn thành: 100%**

***Những mục chưa làm được: 0**

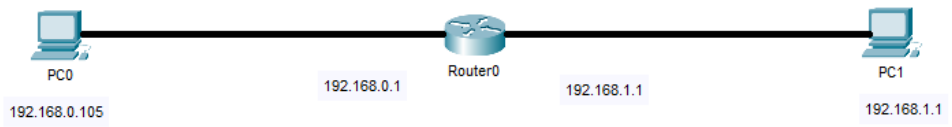
Phần III: Bảng phân công công việc

Họ Và Tên	MSSV	Công việc
Đặng Ngọc Tiến	20127641	Phụ trách câu 1, 2; hỗ trợ làm thêm câu 3, 4
Trần Xuân Quang	20127608	Phụ trách câu 3, 4; hỗ trợ làm thêm câu 1, 2

Phần IV: Nội dung đồ án

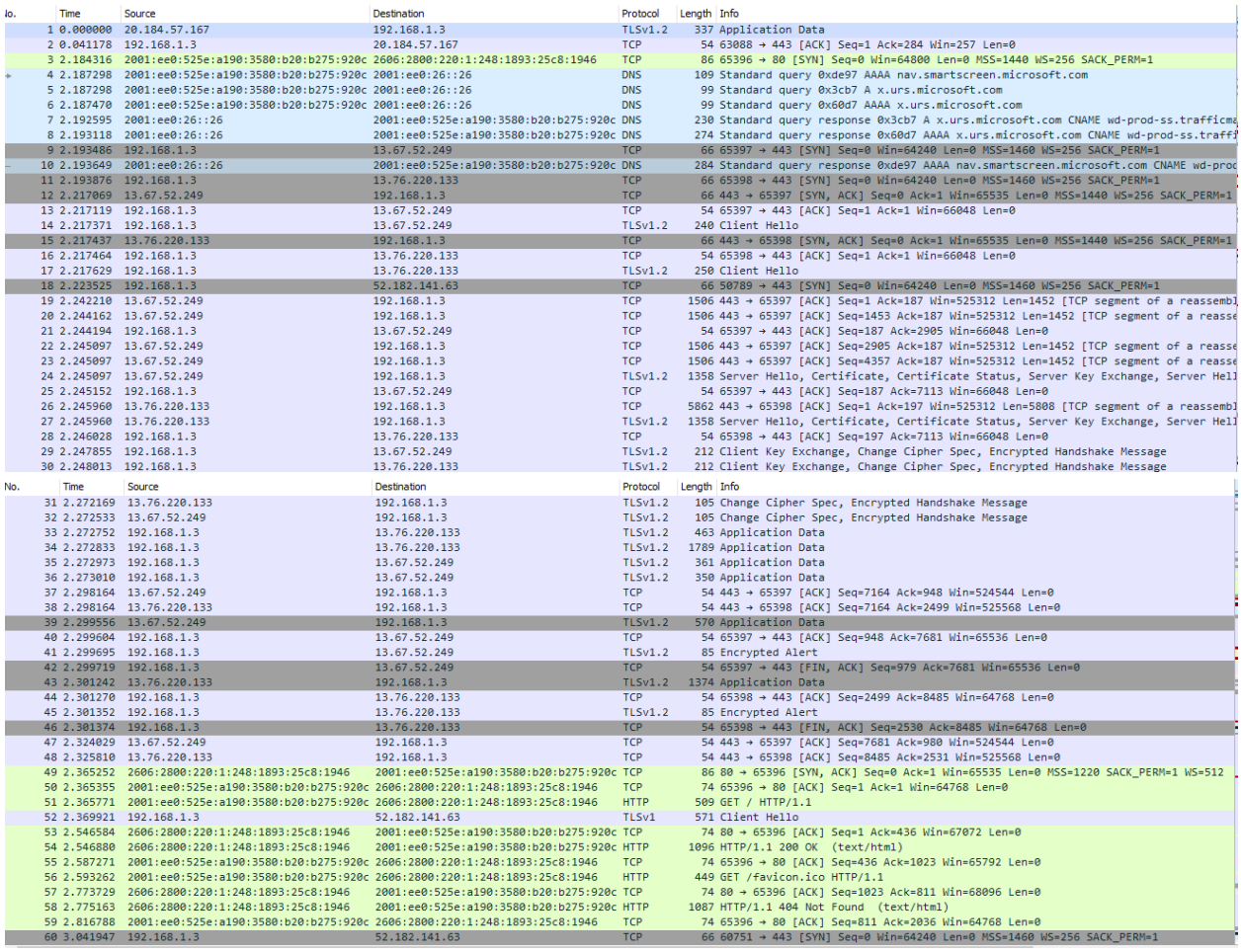
Câu 1: PING

1. **Địa chỉ IP của host ping:** 192.168.0.105
   Địa chỉ IP của host được ping: 192.168.1.1
2. **Port được sử dụng:** ICMP không có giá trị port bởi vì ICMP nằm cùng tầng với IP (phía dưới transport player) trong bộ giao thức TCP/IP.
3. **Thành phần trong diagram ICMP Request:**
   ICMP Data: 48 bytes
   ICMP Header: 16 bytes
   IP Header: 20 bytes
   Ethernet Header: 14 bytes
4. **Lý do có 2 gói ARP:** Vì một thiết bị IP trong mạng phải gửi một gói tin broadcast đến toàn mạng yêu cầu thiết bị khác gửi trả lại địa chỉ phần cứng nên phải có 2 gói, 1 gói request 1 gói response. ARP có tác dụng chuyển IP thành địa chỉ MAC
5. **Sơ đồ mạng:**



Câu 2: HTTP

1. **Hình:**



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	20.184.57.167	192.168.1.3	TLSv1.2	337	Application Data
2	0.041178	192.168.1.3	20.184.57.167	TCP	54	63088 → 443 [ACK] Seq=1 Ack=284 Win=257 Len=0
3	2.184316	2001:ee0:525e:a190:3580:b20:b275:920c	2606:2800:220:1:248:1893:25c8:1946	TCP	86	65396 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
4	2.187298	2001:ee0:525e:a190:3580:b20:b275:920c	2001:ee0:26::26	DNS	109	Standard query 0xde97 AAAA nav.smartscreen.microsoft.com
5	2.187298	2001:ee0:525e:a190:3580:b20:b275:920c	2001:ee0:26::26	DNS	99	Standard query 0x3cb7 A x.urs.microsoft.com
6	2.187470	2001:ee0:525e:a190:3580:b20:b275:920c	2001:ee0:26::26	DNS	99	Standard query 0x60d7 AAAA x.urs.microsoft.com
7	2.192595	2001:ee0:26::26	2001:ee0:525e:a190:3580:b20:b275:920c	DNS	230	Standard query response 0x3cb7 A x.urs.microsoft.com CNAME wd-prod-ss.trafficma
8	2.193118	2001:ee0:26::26	2001:ee0:525e:a190:3580:b20:b275:920c	DNS	274	Standard query response 0x60d7 AAAA x.urs.microsoft.com CNAME wd-prod-ss.traffi
9	2.193486	192.168.1.3	13.67.52.249	TCP	66	65397 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	2.193649	2001:ee0:26::26	2001:ee0:525e:a190:3580:b20:b275:920c	DNS	284	Standard query response 0xde97 AAAA nav.smartscreen.microsoft.com CNAME wd-proc
11	2.193876	192.168.1.3	13.76.220.133	TCP	66	65398 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
12	2.217069	13.67.52.249	192.168.1.3	TCP	66	443 → 65397 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
13	2.217119	192.168.1.3	13.67.52.249	TCP	54	65397 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
14	2.217371	192.168.1.3	13.67.52.249	TLSv1.2	240	Client Hello
15	2.217437	13.76.220.133	192.168.1.3	TCP	66	443 → 65398 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
16	2.217464	192.168.1.3	13.76.220.133	TCP	54	65398 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
17	2.217629	192.168.1.3	13.76.220.133	TLSv1.2	250	Client Hello
18	2.223525	192.168.1.3	52.182.141.63	TCP	66	50789 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	2.242210	13.67.52.249	192.168.1.3	TCP	1506	443 → 65397 [ACK] Seq=1 Ack=187 Win=525312 Len=1452 [TCP segment of a reassembl
20	2.244162	13.67.52.249	192.168.1.3	TCP	1506	443 → 65397 [ACK] Seq=1453 Ack=187 Win=525312 Len=1452 [TCP segment of a reasse
21	2.244194	192.168.1.3	13.67.52.249	TCP	54	65397 → 443 [ACK] Seq=187 Ack=2905 Win=66048 Len=0
22	2.245097	13.67.52.249	192.168.1.3	TCP	1506	443 → 65397 [ACK] Seq=2905 Ack=187 Win=525312 Len=1452 [TCP segment of a reasse
23	2.245097	13.67.52.249	192.168.1.3	TCP	1506	443 → 65397 [ACK] Seq=4357 Ack=187 Win=525312 Len=1452 [TCP segment of a reasse
24	2.245097	13.67.52.249	192.168.1.3	TLSv1.2	1358	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hell
25	2.245152	192.168.1.3	13.67.52.249	TCP	54	65397 → 443 [ACK] Seq=187 Ack=7113 Win=66048 Len=0
26	2.245960	13.76.220.133	192.168.1.3	TCP	5862	443 → 65398 [ACK] Seq=1 Ack=197 Win=525312 Len=5808 [TCP segment of a reassembl
27	2.245960	13.76.220.133	192.168.1.3	TLSv1.2	1358	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hell
28	2.246028	192.168.1.3	13.76.220.133	TCP	54	65398 → 443 [ACK] Seq=197 Ack=7113 Win=66048 Len=0
29	2.247855	192.168.1.3	13.67.52.249	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
30	2.248013	192.168.1.3	13.76.220.133	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
31	2.272169	13.76.220.133	192.168.1.3	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
32	2.272533	13.67.52.249	192.168.1.3	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
33	2.272752	192.168.1.3	13.76.220.133	TLSv1.2	463	Application Data
34	2.272833	192.168.1.3	13.76.220.133	TLSv1.2	1789	Application Data
35	2.272973	192.168.1.3	13.67.52.249	TLSv1.2	361	Application Data
36	2.273010	192.168.1.3	13.67.52.249	TLSv1.2	350	Application Data
37	2.298164	13.67.52.249	192.168.1.3	TCP	54	443 → 65397 [ACK] Seq=7164 Ack=948 Win=524544 Len=0
38	2.298164	13.76.220.133	192.168.1.3	TCP	54	443 → 65398 [ACK] Seq=7164 Ack=2499 Win=525568 Len=0
39	2.299556	13.67.52.249	192.168.1.3	TLSv1.2	570	Application Data
40	2.299604	192.168.1.3	13.67.52.249	TCP	54	65397 → 443 [ACK] Seq=948 Ack=7681 Win=65536 Len=0
41	2.299695	192.168.1.3	13.67.52.249	TLSv1.2	85	Encrypted Alert
42	2.299719	192.168.1.3	13.67.52.249	TCP	54	65397 → 443 [FIN, ACK] Seq=979 Ack=7681 Win=65536 Len=0
43	2.301242	13.76.220.133	192.168.1.3	TLSv1.2	1374	Application Data
44	2.301270	192.168.1.3	13.76.220.133	TCP	54	65398 → 443 [ACK] Seq=2499 Ack=8485 Win=64768 Len=0
45	2.301352	192.168.1.3	13.76.220.133	TLSv1.2	85	Encrypted Alert
46	2.301374	192.168.1.3	13.76.220.133	TCP	54	65398 → 443 [FIN, ACK] Seq=2530 Ack=8485 Win=64768 Len=0
47	2.324029	13.67.52.249	192.168.1.3	TCP	54	443 → 65397 [ACK] Seq=7681 Ack=980 Win=524544 Len=0
48	2.325810	13.76.220.133	192.168.1.3	TCP	54	443 → 65398 [ACK] Seq=8485 Ack=2531 Win=525568 Len=0
49	2.365252	2606:2800:220:1:248:1893:25c8:1946	2001:ee0:525e:a190:3580:b20:b275:920c	TCP	86	80 → 65396 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1220 SACK_PERM=1 WS=512
50	2.365355	2001:ee0:525e:a190:3580:b20:b275:920c	2606:2800:220:1:248:1893:25c8:1946	TCP	74	65396 → 80 [ACK] Seq=1 Ack=1 Win=64768 Len=0
51	2.365771	2001:ee0:525e:a190:3580:b20:b275:920c	2606:2800:220:1:248:1893:25c8:1946	HTTP	509	GET / HTTP/1.1
52	2.369921	192.168.1.3	52.182.141.63	TLSv1	571	Client Hello
53	2.546584	2606:2800:220:1:248:1893:25c8:1946	2001:ee0:525e:a190:3580:b20:b275:920c	TCP	74	80 → 65396 [ACK] Seq=1 Ack=436 Win=67072 Len=0
54	2.546880	2606:2800:220:1:248:1893:25c8:1946	2001:ee0:525e:a190:3580:b20:b275:920c	HTTP	1096	HTTP/1.1 200 OK (text/html)
55	2.587271	2001:ee0:525e:a190:3580:b20:b275:920c	2606:2800:220:1:248:1893:25c8:1946	TCP	74	65396 → 80 [ACK] Seq=436 Ack=1023 Win=65792 Len=0
56	2.593262	2001:ee0:525e:a190:3580:b20:b275:920c	2606:2800:220:1:248:1893:25c8:1946	HTTP	449	GET /favicon.ico HTTP/1.1
57	2.773729	2606:2800:220:1:248:1893:25c8:1946	2001:ee0:525e:a190:3580:b20:b275:920c	TCP	74	80 → 65396 [ACK] Seq=1023 Ack=811 Win=68096 Len=0
58	2.775163	2606:2800:220:1:248:1893:25c8:1946	2001:ee0:525e:a190:3580:b20:b275:920c	HTTP	1087	HTTP/1.1 404 Not Found (text/html)
59	2.816788	2001:ee0:525e:a190:3580:b20:b275:920c	2606:2800:220:1:248:1893:25c8:1946	TCP	74	65396 → 80 [ACK] Seq=811 Ack=2036 Win=64768 Len=0
60	3.041947	192.168.1.3	52.182.141.63	TCP	66	60751 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

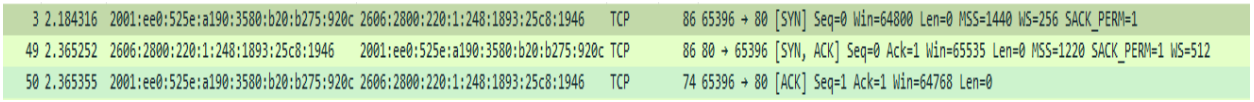
2. **IP của host:** 192.168.1.3
3. **Cho biết IP của router (default gateway) (nếu không thấy được thì trả lời không có và giải thích tại sao)?**

   Vì Local dns server nằm sẵn trong modem wifi nên dns query không cần thông qua router.Do đó ta sẽ không thấy được ip default gateway.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Home
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : 24-41-8C-19-52-21
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:ee0:525e:a190:58bb:3033:161e:c56b(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:ee0:525e:a190:38a3:7454:f76e:6a9a(Preferred)
   Link-local IPv6 Address . . . . . : fe80::58bb:3033:161e:c56b%19(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, September 1, 2021 9:02:26 PM
   Lease Expires . . . . . . . . . . : Thursday, September 2, 2021 9:02:26 PM
   Default Gateway . . . . . . . . . : fe80::d69a:a0ff:fe64:4f28%19
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 186925452
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-8C-A6-50-24-41-8C-19-52-21
   DNS Servers . . . . . . . . . . . : 2001:ee0:23::23
                                       2001:ee0:26::26
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

4. **Địa chỉ MAC của host:** 24:41:8c:19:52:21
5. **Địa chỉ MAC của router (default getway):** d4:9a:a0:64:4f:28
6. **Protocol nào được sử dụng để phân giải tên miền của trang web:** DNS
7. **Cho biết IP của HTTP server:** ipv6: 2606:2800:220:1:248:1893:25c8:1946
8. **Cho biết Protocol của tầng Transport được sử dụng bởi DNS:** UDP
9. **Cho biết port sử dụng khi truy vấn DNS Server**
   - Port của host khi truy vấn DNS Server: 65396
   - Port của DSN Server: 53
10. **Bao lâu thì quá trình bắt tay 3 bước (3-way handshake) hoàn thành:**
    Quy trình bắt tay ba bước (3-way handshake) diễn ra trong 3 bước: SYN, SYN-ACK, ACK. Vậy nên quá trình bắt tay 3 bước hoàn thành khi Source port gửi tín hiệu ACK cho Destination port.

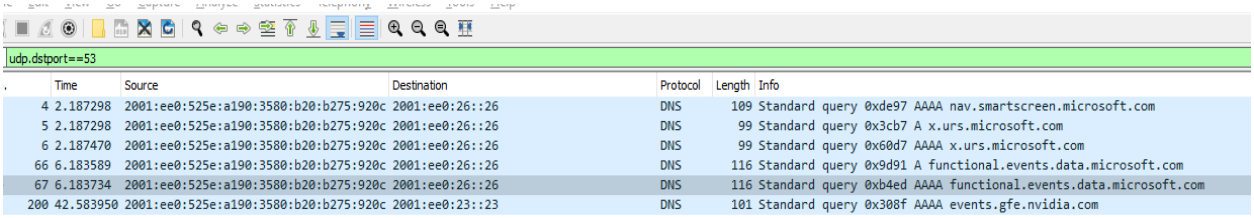


    VD:Source port: 65396 gửi tín hiệu SYN với Seq=0 cho Server. Server gửi lại tín hiệu SYN,ACK với Seq (server) =0 và Ack=seq (host) +1 = 0+1 = 1. Và quá trình bắt tay 3 bước hoàn thành khi source port : 65396 gửi tín hiệu ACK với Seq (host)=1 và Ack= seq(server)+1=0+1=1.

11. **Cho biết host machine của website đang truy cập (Application):**
    ECS (sab/5783)\r\n
12. **Version HTTP mà trình duyệt web (bowser) đang sử dụng (Application)**
    Version HTTP/1.1

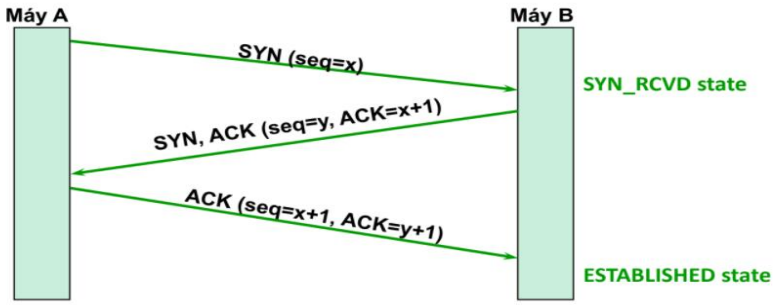
13. **Trong cái mục filter, nhập câu query sau đây:** udp.dstport==53 **và click apply. Hãy cho biết chức năng và kết quả của câu query vừa thực hiện?**

Chức năng của câu query này là sẽ lọc ra những destination có port number là 53 có giao thức là UDP. Từ đó kết quả của câu query trên sẽ là dãy DNS có giao thức UDP và destination port number là 53.



14. Trình bày quá trình gửi data (Sequence number, Acknowledgement number) từ khi kết nối đến khi kết thúc nhận data HTTP server.

- Quá trình bắt tay 3 bước:



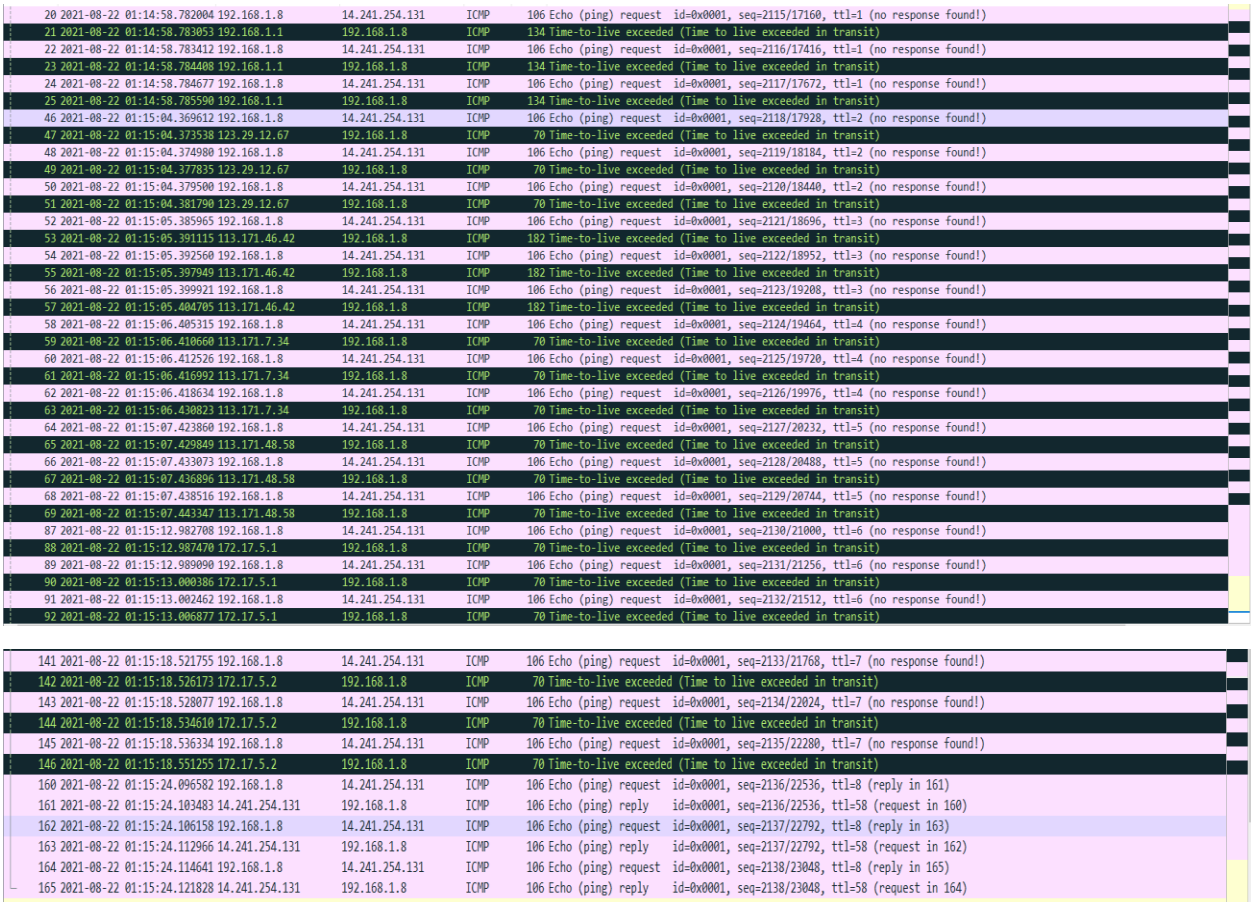
(Source port: 65396, Destination port: 80)

1. Source port gửi tín hiệu SYN tới Destination port với Sequence number (Host) =0
2. Destination port gửi tín hiệu SYN,ACK tới Source port với Sequence number (Server)=0 , acknowledgement number = Sequence number (Host) +1= 0+1=1
3. Source port gửi lại tín hiệu ACK tới Destination port với sequence number (Host)=0+1=1 và acknowledgement number = Sequence number (Server)+1=0+1=1

- Quá trình truyền dữ liệu:
  - Destination port(Server) gửi data tới cho Source port(Host) tín hiệu ACK với Sequence number (Server)=1 và acknowledgement number=Length (Request) +1 = 435 +1 =436
  - Source port (Host) phản hồi là đã nhận được data từ Destination port (Server) gửi đến bằng tín hiệu ACK với Sequence number (Host)=436 và acknowledgement number = 1022 +1 = 1023.

Câu 3: Traceroute

1. Hình ảnh cho qua trình tracert:



20	2021-08-22 01:14:58.782004	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2115/17160, ttl=1 (no response found!)
21	2021-08-22 01:14:58.783053	192.168.1.1	192.168.1.8	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
22	2021-08-22 01:14:58.783412	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2116/17416, ttl=1 (no response found!)
23	2021-08-22 01:14:58.784408	192.168.1.1	192.168.1.8	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
24	2021-08-22 01:14:58.784677	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2117/17672, ttl=1 (no response found!)
25	2021-08-22 01:14:58.785590	192.168.1.1	192.168.1.8	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
46	2021-08-22 01:15:04.369612	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2118/17928, ttl=2 (no response found!)
47	2021-08-22 01:15:04.373538	123.29.12.67	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
48	2021-08-22 01:15:04.374980	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2119/18184, ttl=2 (no response found!)
49	2021-08-22 01:15:04.377835	123.29.12.67	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
50	2021-08-22 01:15:04.379500	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2120/18440, ttl=2 (no response found!)
51	2021-08-22 01:15:04.381790	123.29.12.67	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
52	2021-08-22 01:15:05.385965	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2121/18696, ttl=3 (no response found!)
53	2021-08-22 01:15:05.391115	113.171.46.42	192.168.1.8	ICMP	182 Time-to-live exceeded (Time to live exceeded in transit)
54	2021-08-22 01:15:05.392560	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2122/18952, ttl=3 (no response found!)
55	2021-08-22 01:15:05.397949	113.171.46.42	192.168.1.8	ICMP	182 Time-to-live exceeded (Time to live exceeded in transit)
56	2021-08-22 01:15:05.399921	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2123/19208, ttl=3 (no response found!)
57	2021-08-22 01:15:05.404705	113.171.46.42	192.168.1.8	ICMP	182 Time-to-live exceeded (Time to live exceeded in transit)
58	2021-08-22 01:15:06.405315	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2124/19464, ttl=4 (no response found!)
59	2021-08-22 01:15:06.410660	113.171.7.34	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
60	2021-08-22 01:15:06.412526	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2125/19720, ttl=4 (no response found!)
61	2021-08-22 01:15:06.416992	113.171.7.34	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
62	2021-08-22 01:15:06.418634	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2126/19976, ttl=4 (no response found!)
63	2021-08-22 01:15:06.430823	113.171.7.34	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
64	2021-08-22 01:15:07.423860	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2127/20232, ttl=5 (no response found!)
65	2021-08-22 01:15:07.429849	113.171.48.58	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
66	2021-08-22 01:15:07.433073	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2128/20488, ttl=5 (no response found!)
67	2021-08-22 01:15:07.436896	113.171.48.58	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
68	2021-08-22 01:15:07.438516	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2129/20744, ttl=5 (no response found!)
69	2021-08-22 01:15:07.443347	113.171.48.58	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
87	2021-08-22 01:15:12.982708	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2130/21000, ttl=6 (no response found!)
88	2021-08-22 01:15:12.987470	172.17.5.1	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
89	2021-08-22 01:15:12.989090	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2131/21256, ttl=6 (no response found!)
90	2021-08-22 01:15:13.000386	172.17.5.1	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
91	2021-08-22 01:15:13.002462	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2132/21512, ttl=6 (no response found!)
92	2021-08-22 01:15:13.006877	172.17.5.1	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)

141	2021-08-22 01:15:18.521755	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2133/21768, ttl=7 (no response found!)
142	2021-08-22 01:15:18.526173	172.17.5.2	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
143	2021-08-22 01:15:18.528077	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2134/22024, ttl=7 (no response found!)
144	2021-08-22 01:15:18.534610	172.17.5.2	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
145	2021-08-22 01:15:18.536334	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2135/22280, ttl=7 (no response found!)
146	2021-08-22 01:15:18.551255	172.17.5.2	192.168.1.8	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
160	2021-08-22 01:15:24.096582	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2136/22536, ttl=8 (reply in 161)
161	2021-08-22 01:15:24.103483	14.241.254.131	192.168.1.8	ICMP	106 Echo (ping) reply id=0x0001, seq=2136/22536, ttl=58 (request in 160)
162	2021-08-22 01:15:24.106158	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2137/22792, ttl=8 (reply in 163)
163	2021-08-22 01:15:24.112966	14.241.254.131	192.168.1.8	ICMP	106 Echo (ping) reply id=0x0001, seq=2137/22792, ttl=58 (request in 162)
164	2021-08-22 01:15:24.114641	192.168.1.8	14.241.254.131	ICMP	106 Echo (ping) request id=0x0001, seq=2138/23048, ttl=8 (reply in 165)
165	2021-08-22 01:15:24.121828	14.241.254.131	192.168.1.8	ICMP	106 Echo (ping) reply id=0x0001, seq=2138/23048, ttl=58 (request in 164)

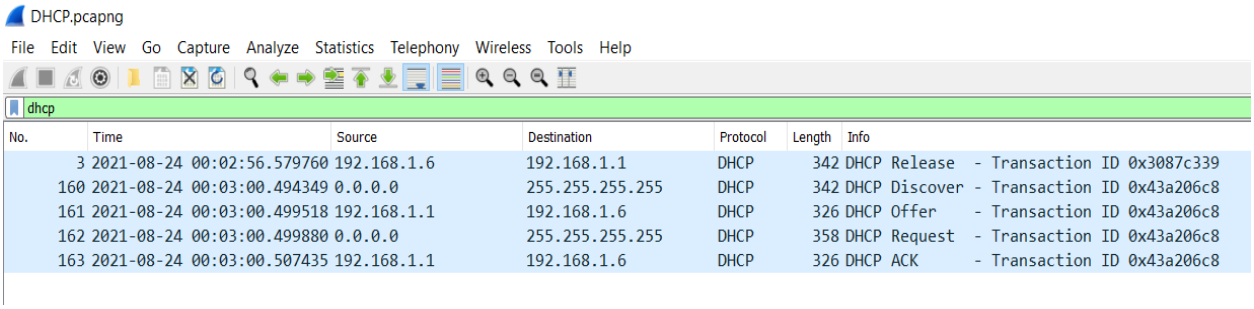
2. **Tác dụng của traceroute/tracert:** Công dụng của lệnh này khá giống với ping nhưng nhỉnh hơn, nó có thể kiểm tra được đường đi của các gói tin của lệnh ping, giúp ta có thể kiểm tra chi tiết hơn cấu trúc của mạng.
3. **Địa chỉ IP của máy gửi request:** 192.168.1.8
4. **Cách máy tính xác định được địa chỉ IP của FIT:** Đầu tiên máy tính sẽ gửi nhiều tín hiệu. Sau khi bên FIT nhận được tín hiệu thì sẽ phản hồi lại về máy tính của ta cho biết rằng đã kết nối được tới. Trong tín hiệu này có thông tin IP của FIT.
5. **Quá trình gửi gói tin đến web FIT:**
    a) **Protocol sử dụng:** ICMP
    b) **Số lượng gói tin được gửi đi (request) trước khi nhận được response đầu tiên:** 22
    c) **Time – to – live của các gói tin cuối cùng được gửi trước khi nhận được respone đầu tiên:** 8

d) **Port:** Không có port bởi vì tương tự câu 1, ICMP không có giá trị port bởi vì ICMP nằm cùng tầng với IP (phía dưới transport player) trong bộ giao thức TCP/IP.

e) **Gói tin response đầu tiên là trả lời cho gói tin request thứ:** 22

Câu 4: DHCP

1. **Quá trình bắt gói tin DHCP sau khi nhập lệnh release/renew:**



2. **DHCP message dùng UDP hay TCP ở tầng transport:** DHCP message sử dụng UDP.

   Lý do: DHCP là một phần mở rộng của BOOTP. BOOTP là một giao thức mà máy tính khách sử dụng để lấy thông tin cấu hình từ máy chủ, trong khi máy khách đang khởi động. Để xác định vị trí máy chủ, một chương trình phát được gửi yêu cầu máy chủ BOOTP (hoặc DHCP). Phát sóng chỉ có thể được gửi qua một giao thức không kết nối, chẳng hạn như UDP. Do đó, BOOTP yêu cầu ít nhất một gói UDP, để phát sóng định vị máy chủ. Hơn nữa, vì BOOTP đang chạy trong khi máy khách ... khởi động và đây là khoảng thời gian mà máy khách có thể không tải và chạy toàn bộ ngăn xếp TCP / IP, UDP có thể là giao thức duy nhất mà máy khách sẵn sàng xử lý thời gian. Cuối cùng, một số máy khách DHCP / BOOTP chỉ có UDP trên tàu. Ví dụ, một số bộ điều nhiệt IP chỉ thực hiện UDP.

3. **Mục đích của DHCP release messages:** DHCP release messages được gửi bởi DHCP client để giải phóng ip. Sau khi nhận được DHCP release messages, DHCP sever có thể gán địa chỉ IP này cho DHCP client khác.

   DHCP Server có đảm bảo lúc nào cũng nhận được ACK message từ Client?

   Không thể đảm bảo DHCP sever sẽ luôn nhận được ACK message bởi không có cơ sở nào để xác nhận nó cả.

   Chuyện gì xảy ra nếu DHCP release message của Client bị mất?

   Nếu DHCP release message của client bị mất, client sẽ giải phóng ip, nhưng sau đó sever sẽ không gán lại ip cho đến khi client rời khỏi địa chỉ.

4. **Lý do người khách không kết nối được:** Do cục router wifi của quán đã cấp hết địa chỉ IP, và mới chỉ 4 tiếng cho tới đủ 8 tiếng là lúc mà modem reset việc cấp ip.
   Những vị khách 93, 94, 95…: Cũng sẽ không thể truy cập vào, họ có thể truy cập vào lúc 15 giờ tức là 8 tiếng kể từ 7 giờ sáng.
   Để người thứ 92 có thể truy cập: Chủ quán có thể khởi động lại cục modem để release toàn bộ ip. Sau đó có thể đặt giới hạn sử dụng cho mỗi người khách đến quán coffee (60 phút).