

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA: CÔNG NGHỆ THÔNG TIN**



BÁO CÁO ĐỒ ÁN THỰC HÀNH - WIRESHARK MÔN MẠNG MÁY TÍNH

NHÓM THỰC HIỆN:

MSSV: 20120049 – HỌ TÊN: Nguyễn Hải Đăng

MSSV: 20120050 – HỌ TÊN: Nguyễn Nhật Đăng

MSSV: 20120061 – HỌ TÊN: Phạm Dương Trường Đức

Giảng viên lý thuyết: Đỗ Hoàng Cường

Lớp lý thuyết/Nhóm thực hành: 20CTT1/20CTT1A

Học kỳ - Niên khoá: HK1 - 2021-2022

MỤC LỤC

I. THÔNG TIN THÀNH VIÊN	3
II. ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH.....	3
III. BẢNG PHÂN CÔNG CÔNG VIỆC TRONG ĐỒ ÁN	3
IV. TRẢ LỜI CÂU HỎI.....	4
• <i>BÀI 1:</i>	<i>4</i>
• <i>BÀI 2:</i>	<i>10</i>
• <i>BÀI 3:</i>	<i>19</i>
• <i>BÀI 4:</i>	<i>23</i>
V. TÀI LIỆU THAM KHẢO	27

THÔNG TIN CHUNG VỀ ĐỒ ÁN

I. THÔNG TIN THÀNH VIÊN

Bảng thông tin thành viên trong đồ án:

MÃ SỐ SINH VIÊN	HỌ VÀ TÊN
20120049	Nguyễn Hải Đăng
20120050	Nguyễn Nhật Đăng
20120061	Phạm Dương Trường Đức

II. ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH

Bảng đánh giá mức độ hoàn thành và những yêu cầu còn chưa làm được và còn lỗi.

BÀI	MỨC ĐỘ HOÀN THÀNH	GHI CHÚ
1	100%	
2	100%	
3	100%	
4	100%	

III. BẢNG PHÂN CÔNG CÔNG VIỆC TRONG ĐỒ ÁN

Bảng phân công công việc trong đồ án:

BÀI	NGƯỜI THỰC HIỆN
1 và 4	Hải Đăng
2	Nhật Đăng
3	Trường Đức

PHẦN BÀI LÀM

IV. TRẢ LỜI CÂU HỎI

• BÀI 1:

– Câu 1:

Địa chỉ IP của host ping là **192.168.0.105**.

Địa chỉ IP của host được ping là **192.168.1.1**.

3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98 Echo (ping) request	id=0x000d, seq=1/256, ttl=64 (reply in 4)
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98 Echo (ping) reply	id=0x000d, seq=1/256, ttl=63 (request in 3)


```
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x7b02 (31490)
> Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0x3cec [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.105
  Destination Address: 192.168.1.1
```

Hình 1. Địa chỉ IP của host ping và host được ping.

– Câu 2:

Không có port được sử dụng trong lệnh ping này. Gói tin ICMP không có số port nguồn và đích, bởi vì giao thức ICMP được sử dụng để giao tiếp thông tin tầng mạng giữa các máy chủ (host) và bộ định tuyến, không phải giữa các tiến trình trong tầng ứng dụng. Mỗi gói tin ICMP có một type/code. Sự kết hợp type/code này xác định được thông điệp đang được nhận. Vì phần mềm mạng tự diễn giải tất cả thông điệp của ICMP, nên không cần số port để điều khiển thông điệp của ICMP đến tiến trình của tầng ứng dụng.

```
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
```

Hình 2. Type/Code của gói tin ICMP reply.

– Câu 3: Trong gói tin ICMP request:

- Kích thước của ICMP Data bằng tổng kích thước của Data (48 bytes) và Timestamp From ICMP Data (8 bytes). Tổng cộng là **56 bytes**.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request...
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply ...

Destination Address: 192.168.1.1

Internet Control Message Protocol

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x0cce [correct]
[Checksum Status: Good]
Identifier (BE): 13 (0x000d)
Identifier (LE): 3328 (0x0d00)
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]

Data (48 bytes)

Data: b1af09000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b...
[Length: 48]

0000	18 d6 c7 fc 53 7e a0 d3	7a 3c ac 58 08 00 45 00S~.. z<-X--E-
0010	00 54 7b 02 40 00 40 01	3c ec c0 a8 00 69 c0 a8	-T{:@-@- <....i-
0020	01 01 08 00 0c ce 00 0d	00 01 0c 41 65 60 00 00-Ae`..
0030	00 00 b1 af 09 00 00 00	00 00 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25 !"#\$\$%
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,-./012345
0060	36 37		67

Data (data), 48 bytes
Packets: 4 · Displayed: 4 (100.0%)
Profile: Default

Hình 3. Kích thước Data.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request...
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply ...

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x0cce [correct]
[Checksum Status: Good]
Identifier (BE): 13 (0x000d)
Identifier (LE): 3328 (0x0d00)
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]

Data (48 bytes)

Data: b1af09000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b...
[Length: 48]

0000	18 d6 c7 fc 53 7e a0 d3	7a 3c ac 58 08 00 45 00S~.. z<-X--E-
0010	00 54 7b 02 40 00 40 01	3c ec c0 a8 00 69 c0 a8	-T{:@-@- <....i-
0020	01 01 08 00 0c ce 00 0d	00 01 0c 41 65 60 00 00-Ae`..
0030	00 00 b1 af 09 00 00 00	00 00 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25 !"#\$\$%
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,-./012345
0060	36 37		67

The timestamp in the first 8 bytes of the icmp data (icmp.data_time), 8 bytes
Packets: 4 · Displayed: 4 (100.0%)
Profile: Default

Hình 4. Kích thước icmp.data_time.

- Kích thước ICMP Header bằng tổng kích thước của Type (1 byte), Code (1 byte), Checksum (2 bytes), Identifier (2 bytes), Sequence Number (2 bytes). Tổng cộng là **8 bytes**.

3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98 Echo (ping) request...
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98 Echo (ping) reply ...

Destination Address: 192.168.1.1	
Internet Control Message Protocol	Type: 8 (Echo (ping) request)
	Code: 0
	Checksum: 0x0cce [correct]
	[Checksum Status: Good]
	Identifier (BE): 13 (0x000d)
	Identifier (LE): 3328 (0xd00)
	Sequence Number (BE): 1 (0x0001)
	Sequence Number (LE): 256 (0x100)
	[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]
Data (48 bytes)	

0000	18 d6 c7 fc 53 7e a0 d3	7a 3c ac 58 08 00 45 00S~.. z<·X··E·
0010	00 54 7b 02 40 00 40 01	3c ec c0 a8 00 69 c0 a8	·T{·@·@· <····i·
0020	01 01 08 00 0c ce 00 0d	00 01 0c 41 65 60 00 00	···.····· ··Ae`··
0030	00 00 b1 af 09 00 00 00	00 00 10 11 12 13 14 15	··········
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25	·········· !"#\$\$%
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,- ./012345
0060	36 37		67

Type (icmp.type), 1 byte Packets: 4 · Displayed: 4 (100.0%) Profile: Default

Hình 5. Kích thước icmp.type trong ICMP Header.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request...
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply ...

Destination Address: 192.168.1.1	
Internet Control Message Protocol	Type: 8 (Echo (ping) request)
	Code: 0
	Checksum: 0x0cce [correct]
	[Checksum Status: Good]
	Identifier (BE): 13 (0x000d)
	Identifier (LE): 3328 (0xd00)
	Sequence Number (BE): 1 (0x0001)
	Sequence Number (LE): 256 (0x100)
	[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]
Data (48 bytes)	

0000	18 d6 c7 fc 53 7e a0 d3	7a 3c ac 58 08 00 45 00S~.. z<·X··E·
0010	00 54 7b 02 40 00 40 01	3c ec c0 a8 00 69 c0 a8	·T{·@·@· <····i·
0020	01 01 08 00 0c ce 00 0d	00 01 0c 41 65 60 00 00	···.····· ··Ae`··
0030	00 00 b1 af 09 00 00 00	00 00 10 11 12 13 14 15	··········
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25	·········· !"#\$\$%
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,- ./012345
0060	36 37		67

Code (icmp.code), 1 byte Packets: 4 · Displayed: 4 (100.0%) Profile: Default

Hình 6. Kích thước icmp.code trong ICMP Header.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request...
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply ...

Destination Address: 192.168.1.1

Internet Control Message Protocol

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x0cce [correct]
[Checksum Status: Good]
Identifier (BE): 13 (0x000d)
Identifier (LE): 3328 (0x0d00)
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]

Data (48 bytes)

0000	18 d6 c7 fc 53 7e a0 d3	7a 3c ac 58 08 00 45 00S~.. z<-X--E-
0010	00 54 7b 02 40 00 40 01	3c ec c0 a8 00 69 c0 a8	-T{-.@-@- <----i--
0020	01 01 08 00 0c ce 00 0d	00 01 0c 41 65 60 00 00-.. Ae`..
0030	00 00 b1 af 09 00 00 00	00 00 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25 !"#\$\$%
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,- ./012345
0060	36 37		67

Checksum (icmp.checksum), 2 bytes
Packets: 4 · Displayed: 4 (100.0%)
Profile: Default

Hình 7. Kích thước icmp.checksum trong ICMP Header.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request...
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply ...

Destination Address: 192.168.1.1

Internet Control Message Protocol

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x0cce [correct]
[Checksum Status: Good]
Identifier (BE): 13 (0x000d)
Identifier (LE): 3328 (0x0d00)
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]

Data (48 bytes)

0000	18 d6 c7 fc 53 7e a0 d3	7a 3c ac 58 08 00 45 00S~.. z<-X--E-
0010	00 54 7b 02 40 00 40 01	3c ec c0 a8 00 69 c0 a8	-T{-.@-@- <----i--
0020	01 01 08 00 0c ce 00 0d	00 01 0c 41 65 60 00 00-.. Ae`..
0030	00 00 b1 af 09 00 00 00	00 00 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25 !"#\$\$%
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,- ./012345
0060	36 37		67

Identifier (big endian representation) (icmp.ident), 2 bytes
Packets: 4 · Displayed: 4 (100.0%)
Profile: Default

Hình 8. Kích thước icmp.ident trong ICMP Header.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request...
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply ...

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x0cce [correct]
[Checksum Status: Good]
Identifier (BE): 13 (0x000d)
Identifier (LE): 3328 (0x0d00)
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]
Data (48 bytes)
Data: b1af090000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b...
[Length: 48]

0000	18 d6 c7 fc 53 7e a0 d3	7a 3c ac 58 08 00 45 00S~.. z<X..E.
0010	00 54 7b 02 40 00 40 01	3c ec c0 a8 00 69 c0 a8	.T{.@.@. <....i..
0020	01 01 08 00 0c ce 00 0d	00 01 0c 41 65 60 00 00	..-.....-Ae`..
0030	00 00 b1 af 09 00 00 00	00 00 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25 !"#\$\$
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,- ./012345
0060	36 37		67

Sequence Number (big endian representation) (icmp.seq), 2 bytes Packets: 4 · Displayed: 4 (100.0%) Profile: Default

Hình 9. Kích thước icmp.seq trong ICMP Header.

- IP Header có kích thước là **20 bytes**.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request...
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply ...

> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp2s0, id 0
> Ethernet II, Src: IntelCor_3c:ac:58 (a0:d3:7a:3c:ac:58), Dst: Tp-LinkT_fc:53:7e (18:d6:c7:fc:53:7e)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.1.1
> Internet Control Message Protocol

0000	18 d6 c7 fc 53 7e a0 d3	7a 3c ac 58 08 00 45 00S~.. z<X..E.
0010	00 54 7b 02 40 00 40 01	3c ec c0 a8 00 69 c0 a8	.T{.@.@. <....i..
0020	01 01 08 00 0c ce 00 0d	00 01 0c 41 65 60 00 00	..-.....-Ae`..
0030	00 00 b1 af 09 00 00 00	00 00 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25 !"#\$\$
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,- ./012345
0060	36 37		67

Internet Protocol Version 4 (ip), 20 bytes Packets: 4 · Displayed: 4 (100.0%) Profile: Default

Hình 10. Kích thước IP Header.

- Ethernet Header có kích thước là **14 bytes**.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request...
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply ...

> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp2s0, id 0
 > Ethernet II, Src: IntelCor_3c:ac:58 (a0:d3:7a:3c:ac:58), Dst: Tp-LinkT_fc:53:7e (18:d6:c7:fc:53:7e)
 > Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.1.1
 > Internet Control Message Protocol

0000	18 d6 c7 fc 53 7e	a0 d3 7a 3c ac 58 08 00 45 00S~.. z<X..E-
0010	00 54 7b 02 40 00 40 01	3c ec c0 a8 00 69 c0 a8	-T{:@-@- <...i..
0020	01 01 08 00 0c ce 00 0d	00 01 0c 41 65 60 00 00 Ae`..
0030	00 00 b1 af 09 00 00 00	00 00 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25 !"#\$\$%
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,- ./012345
0060	36 37		67

Ethernet (eth), 14 bytes
 Packets: 4 · Displayed: 4 (100.0%) Profile: Default

Hình 11. Kích thước Ethernet Header.

56 bytes	8 bytes	20 bytes	14 bytes	98 bytes
ICMP Data	ICMP header	IP Header	Ethernet Header	Tổng kích thước gói tin ICMP Request

– Câu 4:

Ở frame đầu tiên (dòng đầu tiên) của gói tin, ta có thể thấy phần info được giải mã có một câu hỏi: Who has 192.168.0.1? Tell 192.168.0.105.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	IntelCor_3c:ac:58	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.105
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
3	0.001835170	192.168.0.105	192.168.1.1	ICMP	98	Echo (ping) request id=0x000d, seq=1/256,
4	0.004770309	192.168.1.1	192.168.0.105	ICMP	98	Echo (ping) reply id=0x000d, seq=1/256,

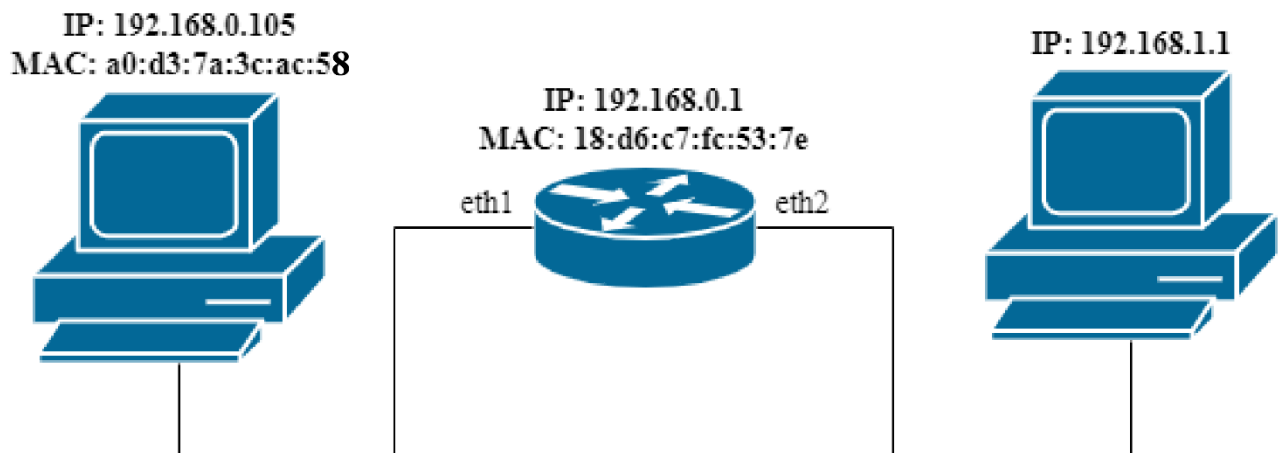
Hình 12. Frame đầu tiên của gói tin.

Để gửi gói tin từ một máy qua máy khác thì trong trường hợp này thì cần thông qua 1 router, ta đã biết địa chỉ IP của router nhưng làm thế nào để biết được địa chỉ MAC của router để gửi frame cho router. Đây là lúc ARP, giao thức phân giải địa chỉ IP thành địa chỉ MAC làm việc.

ARP thứ nhất (ARP Request) là gói tin ở layer 2, tức là nó không chứa IP header, nó gửi gói tin cho broadcast (ff:ff:ff:ff:ff:ff), tức là nó sẽ hỏi tất cả các máy trong mạng LAN, ở đây ta tìm địa chỉ MAC của địa chỉ IP 192.168.0.1, vì router có địa chỉ IP này nên router sẽ trả lời bằng gói ARP thứ hai (ARP Reply), và gói này là gói unicast, tức là nó chỉ gửi

gói cho đúng máy đã hỏi. Và sau khi hỏi xong, máy gửi đã có địa chỉ MAC của máy nhận, và nó sẽ điền vào phần destination MAC trong layer 2 header. Vậy là đủ thông tin.

– Câu 5:



Hình 13. Sơ đồ mạng tương ứng với nội dung gói pcap đó.

• BÀI 2:

– Câu 1:

- Bắt đầu DNS:

bai2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.8 && dns

No.	Time	Source	Destination	Protocol	Length	Info
18	7.519724	192.168.1.8	8.8.8.8	DNS	69	Standard query 0x3683 A wpad.Home
19	7.520002	192.168.1.8	8.8.8.8	DNS	69	Standard query 0xfeb2 AAAA wpad.Home
21	7.569477	8.8.8.8	192.168.1.8	DNS	144	Standard query response 0xfeb2 No such name AAAA wpad.Home SOA a.root-servers.net
25	7.573100	8.8.8.8	192.168.1.8	DNS	144	Standard query response 0x3683 No such name A wpad.Home SOA a.root-servers.net
41	7.627094	192.168.1.8	8.8.8.8	DNS	79	Standard query 0x967f A x.urs.microsoft.com
42	7.627094	192.168.1.8	8.8.8.8	DNS	89	Standard query 0x9ba0 A nav.smartscreen.microsoft.com
43	7.627237	192.168.1.8	8.8.8.8	DNS	89	Standard query 0x3091 AAAA nav.smartscreen.microsoft.com
44	7.627255	192.168.1.8	8.8.8.8	DNS	79	Standard query 0xb3a5 AAAA x.urs.microsoft.com
46	7.675315	8.8.8.8	192.168.1.8	DNS	220	Standard query response 0x9ba0 A nav.smartscreen.microsoft.com CNAME wd-prod-s
47	7.676513	8.8.8.8	192.168.1.8	DNS	210	Standard query response 0x967f A x.urs.microsoft.com CNAME wd-prod-ss.trafficm
48	7.677142	8.8.8.8	192.168.1.8	DNS	264	Standard query response 0x3091 AAAA nav.smartscreen.microsoft.com CNAME wd-pro
50	7.686097	8.8.8.8	192.168.1.8	DNS	254	Standard query response 0xb3a5 AAAA x.urs.microsoft.com CNAME wd-prod-ss.traff

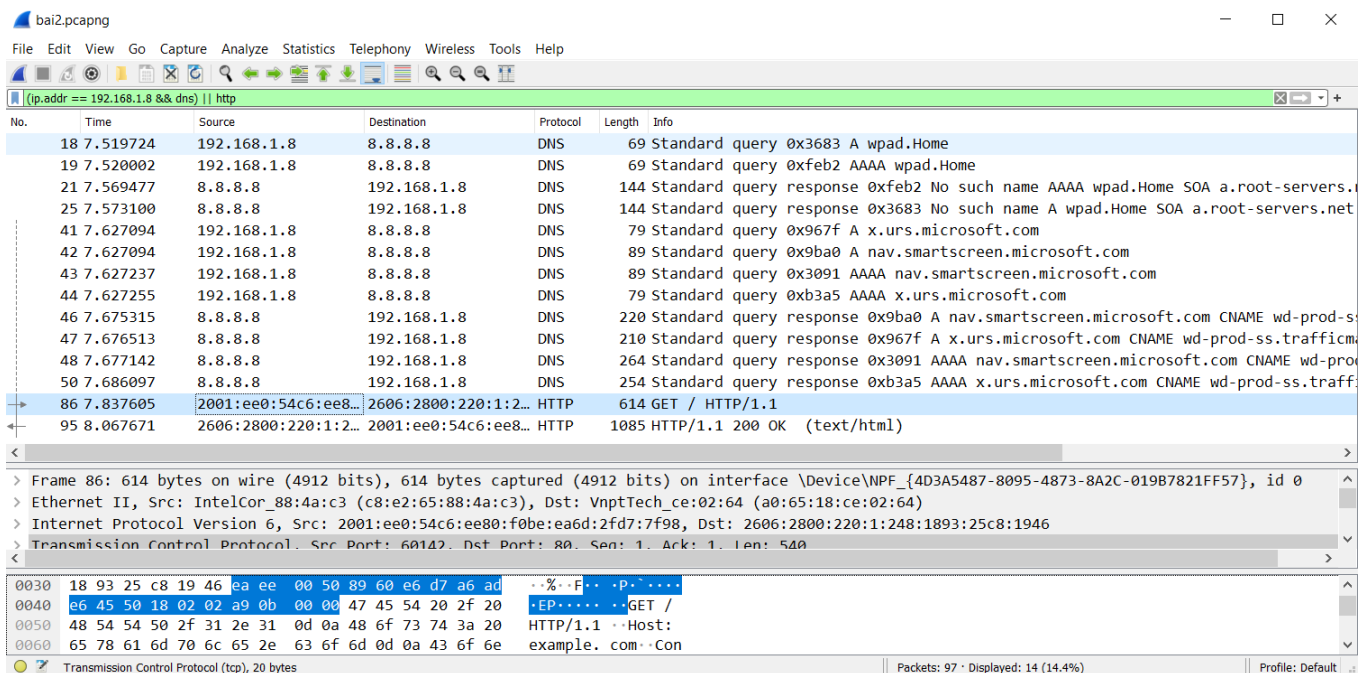
Domain Name System: Protocol

Packets: 97 · Displayed: 12 (12.4%)

Profile: Default

Hình 14. Những gói tin liên quan trong quá trình DNS.

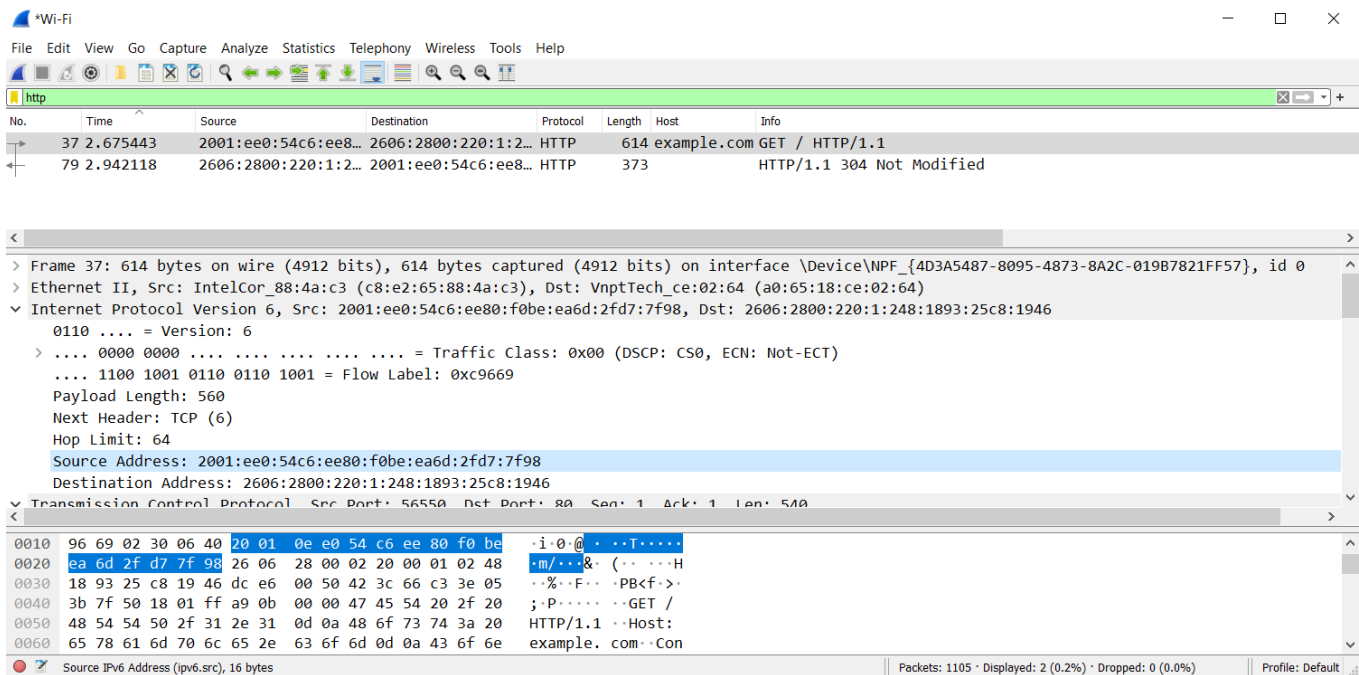
- Sau khi gửi HTTP request:



Hình 15. Gói Tin bắt được sau khi gửi HTTP request.

Câu 2:

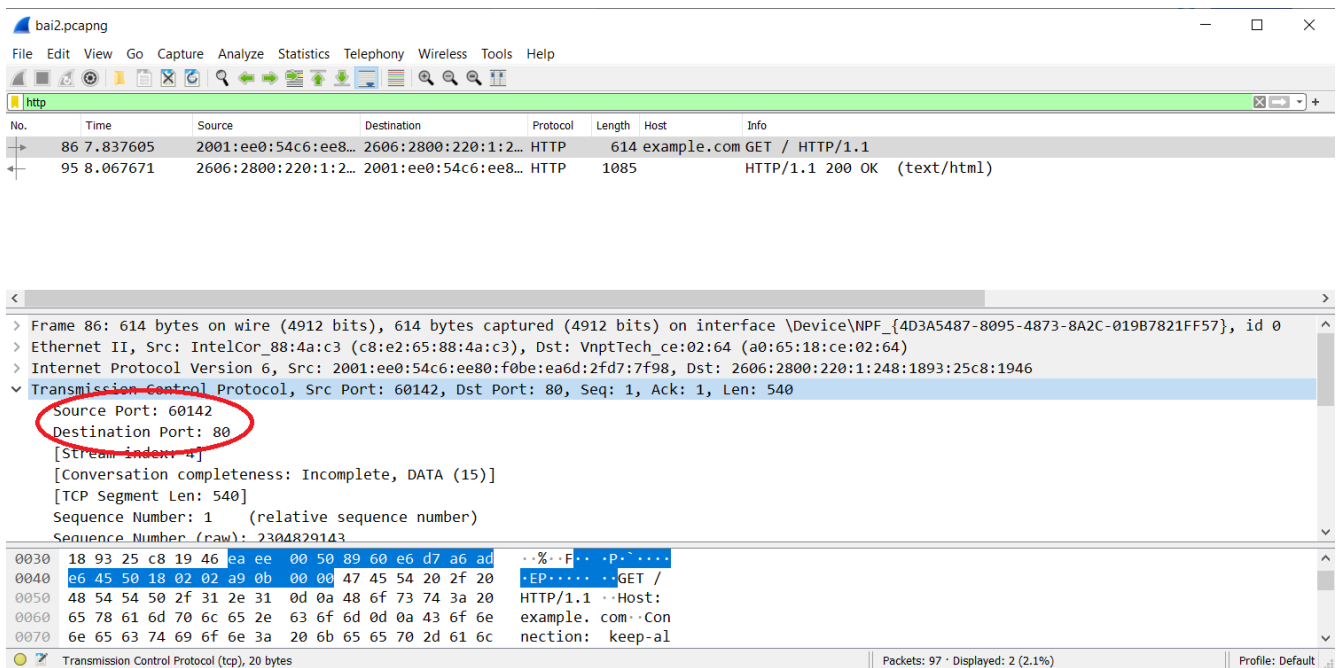
- Địa chỉ IP của host là: 2001:ee0:54c6:ee80:f0be:ea6d:2fd7:7f98



Hình 16. Địa chỉ IP của host.

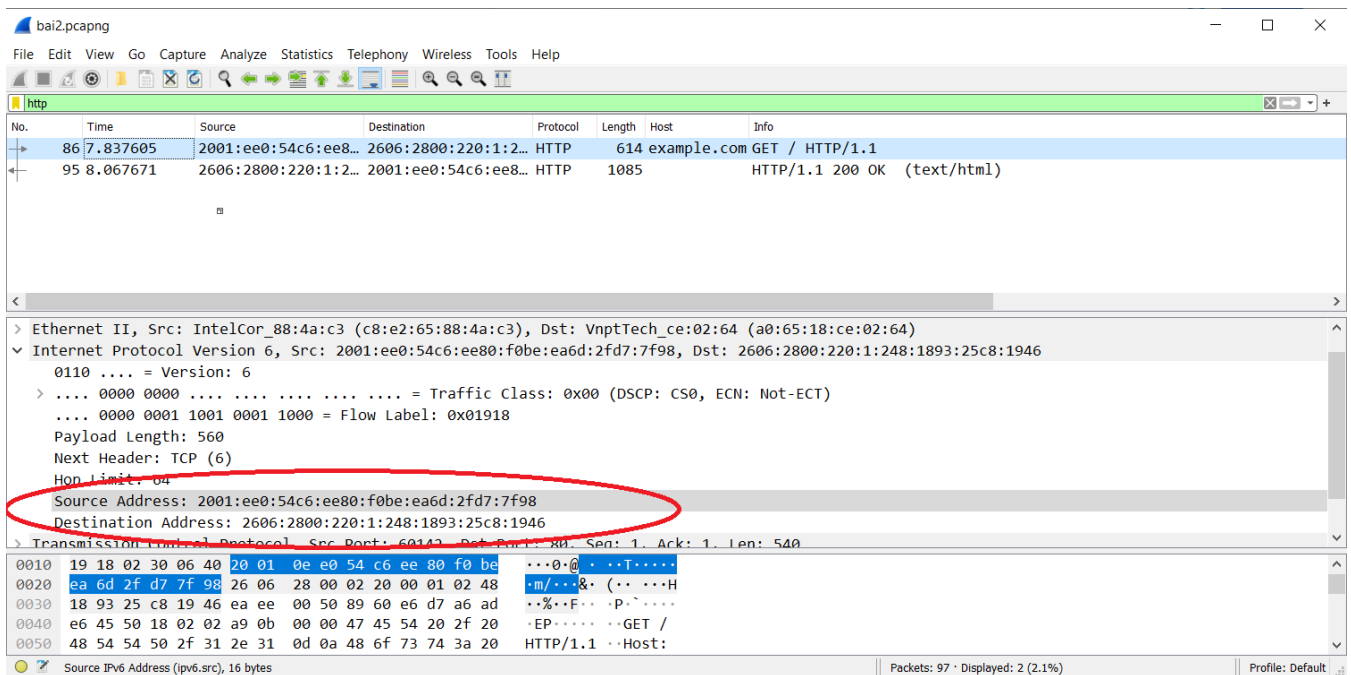
Câu 3:

- Địa chỉ IP của router (default gateway) là không có vì trong thức của các tầng đều không cần địa chỉ IP của router. Ví dụ khi ta gửi thông điệp GET, ở tầng transport, thông tin được quan tâm và lưu lại là port nguồn (60142) và port cuối (80)



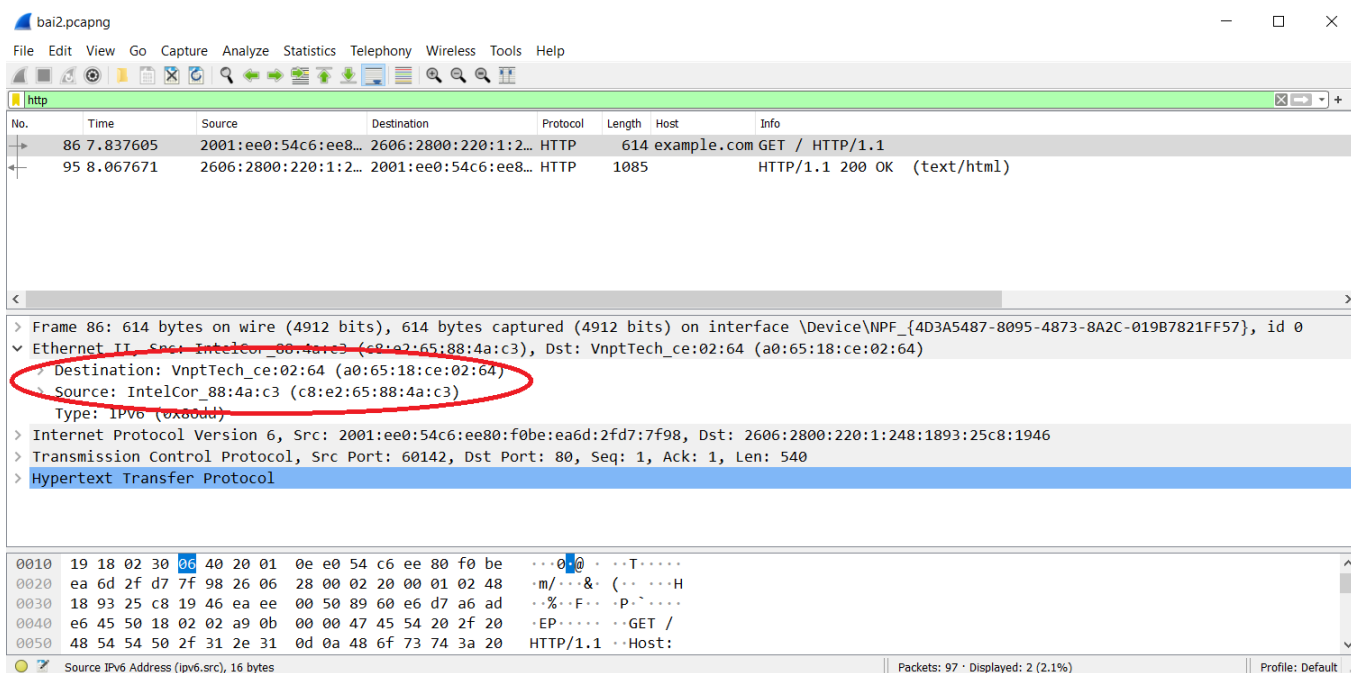
Hình 17. Port nguồn và Port đích lưu trữ ở tầng transport.

- Ở tầng network, thông tin được quan tâm là **IP** của người dùng (host) và **IP** của HTTP server.



Hình 18. Địa chỉ nguồn và địa chỉ đích được lưu ở tầng network.

- Ở tầng data-link, thông tin được quan tâm là **địa chỉ MAC** của người dùng và **địa chỉ MAC** của router.

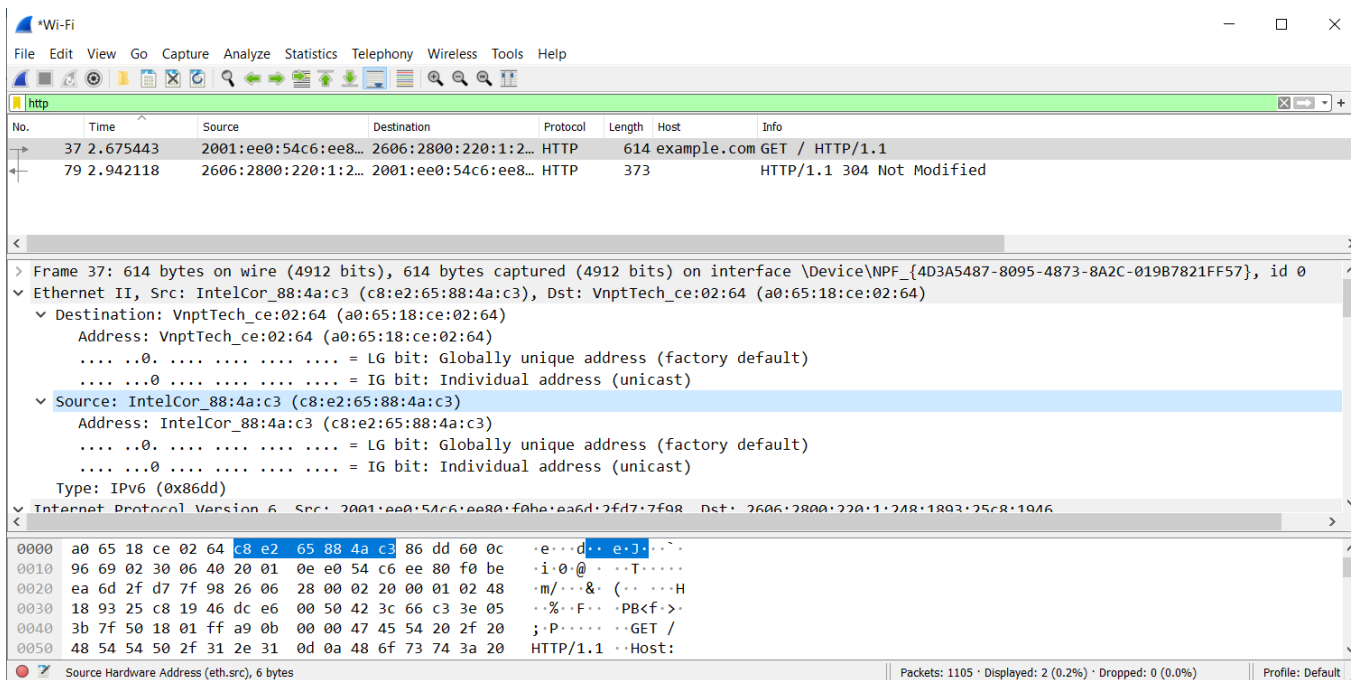


Hình 19. Địa chỉ MAC nguồn và Địa chỉ MAC đích lưu ở tầng data-link.

=> Không tồn tại IP của router.

Câu 4:

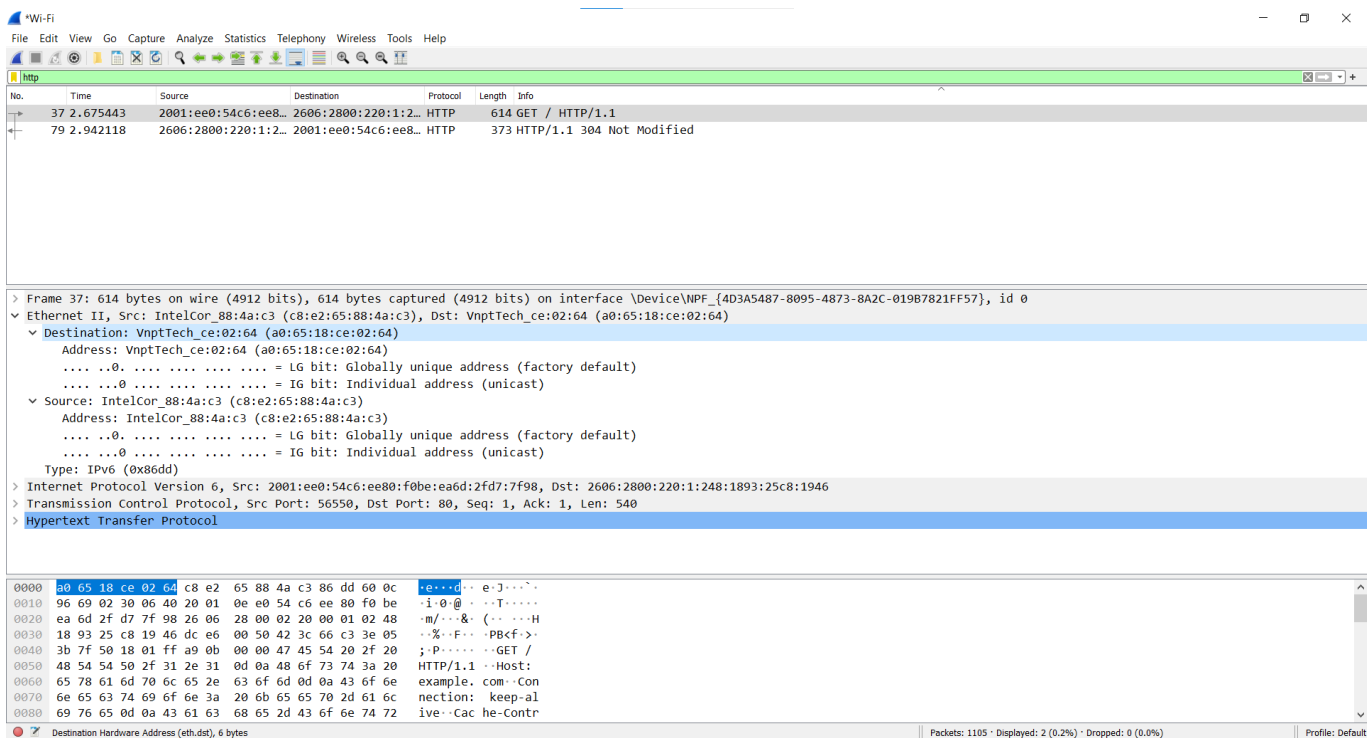
- Địa chỉ MAC của host là: **e8:e2:65:88:4a:c3**



Hình 20. Địa chỉ MAC của host.

Câu 5:

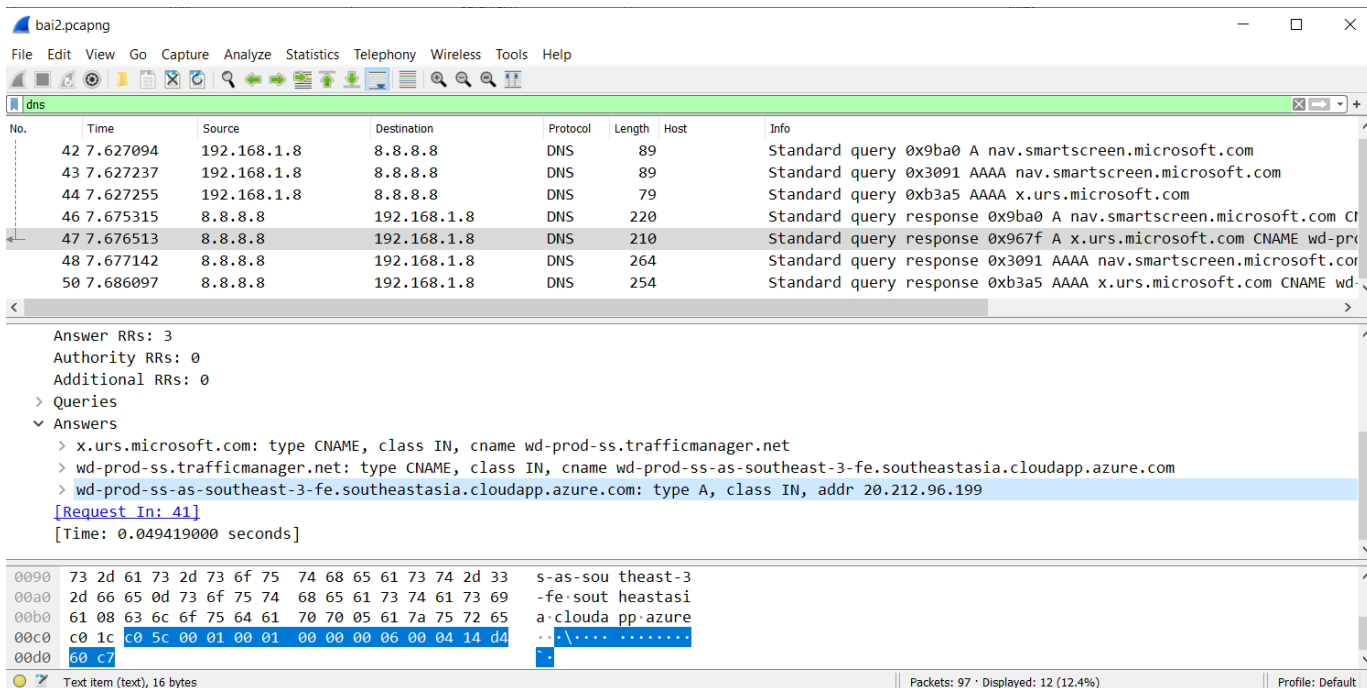
- Địa chỉ MAC của router (default gateway) là: **a0:65:18:ce:02:64**.



Hình 21. Địa chỉ MAC của router.

Câu 6:

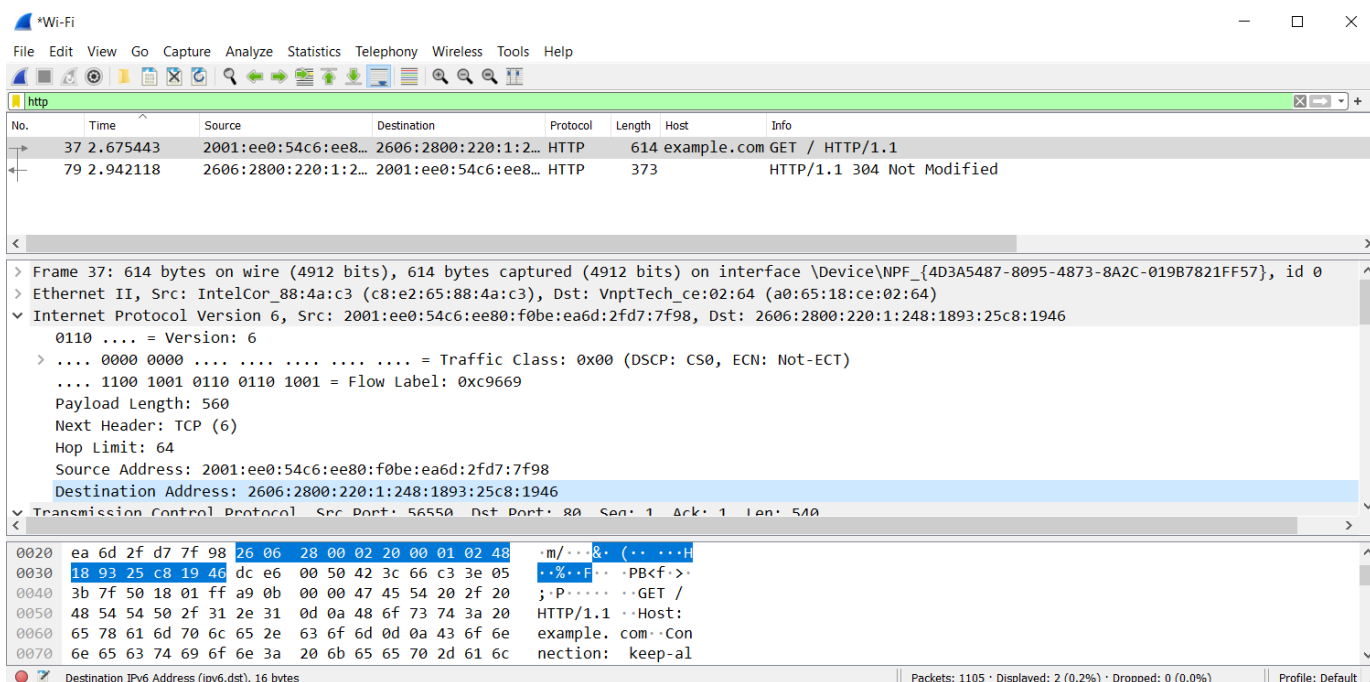
- Protocol được sử dụng để phân giải tên miền thành địa chỉ IP là **DNS**.



Hình 22. DNS trả về kết quả là địa chỉ IP từ tên trang web.

Câu 7:

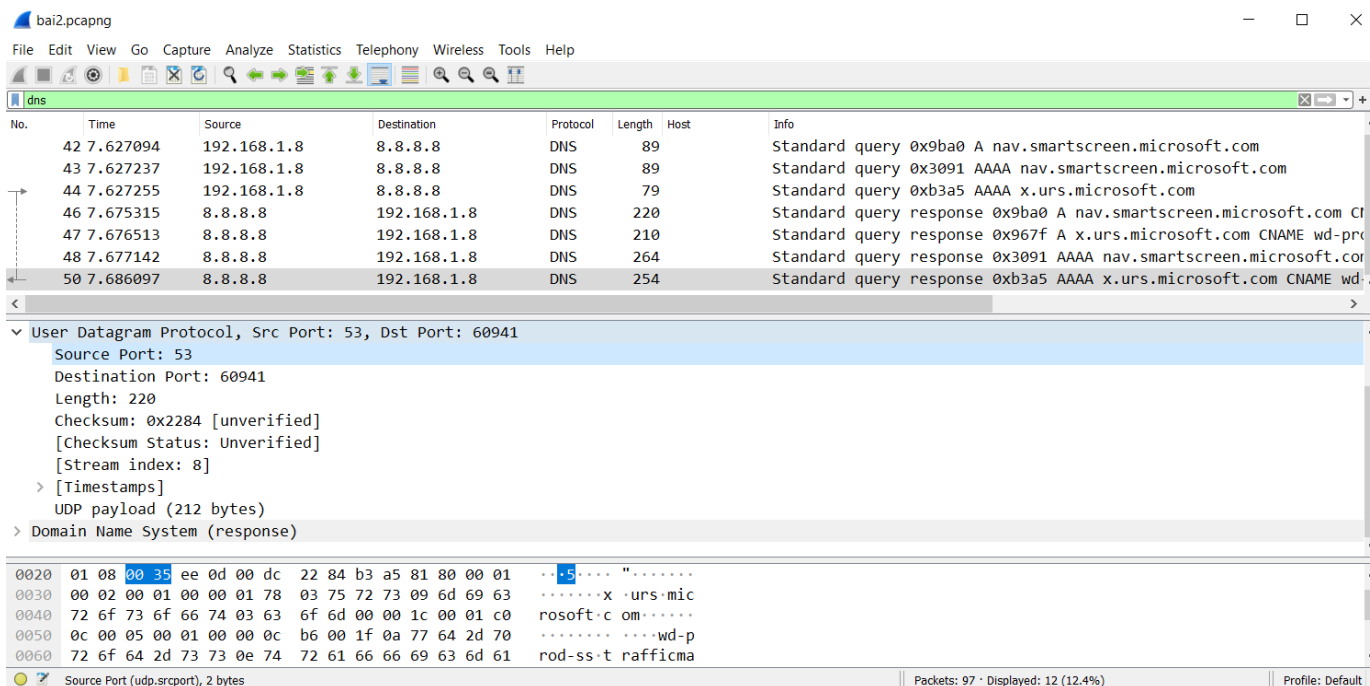
- Địa chỉ IP của HTTP server là: **2606:2800:220:1:248:1893:25c8:1946**.



Hình 23. Địa chỉ IP của HTTP server.

Câu 8:

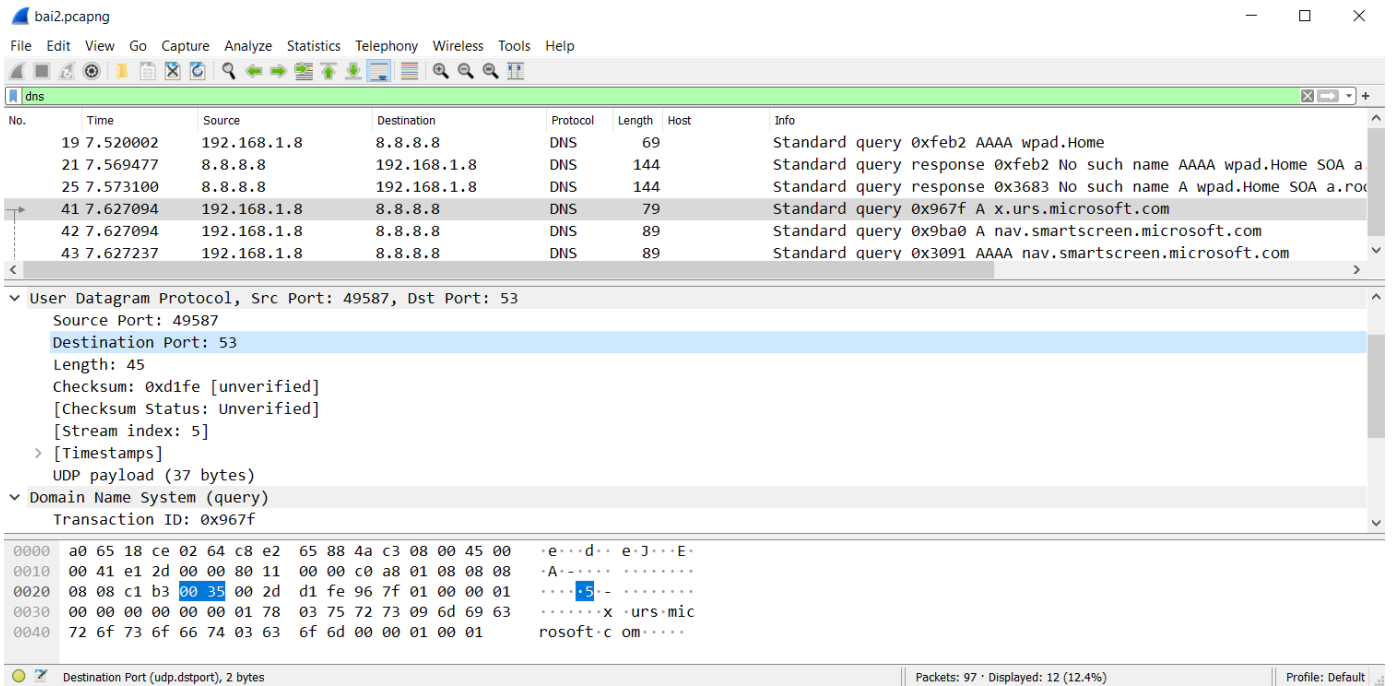
- DNS sử dụng cả 2 giao thức của tầng transport là UDP và TCP:
 - UDP: Port 53 được sử dụng để thực hiện các truy vấn giữa DNS client và DNS server. UDP được sử dụng trong đa số trường hợp vì có tốc độ cao.
 - TCP: được dùng trong việc trao đổi dữ liệu giữa DNS server chính và DNS server phụ (zone transfer)



Hình 24. DNS sử dụng giao thức UDP ở port 53

Câu 9:

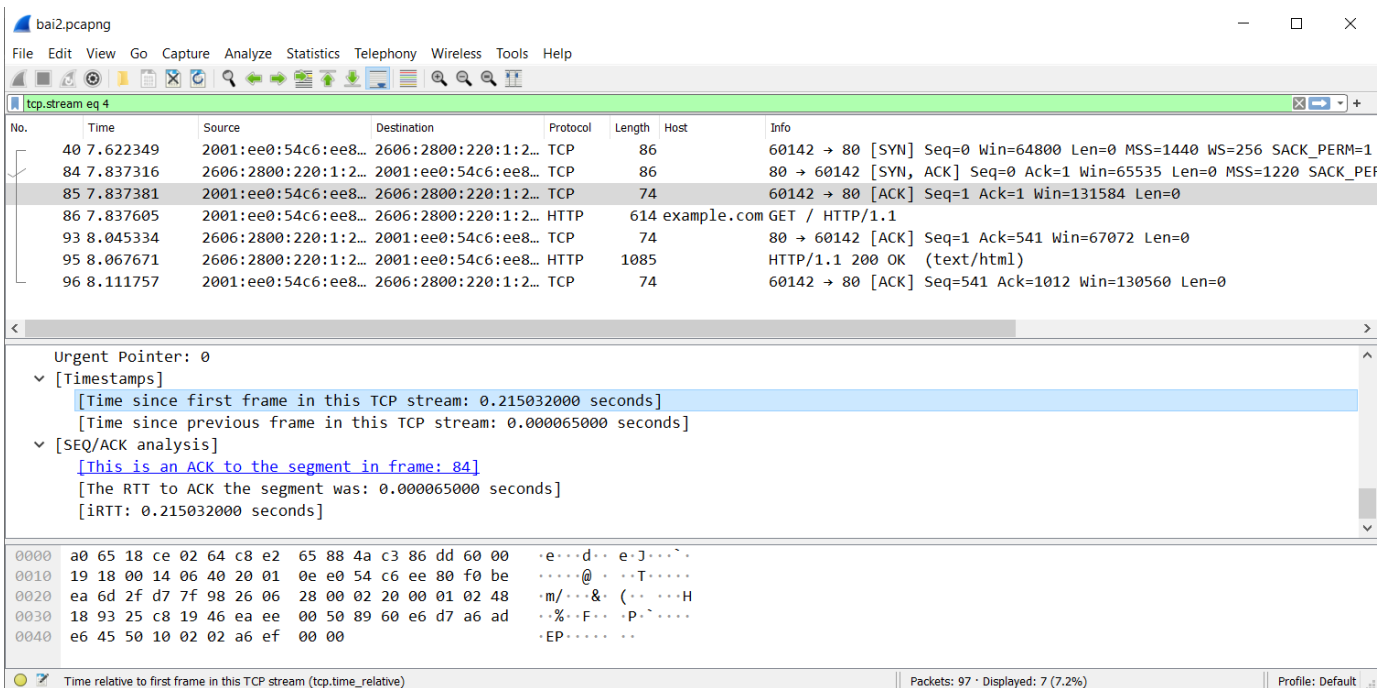
- Port được sử dụng khi truy vấn DNS server là port 53



Hình 25. Port 53 được sử dụng khi truy vấn DNS server.

Câu 10:

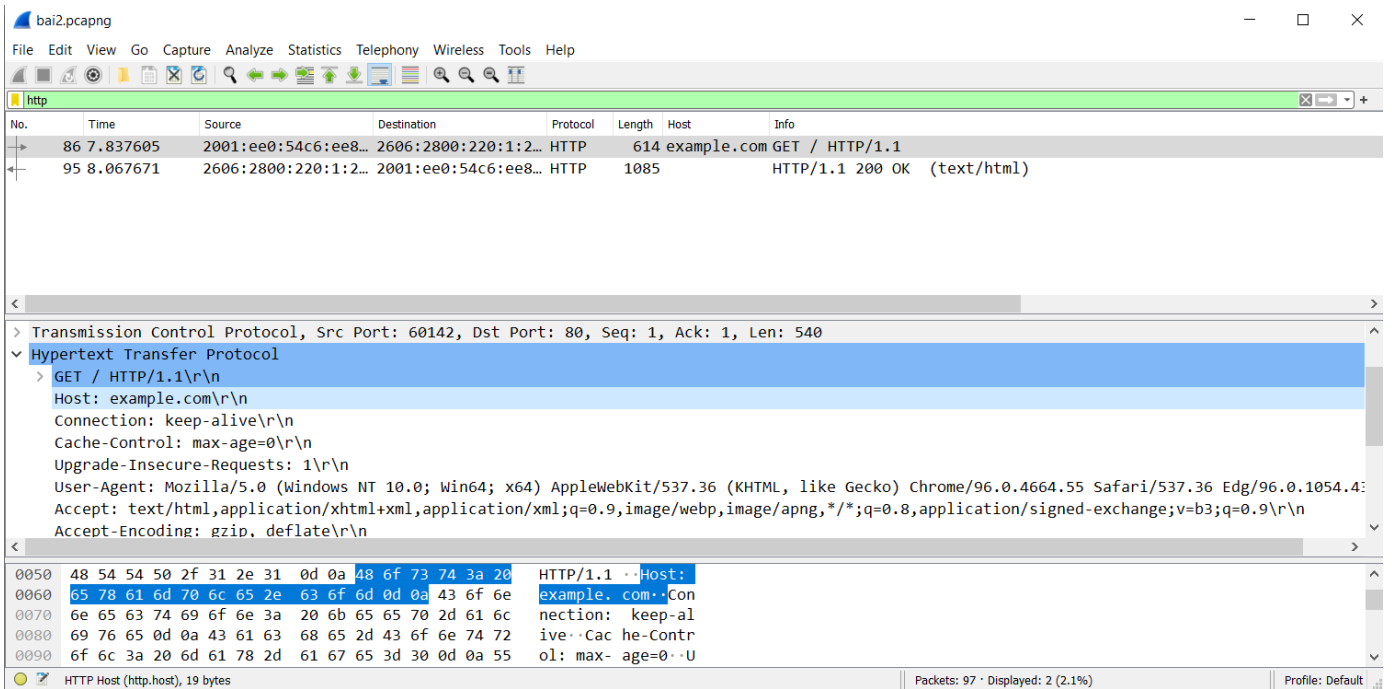
- Quá trình bắt tay 3 bước tốn 0.215s để hoàn thành.



Hình 26. Các gói tin bắt được trong quá trình bắt tay 3 bước.

Câu 11:

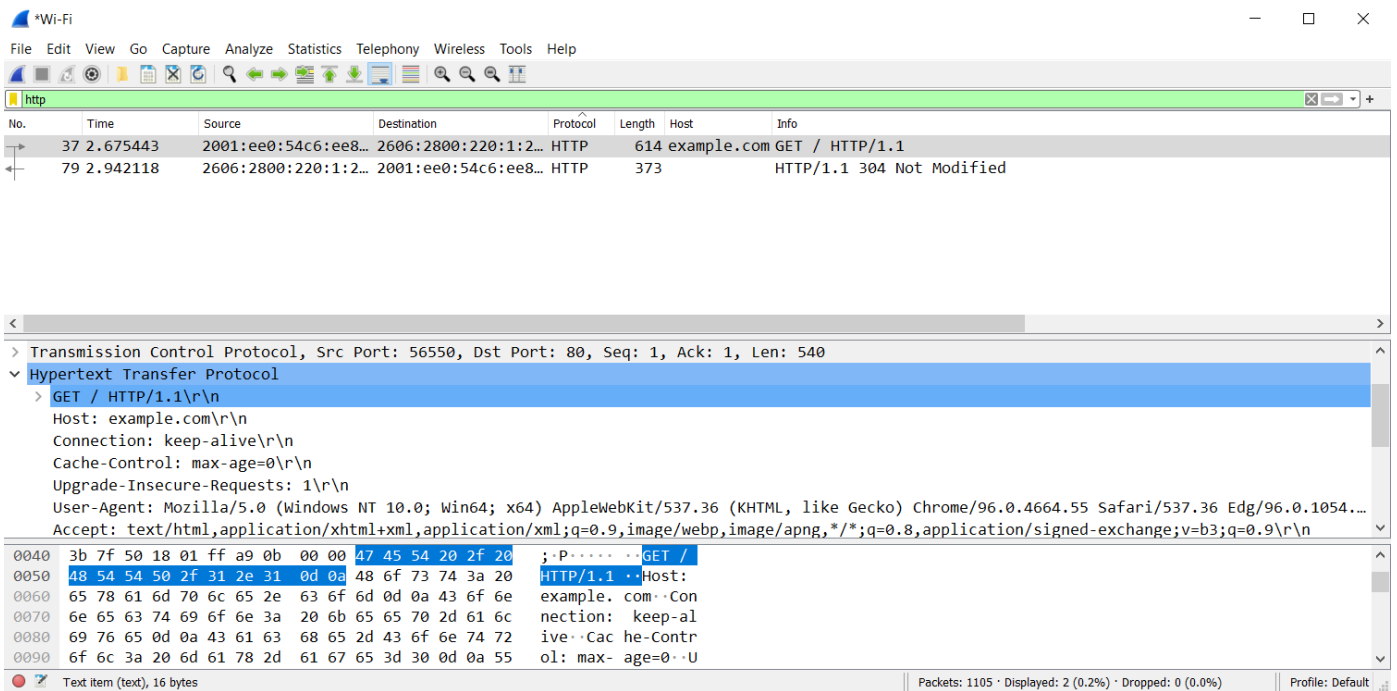
- Host machine của website là example.com.



Hình 27. Host của website.

Câu 12:

- Version HTTP mà trình duyệt web đang sử dụng là version 1.1.



Hình 28. HTTP version 1.1 được trình duyệt sử dụng.

– Câu 13:

The image shows a Wireshark capture of network traffic. The top pane displays a list of captured packets, filtered by 'udp.dstport==53'. The bottom pane shows the details of the selected packet (No. 44), including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The packet is a DNS standard query from 192.168.1.8 to 8.8.8.8.

No.	Time	Source	Destination	Protocol	Length	Host	Info
18	7.519724	192.168.1.8	8.8.8.8	DNS	69		Standard query 0x3683 A wpad.Home
19	7.520002	192.168.1.8	8.8.8.8	DNS	69		Standard query 0xfeb2 AAAA wpad.Home
41	7.627094	192.168.1.8	8.8.8.8	DNS	79		Standard query 0x967f A x.urs.microsoft.com
42	7.627094	192.168.1.8	8.8.8.8	DNS	89		Standard query 0x9ba0 A nav.smartscreen.microsoft.com
43	7.627237	192.168.1.8	8.8.8.8	DNS	89		Standard query 0x3091 AAAA nav.smartscreen.microsoft.com
44	7.627255	192.168.1.8	8.8.8.8	DNS	79		Standard query 0xb3a5 AAAA x.urs.microsoft.com

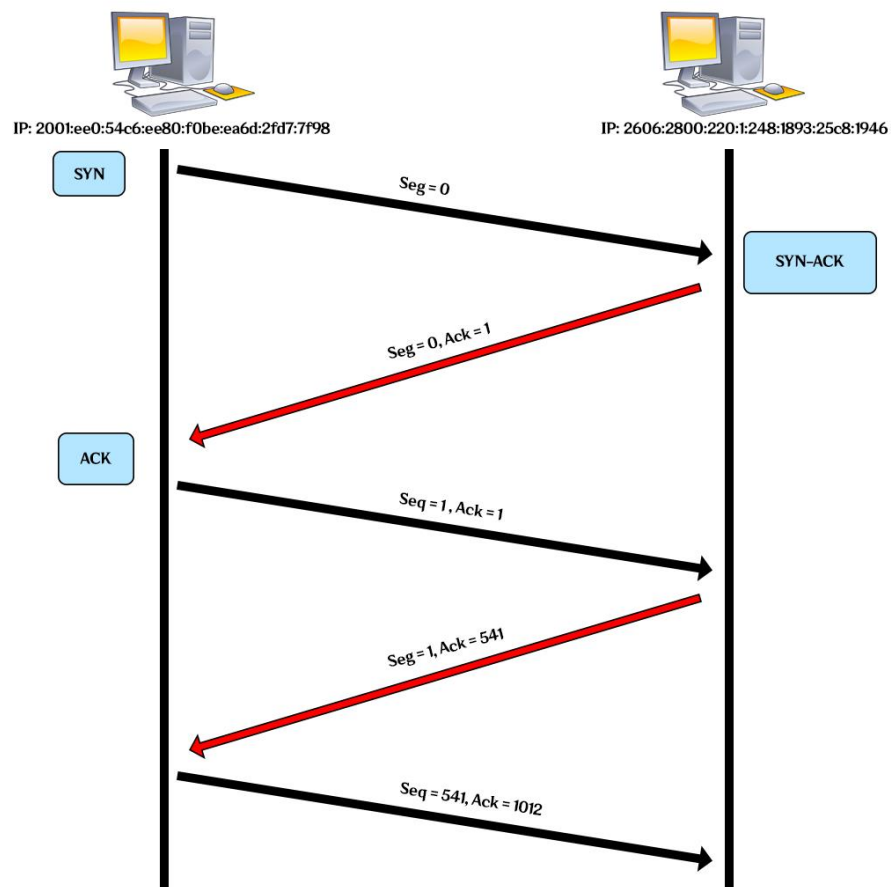
Frame 44: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{4D3A5487-8095-4873-8A2C-019B7821FF57}, id 0
> Ethernet II, Src: IntelCor_88:4a:c3 (c8:e2:65:88:4a:c3), Dst: VnptTech_ce:02:64 (a0:65:18:ce:02:64)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 60941, Dst Port: 53
Source Port: 60941
Destination Port: 53
Length: 45
Checksum: 0xd1fe [unverified]
[Checksum Status: Unverified]

0000 a0 65 18 ce 02 64 c8 e2 65 88 4a c3 08 00 45 00 ·e···d·· e·J···E·
0010 00 41 e1 30 00 00 80 11 00 00 c0 a8 01 08 08 08 ·A·0···· ······
0020 08 08 ee 0d 00 35 00 2d d1 fe b3 a5 01 00 00 01 ·····5·· ······
0030 00 00 00 00 00 00 01 78 03 75 72 73 09 6d 69 63 ······x ·urs·mic
0040 72 6f 73 6f 66 74 03 63 6f 6d 00 00 1c 00 01 ·rosoft·c om····

Hình 29. Những gói tin hiển thị sau khi nhập `udp.dstport==53` vào filter.

- Chức năng của câu query vừa thực hiện: Yêu cầu wireshark chỉ hiển thị những gói tin được truyền bằng giao thức UDP vào port 53, hay nói cách khác là chỉ hiển thị những truy vấn được gửi từ máy của người dùng đến DNS server.

– Câu 14:



Hình 30. Quá trình gửi ACK.

• **BÀI 3:**

Sử dụng hệ điều hành Windows

– Câu 1: Chụp hình kết quả bắt gói tin sau khi tracert

```

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

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

  1    3 ms    1 ms    1 ms    gateway [192.168.1.1]
  2    3 ms    3 ms    4 ms    100.123.0.76
  3   13 ms   10 ms    8 ms    118.69.189.24
  4   16 ms    8 ms    8 ms    100.123.0.21
  5    9 ms   11 ms    9 ms    118.69.132.167
  6    9 ms   10 ms   10 ms    118.69.189.63
  7    8 ms    9 ms    9 ms    static.vnpt.vn [123.29.16.13]
  8   10 ms    9 ms    9 ms    static.vnpt.vn [113.171.7.209]
  9    9 ms    9 ms    9 ms    static.vnpt.vn [113.171.44.102]
 10   12 ms    9 ms   14 ms    static.vnpt.vn [113.171.48.238]
 11    *      *      *      Request timed out.
 12   11 ms   10 ms   18 ms    static.vnpt.vn [14.161.23.204]

Trace complete.

```

Hình 31. Lệnh tracert trong cmd.

209	21.679565	100.123.0.21	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
210	21.681093	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=44/11264, ttl=4 (no response found...)
211	21.689975	100.123.0.21	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	21.691610	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=45/11520, ttl=4 (no response found...)
213	21.700183	100.123.0.21	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
467	31.729452	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=46/11776, ttl=5 (no response found...)
468	31.738586	118.69.132.1...	192.168.1.43	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
469	31.739341	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=47/12032, ttl=5 (no response found...)
470	31.750631	118.69.132.1...	192.168.1.43	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
471	31.752103	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=48/12288, ttl=5 (no response found...)
472	31.761590	118.69.132.1...	192.168.1.43	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
535	42.002624	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=49/12544, ttl=6 (no response found...)
536	42.012319	118.69.189.63	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
537	42.013860	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=50/12800, ttl=6 (no response found...)
538	42.023887	118.69.189.63	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
539	42.025241	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=51/13056, ttl=6 (no response found...)
540	42.035849	118.69.189.63	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
657	52.405961	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=52/13312, ttl=7 (no response found...)
658	52.414854	123.29.16.13	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

icmp						
No.	Time	Source	Destination	Protoc	Len	Info
5	0.027255	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=34/8704, ttl=1 (no response found!)
6	0.031065	192.168.1.1	192.168.1.43	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
7	0.031847	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=35/8960, ttl=1 (no response found!)
8	0.033207	192.168.1.1	192.168.1.43	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
9	0.033949	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=36/9216, ttl=1 (no response found!)
10	0.035276	192.168.1.1	192.168.1.43	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
13	1.053424	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=2 (no response found!)
14	1.056614	100.123.0.76	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
15	1.058140	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=38/9728, ttl=2 (no response found!)
16	1.061117	100.123.0.76	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
17	1.062437	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=39/9984, ttl=2 (no response found!)
18	1.067232	100.123.0.76	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
65	11.092011	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=40/10240, ttl=3 (no response found...)
66	11.105604	118.69.189.24	192.168.1.43	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
67	11.106451	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=41/10496, ttl=3 (no response found...)
68	11.116502	118.69.189.24	192.168.1.43	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
69	11.117999	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=42/10752, ttl=3 (no response found...)
70	11.126439	118.69.189.24	192.168.1.43	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
208	21.662979	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=43/11008, ttl=4 (no response found...)
659	52.415598	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=53/13568, ttl=7 (no response found...)
660	52.424701	123.29.16.13	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
661	52.425782	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=54/13824, ttl=7 (no response found...)
662	52.434882	123.29.16.13	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
678	53.545874	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=55/14080, ttl=8 (no response found...)
679	53.556173	113.171.7.209	192.168.1.43	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
680	53.557788	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=56/14336, ttl=8 (no response found...)
681	53.567533	113.171.7.209	192.168.1.43	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
682	53.569147	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=57/14592, ttl=8 (no response found...)
683	53.578861	113.171.7.209	192.168.1.43	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
694	54.628829	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=58/14848, ttl=9 (no response found...)
695	54.637917	113.171.44.1...	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
696	54.639437	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=59/15104, ttl=9 (no response found...)
697	54.649100	113.171.44.1...	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
698	54.650485	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=60/15360, ttl=9 (no response found...)
699	54.659818	113.171.44.1...	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
711	55.770335	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=61/15616, ttl=10 (no response found...)
712	55.783001	113.171.48.2...	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
713	55.784541	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=62/15872, ttl=10 (no response found...)

714	55.793659	113.171.48.2...	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)	
715	55.795084	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request	id=0x0001, seq=63/16128, ttl=10 (no response foun...
716	55.809873	113.171.48.2...	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)	
725	56.897746	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request	id=0x0001, seq=64/16384, ttl=11 (no response foun...
775	60.816236	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request	id=0x0001, seq=65/16640, ttl=11 (no response foun...
804	64.816318	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request	id=0x0001, seq=66/16896, ttl=11 (no response foun...
823	68.821652	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request	id=0x0001, seq=67/17152, ttl=12 (reply in 825)
825	68.833028	14.161.23.204	192.168.1.43	ICMP	106	Echo (ping) reply	id=0x0001, seq=67/17152, ttl=53 (request in 823)
826	68.834046	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request	id=0x0001, seq=68/17408, ttl=12 (reply in 827)
827	68.844950	14.161.23.204	192.168.1.43	ICMP	106	Echo (ping) reply	id=0x0001, seq=68/17408, ttl=53 (request in 826)
828	68.845812	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request	id=0x0001, seq=69/17664, ttl=12 (reply in 829)
829	68.863939	14.161.23.204	192.168.1.43	ICMP	106	Echo (ping) reply	id=0x0001, seq=69/17664, ttl=53 (request in 828)

Hình 32. Bắt các gói tin trong wireshark.

– Câu 2:

Lệnh **tracert/traceroute** là một công cụ để truy vết để chẩn đoán mạng máy tính, có công dụng hiển thị các tuyến đường (đường dẫn từ **source** đến **destination**) và đo lường sự chậm trễ của các gói dữ liệu trên một giao thức Internet.

– Câu 3:

Địa chỉ IP của máy gửi request : **192.168.1.43**.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.027255	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=34/8704, ttl=1 (no response found!)

```

Wireless LAN adapter Wi-Fi:

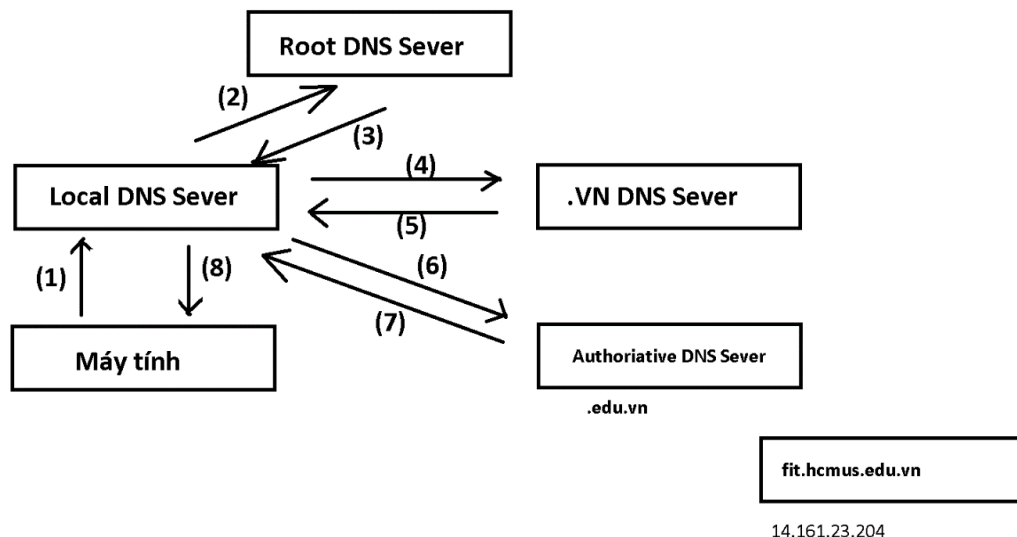
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2405:4800:6299:c5e:6d14:4a76:ba96:7099
    IPv6 Address. . . . . : 2405:4800:6299:c5e:ffff:ffff:ffff:ff9e
    Temporary IPv6 Address. . . . . : 2405:4800:6299:c5e:6116:621d:4bff:ee4b
    Link-local IPv6 Address . . . . . : fe80::6d14:4a76:ba96:7099%13
    IPv4 Address. . . . . : 192.168.1.43
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%13
                                192.168.1.1

```

Hình 33. Địa chỉ IPv4 của máy gửi request.

– Câu 4:

Để xác định địa chỉ IP của FIT máy tính sử dụng hệ thống phân giải tên miền DNS từ URL: www.fit.hcmus.edu.vn (FIT)



Hình 34. Minh họa hoạt động của DNS.

- (1): **Máy tính** sẽ tìm IP của FIT trong **cache memory** của máy, nếu không có máy sẽ tìm tiếp trên **local DNS server**.
- (2): Nếu không tìm được IP của FIT tại **cache memory** của **local DNS server** thì nó sẽ truy vấn lên **root DNS server**.
- (3): **Root DNS server** sẽ điều hướng nơi cần truy vấn tiếp theo về lại **local DNS server**.
- (4): Local DNS sever sẽ gửi truy vấn đến .vn DNS sever.
- (5): **.vn DNS server** sẽ gửi thông tin điều hướng đến nơi cuối cùng về lại **local DNS server**.
- (6): **Local DNS server** gửi truy vấn về FIT đến **authoritative DNS server**.
- (7): **Authoriative DNS server** sẽ tìm địa chỉ IP của FIT và gửi lại cho **local DNS server**.
- (8): **Máy tính** sẽ nhận được địa chỉ IP của FIT từ **local DNS server**.

– **Câu 5:**

- a) Protocol được sử dụng của những gói tin đó là: **ICMP**.
- b)

No.	Time	Source	Destination	Proto	Len	Info
471	31.752103	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=48/12288, ttl=5 (no response found...
535	42.002624	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=49/12544, ttl=6 (no response found...
537	42.013860	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=50/12800, ttl=6 (no response found...
539	42.025241	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=51/13056, ttl=6 (no response found...
657	52.405961	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=52/13312, ttl=7 (no response found...
659	52.415598	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=53/13568, ttl=7 (no response found...
661	52.425782	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=54/13824, ttl=7 (no response found...
678	53.545874	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=55/14080, ttl=8 (no response found...
680	53.557788	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=56/14336, ttl=8 (no response found...
682	53.569147	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=57/14592, ttl=8 (no response found...
694	54.628829	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=58/14848, ttl=9 (no response found...
696	54.639437	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=59/15104, ttl=9 (no response found...
698	54.650485	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=60/15360, ttl=9 (no response found...
711	55.770335	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=61/15616, ttl=10 (no response found...
713	55.784541	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=62/15872, ttl=10 (no response found...
715	55.795084	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=63/16128, ttl=10 (no response found...
725	56.897746	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=64/16384, ttl=11 (no response found...
775	60.816236	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=11 (no response found...
804	64.816318	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=11 (no response found...

Hình 35. Giao thức ICMP.

Số lượng gói tin được gửi đi trước khi nhận được response đầu tiên trả lời là:

$$11 \times 3 + 1 = 34 \text{ (gói tin)}$$

- c) TTL của gói tin cuối cùng được gửi đi trước khi nhận được gói tin response đầu tiên trả lời là: 12.

715	55.795084	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=63/16128, ttl=10 (no response found...
716	55.809873	113.171.48.2...	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
725	56.897746	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=64/16384, ttl=11 (no response found...
775	60.816236	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=11 (no response found...
804	64.816318	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=11 (no response found...
823	68.821652	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=12 (reply in 825)
825	68.833028	14.161.23.204	192.168.1.43	ICMP	106	Echo (ping) reply id=0x0001, seq=67/17152, ttl=53 (request in 823)
826	68.834046	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=12 (reply in 827)

Hình 36.

- d) Không thấy thông tin **port** trong các gói tin gửi đi vì giao thức **ICMP** nằm trong **tầng Internet** nằm dưới **tầng Transport** trong mô hình TCP/IP.

- e) Gói tin response đầu tiên là **trả lời cho gói tin request thứ 34** (gói tin No. 823).

No.	Time	Source	Destination	Proto	Len	Info
716	55.809873	113.171.48.2...	192.168.1.43	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
725	56.897746	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=64/16384, ttl=11 (no response found...
775	60.816236	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=11 (no response found...
804	64.816318	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=11 (no response found...
823	68.821652	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=12 (reply in 825)
825	68.833028	14.161.23.204	192.168.1.43	ICMP	106	Echo (ping) reply id=0x0001, seq=67/17152, ttl=53 (request in 823)
826	68.834046	192.168.1.43	14.161.23.204	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=12 (reply in 827)

Hình 37.

• BÀI 4:

Hệ điều hành: Windows

– Câu 1:

Đây là hình ảnh những gói tin DHCP bắt được trong quá trình release và renew:

No.	Time	Source	Destination	Protocol	Length	Info
754	7.754920	192.168.1.6	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x94d3f66b
2400	17.230999	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xba000817
2401	17.235881	192.168.1.1	192.168.1.6	DHCP	326	DHCP Offer - Transaction ID 0xba000817
2402	17.237599	0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0xba000817
2403	17.243324	192.168.1.1	192.168.1.6	DHCP	326	DHCP ACK - Transaction ID 0xba000817

> Frame 754: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{EEB8BBD8-690D-40F6-84A4-A8B43F23D04} Ethernet II, Src: IntelCor_ae:6a:c8 (a8:7e:ea:ae:6a:c8), Dst: VnptTech_a5:09:8c (a4:f4:c2:a5:09:8c)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Release)

Hình 38. Những gói tin DHCP bắt được.

– Câu 2:

DHCP message dùng giao thức UDP tại tầng transport.

DHCP không thể sử dụng TCP là giao thức truyền tải vì TCP bắt buộc 2 máy đầu-cuối phải có địa chỉ IP duy nhất cho mỗi máy. Tại thời điểm một client được yêu cầu sử dụng DHCP, do nó chưa được cấu hình địa chỉ IP nên nó không có địa chỉ IP mà nó có thể lấy các gói tin, cũng như không có địa chỉ IP của DHCP server. Vì vậy các client sử dụng 0.0.0.0 làm địa chỉ IP nguồn và 255.255.255.255 (broadcast) như địa chỉ IP đích. Các địa chỉ IP này không phải địa chỉ IP hợp lệ cho host và nhiều host có thể sử dụng bất cứ lúc nào. Vì vậy kết nối TCP sẽ không phù hợp vì bản chất của TCP là giao thức hướng kết nối, phải là mối quan hệ 1:1 nên sẽ không phù hợp.

Nhưng ngay cả khi xác định được hướng kết nối, thì dữ liệu của gói tin DHCP khá nhỏ (~300 bytes), việc sử dụng TCP là lãng phí.

UDP là giao thức phi kết nối. Giao thức UDP dành cho dữ liệu ứng dụng đủ đơn giản để không yêu cầu độ tin cậy và kiểm soát luồng như TCP. Phù hợp dịch vụ DHCP.

No.	Time	Source	Destination	Protocol	Length	Info
754	7.754920	192.168.1.6	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x94d3f66b
2400	17.230999	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xba000817
2401	17.235881	192.168.1.1	192.168.1.6	DHCP	326	DHCP Offer - Transaction ID 0xba000817
2402	17.237599	0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0xba000817
2403	17.243324	192.168.1.1	192.168.1.6	DHCP	326	DHCP ACK - Transaction ID 0xba000817

Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.1
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 328
Identification: 0xcb7e (52094)
> Flags: 0x00
Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.6
Destination Address: 192.168.1.1

Hình 39. DHCP sử dụng giao thức UDP ở tầng transport.

– **Câu 3:**

- Mục đích của DHCP Release nhằm cho DHCP Server biết rằng DHCP Client đã sử dụng địa chỉ IP, đây là thông điệp khi client trả lại địa chỉ IP cho DHCP Server khi DHCP Server nhận được thông báo release từ client. Sau đó, DHCP Server sẽ ghi lại rằng địa chỉ IP này trống và có thể gán cho các client khác.
- Client không thể đảm bảo chắc chắn rằng lúc nào cũng nhận được ACK message của server, vì DHCP dùng giao thức UDP, không đảm bảo tính tin cậy khi truyền dữ liệu và không chắc chắn rằng gói tin có đến đích hay không hay đã bị mất mát trên đường truyền.
- Nếu DHCP release message bị mất thì khi client trả lại địa chỉ IP cho server thì server sẽ không thể gán địa chỉ IP đó cho máy khác cho đến khi địa chỉ IP đó đã hết thời gian cấp phát vì server không nhận được thông điệp trả lại địa chỉ IP của client đã sử dụng trước đó.

– **Câu 4:**

- a) Theo yêu cầu của đề bài và dải địa chỉ IP được cấp phát thì sẽ có 91 vị khách có thể truy cập Internet của quán cà phê khi IP chưa hết thời gian cấp phát mà không gặp vấn đề gì. Tới vị khách thứ 92, do địa chỉ IP đã được cấp phát và thời gian cấp địa chỉ IP là 8 tiếng mà từ 7:00 AM đến 11:00 AM thì mới có 4 tiếng và các vị khách đã rời quán cà phê không trả lại địa chỉ IP cho DHCP Server (ngay cả khi client đã ngắt kết nối thì DHCP Server vẫn nhớ là địa chỉ IP đó đã cấp phát để tránh xung đột) nên địa chỉ IP đó vẫn còn đang sử dụng, nên vị khách thứ 92 sẽ không thể truy cập Internet của quán cà phê.
- b) Vậy những vị khách thứ 93, 94, ... có khả năng không truy cập được mạng Internet, tùy vào thời điểm mà các vị khách truy cập. Ví dụ như truy cập trong khoảng từ 7:00 đến 3:00 PM thì khả năng lớn là sẽ không truy cập được trong khoảng thời gian này vì địa chỉ IP đang được cấp phát và chưa đến thời gian tự release. Sau 3:00 PM, nếu có một số địa chỉ IP tự release và trả về cho DHCP Server thì các vị khách 92, 93, 94, ... có thể truy cập Internet bình thường.
- c) Để vị khách thứ 92 có thể truy cập được Internet thì hướng giải quyết tình thế là rút dây nguồn router hoặc reset router và cắm lại. Router khi đó sẽ release toàn bộ địa chỉ IP và cấp phát lại từ đầu, kể cả những địa chỉ IP đã cấp phát trước đó cho client nhưng sau đó client ngắt kết nối (vì trong đề chỉ có 20 vị khách đang truy cập Internet tại thời điểm 11:00 AM). Khi đó vị khách thứ 92 có thể truy cập Internet của quán cà phê bình thường.

Hướng giải quyết lâu dài là quán cà phê nên nâng cấp DHCP Server để server có thể tăng range địa chỉ IP lên và giảm thời gian cấp phát IP xuống. Như vậy số khách truy

cập được Internet sẽ nhiều hơn và sự trả lại địa chỉ IP cho server sau khi hết thời gian cấp phát sẽ sớm hơn.

TÀI LIỆU THAM KHẢO

V. TÀI LIỆU THAM KHẢO

Kích thước gói ICMP: <https://www.youtube.com/watch?v=lJnU8w4ALY0>.

ARP and ping packets: <https://www.youtube.com/watch?v=xNbdeyEI-nE>.

Traceroute: <https://www.youtube.com/watch?v=up3bcBLZS74&t=4s>.

HTTP Lab: <https://youtu.be/yfi7w9p3QnU>.