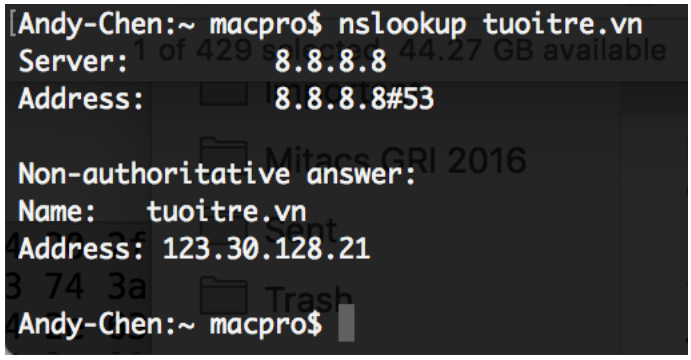
Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

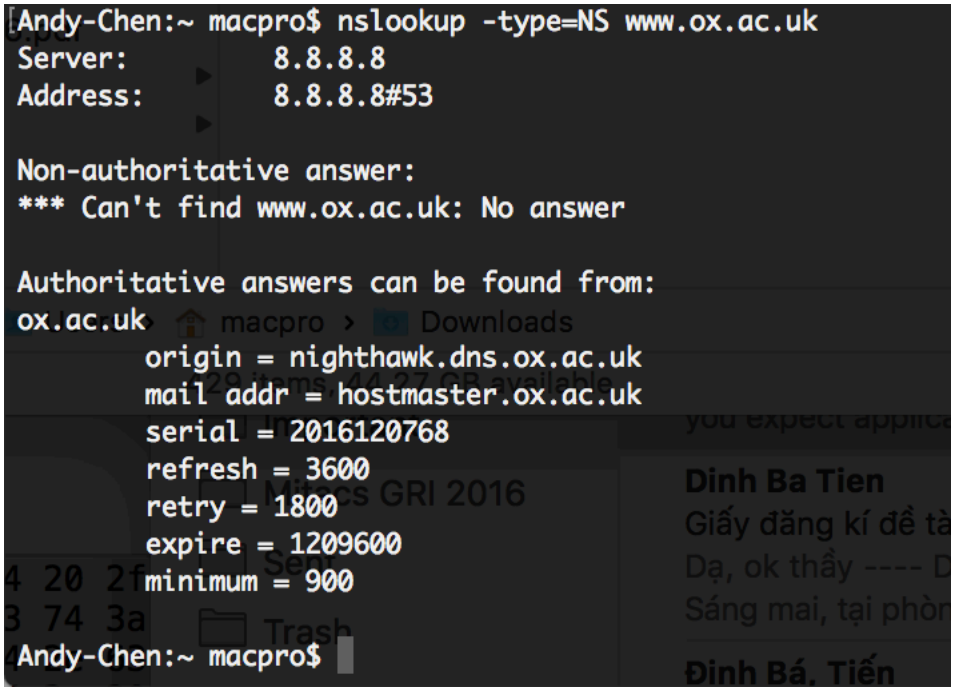
Wireshark DNS

[1] Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?



Target web server is tuoitre.vn
The IP address is 123.30.128.21

[2] Run nslookup to determine the authoritative DNS servers for a university in Europe.



Target web server is www.ox.ac.uk
The authoritative DNS server is nighthawk.dns.ox.ac.uk

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

[3] Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Selected DNS server of Oxford University: nighthawk.dns.ox.ac.uk

```
[Andy-Chen:~ macpro$ nslookup nighthawk.dns.ox.ac.uk mail.yahoo.com ]
;; connection timed out; no servers could be reached
```

I did not get any result from **mail.yahoo.com**. Thus, I use **8.8.8.8** (Google DNS server) instead.

```
[Andy-Chen:~ macpro$ nslookup nighthawk.dns.ox.ac.uk 8.8.8.8        ]
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   nighthawk.dns.ox.ac.uk
Address: 163.1.2.189
```

The IP address is **163.1.2.189**

[4] Locate the DNS query and response messages. Are then sent over UDP or TCP?

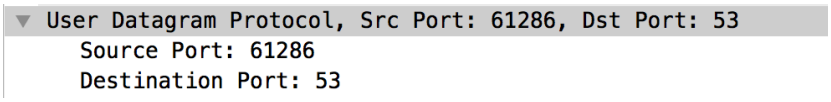
No.	Time	Source	Destination	Prot ▲	Length	Info
418	10.813527	192.168.2.102	255.255.255.2…	DB-…	234	Dropbox LAN sync Discovery Protocol
419	10.813796	192.168.2.102	192.168.2.255	DB-…	234	Dropbox LAN sync Discovery Protocol
228	6.158821	192.168.2.102	8.8.8.8	DNS	73	Standard query 0x4536 A www6.ietf.org
233	6.169619	192.168.2.102	8.8.8.8	DNS	80	Standard query 0xef51 A datatracker.ietf.c
234	6.169803	192.168.2.102	8.8.8.8	DNS	73	Standard query 0x86ff A iaoc.ietf.org
235	6.170057	192.168.2.102	8.8.8.8	DNS	80	Standard query 0xce80 A mailarchive.ietf.c
266	6.236720	8.8.8.8	192.168.2.102	DNS	110	Standard query response 0xef51 A datatrack
271	6.238465	192.168.2.102	8.8.8.8	DNS	74	Standard query 0x8412 A rfc-editor.org
272	6.245168	8.8.8.8	192.168.2.102	DNS	103	Standard query response 0x86ff A iaoc.iet
276	6.247174	192.168.2.102	8.8.8.8	DNS	74	Standard query 0x113a A tools.ietf.org
278	6.302794	8.8.8.8	192.168.2.102	DNS	90	Standard query response 0x8412 A rfc-editc
279	6.304006	192.168.2.102	8.8.8.8	DNS	76	Standard query 0x997f A trustee.ietf.org

```
▶ Frame 228: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▶ Ethernet II, Src: Apple_d0:11:b2 (78:31:c1:d0:11:b2), Dst: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
▶ Internet Protocol Version 4, Src: 192.168.2.102, Dst: 8.8.8.8
▼ User Datagram Protocol, Src Port: 61286, Dst Port: 53
    Source Port: 61286
    Destination Port: 53
    Length: 39
    Checksum: 0xef19 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
▶ Domain Name System (query)
```

Sent over **UDP**

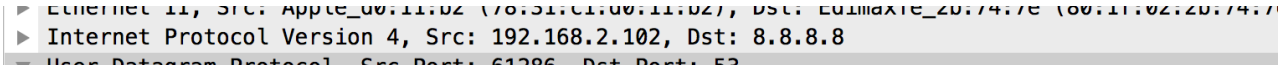
Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

[5] What is the destination port for the DNS query message? What is the source port of DNS response message?



Destination port: 53
Source port: 61286

[6] To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?



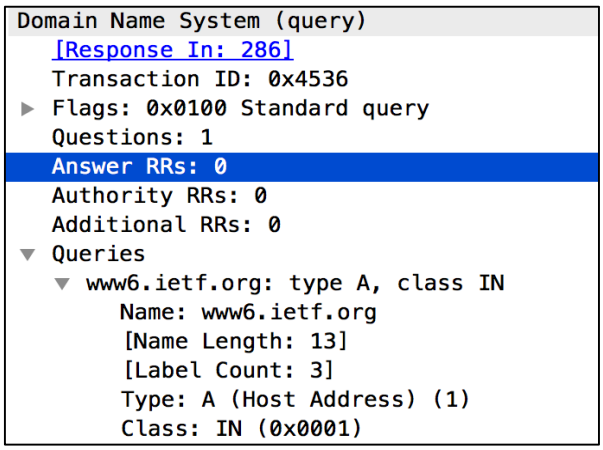
The DNS query message was sent: 8.8.8.8

(There is no command like ipconfig /displaydns on macOS)
Local DNS server IP: 8.8.8.8 or 8.8.4.4

- The two IP addresses are the same

[7] Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Type of DNS query: A
It does not contain any "answers".



Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

[8] Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

```
Domain Name System (response)
   [Request In: 228]
   [Time: 0.497701000 seconds]
   Transaction ID: 0x4536
▶  Flags: 0x8180 Standard query response, No error
   Questions: 1
   Answer RRs: 2
   Authority RRs: 0
   Additional RRs: 0
▶  Queries
▼  Answers
   ▼ www6.ietf.org: type CNAME, class IN, cname ietf.org
        Name: www6.ietf.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1799
        Data length: 2
        CNAME: ietf.org
   ▼ ietf.org: type A, class IN, addr 4.31.198.44
        Name: ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1799
        Data length: 4
        Address: 4.31.198.44
```

There are 2 answers:

- The 1st one contains the Canonical name of the queried website, the Class, Type of Answer, TTL, Data length.
- The 2nd one contains the Host Name and IP address of the queried website, the Class, Type of Answer, TTL, Data length.
-

[9] Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

```
286 6.656522    8.8.8.8         192.168.2.102   DNS     103 Standard query response 0x4536 A www6.ie
287 6.657806    192.168.2.102   4.31.198.44     TCP      78 50410→80 [SYN] Seq=0 Win=65535 Len=0 MSS
```

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

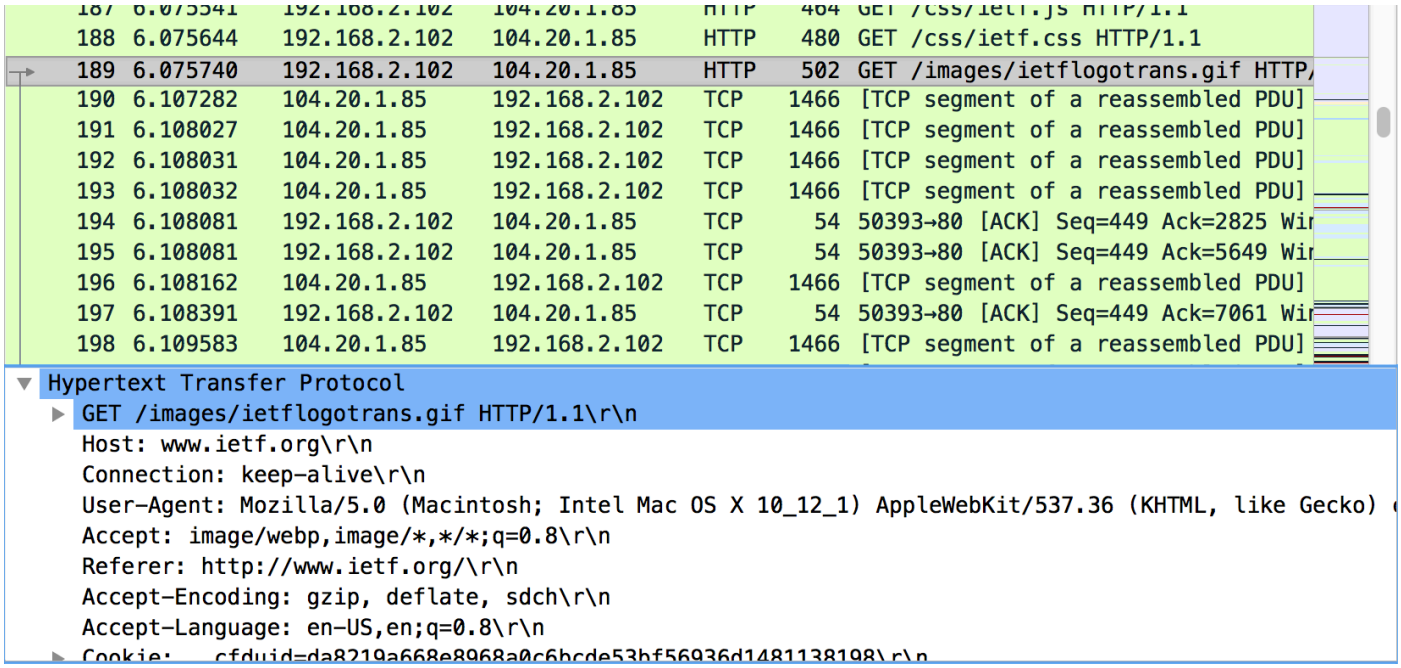
The destination IP address of the subsequent TCP SYN (of the DNS response message): **4.31.198.44**

```
▼ ietf.org: type A, class IN, addr 4.31.198.44
    Name: ietf.org
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 1799
    Data length: 4
    Address: 4.31.198.44
```

The IP address of the 2nd answer from DNS response message: **4.31.198.44**

- The destination IP address of the SYN packet correspond to one of the IP addresses provided in the DNS response message

[10] This web page contains images. Before retrieving each image, does your host issue new DNS queries?



- No, the images are all loaded from www.ietf.org, so no additional DNS queries are necessary (the host uses a cached address).

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

[11] What is the destination port for the DNS query message? What is the source port of DNS response message?

```
   12 4.858607    192.168.2.102   8.8.8.8         DNS      71 Standard query 0x0cbe A www.mi
   13 4.982116    8.8.8.8         192.168.2.102   DNS     160 Standard query response 0x0cbe
    6 1.554712    192.168.2.102   239.192.152.1…  IGM…     46 Membership Report group 239.19
Internet Protocol Version 4, Src: 192.168.2.102, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 62054, Dst Port: 53
   Source Port: 62054
   Destination Port: 53
   Length: 37
```

Source port: 62054
Destination port: 53

[12] To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

```
   12 4.858607    192.168.2.102   8.8.8.8         DNS      71 Standard query 0x0cbe A www.mi
   13 4.982116    8.8.8.8         192.168.2.102   DNS     160 Standard query response 0x0cbe
    6 1.554712    192.168.2.102   239.192.152.1…  IGM…     46 Membership Report group 239.19
Internet Protocol Version 4, Src: 192.168.2.102, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 62054, Dst Port: 53
   Source Port: 62054
   Destination Port: 53
   Length: 37
```

It sends to 8.8.8.8

```
Andy-Chen:~ macpro$ networksetup -getdnsservers Wi-Fi
8.8.8.8
8.8.4.4
```

My local DNS server: 8.8.8.8

- The 2 IP addresses are the same

[13] Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Type of DNS query: A
It does not contain any "answers".

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

```
Domain Name System (query)
    [Response In: 13]
    Transaction ID: 0x0cbe
▶   Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
▼   Queries
  ▼   www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

[14] Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

```
Domain Name System (response)
    [Request In: 12]
    [Time: 0.123509000 seconds]
    Transaction ID: 0x0cbe
▶   Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
▶   Queries
▼   Answers
  ▼   www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 800
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
  ▼   www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 59
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
  ▼   e9566.dscb.akamaiedge.net: type A, class IN, addr 23.198.138.27
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 19
        Data length: 4
        Address: 23.198.138.27
```

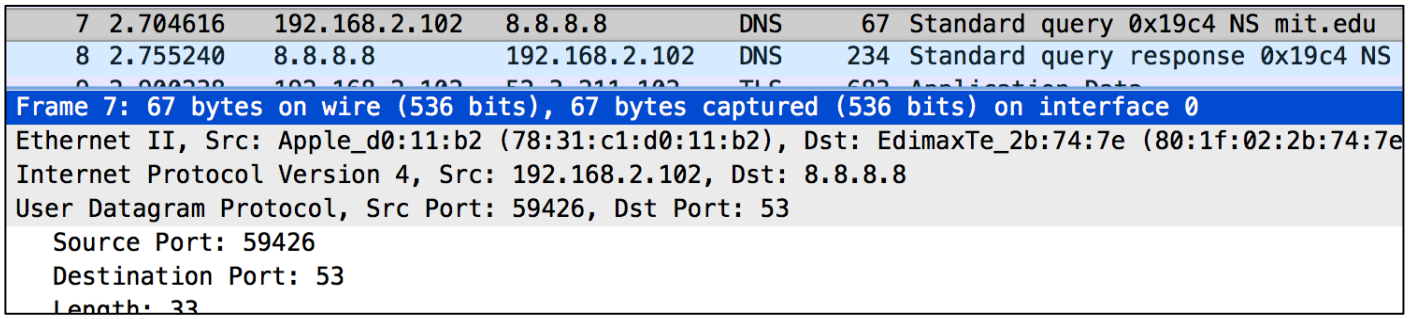
Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

There are 3 answers:

- The 1st and the 2nd ones contain the Canonical Name of the queried website, the Class, Type of Answer, TTL, Data length.
- The 3rd one contains the Host Name and IP address of the queried website, the Class, Type of Answer, TTL, Data length.

[15] Provide a screenshot.

[16] To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



It sends to 8.8.8.8

My local DNS server: 8.8.8.8

➢ The 2 IP addresses are the same

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

[17] Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

```
Domain Name System (query)
    [Response In: 8]
    Transaction ID: 0x19c4
▶   Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
▼   Queries
    ▼ mit.edu: type NS, class IN
          Name: mit.edu
          [Name Length: 7]
          [Label Count: 2]
          Type: NS (authoritative Name Server) (2)
          Class: IN (0x0001)
```

Type of DNS query: NS
It does not contain any "answers".

[18] Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

```
Domain Name System (response)
    [Request In: 7]
    [Time: 0.050624000 seconds]
    Transaction ID: 0x19c4
▶   Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
▼   Queries
    ▼ mit.edu: type NS, class IN
          Name: mit.edu
          [Name Length: 7]
          [Label Count: 2]
          Type: NS (authoritative Name Server) (2)
          Class: IN (0x0001)
▼   Answers
    ▶ mit.edu: type NS, class IN, ns usw2.akam.net
    ▶ mit.edu: type NS, class IN, ns use2.akam.net
    ▶ mit.edu: type NS, class IN, ns use5.akam.net
    ▶ mit.edu: type NS, class IN, ns asia2.akam.net
    ▶ mit.edu: type NS, class IN, ns eur5.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-173.akam.net
    ▶ mit.edu: type NS, class IN, ns asia1.akam.net
```

It provides 6 nameservers as shown in the **Answers**

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

It does not provide the IP address of the MIT nameservers.

[19] Provide a screenshot.

I cannot perform:

nslookup www.aiit.or.kr bitsy.mit.edu

on my computer. Thus the following answers will be based on the trace file from another computer.

[20] To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

```
  104 4.293517    128.238.38.160  18.72.0.3       DNS      74 Standard query 0x0003 A www.aiit.or.k
  105 4.307859    18.72.0.3       128.238.38.160  DNS     156 Standard query response 0x0003 A www.
Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: IbmCorp_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00
Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
User Datagram Protocol, Src Port: 3753, Dst Port: 53
   Source Port: 3753
   Destination Port: 53
   Length: 40
```

It sends to IP address: 18.72.0.3, which is not my default local DNS server (in the case of the trace file).

```
Andy-Chen:~ macpro$ nslookup bitsy.mit.edu
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   bitsy.mit.edu
Address: 18.72.0.3
```

Instead, it corresponds to the IP address of bitsty.mit.edu

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

[21] Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

```
  104 4.293517    128.238.38.160  18.72.0.3       DNS      74 Standard query 0x0003 A www.aiit.or.k
  105 4.307859    18.72.0.3       128.238.38.160  DNS     156 Standard query response 0x0003 A www.a
   41 1.866140    128.238.38.2    224.0.0.2       HSRP     62 Hello (state Active)
Domain Name System (query)
    [Response In: 105]
    Transaction ID: 0x0003
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Type: A
The message contains no answer.

[22] Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

```
  105 4.307859    18.72.0.3       128.238.38.160  DNS     156 Standard query response 0x0003 A w
   41 1.866140    128.238.38.2    224.0.0.2       HSRP     62 Hello (state Active)
Domain Name System (response)
    [Request In: 104]
    [Time: 0.014342000 seconds]
    Transaction ID: 0x0003
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  ▶ Queries
  ▼ Answers
    ▼ www.aiit.or.kr: type A, class IN, addr 218.36.94.200
        Name: www.aiit.or.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3338
        Data length: 4
        Address: 218.36.94.200
```

It contains 1 answer. The answer contains the Host Name and the IP address, TTL, Data length, Class, Type.

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

[23] Provide a screenshot.