

# 计算机网络实验 3

傅申 PB20000051

## 1. nslookup

```
→ ~ nslookup www.tsinghua.edu.cn
Server:      202.38.64.56
Address:     202.38.64.56#53

Non-authoritative answer:
Name:   www.tsinghua.edu.cn
Address: 166.111.4.100
Name:   www.tsinghua.edu.cn
Address: 2402:f000:1:404:166:111:4:100

→ ~ nslookup -type=NS www.ucl.ac.uk
Server:      202.38.64.56
Address:     202.38.64.56#53

Non-authoritative answer:
www.ucl.ac.uk canonical name = www.ucl.ac.uk.cdn.cloudflare.net.

Authoritative answers can be found from:
cloudflare.net
    origin = ns1.cloudflare.net
    mail addr = dns.cloudflare.com
    serial = 1665079449
    refresh = 10000
    retry = 2400
    expire = 604800
    minimum = 3600

→ ~ nslookup mail.yahoo.com ns1.cloudflare.com
Server:      ns1.cloudflare.com
Address:     173.245.58.100#53

** server can't find mail.yahoo.com: NXDOMAIN

→ ~ nslookup mail.yahoo.com mx.ustc.edu.cn
Server:      mx.ustc.edu.cn
Address:     2001:da8:d800::56#53

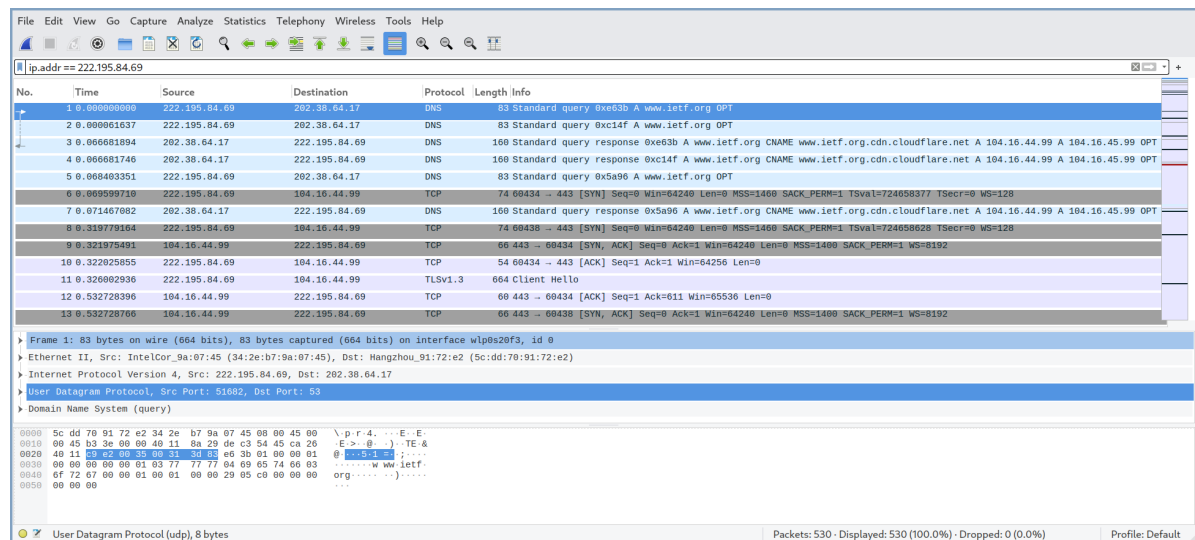
Non-authoritative answer:
mail.yahoo.com canonical name = edge.gycpi.b.yahoodns.net.
Name:   edge.gycpi.b.yahoodns.net
Address: 69.147.80.12
Name:   edge.gycpi.b.yahoodns.net
Address: 69.147.80.15
Name:   edge.gycpi.b.yahoodns.net
Address: 2001:4998:64:800::6001
Name:   edge.gycpi.b.yahoodns.net
Address: 2001:4998:64:800::6000

→ ~
```

1. 查询到清华大学网络服务器的 IP 地址为 166.111.4.100 (IPv4) 和 2402:f000:1:404:166:111:4:100 (IPv6).
2. UCL 的权威 DNS 服务器为 ns1.cloudflare.com.
3. (cloudflare 的 DNS 服务器查不到, 换成科大的了) Yahoo! 邮件的 IP 地址有 69.147.80.12, 69.147.80.15, 2001:4998:64:800::6001 和 2001:4998:64:800::6000.

### 3. Tracing DNS with Wireshark

#### Problem 4 - 10



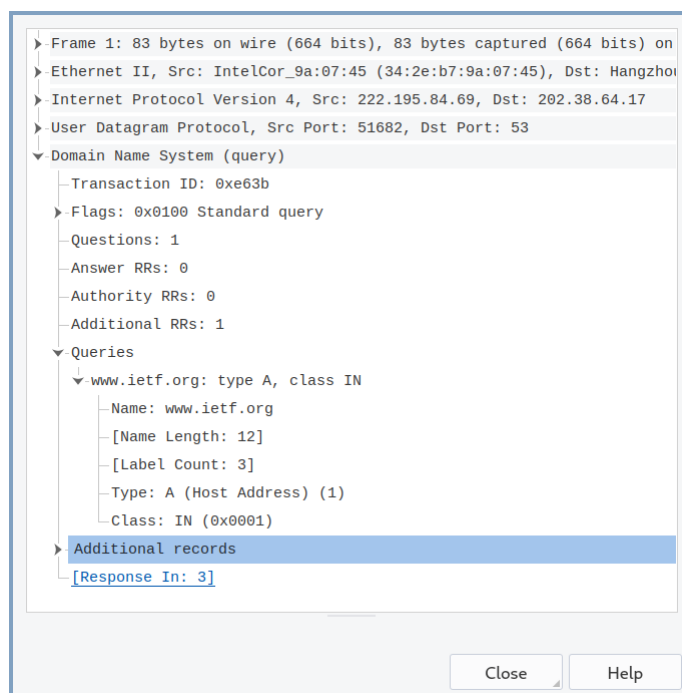
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	222.195.84.69	202.38.64.17	DNS	83	Standard query 0xe63b A www.ietf.org OPT
2	0.00001637	222.195.84.69	202.38.64.17	DNS	83	Standard query 0xc14f A www.ietf.org OPT
3	0.006681894	202.38.64.17	222.195.84.69	DNS	160	Standard query response 0xe63b A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99 OPT
4	0.006681746	202.38.64.17	222.195.84.69	DNS	160	Standard query response 0xc14f A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99 OPT
5	0.008403351	222.195.84.69	202.38.64.17	DNS	83	Standard query 0x5a96 A www.ietf.org OPT
6	0.009599710	222.195.84.69	104.16.44.99	TCP	74	60434 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=724658377 TSecr=0 WS=128
7	0.071467682	202.38.64.17	222.195.84.69	DNS	160	Standard query response 0x5a96 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99 OPT
8	0.319779164	222.195.84.69	104.16.44.99	TCP	74	60438 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=724658628 TSecr=0 WS=128
9	0.321975481	104.16.44.99	222.195.84.69	TCP	60	443 → 60434 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
10	0.322025855	222.195.84.69	104.16.44.99	TCP	54	60434 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
11	0.326092936	222.195.84.69	104.16.44.99	TLSv1.3	664	Client Hello
12	0.532728396	104.16.44.99	222.195.84.69	TCP	60	443 → 60434 [ACK] Seq=1 Ack=611 Win=65536 Len=0
13	0.532728766	104.16.44.99	222.195.84.69	TCP	60	443 → 60438 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192

打印的文件截图见 [Printouts](#).

4. UDP.
5. 查询报文的目的端口为 53 , 回答报文的源端口为 53 .
6. DNS 查询报文送到了 202.38.64.17 , 与本地 DNS 服务器的 IP 地址相同.

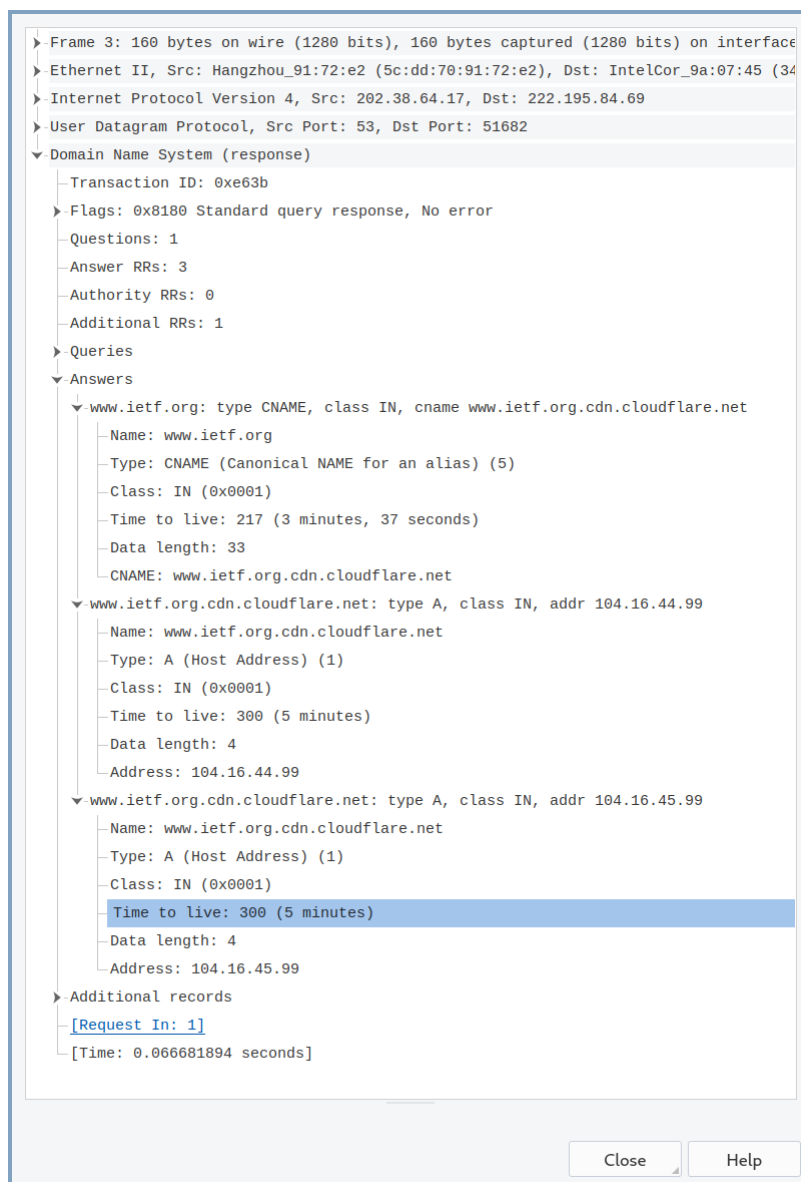
```
→ ~ cat /etc/resolv.conf
# Generated by NetworkManager
search ustc.edu.cn
nameserver 202.38.64.56
nameserver 202.38.64.17
→ ~ |
```

7. 以编号为 1 的查询报文为例: 类型为 A , 不包含回答.

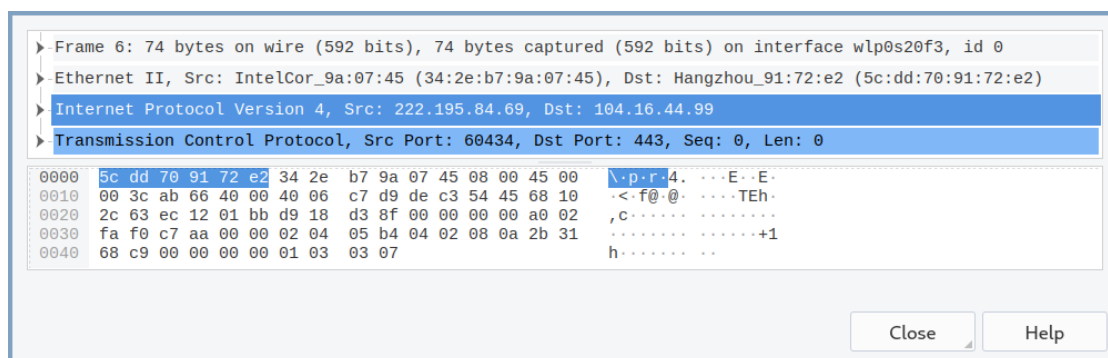


```
Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on
Ethernet II, Src: IntelCor_9a:07:45 (34:2e:b7:9a:07:45), Dst: Hangzhou
Internet Protocol Version 4, Src: 222.195.84.69, Dst: 202.38.64.17
User Datagram Protocol, Src Port: 51682, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0xe63b
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
    www.ietf.org: type A, class IN
      Name: www.ietf.org
      [Name Length: 12]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Additional records
    [Response In: 3]
```

8. 以编号为 3 的回答报文为例: 有 3 个回答, 第一个回答中有别名, 类别, TTL 和规范主机名, 后两个回答中有主机名, 类别, TTL 和 IP 地址.



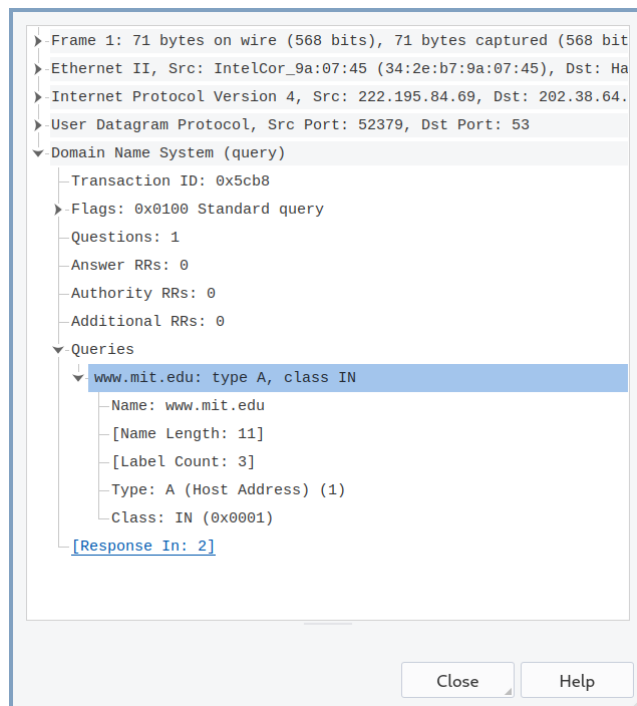
9. 以编号为 6 的 TCP SYN 包为例: 目的 IP 地址与 DNS 回答报文中的相同, 均为 104.16.44.99 .



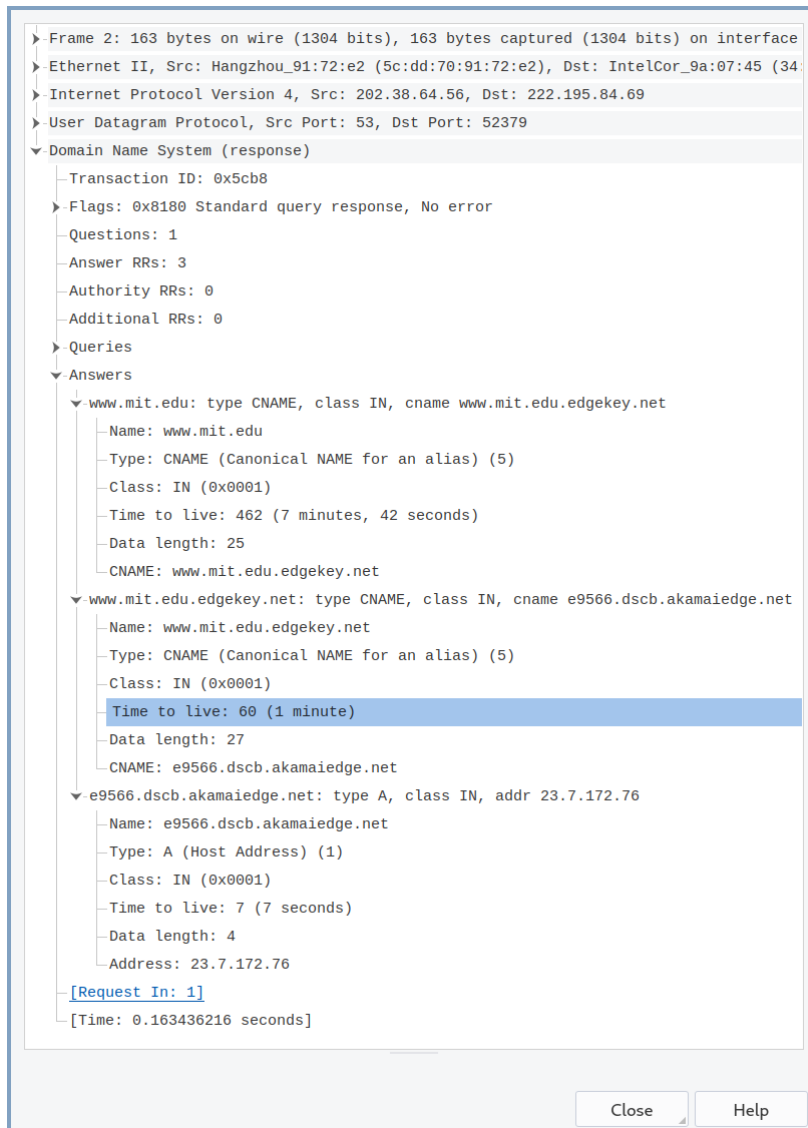
10. 没有, 因为网页中的图像都在 [www.ietf.org](http://www.ietf.org) 中.

## Problem 11 - 15

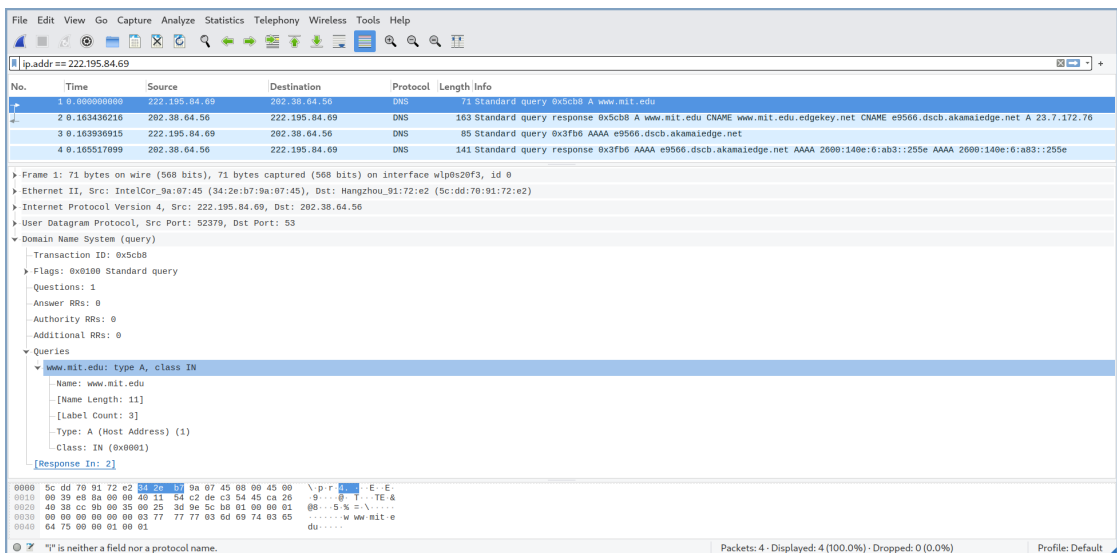
11. 查询报文的端口为 53 , 回答报文的源端口为 53 .
12. DNS 查询报文送到了 202.38.64.56 , 与本地 DNS 服务器的 IP 地址相同.
13. 类型为 A , 不包含回答.



14. 有 3 个回答, 前两个回答中有别名, 类别, TTL 和规范主机名, 最后一个回答中有主机名, 类别, TTL 和 IP 地址.



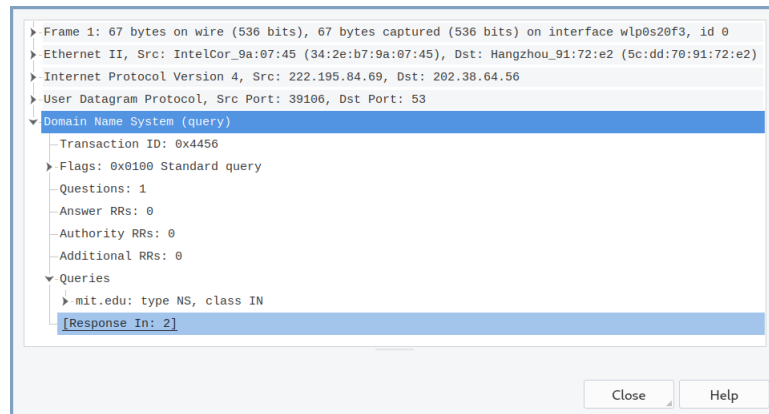
- 15.



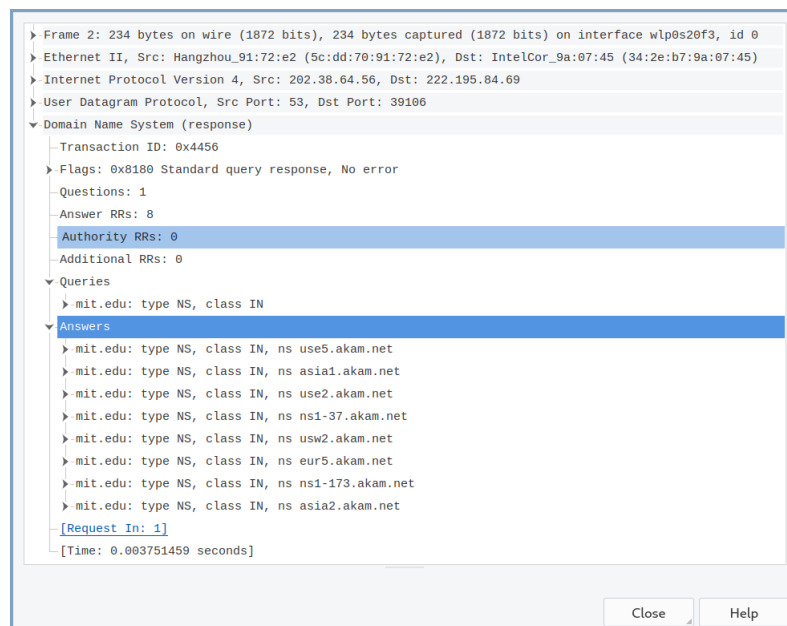
## Problem 16 - 19

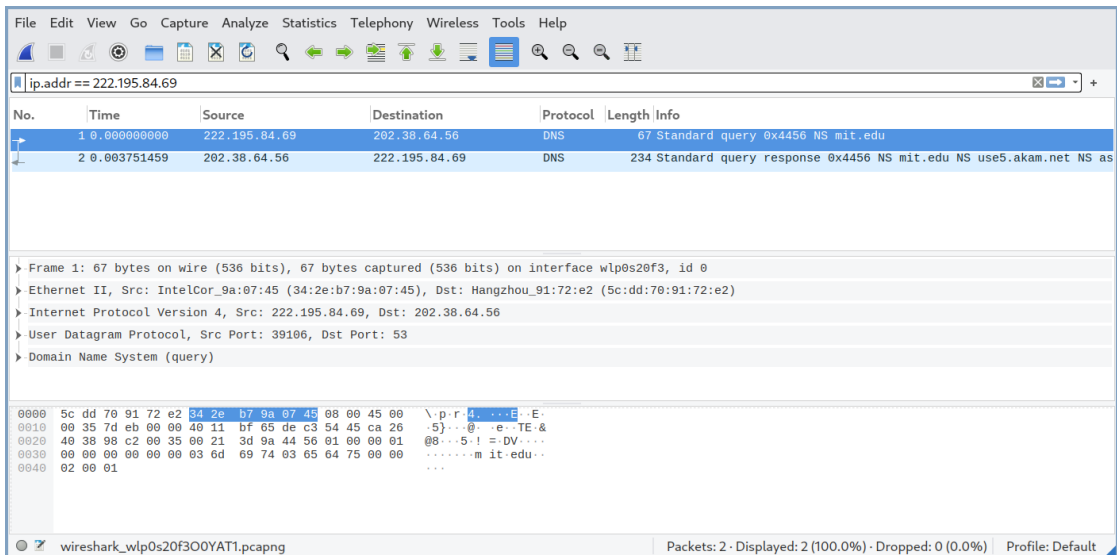
16. DNS 查询报文送到了 202.38.64.56 , 与本地 DNS 服务器的 IP 地址相同.

17. 类型为 NS , 不包含回答.



18. 回答报文提供了 use5.akam.net , asia1.akam.net , use2.akam.net , ns1-37.akam.net , usw2.akam.net , eur5.akam.net , ns1-173.akam.net , asia2.akam.net 共 8 个名称服务器, 没有提供 IP 地址.





## Problem 20 - 23

改用 Google 的 DNS 解析服务 [dns.google.com](https://dns.google.com).

```

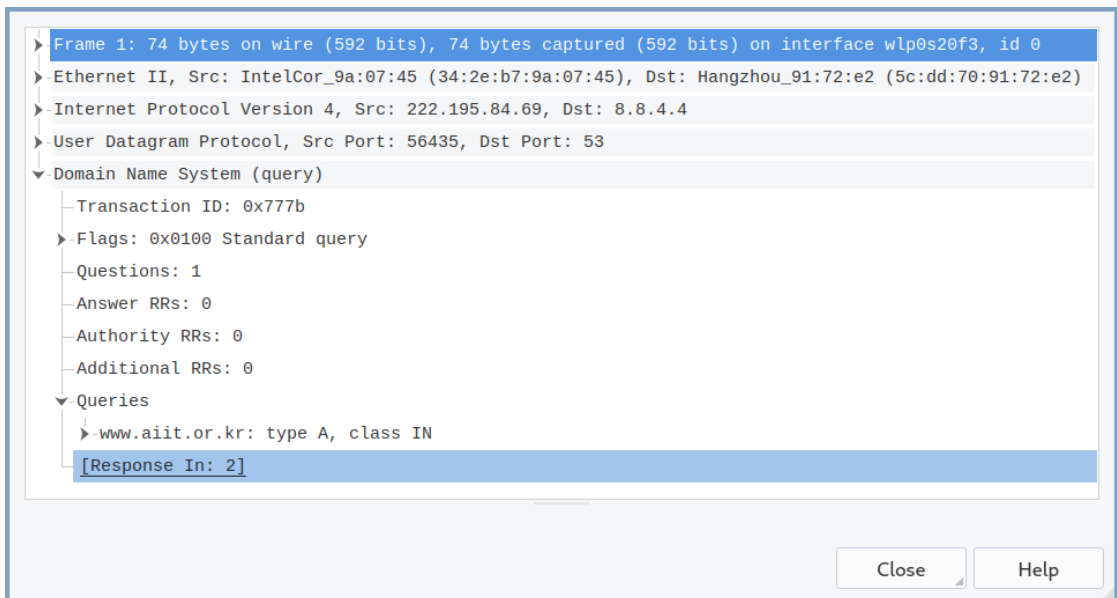
> ~ nslookup www.aiit.or.kr 8.8.4.4
Server:      8.8.4.4
Address:     8.8.4.4#53

Non-authoritative answer:
Name:   www.aiit.or.kr
Address: 58.229.6.225

> ~

```

20. DNS 查询报文送到了 **8.8.4.4**，与本地 DNS 服务器的 IP 地址不同, 它是 Google DNS 解析服务的地址.
21. 以编号为 1 的查询报文为例: 类型为 **A**，不包含回答.



22. 以编号为 2 的回答报文为例: 有 1 个回答, 包含了有主机名, 类别, TTL 和 IP 地址.

▶ Frame 2: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface wlp0s20f3, id 0  
 ▶ Ethernet II, Src: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor\_9a:07:45 (34:2e:b7:9a:07:45)  
 ▶ Internet Protocol Version 4, Src: 8.8.4.4, Dst: 222.195.84.69  
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 56435  
 ▶ Domain Name System (response)

- Transaction ID: 0x777b
- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- 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)
- Answers
  - [\[Request In: 1\]](#)
  - [Time: 0.183246172 seconds]

Close Help

23.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 222.195.84.69 && dns

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	222.195.84.69	8.8.4.4	DNS	74	Standard query 0x777b A www.aiit.or.kr
2	0.183246172	8.8.4.4	222.195.84.69	DNS	90	Standard query response 0x777b A www.aiit.or.kr A 58.229.6.225
3	0.183700182	222.195.84.69	8.8.4.4	DNS	74	Standard query 0xbe99 AAAA www.aiit.or.kr
4	0.387431184	8.8.4.4	222.195.84.69	DNS	128	Standard query response 0xbe99 AAAA www.aiit.or.kr SOA ns9.dnszi

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp0s20f3, id 0  
 ▶ Ethernet II, Src: IntelCor\_9a:07:45 (34:2e:b7:9a:07:45), Dst: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2)  
 ▶ Internet Protocol Version 4, Src: 222.195.84.69, Dst: 8.8.4.4  
 ▶ User Datagram Protocol, Src Port: 56435, Dst Port: 53  
 ▶ Domain Name System (query)

```

0000  5c dd 70 91 72 e2 34 2e b7 9a 07 45 08 00 45 00  \p.r.4. ...E.
0010  00 3c 96 af 00 00 40 11 a4 ed de c3 54 45 08 08  .<...@. ....TE.
0020  04 04 dc 73 00 35 00 28 3f 4e 77 7b 01 00 00 01  ...s.5( ?Nw{...
0030  00 00 00 00 00 00 03 77 77 77 04 01 69 69 74 02  ....w ww.aiit-
0040  0f 72 02 0b 72 00 00 01 00 01                   or.kr...
  
```

Domain Name System: Protocol      Packets: 10 · Displayed: 4 (40.0%) · Dropped: 0 (0.0%)      Profile: Default

```
/tmp/wireshark_wlp0s20f3A4N3S1.pcapng 530 total packets, 530 shown
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	222.195.84.69	202.38.64.17	DNS	83	Standard query 0xe63b A www.ietf.org
OPT						
Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface wlp0s20f3, id 0						
Ethernet II, Src: IntelCor_9a:07:45 (34:2e:b7:9a:07:45), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)						
Internet Protocol Version 4, Src: 222.195.84.69, Dst: 202.38.64.17						
User Datagram Protocol, Src Port: 51682, Dst Port: 53						
Domain Name System (query)						
No.	Time	Source	Destination	Protocol	Length	Info
2	0.000061637	222.195.84.69	202.38.64.17	DNS	83	Standard query 0xc14f A www.ietf.org
OPT						
Frame 2: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface wlp0s20f3, id 0						
Ethernet II, Src: IntelCor_9a:07:45 (34:2e:b7:9a:07:45), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)						
Internet Protocol Version 4, Src: 222.195.84.69, Dst: 202.38.64.17						
User Datagram Protocol, Src Port: 53462, Dst Port: 53						
Domain Name System (query)						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.066681894	202.38.64.17	222.195.84.69	DNS	160	Standard query response 0xe63b A
www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99 OPT						
Frame 3: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface wlp0s20f3, id 0						
Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor_9a:07:45 (34:2e:b7:9a:07:45)						
Internet Protocol Version 4, Src: 202.38.64.17, Dst: 222.195.84.69						
User Datagram Protocol, Src Port: 53, Dst Port: 51682						
Domain Name System (response)						
No.	Time	Source	Destination	Protocol	Length	Info
4	0.066681746	202.38.64.17	222.195.84.69	DNS	160	Standard query response 0xc14f A
www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99 OPT						
Frame 4: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface wlp0s20f3, id 0						
Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor_9a:07:45 (34:2e:b7:9a:07:45)						
Internet Protocol Version 4, Src: 202.38.64.17, Dst: 222.195.84.69						
User Datagram Protocol, Src Port: 53, Dst Port: 53462						
Domain Name System (response)						
No.	Time	Source	Destination	Protocol	Length	Info
5	0.068403351	222.195.84.69	202.38.64.17	DNS	83	Standard query 0x5a96 A www.ietf.org
OPT						
Frame 5: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface wlp0s20f3, id 0						
Ethernet II, Src: IntelCor_9a:07:45 (34:2e:b7:9a:07:45), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)						
Internet Protocol Version 4, Src: 222.195.84.69, Dst: 202.38.64.17						
User Datagram Protocol, Src Port: 55745, Dst Port: 53						
Domain Name System (query)						
No.	Time	Source	Destination	Protocol	Length	Info
6	0.069599710	222.195.84.69	104.16.44.99	TCP	74	60434 → 443 [SYN] Seq=0 Win=64240 Len=0
MSS=1460 SACK_PERM=1 TSval=724658377 TSecr=0 WS=128						
Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp0s20f3, id 0						
Ethernet II, Src: IntelCor_9a:07:45 (34:2e:b7:9a:07:45), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)						
Internet Protocol Version 4, Src: 222.195.84.69, Dst: 104.16.44.99						
Transmission Control Protocol, Src Port: 60434, Dst Port: 443, Seq: 0, Len: 0						
No.	Time	Source	Destination	Protocol	Length	Info
7	0.071467082	202.38.64.17	222.195.84.69	DNS	160	Standard query response 0x5a96 A
www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99 OPT						
Frame 7: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface wlp0s20f3, id 0						
Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor_9a:07:45 (34:2e:b7:9a:07:45)						
Internet Protocol Version 4, Src: 202.38.64.17, Dst: 222.195.84.69						
User Datagram Protocol, Src Port: 53, Dst Port: 55745						
Domain Name System (response)						
No.	Time	Source	Destination	Protocol	Length	Info
8	0.319779164	222.195.84.69	104.16.44.99	TCP	74	60438 → 443 [SYN] Seq=0 Win=64240 Len=0
MSS=1460 SACK_PERM=1 TSval=724658628 TSecr=0 WS=128						
Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp0s20f3, id 0						
Ethernet II, Src: IntelCor_9a:07:45 (34:2e:b7:9a:07:45), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)						
Internet Protocol Version 4, Src: 222.195.84.69, Dst: 104.16.44.99						
Transmission Control Protocol, Src Port: 60438, Dst Port: 443, Seq: 0, Len: 0						
No.	Time	Source	Destination	Protocol	Length	Info
9	0.321975491	104.16.44.99	222.195.84.69	TCP	66	443 → 60434 [SYN, ACK] Seq=0 Ack=1
Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192						
Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp0s20f3, id 0						
Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor_9a:07:45 (34:2e:b7:9a:07:45)						
Internet Protocol Version 4, Src: 104.16.44.99, Dst: 222.195.84.69						
Transmission Control Protocol, Src Port: 443, Dst Port: 60434, Seq: 0, Ack: 1, Len: 0						
No.	Time	Source	Destination	Protocol	Length	Info
13	0.532728766	104.16.44.99	222.195.84.69	TCP	66	443 → 60438 [SYN, ACK] Seq=0 Ack=1
Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=8192						
Frame 13: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp0s20f3, id 0						
Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:						