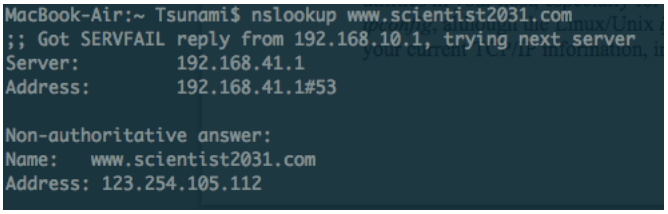
实验报告 Lab 2

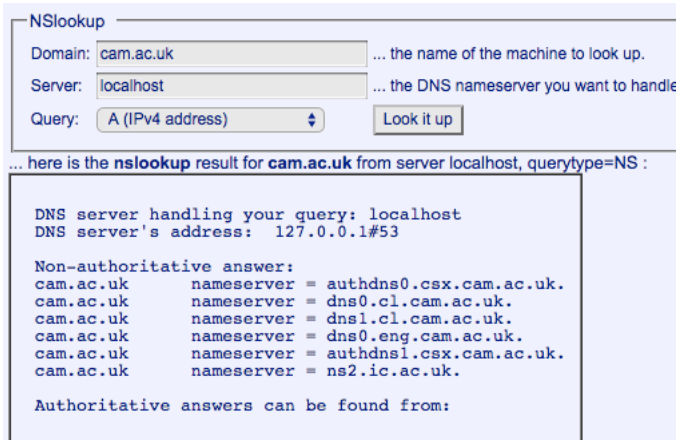
姓名：王钦　学号：13349112

nslookup

1. I use nslookup to find IP of my blog `http://scientist2031.com`



2. Because I connect Internet by router,So I use online nslookup to determine the authoritative DNS servers of University of Cambridge.
`Online nslookup: http://www.kloth.net/services/nslookup.php`



3. Because in Question 2,I didn't get the authoritative DNS servers,so I use google DNS `8.8.8.8`

NSlookup

Domain: cam.ac.uk ... the name of the machine to look up.

Server: 8.8.8.8 ... the DNS nameserver you want to handle your query (just start with this

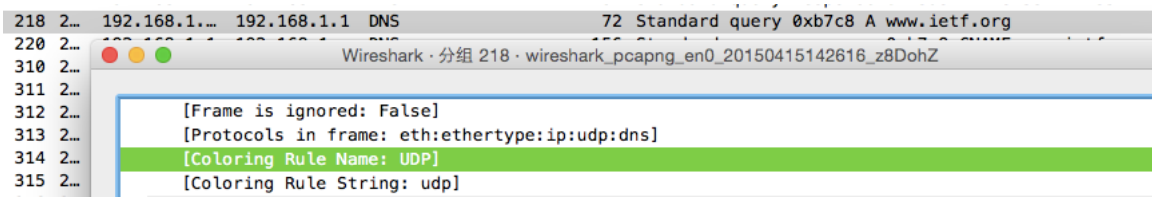
Query: A (IPv4 address) Look it up

... here is the **nslookup** result for **cam.ac.uk** from server 8.8.8.8, querytype=NS :

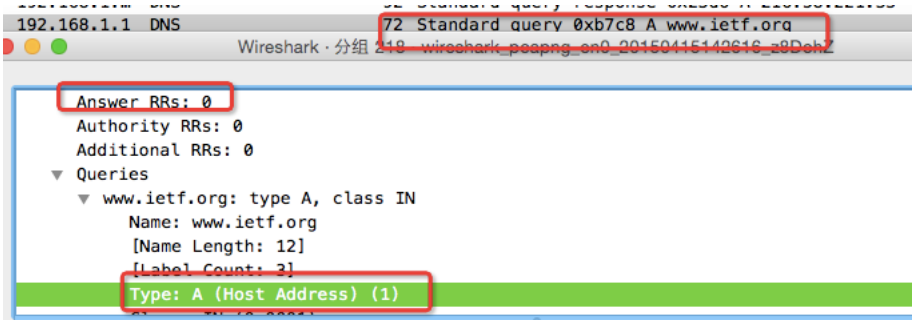
```
DNS server handling your query: 8.8.8.8
DNS server's address:  8.8.8.8#53

Non-authoritative answer:
cam.ac.uk       nameserver = authdns0.csx.cam.ac.uk.
cam.ac.uk       nameserver = ns2.ic.ac.uk.
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk.
cam.ac.uk       nameserver = dns1.cl.cam.ac.uk.
cam.ac.uk       nameserver = authdns1.csx.cam.ac.uk.
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk.

Authoritative answers can be found from:
```

Tracing DNS with wireshark

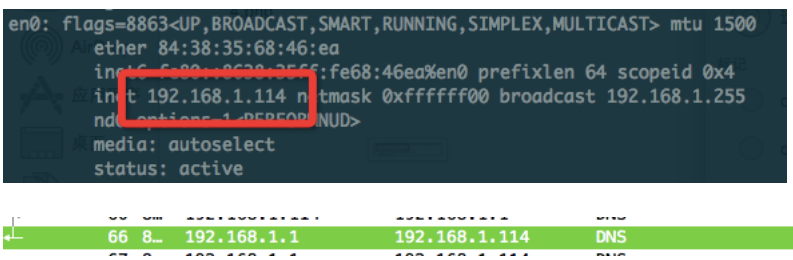
4. They sent over UDP.



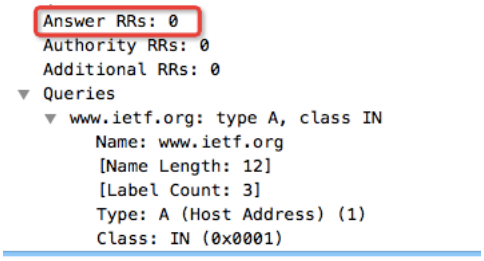
5. Destination Port: `55815 (55815)` Source Port: `53 (53)`



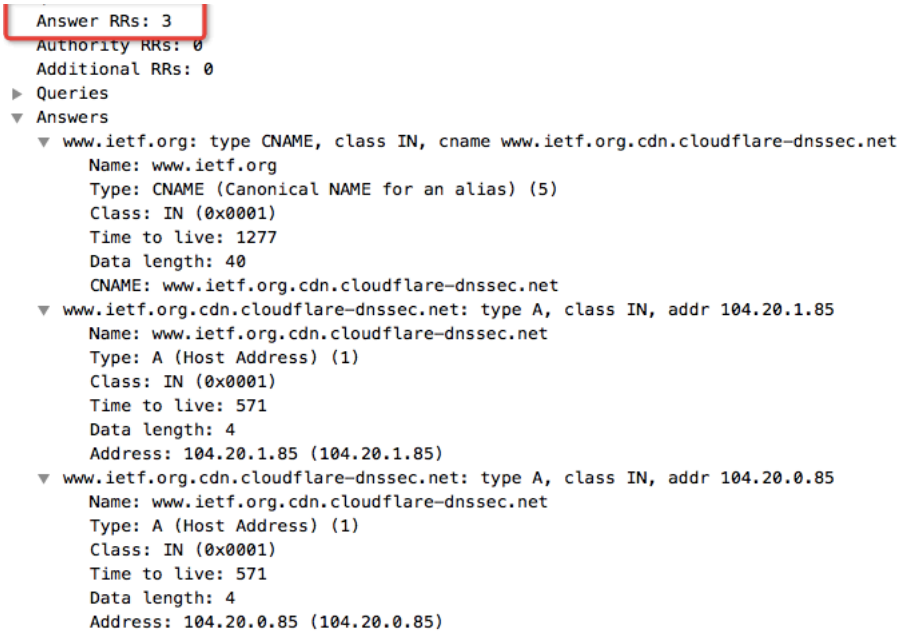
6. Yes,They are same IP



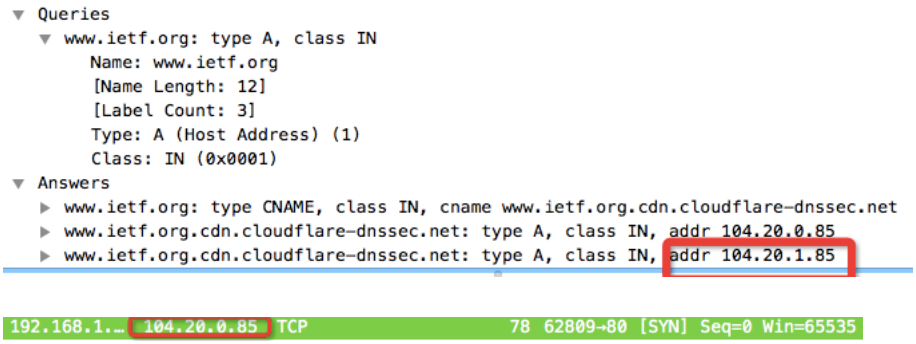
7. Type: `A (Host Address) (1)` .No,it didn't contain answers



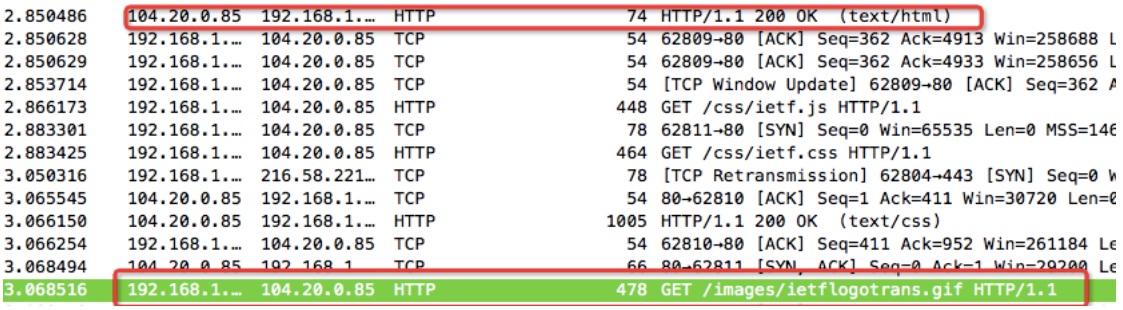
8. They are 3 answers provided,Each answers see below



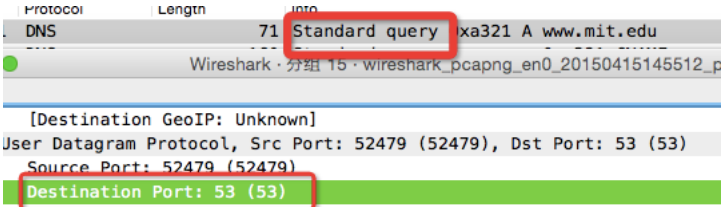
9. Subsequent TCP SYN packet sent by my host contain the IP addresses provided in the DNS response message

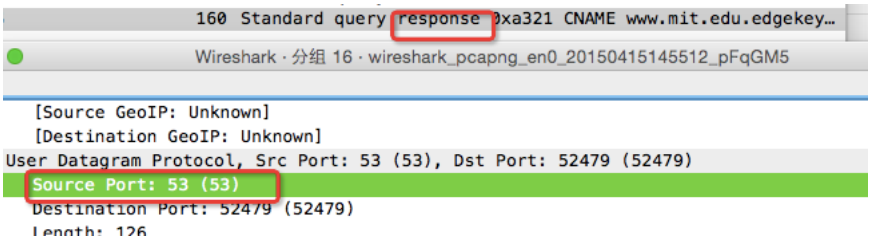


10. After got the html file,My host doesn't issue new DNS queries

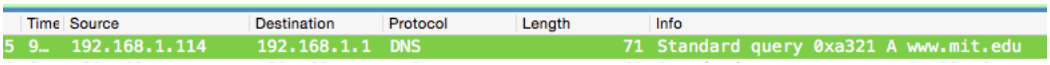


11. Destination port for the DNS query message: `53(53)` ,Source port of DNS response message: `53(53)` .

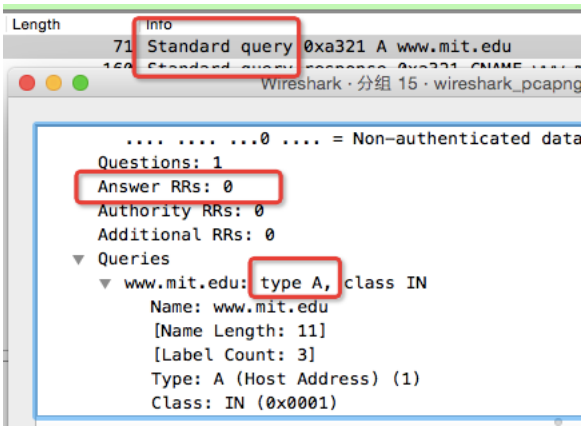




12. IP address is the DNS query message sent:`192.168.1.1`.No it's my laboratory router ip,my router will send query to real DNS server



13. Type: `A (Host Address) (1)` .Query message didn't contain any answers



14. DNS response message provided 3 answers.The detail of each answers contain see below:

```
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▶ www.mit.edu: type A, class IN
▼ 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: 992
      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: 534
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 184.25.226.188
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 534
      Data length: 4
      Address: 184.25.226.188 (184.25.226.188)
```

15. Sceenshot:

```
Destination  Protocol  Length  Info
192.168.1.1  DNS         71  Standard query 0xa321 A www.mit.edu
192.168.1.…  DNS        160  Standard query response 0xa321 CNAME www.mit.edu.edgek
```

16. IP address is the DNS query message sent:`192.168.1.1` ,This address isn't my local dns server,it's my router address. My router will send query to real DNS server

```
Time  Source        Destination     Protocol  Length  Info
7 6…  192.168.1.114 192.168.1.1     DNS         67  Standard query 0x9cd2 A mit.edu
```

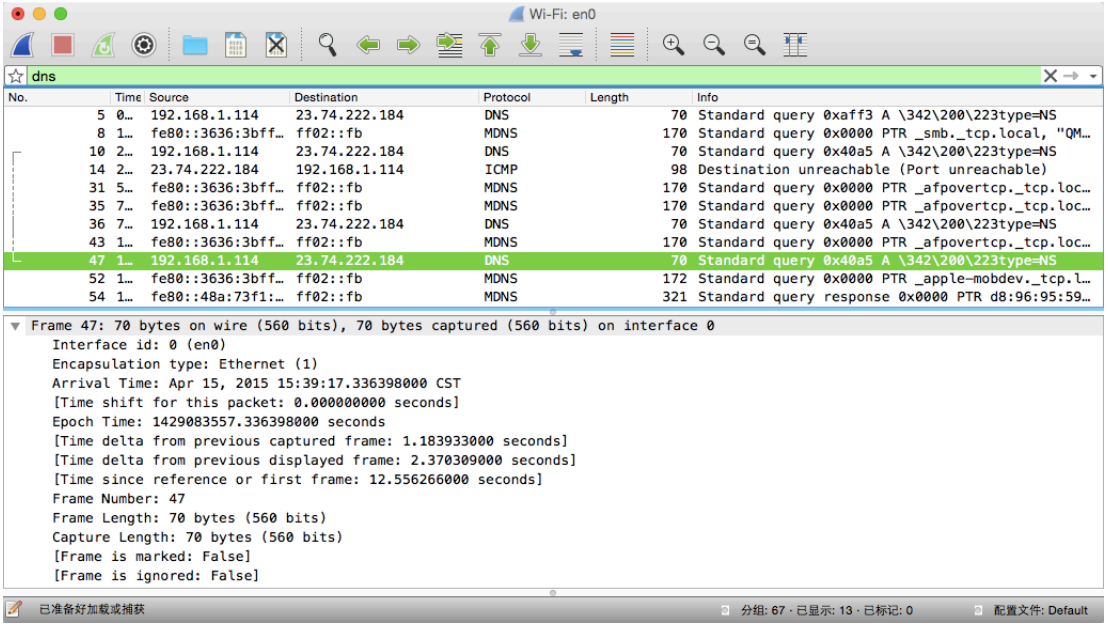
17. Type: `A (Host Address) (1)`. Query message didn't contain any answers

```
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ \342\200\223type=NS: type A, class IN
      Name: \342\200\223type=NS
      [Name Length: 10]
      [Label Count: 1]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

18. MIT name servers see below.It doesn't provide IP of the servers.

```
Answers
  mit.edu: type NS, class IN, ns STRAWB.mit.edu
    Name: mit.edu
    Type: NS (Authoritative name server)
    Class: IN (0x0001)
    Time to live: 56 minutes, 1 second
    Data length: 9
    Name server: STRAWB.mit.edu
  mit.edu: type NS, class IN, ns BITSY.mit.edu
    Name: mit.edu
    Type: NS (Authoritative name server)
    Class: IN (0x0001)
    Time to live: 56 minutes, 1 second
    Data length: 8
    Name server: BITSY.mit.edu
  mit.edu: type NS, class IN, ns W20NS.mit.edu
    Name: mit.edu
    Type: NS (Authoritative name server)
    Class: IN (0x0001)
    Time to live: 56 minutes, 1 second
    Data length: 8
    Name server: W20NS.mit.edu
```

19. screenshot.



20. IP address the DNS query message sent: `Destination: 18.72.0.3 (18.72.0.3)`.Th isn't my local DNS server.IP address correspond to bit.mit.edu

21. Type: `A (Host Address) (1)`. Query message didn't contain any answers

```
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)
```

22. 3 answers provided.Each of these answers contain see below

```
Answers
  www.aiit.or.kr: type A, class IN, addr 222.106.36.115
    Name: www.aiit.or.kr
    Type: A (Host address)
    Class: IN (0x0001)
    Time to live: 59 minutes, 50 seconds
    Data length: 4
    Addr: 222.106.36.115 (222.106.36.115)
Authoritative nameservers
  aiit.or.kr: type NS, class IN, ns w3.aiit.or.kr
    Name: aiit.or.kr
    Type: NS (Authoritative name server)
    Class: IN (0x0001)
    Time to live: 59 minutes, 50 seconds
    Data length: 5
    Name server: w3.aiit.or.kr
  aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr
    Name: aiit.or.kr
    Type: NS (Authoritative name server)
    Class: IN (0x0001)
    Time to live: 59 minutes, 50 seconds
    Data length: 5
    Name server: ns.aiit.or.kr
```

23. screenshot.