

# 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>

```
MacBook-Air:~ Tsunami$ nslookup www.scientist2031.com
;; Got SERVFAIL reply from 192.168.10.1, trying next server
Server:      192.168.41.1
Address:     192.168.41.1#53

Non-authoritative answer:
Name:   www.scientist2031.com
Address: 123.254.105.112
```

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>

The screenshot shows a web-based nslookup tool. The 'Domain' field is set to 'cam.ac.uk', the 'Server' field is set to 'localhost', and the 'Query' type is set to 'A (IPv4 address)'. A 'Look it up' button is visible. Below the input fields, the results are displayed for the query of 'cam.ac.uk' from server 'localhost'.

NSlookup

Domain:  ... the name of the machine to look up.

Server:  ... the DNS nameserver you want to handle

Query:

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

```
DNS server handling your query: localhost
DNS server's address: 127.0.0.1#53

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

Authoritative answers can be found from:
```

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

NSlookup

Domain:  ... the name of the machine to look up.

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

Query:

... 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

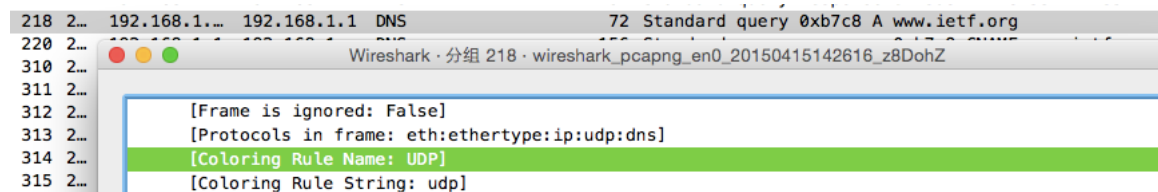
Non-authoritative answer:
cam.ac.uk      nameserver = authdns0.csx.cam.ac.uk.
cam.ac.uk      nameserver = ns2.ic.ac.uk.
cam.ac.uk      nameserver = dns0.cl.cam.ac.uk.
cam.ac.uk      nameserver = dns1.cl.cam.ac.uk.
cam.ac.uk      nameserver = authdns1.csx.cam.ac.uk.
cam.ac.uk      nameserver = dns0.eng.cam.ac.uk.

Authoritative answers can be found from:

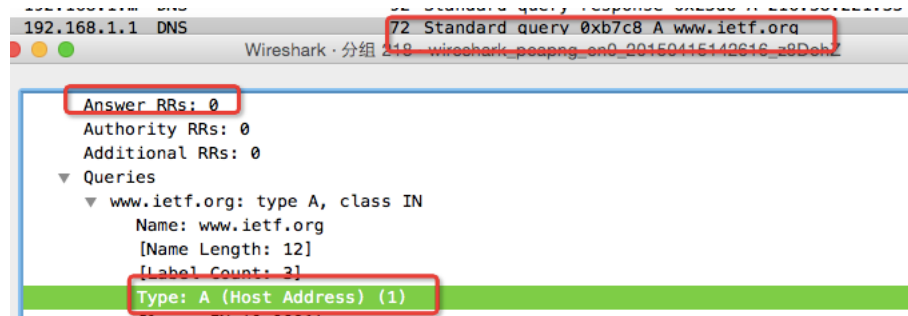
```

## Tracing DNS with wireshark

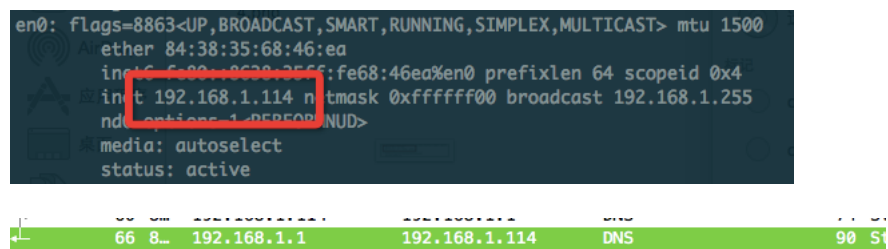
4. They sent over UDP.



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

```
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ 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)
```

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

```
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
► Queries
▼ Answers
  ▼ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare-dnssec.net
    Name: www.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1277
    Data length: 40
    CNAME: www.ietf.org.cdn.cloudflare-dnssec.net
  ▼ www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.1.85
    Name: www.ietf.org.cdn.cloudflare-dnssec.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 571
    Data length: 4
    Address: 104.20.1.85 (104.20.1.85)
  ▼ www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.0.85
    Name: www.ietf.org.cdn.cloudflare-dnssec.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 571
    Data length: 4
    Address: 104.20.0.85 (104.20.0.85)
```

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

```
▼ 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)
▼ Answers
  ► www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare-dnssec.net
  ► www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.0.85
  ► www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.1.85
```

```
192.168.1.1 - 104.20.0.85 TCP 78 62809-80 [SYN] Seq=0 Win=65535
```

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

2.850486	104.20.0.85	192.168.1.1	HTTP	74	HTTP/1.1 200 OK (text/html)
2.850628	192.168.1.1	104.20.0.85	TCP	54	62809-80 [ACK] Seq=362 Ack=4913 Win=258688 L
2.850629	192.168.1.1	104.20.0.85	TCP	54	62809-80 [ACK] Seq=362 Ack=4933 Win=258656 L
2.853714	192.168.1.1	104.20.0.85	TCP	54	[TCP Window Update] 62809-80 [ACK] Seq=362 A
2.866173	192.168.1.1	104.20.0.85	HTTP	448	GET /css/ietf.js HTTP/1.1
2.883301	192.168.1.1	104.20.0.85	TCP	78	62811-80 [SYN] Seq=0 Win=65535 Len=0 MSS=146
2.883425	192.168.1.1	104.20.0.85	HTTP	464	GET /css/ietf.css HTTP/1.1
3.050316	192.168.1.1	216.58.221...	TCP	78	[TCP Retransmission] 62804-443 [SYN] Seq=0 W
3.065545	104.20.0.85	192.168.1.1	TCP	54	80-62810 [ACK] Seq=1 Ack=411 Win=30720 Len=0
3.066150	104.20.0.85	192.168.1.1	HTTP	1005	HTTP/1.1 200 OK (text/css)
3.066254	192.168.1.1	104.20.0.85	TCP	54	62810-80 [ACK] Seq=411 Ack=952 Win=261184 Le
3.068494	104.20.0.85	192.168.1.1	TCP	66	80-62811 [SYN, ACK] Seq=0 Ack=1 Win=29200 Le
3.068516	192.168.1.1	104.20.0.85	HTTP	478	GET /images/ietflogotrans.gif HTTP/1.1

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

Protocol	Length	Info
DNS	71	Standard query 0xa321 A www.mit.edu
Wireshark · 分组 15 · wireshark_pcapng_en0_20150415145512.p		
[Destination GeoIP: Unknown]		
User Datagram Protocol, Src Port: 52479 (52479), Dst Port: 53 (53)		
Source Port: 52479 (52479)		
Destination Port: 53 (53)		

160	Standard query response	0xa321 CNAME www.mit.edu.edgekey...
Wireshark · 分组 16 · wireshark_pcapng_en0_20150415145512_pFqGM5		
[Source GeoIP: Unknown]		
[Destination GeoIP: Unknown]		
User Datagram Protocol, Src Port: 53 (53), Dst Port: 52479 (52479)		
Source Port: 53 (53)		
Destination Port: 52479 (52479)		
Length: 126		

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

Time	Source	Destination	Protocol	Length	Info
5.9...	192.168.1.114	192.168.1.1	DNS	71	Standard query 0xa321 A www.mit.edu

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

Length	Info
71	Standard query 0xa321 A www.mit.edu
Wireshark · 分组 15 · wireshark_pcapng	
.... ..0 .... = Non-authenticated data	
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. DNS response message provided 3 answers. The detail of each answer contains 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. Screenshot:

Destination	Protocol	Length	Info
192.168.1.1	DNS	71	Standard query 0xa321 A www.mit.edu
192.168.1.1...	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 W2ONS.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: W2ONS.mit.edu

```

19. screenshot.

The screenshot shows a Wireshark capture of network traffic on the 'dns' filter. The packet list shows several DNS queries and responses. The selected packet (No. 47) is a DNS query from 192.168.1.114 to 23.74.222.184. The packet details pane shows the following information:

- Interface id: 0 (en0)
- Encapsulation type: Ethernet (1)
- Arrival Time: Apr 15, 2015 15:39:17.336398000 CST
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1429083557.336398000 seconds
- [Time delta from previous captured frame: 1.183933000 seconds]
- [Time delta from previous displayed frame: 2.370309000 seconds]
- [Time since reference or first frame: 12.556266000 seconds]
- Frame Number: 47
- Frame Length: 70 bytes (560 bits)
- Capture Length: 70 bytes (560 bits)
- [Frame is marked: False]
- [Frame is ignored: False]

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

192.168.1.114	18.72.0.3	DNS	74 Standard query 0x8b36 A www.aait.or.kr
192.168.1.114	18.72.0.3	DNS	70 Standard query 0x2f0a A pdlck.a.phifa...

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

```

-----
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ www.aait.or.kr: type A, class IN
    Name: www.aait.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.aait.or.kr: type A, class IN, addr 222.106.36.115
    Name: www.aait.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
    aait.or.kr: type NS, class IN, ns w3.aait.or.kr
      Name: aait.or.kr
      Type: NS (Authoritative name server)
      Class: IN (0x0001)
      Time to live: 59 minutes, 50 seconds
      Data Length: 5
      Name server: w3.aait.or.kr
    aait.or.kr: type NS, class IN, ns ns.aait.or.kr
      Name: aait.or.kr
      Type: NS (Authoritative name server)
      Class: IN (0x0001)
      Time to live: 59 minutes, 50 seconds
      Data Length: 5
      Name server: ns.aait.or.kr

```

23. screenshot.

