

CPS 706 - Wireshark DNS

1. Run *nslookup* to obtain the IP address of a Web server in Asia

```
[01/28/20]seed@VM:~$ nslookup nus.edu.sg
```

Server: 127.0.1.1

Address: 127.0.1.1#53

Non-authoritative answer:

Name: nus.edu.sg

Address: 45.60.35.225

Name: nus.edu.sg

Address: 45.60.33.225

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

- University of Oxford

```
[02/08/20]seed@VM:~$ nslookup -type=NS ox.ac.uk
```

Server: 127.0.1.1

Address: 127.0.1.1#53

Non-authoritative answer:

ox.ac.uk nameserver = auth4.dns.ox.ac.uk.

ox.ac.uk nameserver = auth5.dns.ox.ac.uk.

ox.ac.uk nameserver = dns0.ox.ac.uk.

ox.ac.uk nameserver = dns2.ox.ac.uk.

ox.ac.uk nameserver = auth6.dns.ox.ac.uk.

ox.ac.uk nameserver = dns1.ox.ac.uk.

ox.ac.uk nameserver = ns2.ja.net.

3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.

- It didn't work for Ymail. Accessed a different server (University College London)

```
[02/03/20]seed@VM:~$ nslookup mail.yahoo.com auth6.dns.ox.ac.uk
```

Server: auth6.dns.ox.ac.uk

Address: 185.24.221.32#53

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

```
[02/03/20]seed@VM:~$ nslookup ucl.ac.uk ns2.ja.net
```

Server: ns2.ja.net

Address: 193.63.105.17#53

Name: ucl.ac.uk

Address: 144.82.250.24

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

- They are sent over UDP

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

- Destination port for DNS query message: 53

43.651715145	10.0.2.5	141.117.199.74	DNS	74 Standard qu...
43.652101845	10.0.2.5	141.117.199.74	DNS	74 Standard qu...
43.810927622	141.117.199.74	10.0.2.5	DNS	163 Standard qu...
43.903566621	141.117.199.74	10.0.2.5	DNS	187 Standard qu...
Terminator	10.0.2.5	104.20.0.85	TCP	76 34664 → 80 ...

▶ Frame 56: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
 ▶ Linux cooked capture
 ▶ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 141.117.199.74
 ▶ User Datagram Protocol, Src Port: 29929, Dst Port: 53
 ▶ Domain Name System (query)

- Source port of DNS response message: 53

43.651715145	10.0.2.5	141.117.199.74	DNS	74 Standard qu...
43.652101845	10.0.2.5	141.117.199.74	DNS	74 Standard qu...
43.810927622	141.117.199.74	10.0.2.5	DNS	163 Standard qu...
43.903566621	141.117.199.74	10.0.2.5	DNS	187 Standard qu...
43.904060016	10.0.2.5	104.20.0.85	TCP	76 34664 → 80 ...

▶ Frame 57: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface
 ▶ Linux cooked capture
 ▶ Internet Protocol Version 4, Src: 141.117.199.74, Dst: 10.0.2.5
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 41781
 ▶ Domain Name System (response)

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 is sent to IP address: 141.117.199.74
- This IP address is the same as one of the local DNS server

```
IP4.DNS[1]: 141.117.199.78
IP4.DNS[2]: 141.117.199.74
```

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

- It's a Type A standard DNS query
- The query message doesn't contain any answers

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

- 3 answers are provided.
- The answers contain information such as Name, Type, Class, TTL, datalength and address (one CNAME and two Type A answers)

```

▶ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
▼ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
  Name: www.ietf.org.cdn.cloudflare.net
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 300
  Data length: 4
  Address: 104.20.0.85
▶ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85

```

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?
- The destination IP address correspond to the IP address provided by the “answer” in the DNS response message

```

15:51:43.904060016 10.0.2.5 104.20.0.85 TCP

```

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
- No, the host doesn't issue any new DNS queries
11. What is the dst port for the DNS query message? What is the src port of DNS response message?
- Destination port for DNS query message: 53
 - Source port of DNS response message: 53
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
- IP address of where it's sent: 141.117.199.74
 - Yes it's the IP address of the local DNS server
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
- It's a Type A DNS query
 - It does not contain any answers
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
- 3 answers are provided
 - Each of them contain information such as Name, Type, Class, TTL, datalength and address (two CNAME and one Type A answers)

15. Provide a screenshot.

No.	Time	Source	Destination	Protocol
2	18:09:34.343228321	104.20.1.85	10.0.2.5	TLSv1.2
3	18:09:34.343271499	10.0.2.5	104.20.1.85	TCP
6	18:09:34.457423077	10.0.2.5	141.117.199.78	DNS
7	18:09:34.457589476	10.0.2.5	141.117.199.74	DNS
9	18:09:34.740864674	141.117.199.78	10.0.2.5	DNS
11	18:09:34.741372757	141.117.199.74	10.0.2.5	DNS
12	18:09:34.741393356	10.0.2.5	141.117.199.74	ICMP

Frame 11: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface
 Linux cooked capture
 Internet Protocol Version 4, Src: 141.117.199.74, Dst: 10.0.2.5
 User Datagram Protocol, Src Port: 53, Dst Port: 46857
 Domain Name System (response)

No.	Time	Source	Destination	Protocol
2	18:09:34.343228321	104.20.1.85	10.0.2.5	TLSv1.2
3	18:09:34.343271499	10.0.2.5	104.20.1.85	TCP
6	18:09:34.457423077	10.0.2.5	141.117.199.78	DNS
7	18:09:34.457589476	10.0.2.5	141.117.199.74	DNS
9	18:09:34.740864674	141.117.199.78	10.0.2.5	DNS
11	18:09:34.741372757	141.117.199.74	10.0.2.5	DNS
12	18:09:34.741393356	10.0.2.5	141.117.199.74	ICMP

www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 e9566.dscb.akamaiedge.net: type A, class IN, addr 184.86.198.146
 Name: e9566.dscb.akamaiedge.net
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 20
 Data length: 4
 Address: 184.86.198.146

0020 0a 00 02 05 00 35 b7 09 00 89 40 4b 4f e6 81 805..@K0...
 0030 00 01 00 03 00 00 00 00 03 77 77 77 03 6d 69 74www.mit...
 0040 03 65 64 75 00 00 01 00 01 03 77 77 77 03 6d 69 .edu....www.m...
 0050 74 03 65 64 75 00 00 05 00 01 00 00 06 c8 00 19 t.edu.....
 0060 03 77 77 77 03 6d 69 74 03 65 64 75 07 65 64 67 .www.mit.edu.edg...
 0070 65 6b 65 79 03 6e 65 74 00 c0 34 00 05 00 01 00 ekey.net.4....

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

- DNS query message is sent to IP address: 141.117.199.74
- This is the IP address of the local DNS server

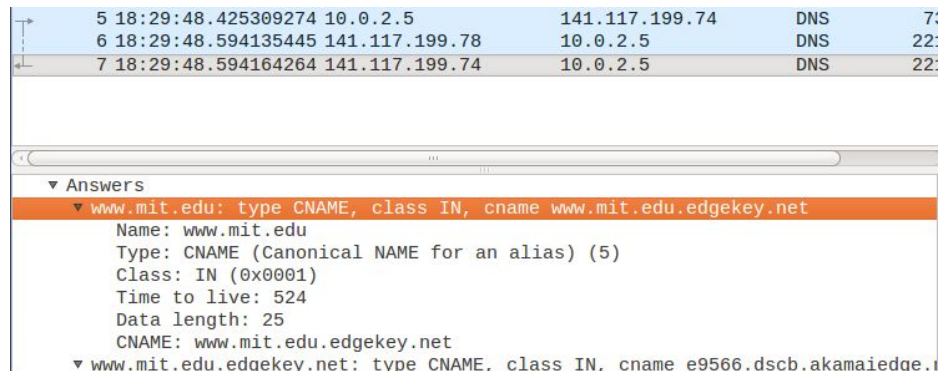
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

- The DNS query is of Type NS
- It does not contain any answer

18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

- MIT name servers provided are www.mit.edu and www.mit.edu.edgekey.net
- The response message does not provide IP addresses the MIT name servers

19. Provide a screenshot.



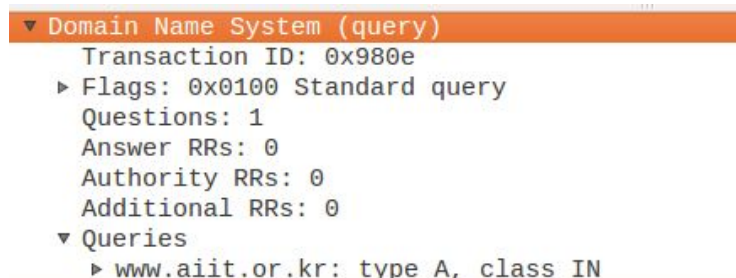
20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

- The DNS query message is sent to IP address: 18.0.2.73
- The IP corresponds to the address of bitsy.mit.edu

```
Non-authoritative answer:
Name:   bitsy.mit.edu
Address: 18.0.72.3
```

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

- The DNS query message is of Type A
- The query message does not contain any answer



22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

- There is no response message received

23. Provide a screenshot.

ip.addr==10.0.2.5					Expression..
No.	Time	Source	Destination	Protocol	
6	19:08:46.646267760	141.117.199.74	10.0.2.5	DNS	
8	19:08:46.647350527	141.117.199.74	10.0.2.5	DNS	
11	19:08:46.647949588	10.0.2.5	18.0.72.3	DNS	
12	19:08:46.717854733	141.117.199.78	10.0.2.5	DNS	
13	19:08:46.717890382	10.0.2.5	141.117.199.78	ICMP	
14	19:08:51.648623013	10.0.2.5	18.0.72.3	DNS	
17	19:08:56.650064346	10.0.2.5	18.0.72.3	DNS	

Frame 11: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.5, Dst: 18.0.72.3
User Datagram Protocol, Src Port: 45259, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x980e
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0

0000	00 04 00 01 00 06 08 00	27 24 f1 88 00 00 08 00 '\$.....
0010	45 00 00 3c b3 49 00 00	40 11 61 60 0a 00 02 05	E.<.I.. @.a'....
0020	12 00 48 03 b0 cb 00 35	00 28 66 41 98 0e 01 00	..H....5 .(fA....
0030	00 01 00 00 00 00 00 00	03 77 77 77 04 61 69 69www.aii
0040	74 02 6f 72 02 6b 72 00	00 01 00 01	t.or.kr.

```
[02/04/20]seed@VM:~$ nslookup aiit.or.kr bitsy.mit.edu  
;; connection timed out; no servers could be reached
```