CMPSCI 453
HW6, Wireshark Lab 3

Tony Gao

February 23, 2018

1 Problem 1

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

```
Tonys-MBP:CS453 rpg711$ nslookup google.com.hk
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
Name: google.com.hk
Address: 172.217.9.35
```

   The type A record for google.com.hk maps it to 172.217.9.35

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

```
Tonys-MBP:CS453 rpg711$ nslookup -type=NS www.cam.ac.uk
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
www.cam.ac.uk canonical name = cam.ac.uk.
cam.ac.uk nameserver = dns0.cl.cam.ac.uk.
cam.ac.uk nameserver = authdns0.csx.cam.ac.uk.
cam.ac.uk nameserver = sns-pb.isc.org.
cam.ac.uk nameserver = dns0.eng.cam.ac.uk.
cam.ac.uk nameserver = ns2.ic.ac.uk.

Authoritative answers can be found from:
authdns0.csx.cam.ac.uk internet address = 131.111.8.37
sns-pb.isc.org internet address = 192.5.4.1
sns-pb.isc.org has AAAA address 2001:500:2e::1
dns0.eng.cam.ac.uk internet address = 129.169.8.8
```

There are 4 type NS records for official authoritative DNS servers for Cambridge University.

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?

```
Tonys-MBP:CS453 rpg711$ nslookup -type=mx yahoo.com authdns0.csx.cam.ac.uk
Server: authdns0.csx.cam.ac.uk
Address: 131.111.8.37#53

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

Doing an nslookup for -type=MX for yahoo.com gives mta7.am0.yahoodns.net as one of the mail servers. A type A query reveals that mta7.am0.yahoodns.net maps to many IP addresses, one of which is 98.137.159.27.

```
Tonys-MBP:CS453 rpg711$ nslookup mta7.am0.yahoodns.net
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
Name: mta7.am0.yahoodns.net
Address: 98.137.159.27
.. truncated ..
```

2 Problem 2

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

   UDP

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

   User Datagram Protocol, Src Port: 45190, Dst Port: 53

7. 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?

   192.168.1.1. I am on a Macbook Pro OS X 10.12 so ifconfig does not list my DNS servers. Instead, scutil must be used.

```
$ scutil --dns
DNS configuration

resolver #1
  nameserver[0] : 192.168.1.1
  if_index : 7 (en0)
  flags    : Request A records
  reach    : 0x00020002 (Reachable,Directly Reachable Address)
```

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

```
Queries
    clients6.google.com: type A, class IN
```

It contains 0 answers and 1 question, the full query is below.

```
Domain Name System (query)
    [Response In: 144]
    Transaction ID: 0x5f53
    Flags: 0x0100 Standard query
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        clients6.google.com: type A, class IN
```

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

2 answers. A canonical name request for clients6.google.com and a hostname-IP mapping for clients.l.google.com

```
Domain Name System (response)
    [Request In: 143]
    [Time: 0.014347000 seconds]
    Transaction ID: 0x5f53
    Flags: 0x8180 Standard query response, No error
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
        .... .0.. .... .... = Authoritative: Server is not an authority for domain
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authent
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
```

```
Authority RRs: 0
Additional RRs: 0
Queries
Answers
    clients6.google.com: type CNAME, class IN, cname clients.l.google.com
    clients.l.google.com: type A, class IN, addr 172.217.11.46
```

10. 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?

    Yes.

```
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 172.217.11.46
Transmission Control Protocol, Src Port: 55588, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 55588
    Destination Port: 80
    [Stream index: 25]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    1011 .... = Header Length: 44 bytes (11)
    Flags: 0x002 (SYN)
    Window size value: 65535
    [Calculated window size: 65535]
    Checksum: 0xb461 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operatio
```

11. This web page contains images. Before retrieving each image, does your host issue new DNS queries? No, the image wireshark capture numbers go from 603-607. DNS queries go from 84-484, 1538-1587 so there is no overlap, implying no DNS queries are done for images. This makes sense, because the images are all local to the ietf.org hostname, which was already resolved.