Tevin Jeffrey – CS 356

Wireshark Lab 3

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

$ nslookup japanprize.jp

Server: google-public-dns-a.google.com

Address: 8.8.8.8

Non-authoritative answer:

Name: japanprize.jp

Address: 182.93.119.63

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

$ nslookup -type=NS www.ox.ac.uk

Server: google-public-dns-a.google.com

Address: 8.8.8.8

ox.ac.uk

primary name server = nighthawk.dns.ox.ac.uk

responsible mail addr = hostmaster.ox.ac.uk

serial = 2016020572

refresh = 3600 (1 hour)

retry = 1800 (30 mins)

expire = 1209600 (14 days)

default TTL = 900 (15 mins)

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

$ nslookup yahoo.com nighthawk.dns.ox.ac.uk

DNS request timed out.

timeout was 2 seconds.

Server: UnKnown

Address: 163.1.2.189

DNS request timed out.

timeout was 2 seconds.

DNS request timed out.

timeout was 2 seconds.

DNS request timed out.

timeout was 2 seconds.

DNS request timed out.

timeout was 2 seconds.

\*\*\* Request to UnKnown timed-out

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

UDP

*Request: User Datagram Protocol, Src Port: 52152 (52152), Dst Port: 53 (53)*

*Response: User Datagram Protocol, Src Port: 53 (53), Dst Port: 52152 (52152)*

**5. What is the destination port for the DNS query message?**

53

**What is the source port of DNS response message?**

53

**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?**

*Request: Internet Protocol Version 4, Src: 192.168.0.108, Dst: 8.8.8.8*

*Ipconfig: DNS Servers . . . . . . . . . . . : 8.8.8.8*

*8.8.4.4*

Yes the two ip addresses are the same.

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

It was a type A query.

No, the query message does not contain any answers.

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

*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*

3 answers are provided. A canonical name for ietf.org which resolves to *www.ietf.org.cdn.cloudflare-dnssec.net. This address resolves to 2 other addresses. 104.20.0.85 and 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?**

*26 06:55:13.194042 192.168.0.108 104.20.0.85 TCP 66 60391 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK\_PERM=1*

Yes, the destination of the SYN packet corresponds to one of the IP address in the answer of the response from the DNS server.

**10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?**

No

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

*Query: User Datagram Protocol, Src Port: 58202 (58202), Dst Port: 53 (53)*

*Response: User Datagram Protocol, Src Port: 53 (53), Dst Port: 58202 (58202)*

The destination port for the query message is 53 and the source port of the response message is 53

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

Query: Internet Protocol Version 4, Src: 192.168.0.108, Dst: 8.8.8.8

The IP address of my default local DNS server is 8.8.8.8. It is exactly what is set in the router.

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

*Queries*

*www.mit.edu: type AAAA, class IN*

*Name: www.mit.edu*

*[Name Length: 11]*

*[Label Count: 3]*

*Type: AAAA (IPv6 Address) (28)*

*Class: IN (0x0001)*

It was a AAAA query, which seems to be a query for a IPv6 address. There were no Answer Resource records.

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

*Answers*

*www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net*

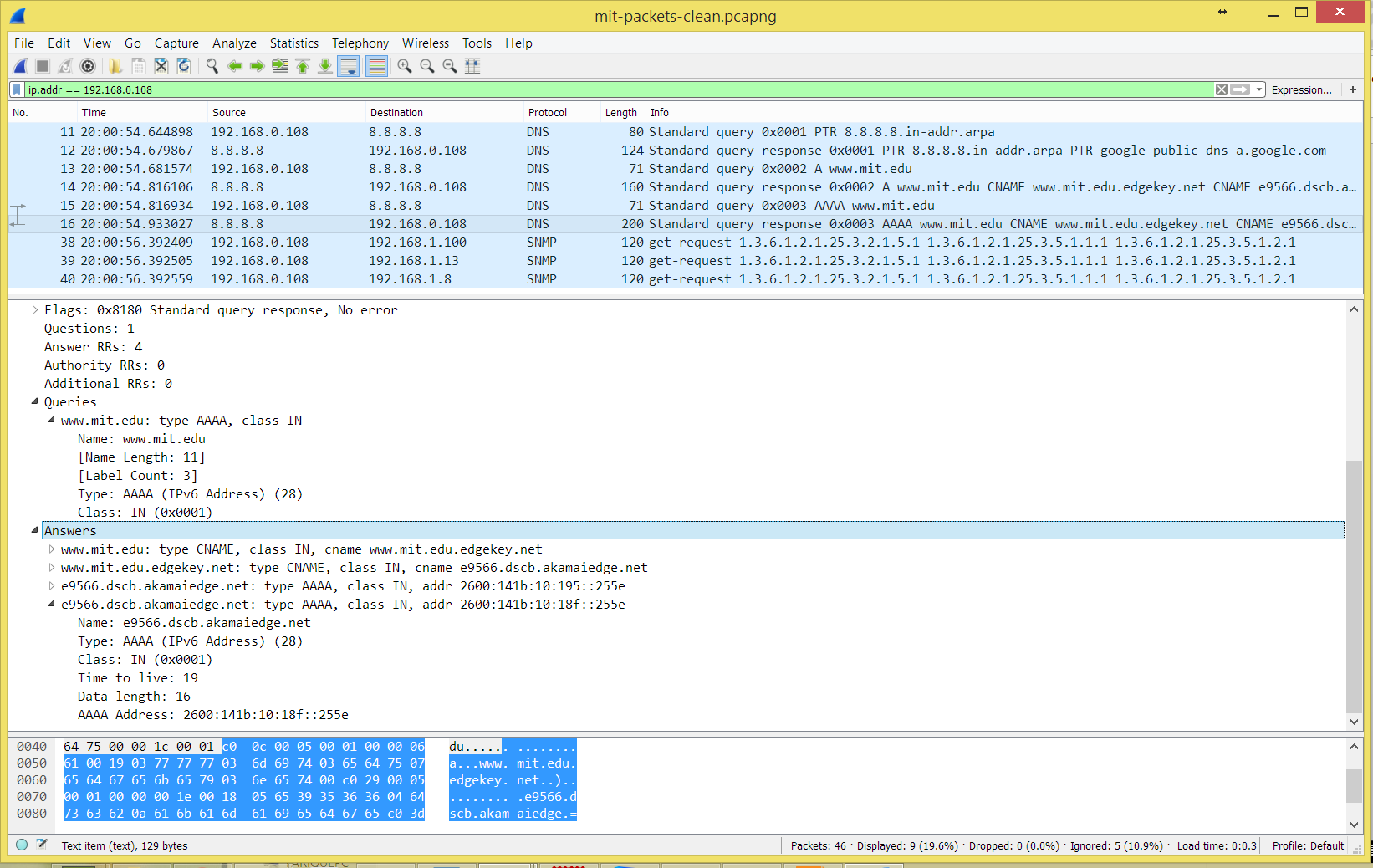
*www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net*

*e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:141b:10:195::255e*

*e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:141b:10:18f::255e*

4 answers were provided. 2 contain a canonical name alias. The last 2 contain a 128-bit IPv6 address.

15. Provide a screenshot.



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

*Internet Protocol Version 4, Src: 192.168.0.108, Dst: 172.231.156.200*

Again, looking at the last query the destination address is *172.231.156.200*, that is not the address of my local DNS server.

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

It was a AAAA query with no answers.

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

It provides an error, unreachable port.

*Internet Control Message Protocol*

*Type: 3 (Destination unreachable)*

*Code: 3 (Port unreachable)*

*Checksum: 0x07f5 [correct]*

*Unused: 00000000*

*Internet Protocol Version 4, Src: 192.168.0.108, Dst: 172.231.156.200*

*User Datagram Protocol, Src Port: 58275 (58275), Dst Port: 53 (53)*

*Source Port: 58275*

*Destination Port: 53*

*Length: 34*

*Checksum: 0x9244 [validation disabled]*

*[Stream index: 4]*

*Domain Name System (query)*

*Transaction ID: 0x0002*

*Flags: 0x0100 Standard query*

*Questions: 1*

*Answer RRs: 0*

*Authority RRs: 0*

*Additional RRs: 0*

*Queries*

*\226type=NS: type A, class IN*

*Name: \226type=NS*

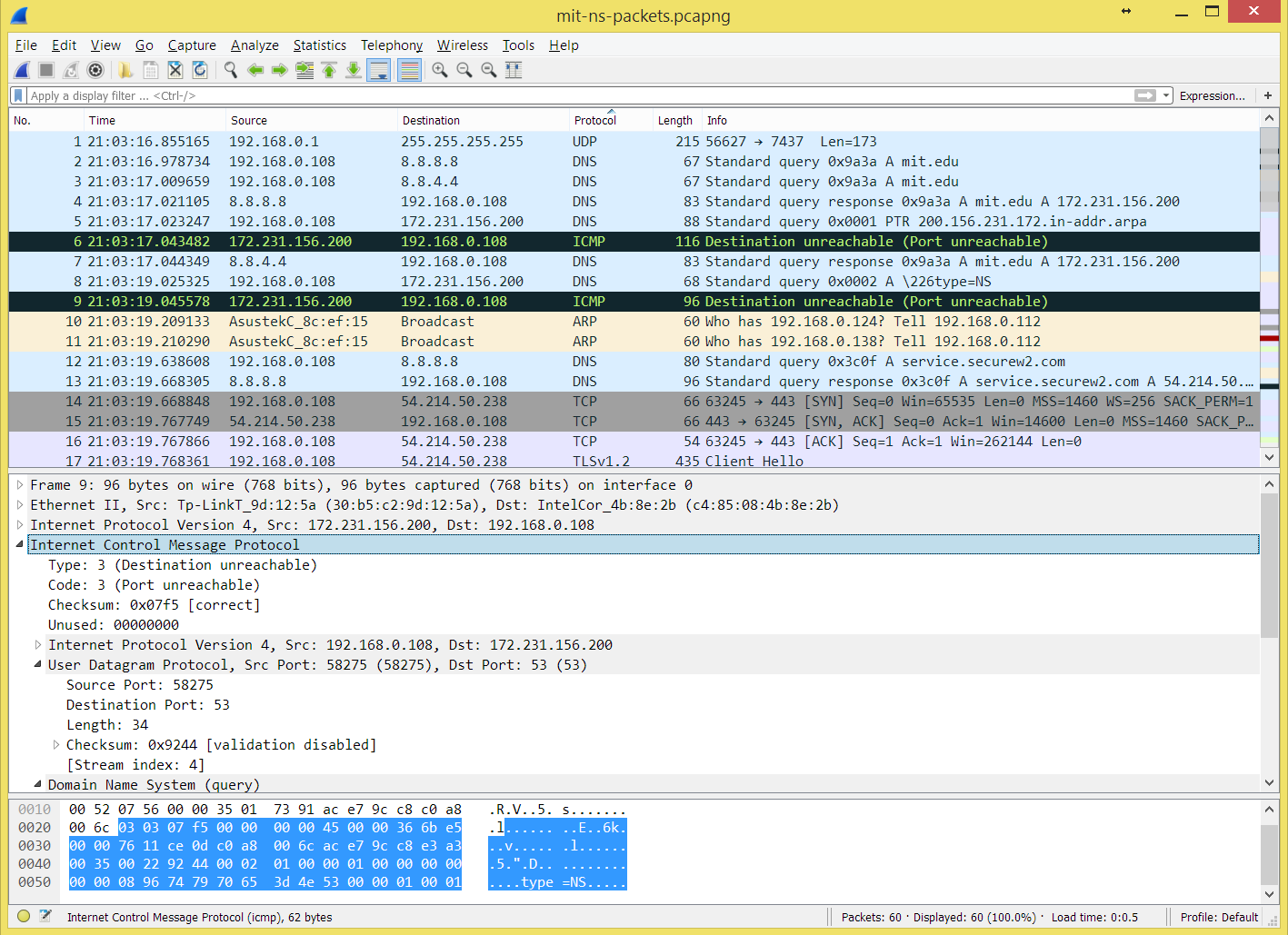
*[Name Length: 8]*

*[Label Count: 1]*

*Type: A (Host Address) (1)*

*Class: IN (0x0001)*

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?**

*Query: Internet Protocol Version 4, Src: 192.168.0.108, Dst: 18.72.0.3*

*bitsy.mit.edu: type A, class IN, addr 18.72.0.3*

*Name: bitsy.mit.edu*

*Type: A (Host Address) (1)*

*Class: IN (0x0001)*

*Time to live: 709*

*Data length: 4*

*Address: 18.72.0.3*

The ip address corresponds to the ip address of bitsy.mit.edu

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

*Domain Name System (query)*

*Transaction ID: 0x0004*

*Flags: 0x0100 Standard query*

*Questions: 1*

*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)*

It was a type A query with no answers.

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

The query to nitsy.mit.edu was successful, but subsequent queries to that nameserver were not successful. There were 4 attempts, 2 A queries and 2 AAAA queries.

**23. Provide a screenshot.**

