Problem 1

In this question, we will deal with the resolution of names through the Domain Name System.

1.a. What is a whois database?

1.b. Use various whois databases on the Internet to obtain the names of two DNS servers. Indicate which whois databases you used

1.c. Use nslookup on your local host to send DNS queries to three DNS servers: your local DNS server and the two DNS servers you found in part (b). Try querying for Type A, NS, and MX reports. Summarize your findings.

1.d. Use nslookup to find a Web server that has multiple IP addresses. Does the Web server of your institution (school or company) have multiple IP addresses?

1.e. Use the ARIN whois database to determine the IP address range used by your university.

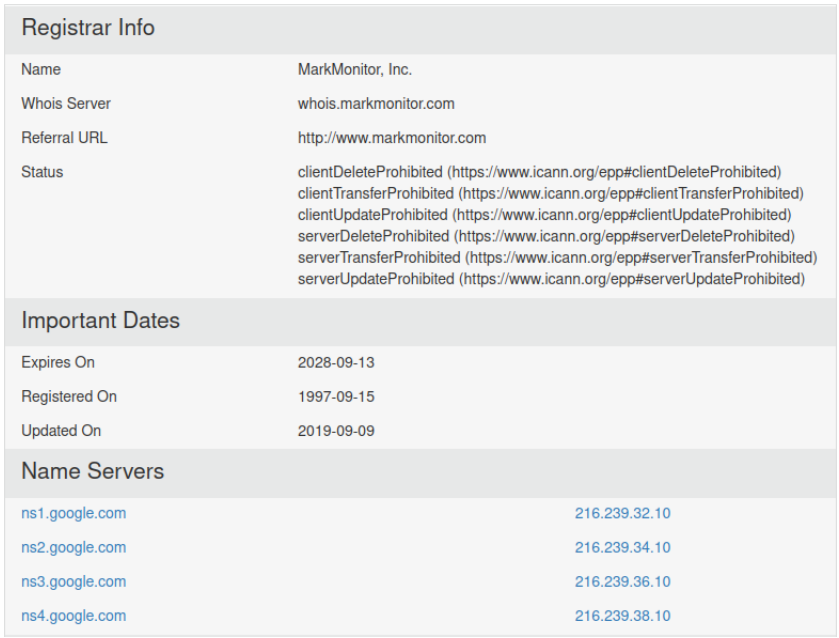
1.f. Describe how an attacker can use whois databases and the nslookup tool to perform reconnaissance on an institution before launching an attack.

1.g. Discuss why whois databases should be publicly available.

Solution

a) A whois database is a database that contains all of the contact information associated with the person, group of people or company that registers a domain name. It contains contact information for the site registrant, registrar, administrative and technical and billing. It also contains expiry and registration dates, as well as name servers.

b)I used https://who.is/ (left) and https://lookup.icann.org/lookup (right) to search for google.com and cnn.com and found the following name servers:



Registrar Info

Name	MarkMonitor, Inc.
Whois Server	whois.markmonitor.com
Referral URL	http://www.markmonitor.com
Status	clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited) clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited) clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited) serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited) serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited) serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

Important Dates

Expires On	2028-09-13
Registered On	1997-09-15
Updated On	2019-09-09

Name Servers

ns1.google.com	216.239.32.10
ns2.google.com	216.239.34.10
ns3.google.com	216.239.36.10
ns4.google.com	216.239.38.10

Domain Information

Name: CNN.COM

Registry Domain ID: 3269879_DOMAIN_COM-VRSN

Domain Status:
clientTransferProhibited
serverDeleteProhibited
serverTransferProhibited
serverUpdateProhibited

Nameservers:
NS-1086.AWSDNS-07.ORG
NS-1630.AWSDNS-11.CO.UK
NS-47.AWSDNS-05.COM
NS-576.AWSDNS-08.NET

Dates

Registry Expiration: 2026-09-21 04:00:00 UTC

Created: 1993-09-22 04:00:00 UTC

c) Nslookup stands for "Name Server Lookup". It is a command for getting information from DNS server. We do three types of nslookup: ns, mx and a.

nslookup -type=ns: An NS (name server) record maps a domain name to a list of DNS servers authoritative for that domain. It shows the name servers that are associated with the domain.

nslookup -type=mx: An MX (mail exchange) record maps a domain name to a list of mail exchange servers for that domain. The MX record tells us where the mail that is sent to the domain should be routed to.

nslookup -type=a: View all the available (a) DNS records for a particular record

```
sawyer@sawyer-System-Product-Name:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.41.78
Name:   google.com
Address: 2607:f8b0:400b:804::200e

sawyer@sawyer-System-Product-Name:~$ nslookup cnn.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   cnn.com
Address: 151.101.193.67
Name:   cnn.com
Address: 151.101.129.67
Name:   cnn.com
Address: 151.101.65.67
Name:   cnn.com
Address: 151.101.1.67
Name:   cnn.com
Address: 2a04:4e42:200::323
Name:   cnn.com
Address: 2a04:4e42:400::323
Name:   cnn.com
Address: 2a04:4e42::323
Name:   cnn.com
Address: 2a04:4e42:600::323

sawyer@sawyer-System-Product-Name:~$ nslookup cogeco.local
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   cogeco.local
Address: 192.168.0.1
```

```
sawyer@sawyer-System-Product-Name:~$ nslookup -type=ns cnn.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
cnn.com nameserver = ns-1086.awsdns-07.org.
cnn.com nameserver = ns-1630.awsdns-11.co.uk.
cnn.com nameserver = ns-47.awsdns-05.com.
cnn.com nameserver = ns-576.awsdns-08.net.

Authoritative answers can be found from:

sawyer@sawyer-System-Product-Name:~$ nslookup -type=mx cnn.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
cnn.com mail exchanger = 10 mxa-00241e02.gslb.pphosted.com.
cnn.com mail exchanger = 10 mxb-00241e02.gslb.pphosted.com.

Authoritative answers can be found from:

sawyer@sawyer-System-Product-Name:~$ nslookup -type=a cnn.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   cnn.com
Address: 151.101.1.67
Name:   cnn.com
Address: 151.101.65.67
Name:   cnn.com
Address: 151.101.129.67
Name:   cnn.com
Address: 151.101.193.67
```

```
sawyer@sawyer-System-Product-Name:~$ nslookup -type=ns cogeco.local
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
*** Can't find cogeco.local: No answer

Authoritative answers can be found from:

sawyer@sawyer-System-Product-Name:~$ nslookup -type=mx cogeco.local
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
*** Can't find cogeco.local: No answer

Authoritative answers can be found from:

sawyer@sawyer-System-Product-Name:~$ nslookup -type=a cogeco.local
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   cogeco.local
Address: 192.168.0.1
```

d) https://www.reddit.com/ uses multiple IP addresses.

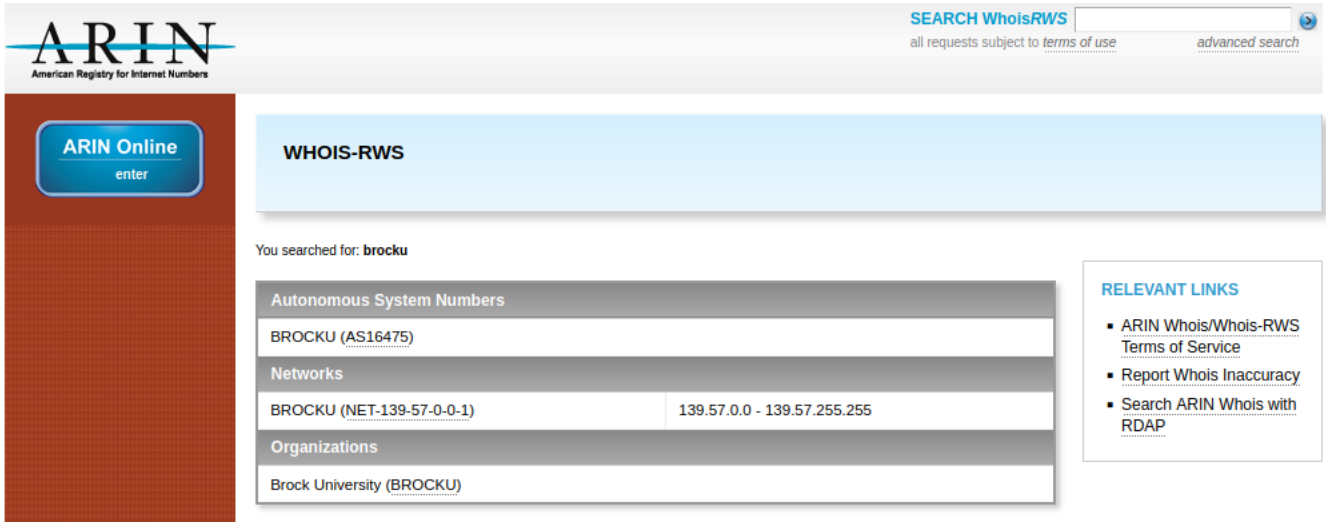
```
sawyer@sawyer-System-Product-Name:~$ nslookup reddit.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   reddit.com
Address: 151.101.65.140
Name:   reddit.com
Address: 151.101.193.140
Name:   reddit.com
Address: 151.101.1.140
Name:   reddit.com
Address: 151.101.129.140
```

Brock University does have multiple IP addresses but they do not appear in an nslookup call:

```
sawyer@sawyer-System-Product-Name:~$ nslookup brocku.ca
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   brocku.ca
Address: 139.57.65.11

sawyer@sawyer-System-Product-Name:~$ nslookup cosc.brocku.ca
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   cosc.brocku.ca
Address: 139.57.100.6
```

You can see here that brocku.ca has an IP Address that differs from cosc.brocku.ca but they are run from the same server.

e) The IP address range used by Brock University is 139.57.0.0 - 139.57.255.255.



f) An attacker could use the whois database to find IP and domain information about the institution. Then they could use nslookup on the addresses that they found in order to get even more detailed information.

g) Whois databases should be publicly available because they are used to find out registration and IP information about domains. If someone wants to gain information about a domain, perhaps they are interested in purchasing the domain, or there is content on the site that is defamatory or inappropriate for the site someone could use the whois database to contact that person and inform them.

Problem 2

In this question, we use the useful dig tool available on Unix and Linux hosts to explore the hierarchy of DNS servers. Recall that a DNS server in the DNS hierarchy delegates a DNS query to a DNS server lower in the hierarchy, by sending back to the DNS client the name of that lower-level DNS server. First read the man page for dig, and then answer the following questions.

2.a. Starting with a root DNS server (from one of the root servers [a-m].root-servers.net), initiate a sequence of queries for the IP address for your department's Web server by using dig. Show the list of the names of DNS servers in the delegation chain in answering your query.

2.b. Repeat part (a) for several popular Web sites, such as google.com, yahoo.com, or amazon.com

Solution

a)

cosc.brocku.ca
a.root-servers.net
c.ca-servers.ca
ns1.d-zone.ca
139.57.100.6

```
sawyer@sawyer-System-Product-Name:~$ dig @a.root-servers.net any www.cosc.brocku.ca

; <<>> DiG 9.16.1-Ubuntu <<>> @a.root-servers.net any www.cosc.brocku.ca
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20301
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.cosc.brocku.ca.            IN      ANY

;; AUTHORITY SECTION:
ca.                     172800  IN      NS      c.ca-servers.ca.
ca.                     172800  IN      NS      j.ca-servers.ca.
ca.                     172800  IN      NS      x.ca-servers.ca.
ca.                     172800  IN      NS      any.ca-servers.ca.

;; ADDITIONAL SECTION:
c.ca-servers.ca.        172800  IN      A       185.159.196.2
j.ca-servers.ca.        172800  IN      A       198.182.167.1
x.ca-servers.ca.        172800  IN      A       199.253.250.68
any.ca-servers.ca.      172800  IN      A       199.4.144.2
c.ca-servers.ca.        172800  IN      AAAA    2620:10a:8053::2
j.ca-servers.ca.        172800  IN      AAAA    2001:500:83::1
x.ca-servers.ca.        172800  IN      AAAA    2620:10a:80ba::68
any.ca-servers.ca.      172800  IN      AAAA    2001:500:a7::2

;; Query time: 23 msec
;; SERVER: 2001:503:ba3e::2:30#53(2001:503:ba3e::2:30)
;; WHEN: Fri Oct 01 19:39:25 EDT 2021
;; MSG SIZE  rcvd: 300
```

```
sawyer@sawyer-System-Product-Name:~$ dig @c.ca-servers.ca any www.cosc.brocku.ca

; <<>> DiG 9.16.1-Ubuntu <<>> @c.ca-servers.ca any www.cosc.brocku.ca
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60086
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.cosc.brocku.ca.            IN      ANY

;; AUTHORITY SECTION:
brocku.ca.              86400   IN      NS      ns1.d-zone.ca.
brocku.ca.              86400   IN      NS      ns2.d-zone.ca.

;; ADDITIONAL SECTION:
ns1.d-zone.ca.          86400   IN      A       162.219.54.2
ns1.d-zone.ca.          86400   IN      AAAA    2620:10a:80eb::2
ns2.d-zone.ca.          86400   IN      A       162.219.55.2
ns2.d-zone.ca.          86400   IN      AAAA    2620:10a:80ec::2

;; Query time: 23 msec
;; SERVER: 2620:10a:8053::2#53(2620:10a:8053::2)
;; WHEN: Fri Oct 01 19:40:33 EDT 2021
;; MSG SIZE  rcvd: 178
```

```
sawyer@sawyer-System-Product-Name:~$ dig @ns1.d-zone.ca any www.cosc.brocku.ca

; <<>> DiG 9.16.1-Ubuntu <<>> @ns1.d-zone.ca any www.cosc.brocku.ca
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40027
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.cosc.brocku.ca.            IN      ANY

;; ANSWER SECTION:
www.cosc.brocku.ca.     86400   IN      A       139.57.100.6

;; Query time: 11 msec
;; SERVER: 2620:10a:80eb::2#53(2620:10a:80eb::2)
;; WHEN: Fri Oct 01 19:40:54 EDT 2021
;; MSG SIZE  rcvd: 63
```

b)

Google
a.root-servers.net
a.gtld-servers.net
ns2.google.com

```
sawyer@sawyer-System-Product-Name:~$ dig @a.root-servers.net any www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> @a.root-servers.net any www.google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10894
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.google.com.                        IN      ANY

;; AUTHORITY SECTION:
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
```

```
sawyer@sawyer-System-Product-Name:~$ dig @a.gtld-servers.net any www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> @a.gtld-servers.net any www.google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8063
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.google.com.                        IN      ANY

;; AUTHORITY SECTION:
google.com.             172800  IN      NS      ns2.google.com.
google.com.             172800  IN      NS      ns1.google.com.
google.com.             172800  IN      NS      ns3.google.com.
google.com.             172800  IN      NS      ns4.google.com.
```

```
sawyer@sawyer-System-Product-Name:~$ dig @ns2.google.com any www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> @ns2.google.com any www.google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38714
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.google.com.                        IN      ANY

;; ANSWER SECTION:
www.google.com.         300     IN      A       142.251.41.68
www.google.com.         300     IN      AAAA    2607:f8b0:400b:804::2004

;; Query time: 39 msec
;; SERVER: 2001:4860:4802:34::a#53(2001:4860:4802:34::a)
;; WHEN: Fri Oct 01 19:50:17 EDT 2021
;; MSG SIZE  rcvd: 87
```

Yahoo
a.root-servers.net
e.gtld-servers.net
ns1.yahoo.com

```
sawyer@sawyer-System-Product-Name:~$ dig @a.root-servers.net any www.yahoo.com

; <<>> DiG 9.16.1-Ubuntu <<>> @a.root-servers.net any www.yahoo.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12393
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.yahoo.com.                 IN      ANY

;; AUTHORITY SECTION:
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
```

```
sawyer@sawyer-System-Product-Name:~$ dig @e.gtld-servers.net any www.yahoo.com

; <<>> DiG 9.16.1-Ubuntu <<>> @e.gtld-servers.net any www.yahoo.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16420
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 10
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.yahoo.com.                 IN      ANY

;; AUTHORITY SECTION:
yahoo.com.              172800  IN      NS      ns1.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns3.yahoo.com.
yahoo.com.              172800  IN      NS      ns4.yahoo.com.
```

```
sawyer@sawyer-System-Product-Name:~$ dig @ns5.yahoo.com any www.yahoo.com

; <<>> DiG 9.16.1-Ubuntu <<>> @ns5.yahoo.com any www.yahoo.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18800
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 10
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1272
; COOKIE: d77abe25333cbec3e268c2d16157edb914c7a7bd08f28cae (good)
;; QUESTION SECTION:
;www.yahoo.com.                 IN      ANY

;; ANSWER SECTION:
www.yahoo.com.          60      IN      CNAME   new-fp-shed.wg1.b.yahoo.com.

;; AUTHORITY SECTION:
yahoo.com.              172800  IN      NS      ns4.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns1.yahoo.com.
yahoo.com.              172800  IN      NS      ns3.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          86400   IN      AAAA    2001:4998:1b0::7961:686f:6f21
ns2.yahoo.com.          86400   IN      AAAA    2001:4998:1c0::7961:686f:6f21
ns3.yahoo.com.          1800    IN      AAAA    2406:8600:f03f:1f8::1003
ns5.yahoo.com.          86400   IN      AAAA    2406:2000:1d0::7961:686f:6f21
ns1.yahoo.com.          1209600 IN      A       68.180.131.16
ns2.yahoo.com.          1209600 IN      A       68.142.255.16
ns3.yahoo.com.          1800    IN      A       27.123.42.42
ns4.yahoo.com.          1209600 IN      A       98.138.11.157
ns5.yahoo.com.          86400   IN      A       202.165.97.53
```

Problem 3

In this question, we will observe/analyze application-layer packets using a sniffer - Wireshark

3.1. HTTP

3.1.a.

(i) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
(ii) What languages (if any) does your browser indicate that it can accept to the server?
(iii) What is the IP address of your computer? Of the gaia.cs.umass.edu server?
(iv) What is the status code returned from the server to your browser?
(v) When was the HTML file that you are retrieving last modified at the server?
(vi) How many bytes of content are being returned to your browser?
(vii) By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

3.1.b

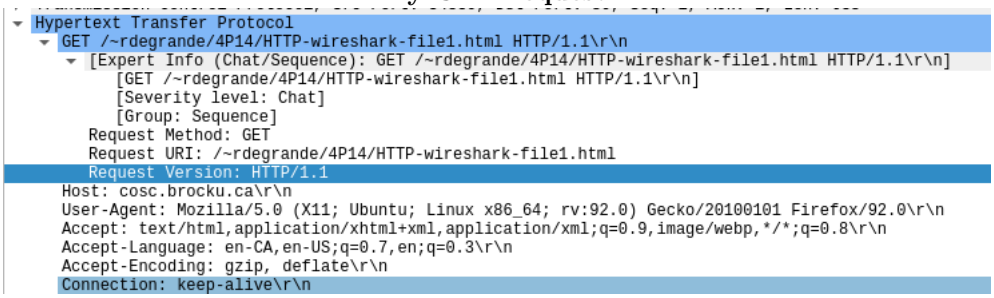
(i) How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
(ii) Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
(iii) What is the status code and phrase in the response?
(iv) How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Solution

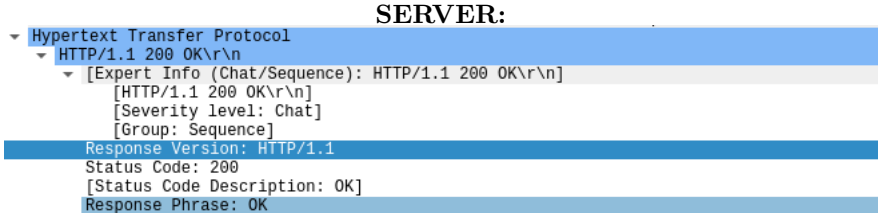
3.1.a

(i) Both are running HTTP 1.1

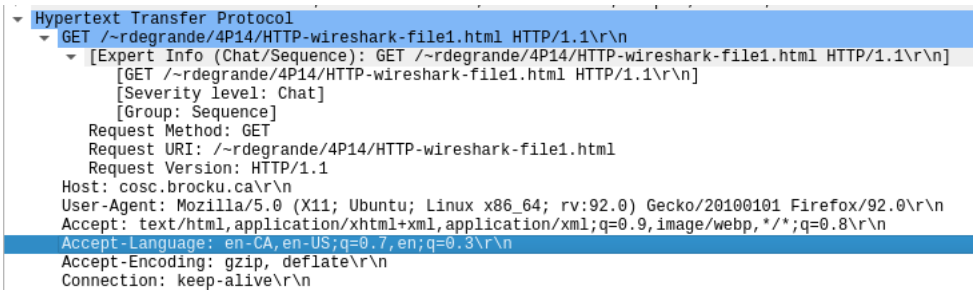
My GET request:



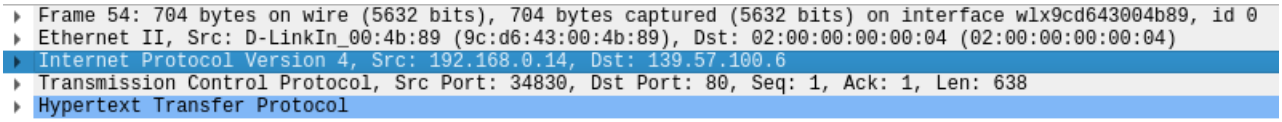
SERVER:



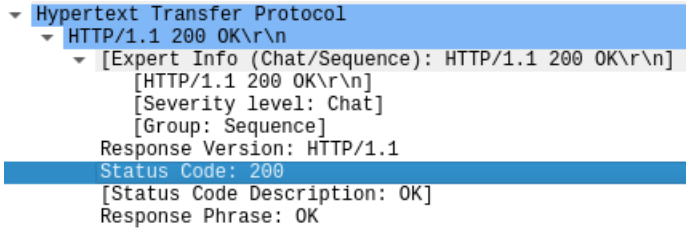
(ii) english - Canada, english - United States



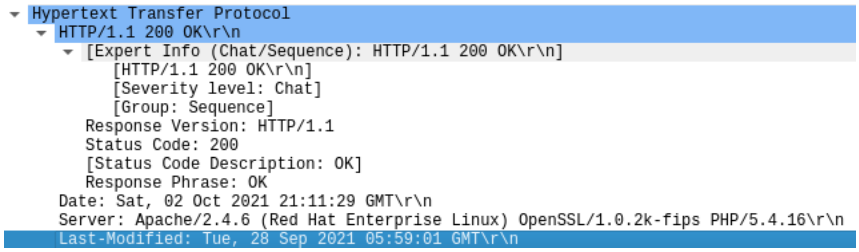
(iii) my computer: 192.168.0.14 , server: 139.57.100.6



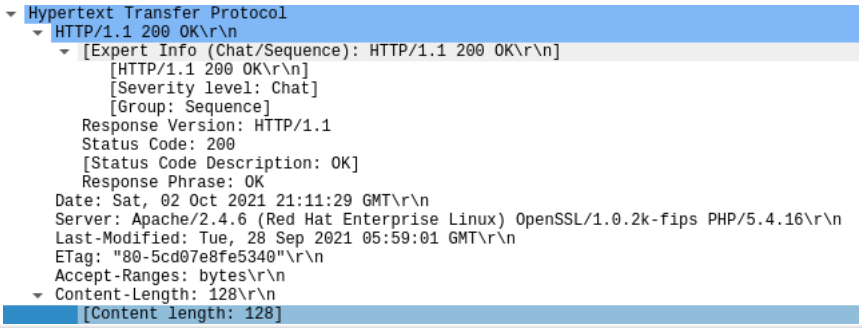
(iv) Status Code is 200

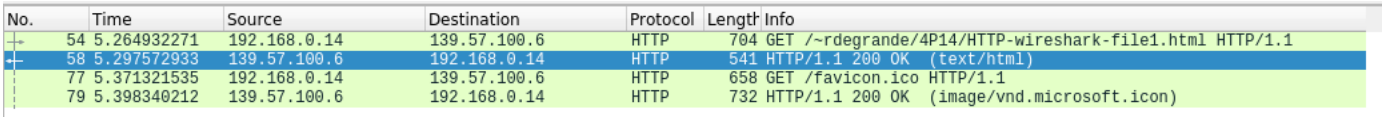


(v) Tuesday September 28 2021 05:59:01 GMT



(vi) 128 Bytes

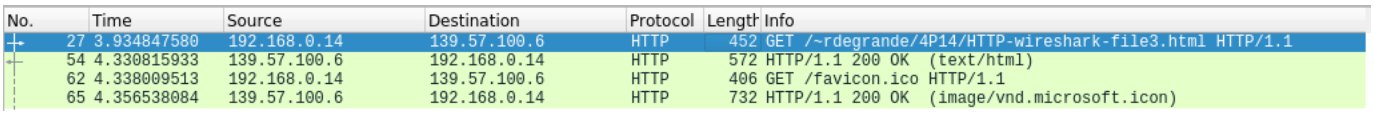




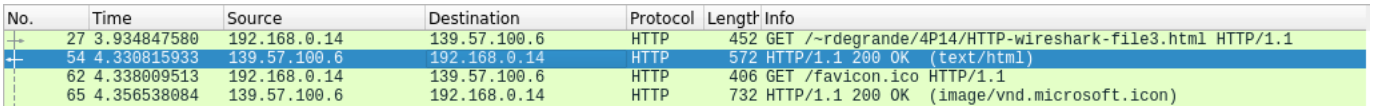
(vii) No, I don't see any.

3.1.b

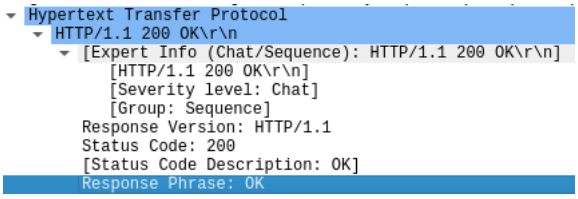
(i) 2 GET Requests, Packet containing GET request for Bill of Rights: 27



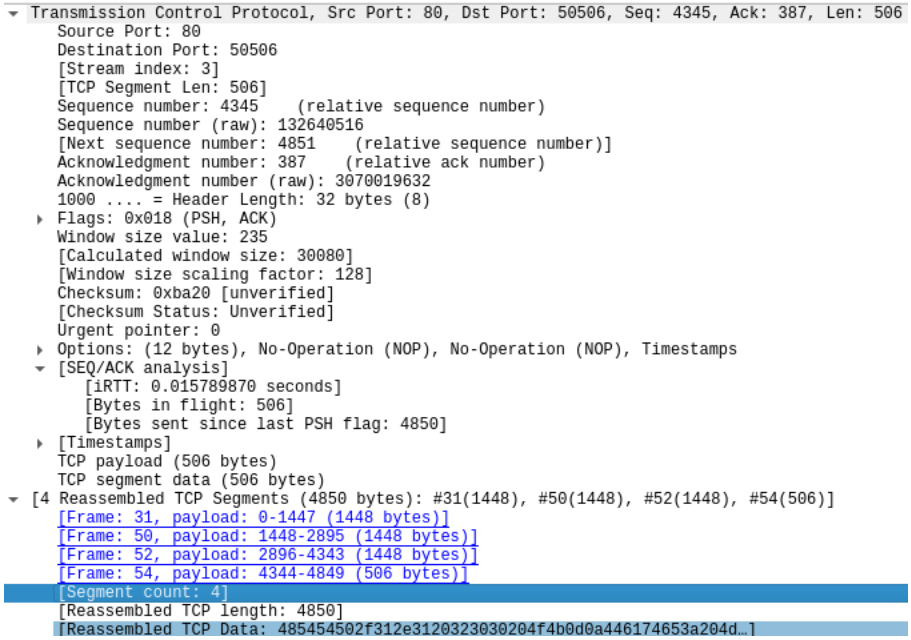
(ii) Packet number: 54



(iii) Status Code: 200, response: OK



(iv) 4 TCP Segments



Problem 3

In this question, we will observe/analyze application-layer packets using a sniffer - Wireshark

3.2. DNS

3.2.a

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

(ii) What is the destination port for the DNS query message? What is the source port of DNS response message?

(iii) To what IP address is the DNS query message sent? Use ifconfig (and other tools) to determine the IP address of your local DNS server. Are these two IP addresses the same?

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

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

3.2.b

(i) What is the destination port for the DNS query message? What is the source port of DNS response message?

(ii) To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

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

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

(v) Provide a screenshot.

Solution

3.2.a

(i) DNS query and response messages:

No.	Time	Source	Destination	Protocol	Length	Info
42	2.996341629	192.168.0.14	192.168.0.1	DNS	83	Standard query 0xfc80 A www.ietf.org OPT
43	2.996471301	192.168.0.14	192.168.0.1	DNS	83	Standard query 0x52b7 AAAA www.ietf.org OPT
44	2.996593659	192.168.0.14	192.168.0.1	DNS	102	Standard query 0xc275 A www.ietf.org.cdn.cloudflare.net OPT
46	2.996749781	192.168.0.14	192.168.0.1	DNS	102	Standard query 0xf75c AAAA www.ietf.org.cdn.cloudflare.net OPT
49	3.021084264	192.168.0.1	192.168.0.14	DNS	160	Standard query response 0xfc80 A www.ietf.org CNAME www.ietf.…
50	3.026340761	192.168.0.1	192.168.0.14	DNS	134	Standard query response 0xc275 A www.ietf.org.cdn.cloudflare.…
55	3.047039694	192.168.0.1	192.168.0.14	DNS	158	Standard query response 0xf75c AAAA www.ietf.org.cdn.cloudfla…
56	3.051176901	192.168.0.1	192.168.0.14	DNS	184	Standard query response 0x52b7 AAAA www.ietf.org CNAME www.ie…

Query and Response are both sent over UDP:

```
▸ Frame 42: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface wlx9cd643004b89, id 0
▸ Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
▸ Internet Protocol Version 4, Src: 192.168.0.14, Dst: 192.168.0.1
▸ User Datagram Protocol, Src Port: 32915, Dst Port: 53
▸ Domain Name System (query)
```

```
▸ Frame 49: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface wlx9cd643004b89, id 0
▸ Ethernet II, Src: 02:00:00:00:00:04 (02:00:00:00:00:04), Dst: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89)
▸ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.14
▸ User Datagram Protocol, Src Port: 53, Dst Port: 32915
▸ Domain Name System (response)
```

(ii) Both are port 53 (see above)
Query: User Datagram Protocol, Dst Port: 53
Response: User Datagram Protocol, Src Port: 53
(iii) DNS Query Message is sent to IP Address: 192.168.0.1

```
42 2.996341629  192.168.0.14  192.168.0.1  DNS  83 Standard query 0xfc80 A www.ietf.org OPT
```

DNS Server IP Address: 192.168.0.1

```
Link 3 (wlx9cd643004b89)
      Current Scopes: DNS
DefaultRoute setting: yes
       LLMNR setting: yes
MulticastDNS setting: no
  DNSOverTLS setting: no
      DNSSEC setting: no
    DNSSEC supported: no
  Current DNS Server: 2001:1970:5ba3:b100:0:ff:fe00:4
         DNS Servers: 192.168.0.1
                      2001:1970:5ba3:b100:0:ff:fe00:4
                      2001:1970:c06e:c0::93
                      2001:1970:c0c0:6ec0::193
          DNS Domain: ~.
                      cogeco.local
```

These are the same.
(iv) There are two types of DNS Queries here: A (Host Address) and AAAA (IPv6 Address). There are no answers.

```
▾ Domain Name System (query)
    Transaction ID: 0xfc80
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ 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)
```

```
▾ Domain Name System (query)
    Transaction ID: 0x52b7
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ www.ietf.org: type AAAA, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
```

(v) The response to Query Type A has 3 answers. The response to Query Type AAAA has 2 answers. Both contain: Name, Type, Class, Time to live, Data length, Address.

```
▾ Domain Name System (response)
    Transaction ID: 0xfc80
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Answers
    ▾ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        Name: www.ietf.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 2907 (48 minutes, 27 seconds)
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
    ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
▾ Domain Name System (response)
    Transaction ID: 0xf75c
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Answers
    ▾ www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700::6810:2d63
        Name: www.ietf.org.cdn.cloudflare.net
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 114 (1 minute, 54 seconds)
        Data length: 16
        AAAA Address: 2606:4700::6810:2d63
    ▸ www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700::6810:2c63
```

3.2.b

(i) Query Destination Port: 53, Response Source Port: 53

```
▸ Frame 17: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface wlx9cd643004b89, id 0
▸ Ethernet II, Src: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
▸ Internet Protocol Version 6, Src: 2001:1970:5ba3:b100:af18:8cd6:9982:b633, Dst: 2001:1970:5ba3:b100:0:ff:fe00:4
▸ User Datagram Protocol, Src Port: 40876, Dst Port: 53
▸ Domain Name System (query)
▸ Frame 18: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface wlx9cd643004b89, id 0
▸ Ethernet II, Src: 02:00:00:00:00:04 (02:00:00:00:00:04), Dst: D-LinkIn_00:4b:89 (9c:d6:43:00:4b:89)
▸ Internet Protocol Version 6, Src: 2001:1970:5ba3:b100:0:ff:fe00:4, Dst: 2001:1970:5ba3:b100:af18:8cd6:9982:b633
▸ User Datagram Protocol, Src Port: 53, Dst Port: 40876
▸ Domain Name System (response)
```

(ii) Query Destination IP Address: 2001:1970:5ba3:b100:0:ff:fe00:4

No.	Time	Source	Destination	Protoc	Length	Info
17	7.256687613	2001:1970:5ba3:b100:af18:8cd6:9982:b633	2001:1970:5ba3:b100:0:ff:fe00:4	DNS	102	Standard query 0xf4c6 A www.mi
18	7.289933325	2001:1970:5ba3:b100:0:ff:fe00:4	2001:1970:5ba3:b100:af18:8cd6:9982:b633	DNS	191	Standard query response 0xf4c6

DNS Server: 2001:1970:5ba3:b100:0:ff:fe00:4

```
Link 3 (wlx9cd643004b89)
      Current Scopes: DNS
DefaultRoute setting: yes
       LLMNR setting: yes
MulticastDNS setting: no
  DNSOverTLS setting: no
      DNSSEC setting: no
    DNSSEC supported: no
  Current DNS Server: 2001:1970:5ba3:b100:0:ff:fe00:4
         DNS Servers: 192.168.0.1
                      2001:1970:5ba3:b100:0:ff:fe00:4
                      2001:1970:c06e:c0::93
                      2001:1970:c0c0:6ec0::193
          DNS Domain: ~.
                      cogeco.local
```

(iii) DNS Query Type: A (Host Address) , No answers.

```
▾ Domain Name System (query)
    Transaction ID: 0xf4c6
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ 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)
```

(iv) 3 Answers containing: Name, Type, Class, Time to live, Data length, CNAME

```
▾ Domain Name System (response)
    Transaction ID: 0xf4c6
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ 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: 1358 (22 minutes, 38 seconds)
        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: 2545 (42 minutes, 25 seconds)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    ▾ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.78.114.33
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 2545 (42 minutes, 25 seconds)
        Data length: 4
        Address: 104.78.114.33
```

Problem 4

In this programming question, you will write a client ping program in Java. Your client will send a simple ping message to a server, receive a corresponding pong message back from the server, and determine the delay between when the client sent the ping message and received the pong message. This delay is called the Round Trip Time (RTT). The functionality provided by the client and server is similar to the functionality provided by standard ping program available in modern operating systems. However, standard ping programs use the Internet Control Message Protocol (ICMP), which we will study later in this course. Here we will create a nonstandard (but simple!) UDP-based ping program. Your ping program is to send 10 ping messages to the target server over UDP. For each message, your client is to determine and print the RTT when the corresponding pong message is returned. Because UDP is an unreliable protocol, a packet sent by the client or server may be lost. For this reason, the client cannot wait indefinitely for a reply to a ping message. You should have the client wait up to one second for a reply from the server; if no reply is received, the client should assume that the packet was lost and print a message accordingly. In this question, your job is to write the client and server codes; both codes (client and server) will be very similar to each other. It is recommended that you first design the server code. You can then write your client code based on the server code, liberally cutting and pasting some lines from the server code.

Solution

You can find my UDPServer and UDPClient code in the file titled "Java" in the submission file. First run the server, then run the client. The client automatically pings the server 10 times and calculates RTT in nanoseconds for each client ping. The screenshots below show the ping / pong server client responses and also what happens if you run the client without a server (to test the timeout, I wasn't getting any timeouts on my end).

Server receives Pings from Client

```
sawyer@sawyer-System-Product-Name:~/Desktop/4P14/Labs/Lab2/Submission/Java$ java UDPServer
ping from Client
ping from Client
ping from Client
ping from Client
ping from Client
ping from Client
ping from Client
ping from Client
ping from Client
ping from Client
```

Client sends 10 Pings to Server, RTT time per packet shown

```
sawyer@sawyer-System-Product-Name:~/Desktop/4P14/Labs/Lab2/Submission/Java$ java UDPClient
Pinging Server 10 Times...
RTT for Packet 0 = 17560829 nano seconds
PING
RTT for Packet 1 = 438345 nano seconds
PING
RTT for Packet 2 = 254339 nano seconds
PING
RTT for Packet 3 = 205597 nano seconds
PING
RTT for Packet 4 = 210917 nano seconds
PING
RTT for Packet 5 = 204866 nano seconds
PING
RTT for Packet 6 = 217259 nano seconds
PING
RTT for Packet 7 = 209655 nano seconds
PING
RTT for Packet 8 = 214364 nano seconds
PING
RTT for Packet 9 = 215266 nano seconds
PING
```

All 10 packets timeout

```
sawyer@sawyer-System-Product-Name:~/Desktop/4P14/Labs/Lab2/Submission/Java$ java UDPClient
Pinging Server 10 Times...
Timeout on Packet 0
Timeout on Packet 1
Timeout on Packet 2
Timeout on Packet 3
Timeout on Packet 4
Timeout on Packet 5
Timeout on Packet 6
Timeout on Packet 7
Timeout on Packet 8
Timeout on Packet 9
```