Lab 2 Jed Alcantara

Tuesday, February 14, 2023 10:47 PM

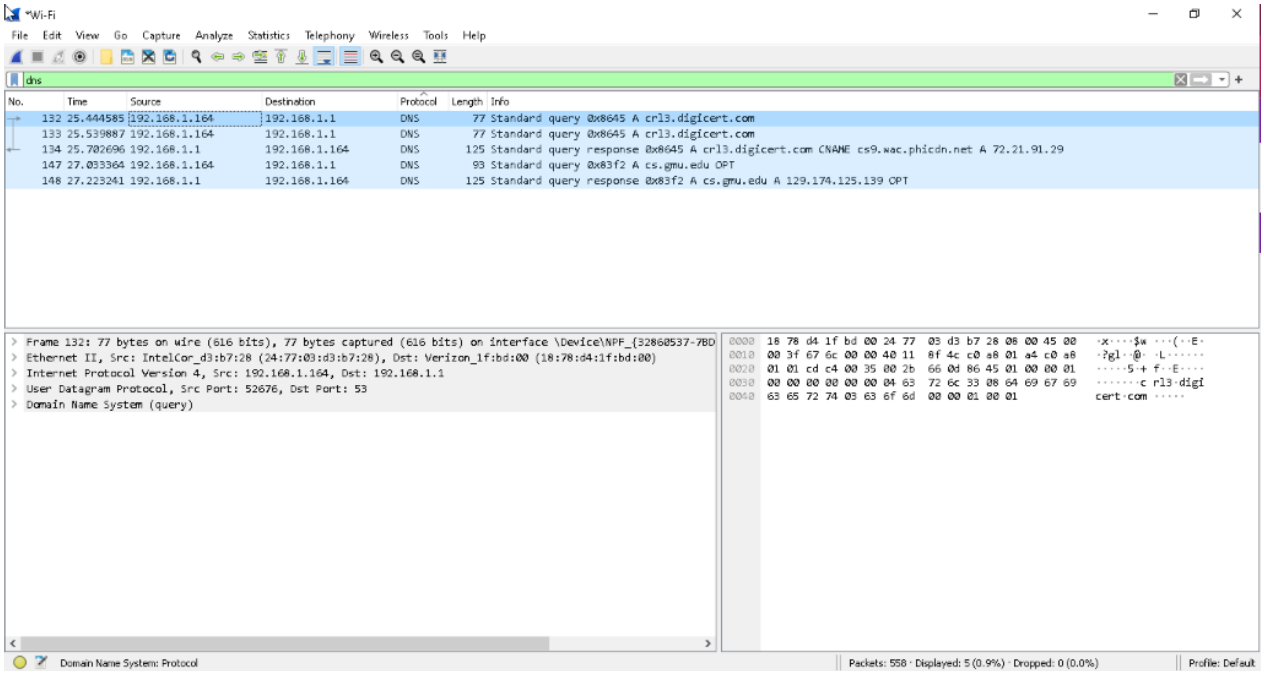
G00846927

A. Provide the dig output and a screenshot of the DNS query and response message from Wireshark

a.

```
JADDY% dig cs.gmu.edu

; <<>> DiG 9.16.37 <<>> cs.gmu.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33778
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d49226e31a3ceab23db9866863ec49ba4109e2ee32c8bf90 (good)
;; QUESTION SECTION:
;cs.gmu.edu.                    IN      A

;; ANSWER SECTION:
cs.gmu.edu.             381     IN      A       129.174.125.139

;; Query time: 190 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Feb 15 02:55:55 Ame 2023
;; MSG SIZE  rcvd: 83
```

b.



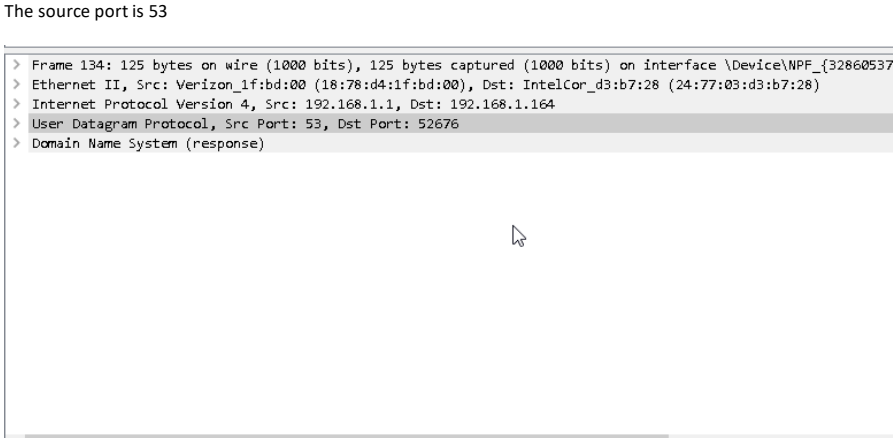
B. Locate the DNS query and response messages in Wireshark capture. What is the IP address of your local DNS server?

a. The address of my local DNS server is 192.168.1.1
b. The address of my router is 192.168.1.164

C. Are the DNS query and response messages sent over UDP or TCP? What is the destination port for the DNS query message? What is the source port for the DNS response message?

a. They were sent over UDP.
b. The destination port is 52676
c. The source port is 53

d.



D. Examine the DNS query message. What "type" of DNS query is it?
   a. This a standard query 0x8645 A
   b.

133	25.539887	192.168.1.164	192.168.1.1	DNS	77	Standard query 0x8645 A crl3.digicert.com
134	25.702696	192.168.1.1	192.168.1.164	DNS	125	Standard query response 0x8645 A crl3.digicert.com CNAME cs9.wac.phicdn.net A 72.21.91.29
147	27.033364	192.168.1.164	192.168.1.1	DNS	93	Standard query 0x83f2 A cs.gmu.edu OPT

E. Examine the DNS response message. How many "answers" are provided (ignore the type OPT records as stated above)? What is the IP address that the hostname resolves to?
   a. There is 1 answer provided.
   b. The ip address is 129.174.125.139 and the host name is cs.gmu.edu
   c.

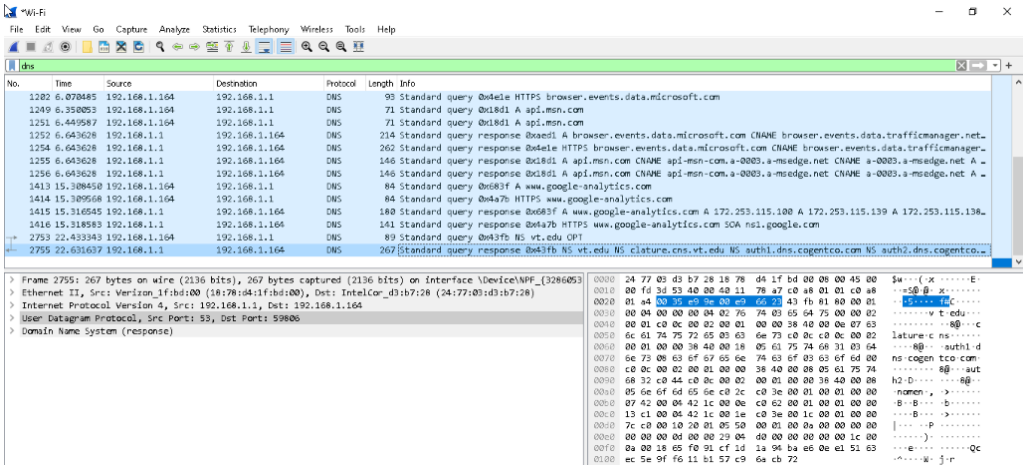
```
JADDY% dig cs.gmu.edu

; <<>> DiG 9.16.37 <<>> cs.gmu.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33778
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d49226e31a3ceab23db9866863ec49ba4109e2ee32c8bf90 (good)
;; QUESTION SECTION:
;cs.gmu.edu.                    IN      A

;; ANSWER SECTION:
cs.gmu.edu.             381     IN      A       129.174.125.139

;; Query time: 190 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Feb 15 02:55:55 Ame 2023
;; MSG SIZE  rcvd: 83
```

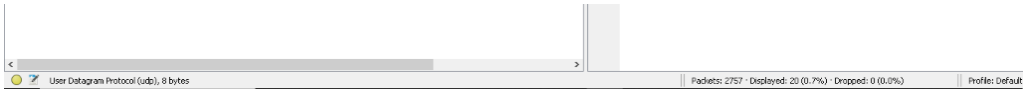
Part II

a. Let's run the above command to know the DNS servers of Virginia Tech University.
   a. $> dig vt.edu NS
   b. List the DNS servers of vt.edu using dig output and DNS response message.
      i. clature.cns.vt.edu.
      ii. auth1.dns.cogentco.com.
      iii. auth2.dns.cogentco.com.
      iv. nomen.cns.vt.edu.
   c.

```
JADDY% dig vt.edu NS

; <<>> DiG 9.16.37 <<>> vt.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17403
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 65f091cf1d1a94bae60ee15163ec5e9ff611b157c96acb72 (good)
;; QUESTION SECTION:
;vt.edu.                        IN      NS

;; ANSWER SECTION:
vt.edu.                 14400   IN      NS      clature.cns.vt.edu.
vt.edu.                 14400   IN      NS      auth1.dns.cogentco.com.
vt.edu.                 14400   IN      NS      auth2.dns.cogentco.com.
vt.edu.                 14400   IN      NS      nomen.cns.vt.edu.

;; ADDITIONAL SECTION:
auth1.dns.cogentco.com. 1858    IN      A       66.28.0.14
auth2.dns.cogentco.com. 5057    IN      A       66.28.0.30
auth1.dns.cogentco.com. 31936   IN      AAAA    2001:550:1:a::d

;; Query time: 198 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Feb 15 04:25:04 Ame 2023
;; MSG SIZE  rcvd: 225
```

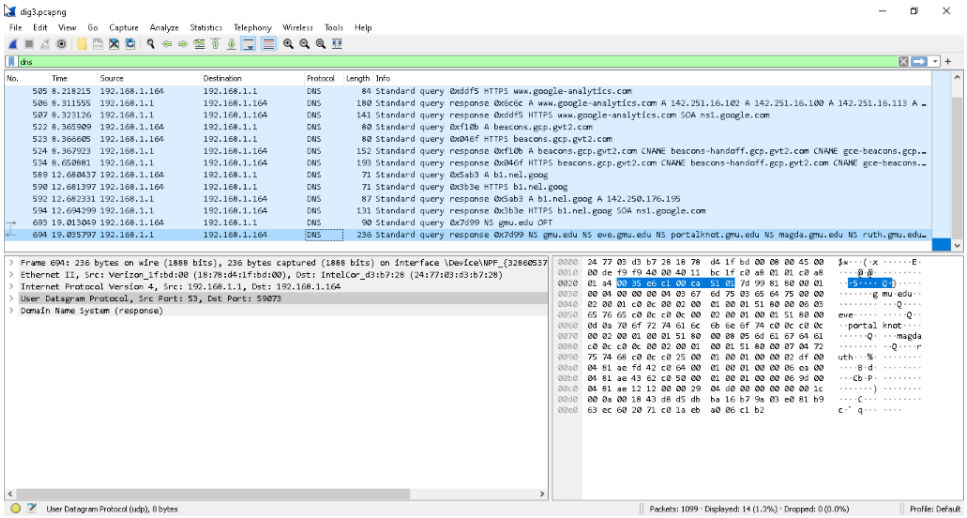
   d.





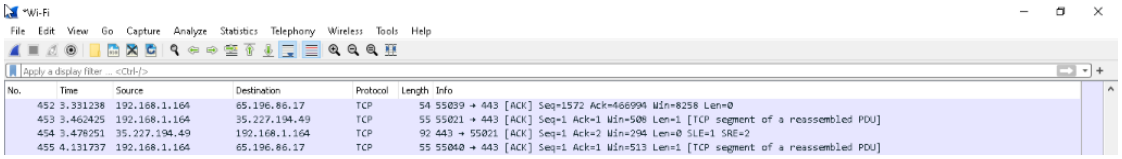
b. Using the same command, find all DNS servers used by gmu.edu domain.
   i. eve.gmu.edu.
   ii. portalknot.gmu.edu.
   iii. magda.gmu.edu.
   iv. ruth.gmu.edu.

a.
```
JADDY% dig gmu.edu NS

; <<>> DiG 9.16.37 <<>> gmu.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32153
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 43d8d5dbba16b79a03e081b963ec602071c01aeba006c1b2 (good)
;; QUESTION SECTION:
;gmu.edu.                       IN      NS

;; ANSWER SECTION:
gmu.edu.                86400   IN      NS      eve.gmu.edu.
gmu.edu.                86400   IN      NS      portalknot.gmu.edu.
gmu.edu.                86400   IN      NS      magda.gmu.edu.
gmu.edu.                86400   IN      NS      ruth.gmu.edu.

;; ADDITIONAL SECTION:
eve.gmu.edu.            735     IN      A       129.174.253.66
ruth.gmu.edu.           1770    IN      A       129.174.67.98
magda.gmu.edu.          1693    IN      A       129.174.18.18

;; Query time: 15 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Feb 15 04:31:29 Ame 2023
;; MSG SIZE  rcvd: 194
```

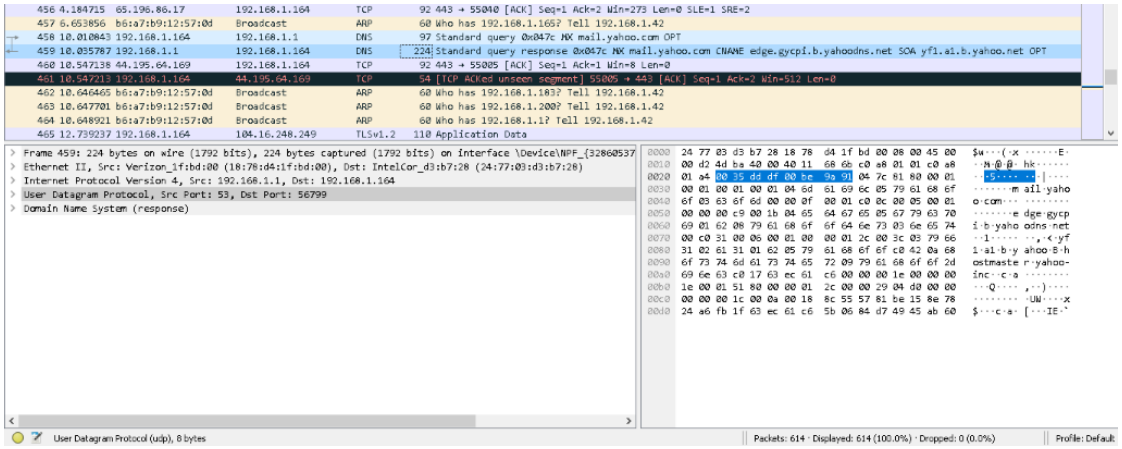
b.


c. Using MX as the type, find out the mail servers for yahoo.com.
   i. Edge.gycpi.b.yahoodns.net

a.
```
JADDY% dig mail.yahoo.com mx

; <<>> DiG 9.16.37 <<>> mail.yahoo.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1148
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8c555781be158e7824a6fb1f63ec61c65b0684d74945ab60 (good)
;; QUESTION SECTION:
;mail.yahoo.com.                IN      MX

;; ANSWER SECTION:
mail.yahoo.com.         201     IN      CNAME   edge.gycpi.b.yahoodns.net.

;; AUTHORITY SECTION:
gycpi.b.yahoodns.net.   300     IN      SOA     yf1.a1.b.yahoo.net. hostmaster.yahoo-inc.com. 1676435910 30 30 86400 300

;; Query time: 29 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Feb 15 04:38:31 Ame 2023
;; MSG SIZE  rcvd: 182
```



b.



d. Using CNAME as the type, find out the canonical name (CNAME) of www.wikipedia.org
   a. Dyna.wikipedia.org
   b.

c.

```
DADDY% dig www.wikipedia.org CNAME

; <<>> DiG 9.16.37 <<>> www.wikipedia.org CNAME
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31060
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7f8f51047aff542135a6ffbc63ec639698e05da736db867a (good)
;; QUESTION SECTION:
;www.wikipedia.org.             IN      CNAME

;; ANSWER SECTION:
www.wikipedia.org.      67414   IN      CNAME   dyna.wikimedia.org.

;; Query time: 13 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Feb 15 04:46:14 Ame 2023
;; MSG SIZE  rcvd: 103
```

d.