

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

```
JADDDY% dig cs.gmu.edu

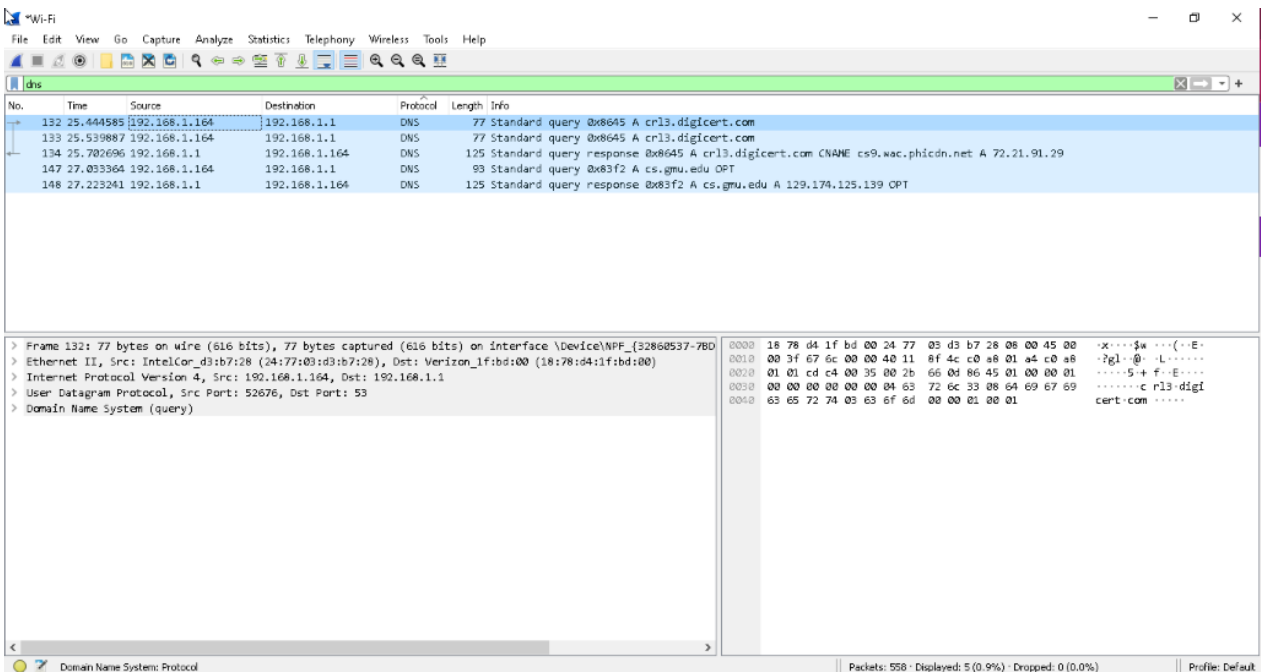
; <<> DiG 9.16.37 <<> cs.gmu.edu
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 33778
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; 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 AM 2023
;; MSG SIZE rcvd: 83
```

a.



b.

> Frame 132: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{32860537-78D...}

> Ethernet II, Src: IntelCor_d3:b7:28 (24:77:03:d3:b7:28), Dst: Verizon_1f:bd:00 (18:78:d4:1f:bd:00)

> Internet Protocol Version 4, Src: 192.168.1.164, Dst: 192.168.1.1

> User Datagram Protocol, Src Port: 52676, Dst Port: 53

> Domain Name System (query)

0000 16 78 d4 1f bd 00 24 77 03 d3 b7 28 08 00 45 00 .x...\$w ...(..E:..

0010 00 3f 67 6c 00 00 40 11 8f 4c c0 a8 01 a4 c0 a8 ?gl..@..L.....

0020 01 01 cd c4 00 35 00 2b 66 0d 86 45 01 00 00 015+ f..E.....

0030 00 00 00 00 00 04 63 72 6c 33 08 64 69 67 69c r13 digf

0040 63 65 72 74 03 63 6f 6d 00 00 01 00 01cert.com

- B. Locate the DNS query and response messages in Wireshark capture. What is the IP address of your local DNS server?
- The address of my local DNS server is 192.168.1.1
 - 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?
- They were sent over UDP.
 - The destination port is 52676
 - The source port is 53

```
> Frame 134: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface \Device\NPF_{32860537-78D...}
```

> Ethernet II, Src: Verizon_1f:bd:00 (18:78:d4:1f:bd:00), Dst: IntelCor_d3:b7:28 (24:77:03:d3:b7:28)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.164

> User Datagram Protocol, Src Port: 53, Dst Port: 52676

> Domain Name System (response)

d.

D. Examine the DNS query message. What “type” of DNS query is it?

- a. This a standard query 0x8645 A

b.

133	25.539087	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.

- clature.cns.vt.edu.
- auth1.dns.cogentco.com.
- auth2.dns.cogentco.com.
- nomen.cns.vt.edu.

c.

```

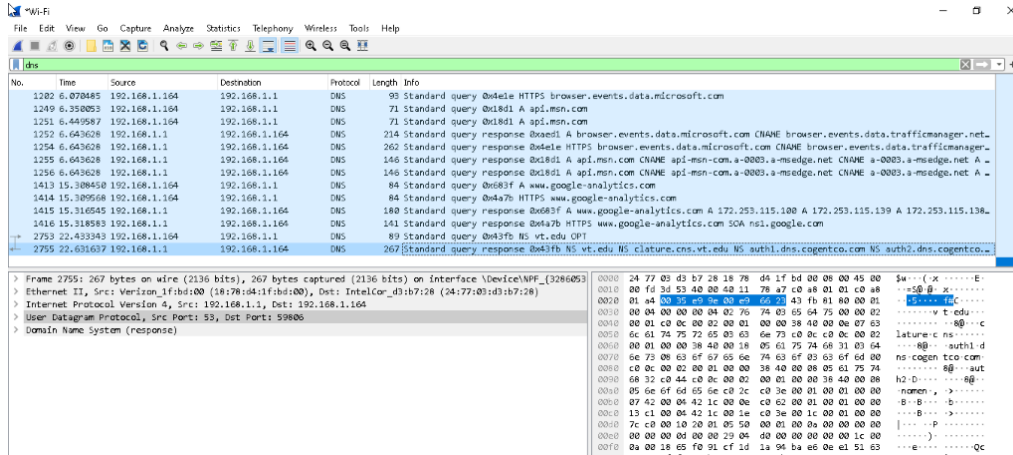
jaddy% dig vt.edu NS

; <<> 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

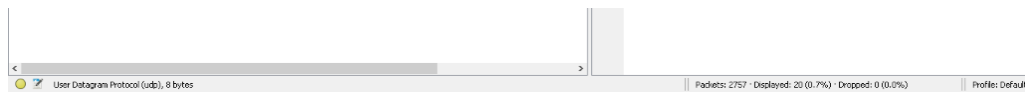
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 1232
; COOKIE: 65f091cf1d1a94bae60ee15163ec5e9ff611b157c96acb72 (good)
; QUESTION SECTION:
; vt.edu.                            IN      NS
;
; ANSWER SECTION:
; vt.edu.                            14400   IN      NS      clature.cns.vt.edu.
; vt.edu.                            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.



The Wireshark packet capture shows a DNS query and response. The query is for vt.edu NS. The response contains four NS records: clature.cns.vt.edu., auth1.dns.cogentco.com., auth2.dns.cogentco.com., and nomen.cns.vt.edu.. The packet details show the query and response structure. The packet bytes show the raw data.



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

```
DADDY% dig gmu.edu NS

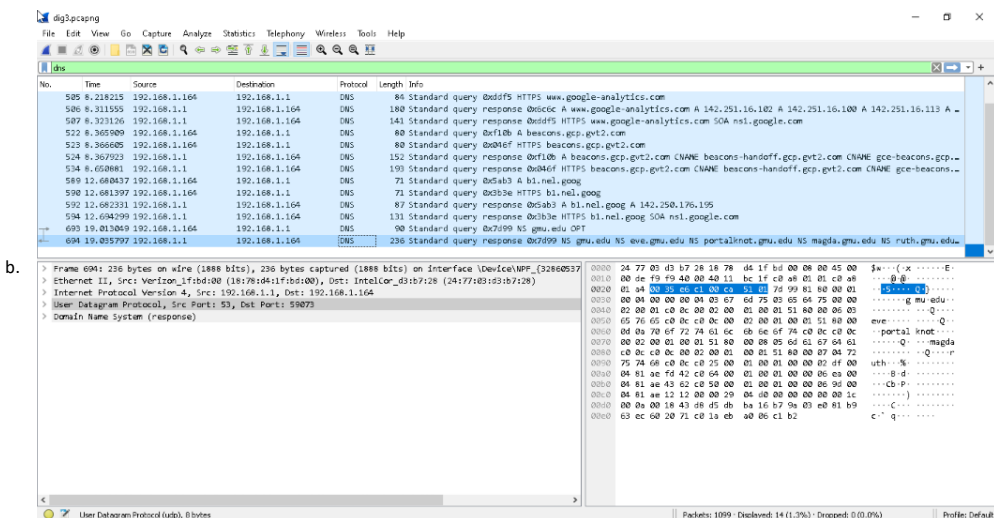
<> DiG 9.16.37 <> gmu.edu NS
; global options: +cmd
; Got answer:
->>HEADER<- opcode: QUERY, status: NOERROR, id: 32153
; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

; 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 AM 2023
; MSG SIZE rcvd: 194
```



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

```
DADDY% dig mail.yahoo.com mx

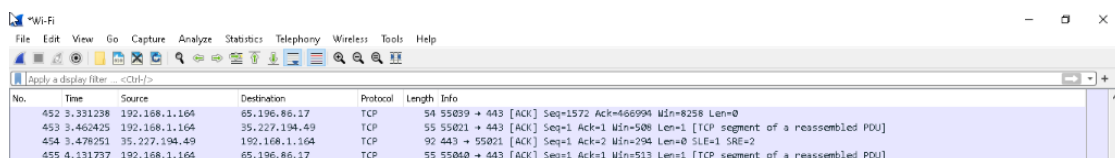
<> DiG 9.16.37 <> mail.yahoo.com mx
; global options: +cmd
; Got answer:
->>HEADER<- opcode: QUERY, status: NOERROR, id: 1148
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

; 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 AM 2023
; MSG SIZE rcvd: 182
```



456	4.18475	65.196.86.17	192.168.1.164	TCP	92	443 > 55000 [ACK] Seq=1 Ack=2 Win=273 Len=0 SLE=1 SRE=2
457	6.653856	b6:a7:b9:12:57:0d	Broadcast	ARP	68	Who has 192.168.1.165? Tell 192.168.1.42
458	10.010843	192.168.1.164	192.168.1.1	DNS	97	Standard query 0x047c NX mail.yahoo.com OPT
459	10.855787	192.168.1.1	192.168.1.164	DNS	224	Standard query response 0x047c NX mail.yahoo.com CNAME edge.gycip.b.yahoodns.net SOA yf1.a1.b.yahoo.net OPT
460	10.547138	44.195.64.169	192.168.1.164	TCP	92	443 > 55005 [ACK] Seq=1 Ack=1 Win=8 Len=0
461	10.557217	192.168.1.164	44.195.64.169	TCP	55	0000 0000 0000 0000 [RST] Seq=1 Ack=2 Win=512 Len=0
462	10.646465	b6:a7:b9:12:57:0d	Broadcast	ARP	68	Who has 192.168.1.183? Tell 192.168.1.42
463	10.647701	b6:a7:b9:12:57:0d	Broadcast	ARP	68	Who has 192.168.1.200? Tell 192.168.1.42
464	10.648921	b6:a7:b9:12:57:0d	Broadcast	ARP	68	Who has 192.168.1.1? Tell 192.168.1.42
465	12.739237	192.168.1.164	104.16.248.249	TLSv1.2	310	Application Data

```

> Frame 456: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface \Device\NPF_{32868537}
> Ethernet II, Src: Verizon_fibsd:00 (18:78:d4:f1:b0:00), Dst: IntelCom_d3:b7:28 (24:77:03:d3:b7:28)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.164
> User Datagram Protocol, Src Port: 53, Dst Port: 56799
> Domain Name System (response)

0000  24 77 03 d3 b7 28 16 78  d4 f1 bd 00 08 00 45 00  $-----x-----E-
0010  00 d2 d4 b6 40 00 40 11  68 66 c0 a8 01 01 c0 a8  -N @ @-hk-----
0020  01 94 05 16 0f 03 3c 0b  04 7c 81 80 00 01 00 00  -all-yaho
0030  00 01 00 01 00 04 5d 61  69 66 05 79 61 08 6f 00  -com-----
0040  6f 03 63 6f 6d 00 00 0f  00 01 c0 0c 00 05 01 01  o com-----
0050  00 00 c0 00 c9 00 1b 04 65  64 67 65 05 67 79 63 70  -----dge gycip
0060  01 62 08 79 61 68 6f 6f  64 64 66 73 03 66 65 74  i-b-yaho ods.net
0070  00 c0 31 00 00 00 00 00  00 01 2c 00 31 79 66 00 00  -a1-b-yahoo S-h
0080  31 02 61 31 01 62 05 79  61 68 6f 6f c0 42 04 08  ostmaster r-yahoo-
0090  6f 73 74 6d 61 73 74 65  72 09 79 61 6f 6f 6f 6d  inc-a
00a0  69 6e 63 c0 17 63 ec 61  c6 00 00 01 00 00 00 00  -Q-----
00b0  16 00 01 51 80 00 00 01  2c 00 29 09 04 00 00 00  -Q-----
00c0  00 00 00 1c 00 00 00 18  8c 55 57 81 15 8c 78 8  ------U-----
00d0  24 a6 f1 6f 63 ec 61 c6  56 84 d7 49 45 ab 60  $-----U-----E-

```

Packets: 614 · Displayed: 614 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

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

```

JADDDY% 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 AM 2023
MSG SIZE rcvd: 103

```

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, and analyzing. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is packet 37, a DNS response from 192.168.1.1 to 192.168.1.144. The details pane shows it's a standard query response for www.wikipedia.org.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and the Domain Name System (DNS) message. The DNS message details include the query type (CNAME) and the response code (0).
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII. The ASCII column shows the domain name www.wikipedia.org and the response code 0.

The status bar at the bottom indicates that 456 packets are displayed, with 2 (0.4%) dropped and 0 (0.0%) profiled.