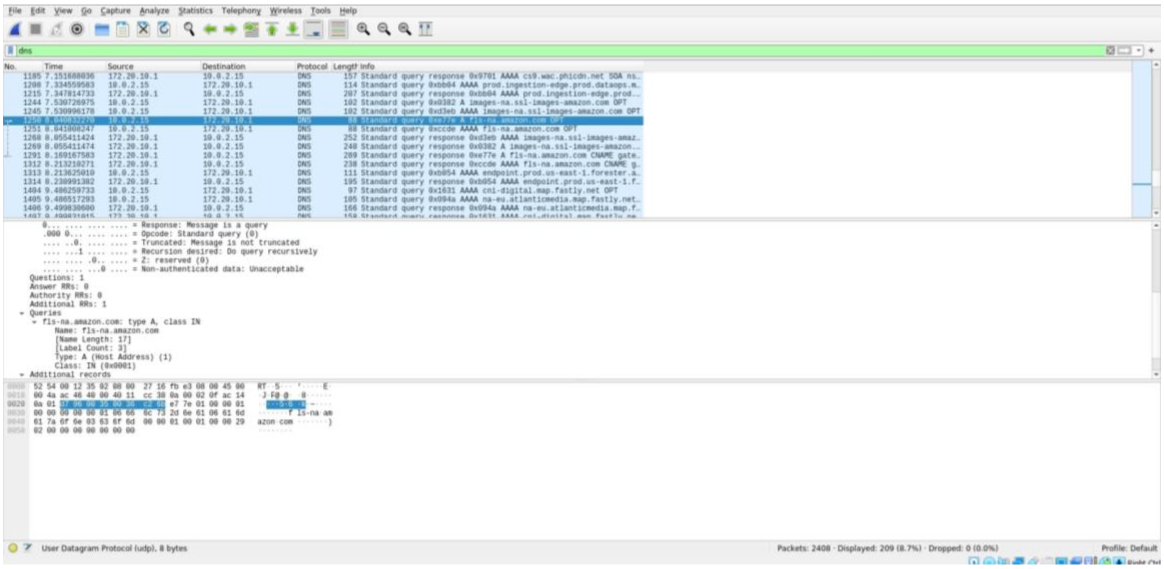
CN LAB WEEK 4

Implementation of Local DNS Server and Authoritative Nameserver

Name: Vanshika Goel	SRN: PES1UG20CS484	Section: H	Roll No: 40

Observation 1



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.   Time         Source        Destination   Protocol Length Info
 1185 7.151688036  172.20.10.1   10.0.2.15     DNS      157 Standard query response 0x9701 AAAA cs9.wac.phicdn.net SOA ns…
 1208 7.334559583  10.0.2.15     172.20.10.1   DNS      114 Standard query 0xbb04 AAAA prod.ingestion-edge.prod.dataops.m…
 1215 7.347814733  172.20.10.1   10.0.2.15     DNS      207 Standard query response 0xbb04 AAAA prod.ingestion-edge.prod…
 1244 7.530726975  10.0.2.15     172.20.10.1   DNS      102 Standard query 0x0382 A images-na.ssl-images-amazon.com OPT
 1245 7.530996178  10.0.2.15     172.20.10.1   DNS      102 Standard query 0xd3eb AAAA images-na.ssl-images-amazon.com OPT
 1250 8.040832270  10.0.2.15     172.20.10.1   DNS       88 Standard query 0xe77e A fls-na.amazon.com OPT
 1251 8.041008247  10.0.2.15     172.20.10.1   DNS       88 Standard query 0xccde AAAA fls-na.amazon.com OPT
 1268 8.055411424  172.20.10.1   10.0.2.15     DNS      252 Standard query response 0xd3eb AAAA images-na.ssl-images-amaz…
 1269 8.055411474  172.20.10.1   10.0.2.15     DNS      240 Standard query response 0x0382 A images-na.ssl-images-amazon…
 1291 8.169167583  172.20.10.1   10.0.2.15     DNS      289 Standard query response 0xe77e A fls-na.amazon.com CNAME gate…
 1312 8.213210271  172.20.10.1   10.0.2.15     DNS      238 Standard query response 0xccde AAAA fls-na.amazon.com CNAME g…
 1313 8.213625010  10.0.2.15     172.20.10.1   DNS      111 Standard query 0xb054 AAAA endpoint.prod.us-east-1.forester.a…
 1314 8.238991382  172.20.10.1   10.0.2.15     DNS      195 Standard query response 0xb054 AAAA endpoint.prod.us-east-1.f…
 1404 9.486259733  10.0.2.15     172.20.10.1   DNS       97 Standard query 0x1631 AAAA cni-digital.map.fastly.net OPT
 1405 9.486517293  10.0.2.15     172.20.10.1   DNS      105 Standard query 0x094a AAAA na-eu.atlanticmedia.map.fastly.net…
 1406 9.499830600  172.20.10.1   10.0.2.15     DNS      166 Standard query response 0x094a AAAA na-eu.atlanticmedia.map.f…
 1407 9.499831015  172.20.10.1   10.0.2.15     DNS      158 Standard query response 0x1631 AAAA cni-digital.map.fastly.ne…
```

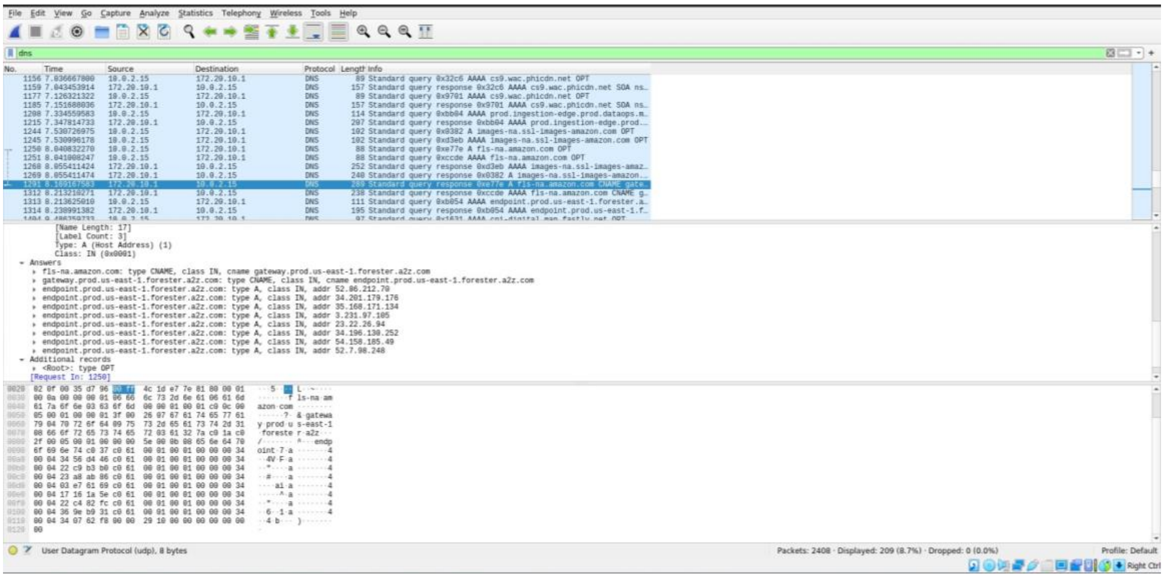
```
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ fls-na.amazon.com: type A, class IN
          Name: fls-na.amazon.com
          [Name Length: 17]
          [Label Count: 3]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
  ▾ Additional records
```

```
0000  52 54 00 12 35 02 08 00  27 16 fb e3 08 00 45 00   RT··5···'·····E·
0010  00 4a ac 46 40 00 40 11  cc 38 0a 00 02 0f ac 14   ·J·F@·@··8······
0020  0a 01 37 06 00 35 00 36  c2 6d e7 7e 01 00 00 01   ··7··5·6·m·~····
0030  00 00 00 00 00 01 06 66  6c 73 2d 6e 61 06 61 6d   ·······f ls-na·am
0040  61 7a 6f 6e 03 63 6f 6d  00 00 01 00 01 00 00 29   azon·com ·······)
0050  02 00 00 00 00 00 00 00                            ········
```

User Datagram Protocol (udp), 8 bytes

Packets: 2408 · Displayed: 209 (8.7%) · Dropped: 0 (0.0%)

Profile: Default



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.   Time         Source        Destination   Protocol Length Info
 1156 7.036667800  10.0.2.15     172.20.10.1   DNS       89 Standard query 0x32c6 AAAA cs9.wac.phicdn.net OPT
 1159 7.043453914  172.20.10.1   10.0.2.15     DNS      157 Standard query response 0x32c6 AAAA cs9.wac.phicdn.net SOA ns…
 1177 7.126321322  10.0.2.15     172.20.10.1   DNS       89 Standard query 0x9701 AAAA cs9.wac.phicdn.net OPT
 1185 7.151688036  172.20.10.1   10.0.2.15     DNS      157 Standard query response 0x9701 AAAA cs9.wac.phicdn.net SOA ns…
 1208 7.334559583  10.0.2.15     172.20.10.1   DNS      114 Standard query 0xbb04 AAAA prod.ingestion-edge.prod.dataops.m…
 1215 7.347814733  172.20.10.1   10.0.2.15     DNS      207 Standard query response 0xbb04 AAAA prod.ingestion-edge.prod…
 1244 7.530726975  10.0.2.15     172.20.10.1   DNS      102 Standard query 0x0382 A images-na.ssl-images-amazon.com OPT
 1245 7.530996178  10.0.2.15     172.20.10.1   DNS      102 Standard query 0xd3eb AAAA images-na.ssl-images-amazon.com OPT
 1250 8.040832270  10.0.2.15     172.20.10.1   DNS       88 Standard query 0xe77e A fls-na.amazon.com OPT
 1251 8.041008247  10.0.2.15     172.20.10.1   DNS       88 Standard query 0xccde AAAA fls-na.amazon.com OPT
 1268 8.055411424  172.20.10.1   10.0.2.15     DNS      252 Standard query response 0xd3eb AAAA images-na.ssl-images-amaz…
 1269 8.055411474  172.20.10.1   10.0.2.15     DNS      240 Standard query response 0x0382 A images-na.ssl-images-amazon…
 1291 8.169167583  172.20.10.1   10.0.2.15     DNS      289 Standard query response 0xe77e A fls-na.amazon.com CNAME gate…
 1312 8.213210271  172.20.10.1   10.0.2.15     DNS      238 Standard query response 0xccde AAAA fls-na.amazon.com CNAME g…
 1313 8.213625010  10.0.2.15     172.20.10.1   DNS      111 Standard query 0xb054 AAAA endpoint.prod.us-east-1.forester.a…
 1314 8.238991382  172.20.10.1   10.0.2.15     DNS      195 Standard query response 0xb054 AAAA endpoint.prod.us-east-1.f…
 1404 9.486259733  10.0.2.15     172.20.10.1   DNS       97 Standard query 0x1631 AAAA cni-digital.map.fastly.net OPT
```

```
          [Name Length: 17]
          [Label Count: 3]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
  ▾ Answers
    ▸ fls-na.amazon.com: type CNAME, class IN, cname gateway.prod.us-east-1.forester.a2z.com
    ▸ gateway.prod.us-east-1.forester.a2z.com: type CNAME, class IN, cname endpoint.prod.us-east-1.forester.a2z.com
    ▸ endpoint.prod.us-east-1.forester.a2z.com: type A, class IN, addr 52.86.212.70
    ▸ endpoint.prod.us-east-1.forester.a2z.com: type A, class IN, addr 34.201.179.176
    ▸ endpoint.prod.us-east-1.forester.a2z.com: type A, class IN, addr 35.168.171.134
    ▸ endpoint.prod.us-east-1.forester.a2z.com: type A, class IN, addr 3.231.97.105
    ▸ endpoint.prod.us-east-1.forester.a2z.com: type A, class IN, addr 23.22.26.94
    ▸ endpoint.prod.us-east-1.forester.a2z.com: type A, class IN, addr 34.196.130.252
    ▸ endpoint.prod.us-east-1.forester.a2z.com: type A, class IN, addr 54.158.185.49
    ▸ endpoint.prod.us-east-1.forester.a2z.com: type A, class IN, addr 52.7.98.248
  ▾ Additional records
    ▸ <Root>: type OPT
    [Request In: 1250]
```

```
0020  02 0f 00 35 d7 96 00 ff  4c 1d e7 7e 81 80 00 01   ···5····L··~····
0030  00 0a 00 00 00 01 06 66  6c 73 2d 6e 61 06 61 6d   ·······f ls-na·am
0040  61 7a 6f 6e 03 63 6f 6d  00 00 01 00 01 c0 0c 00   azon·com ········
0050  05 00 01 00 00 01 3f 00  26 07 67 61 74 65 77 61   ······?· &·gatewa
0060  79 04 70 72 6f 64 09 75  73 2d 65 61 73 74 2d 31   y·prod·u s-east-1
0070  08 66 6f 72 65 73 74 65  72 03 61 32 7a c0 1a c0   ·foreste r·a2z···
0080  2f 00 05 00 01 00 00 00  5e 00 0b 08 65 6e 64 70   /······· ^···endp
0090  6f 69 6e 74 c0 37 c0 61  00 01 00 01 00 00 00 34   oint·7·a ·······4
00a0  00 04 34 56 d4 46 c0 61  00 01 00 01 00 00 00 34   ··4V·F·a ·······4
00b0  00 04 22 c9 b3 b0 c0 61  00 01 00 01 00 00 00 34   ··"····a ·······4
00c0  00 04 23 a8 ab 86 c0 61  00 01 00 01 00 00 00 34   ··#····a ·······4
00d0  00 04 03 e7 61 69 c0 61  00 01 00 01 00 00 00 34   ····ai·a ·······4
00e0  00 04 17 16 1a 5e c0 61  00 01 00 01 00 00 00 34   ·····^·a ·······4
00f0  00 04 22 c4 82 fc c0 61  00 01 00 01 00 00 00 34   ··"····a ·······4
0100  00 04 36 9e b9 31 c0 61  00 01 00 01 00 00 00 34   ··6··1·a ·······4
0110  00 04 34 07 62 f8 00 00  29 10 00 00 00 00 00 00   ··4·b··· )·······
0120  00                                                 ·
```

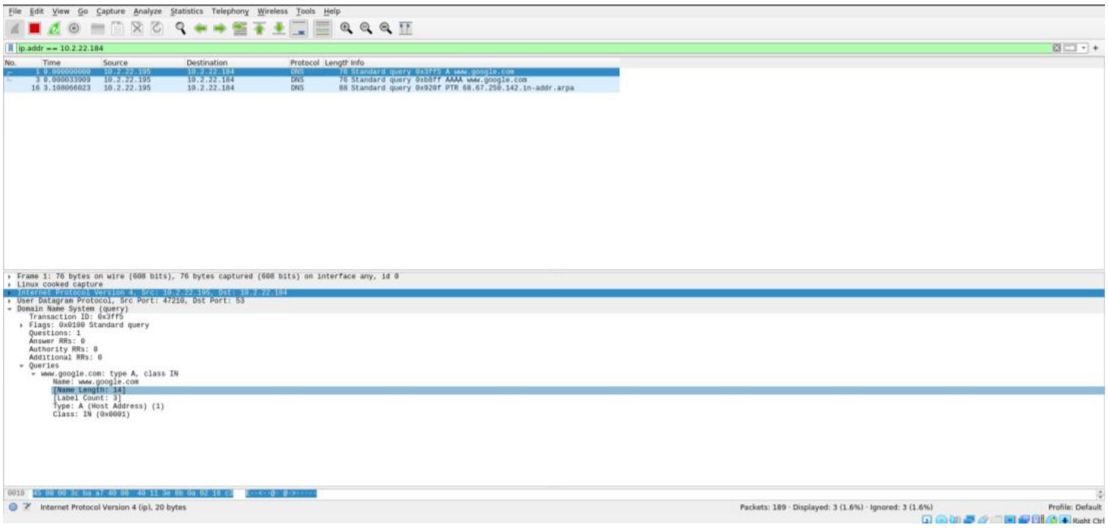
User Datagram Protocol (udp), 8 bytes

Packets: 2408 · Displayed: 209 (8.7%) · Dropped: 0 (0.0%)

Profile: Default

Task 1

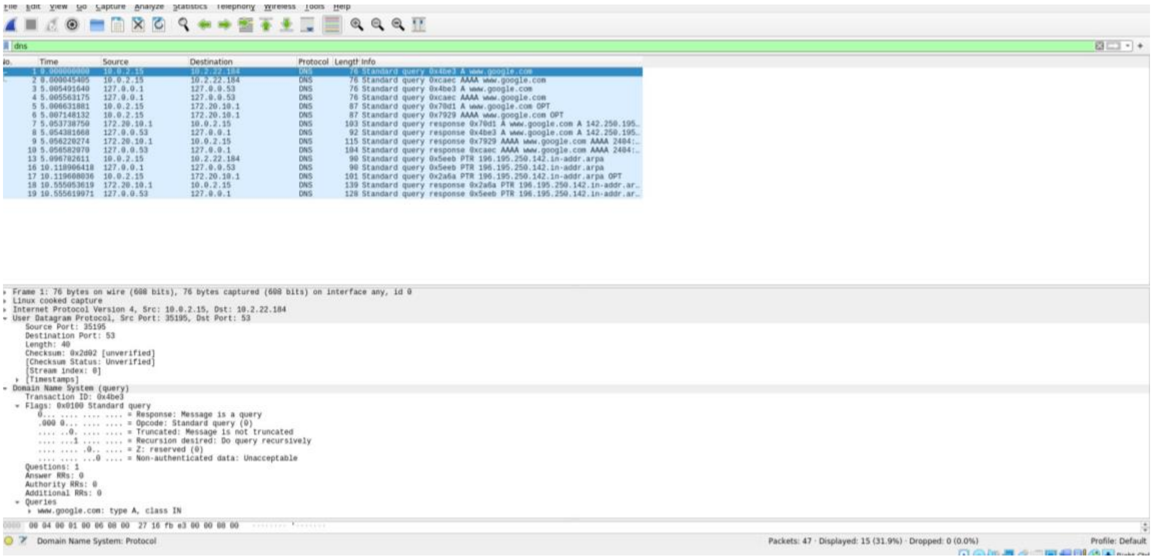
Observation 2


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.2.22.184

No.   Time           Source         Destination    Protocol Length Info
    1 0.000000000    10.2.22.195    10.2.22.184    DNS       76 Standard query 0x3ff5 A www.google.com
    3 0.000033909    10.2.22.195    10.2.22.184    DNS       76 Standard query 0xb8ff AAAA www.google.com
   16 3.108066023    10.2.22.195    10.2.22.184    DNS       88 Standard query 0x920f PTR 68.67.250.142.in-addr.arpa
```

```
▸ Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.2.22.195, Dst: 10.2.22.184
▸ User Datagram Protocol, Src Port: 47210, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x3ff5
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.google.com: type A, class IN
        Name: www.google.com
        [Name Length: 14]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)

0010  45 00 00 3c ba a7 40 00  40 11 3e 8b 0a 02 16 c3   E··<··@· @·>·····

Internet Protocol Version 4 (ip), 20 bytes        Packets: 189 · Displayed: 3 (1.6%) · Ignored: 3 (1.6%)        Profile: Default
```

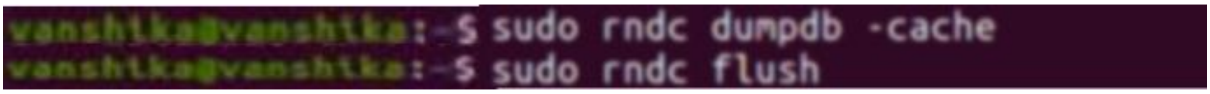
Observation 3


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

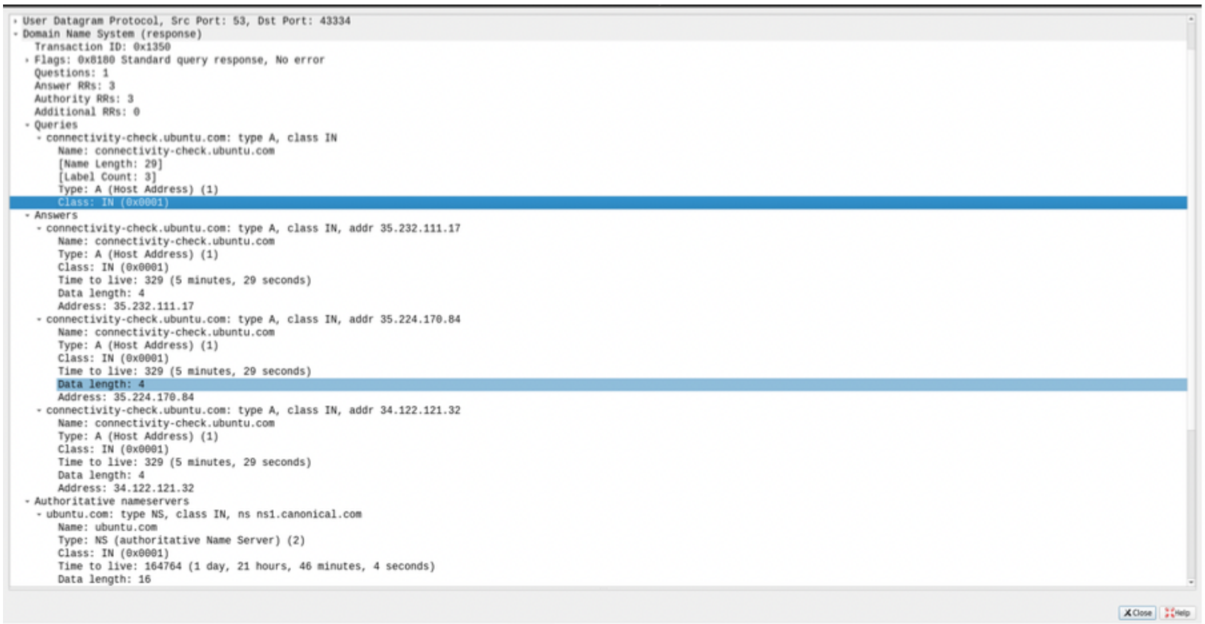
```
dns

No.   Time           Source         Destination    Protocol Length Info
    1 0.000000000    10.0.2.15      10.2.22.184    DNS       76 Standard query 0x4be3 A www.google.com
    2 0.000045405    10.0.2.15      10.2.22.184    DNS       76 Standard query 0xcaec AAAA www.google.com
    3 5.005491640    127.0.0.1      127.0.0.53     DNS       76 Standard query 0x4be3 A www.google.com
    4 5.005563175    127.0.0.1      127.0.0.53     DNS       76 Standard query 0xcaec AAAA www.google.com
    5 5.006631881    10.0.2.15      172.20.10.1    DNS       87 Standard query 0x70d1 A www.google.com OPT
    6 5.007148132    10.0.2.15      172.20.10.1    DNS       87 Standard query 0x7929 AAAA www.google.com OPT
    7 5.053738750    172.20.10.1    10.0.2.15      DNS      103 Standard query response 0x70d1 A www.google.com A 142.250.195…
    8 5.054381668    127.0.0.53     127.0.0.1      DNS       92 Standard query response 0x4be3 A www.google.com A 142.250.195…
    9 5.056220274    172.20.10.1    10.0.2.15      DNS      115 Standard query response 0x7929 AAAA www.google.com AAAA 2404:…
   10 5.056582070    127.0.0.53     127.0.0.1      DNS      104 Standard query response 0xcaec AAAA www.google.com AAAA 2404:…
   13 5.096782611    10.0.2.15      10.2.22.184    DNS       90 Standard query 0x5eeb PTR 196.195.250.142.in-addr.arpa
   16 10.118906418   127.0.0.1      127.0.0.53     DNS       90 Standard query 0x5eeb PTR 196.195.250.142.in-addr.arpa
   17 10.119608036   10.0.2.15      172.20.10.1    DNS      101 Standard query 0x2a6a PTR 196.195.250.142.in-addr.arpa OPT
   18 10.555053619   172.20.10.1    10.0.2.15      DNS      139 Standard query response 0x2a6a PTR 196.195.250.142.in-addr.ar…
   19 10.555619971   127.0.0.53     127.0.0.1      DNS      128 Standard query response 0x5eeb PTR 196.195.250.142.in-addr.ar…
```

```
▸ Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.2.22.184
▾ User Datagram Protocol, Src Port: 35195, Dst Port: 53
    Source Port: 35195
    Destination Port: 53
    Length: 40
    Checksum: 0x2d02 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  ▸ [Timestamps]
▾ Domain Name System (query)
    Transaction ID: 0x4be3
  ▾ 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
    ▸ www.google.com: type A, class IN

0000  00 04 00 01 00 06 08 00  27 16 fb e3 00 00 00 00   ········ '·······

Domain Name System: Protocol        Packets: 47 · Displayed: 15 (31.9%) · Dropped: 0 (0.0%)        Profile: Default
```

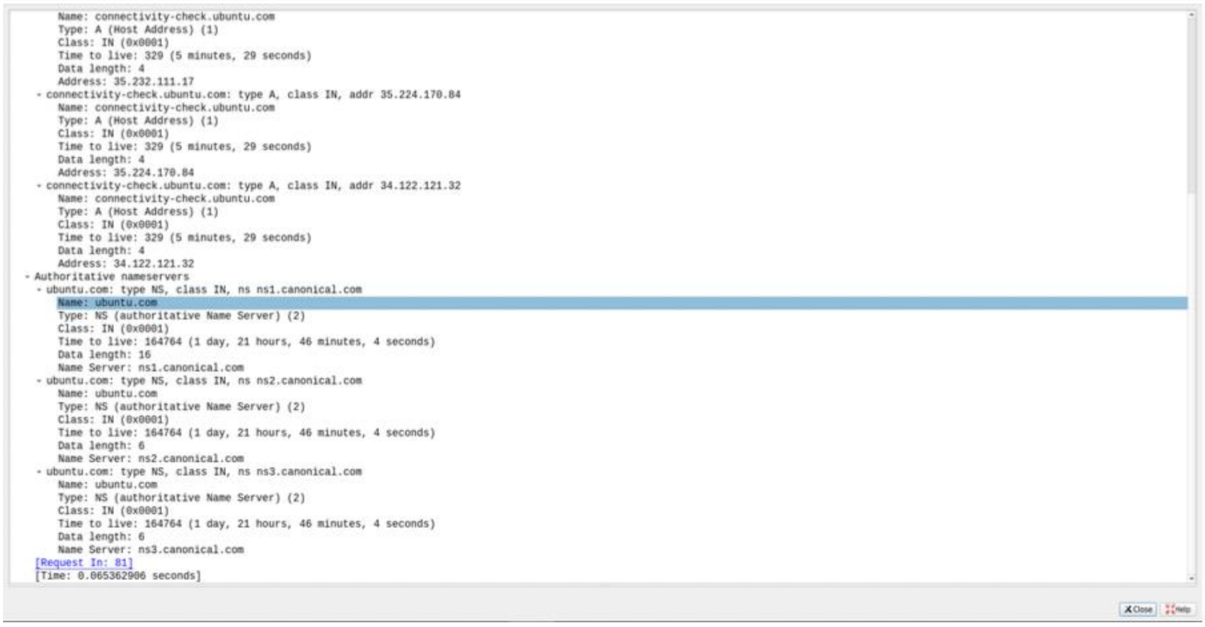
Observation 4



```
[redacted] sudo rndc dumpdb -cache
[redacted] sudo rndc flush
```



```
› User Datagram Protocol, Src Port: 53, Dst Port: 43334
⌄ Domain Name System (response)
    Transaction ID: 0x1350
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 3
    Additional RRs: 0
  ⌄ Queries
    ⌄ connectivity-check.ubuntu.com: type A, class IN
        Name: connectivity-check.ubuntu.com
        [Name Length: 29]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ⌄ Answers
    ⌄ connectivity-check.ubuntu.com: type A, class IN, addr 35.232.111.17
        Name: connectivity-check.ubuntu.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 329 (5 minutes, 29 seconds)
        Data length: 4
        Address: 35.232.111.17
    ⌄ connectivity-check.ubuntu.com: type A, class IN, addr 35.224.170.84
        Name: connectivity-check.ubuntu.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 329 (5 minutes, 29 seconds)
        Data length: 4
        Address: 35.224.170.84
    ⌄ connectivity-check.ubuntu.com: type A, class IN, addr 34.122.121.32
        Name: connectivity-check.ubuntu.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 329 (5 minutes, 29 seconds)
        Data length: 4
        Address: 34.122.121.32
  ⌄ Authoritative nameservers
    ⌄ ubuntu.com: type NS, class IN, ns ns1.canonical.com
        Name: ubuntu.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 164764 (1 day, 21 hours, 46 minutes, 4 seconds)
        Data length: 16
```



```
        Name: connectivity-check.ubuntu.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 329 (5 minutes, 29 seconds)
        Data length: 4
        Address: 35.232.111.17
    ⌄ connectivity-check.ubuntu.com: type A, class IN, addr 35.224.170.84
        Name: connectivity-check.ubuntu.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 329 (5 minutes, 29 seconds)
        Data length: 4
        Address: 35.224.170.84
    ⌄ connectivity-check.ubuntu.com: type A, class IN, addr 34.122.121.32
        Name: connectivity-check.ubuntu.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 329 (5 minutes, 29 seconds)
        Data length: 4
        Address: 34.122.121.32
  ⌄ Authoritative nameservers
    ⌄ ubuntu.com: type NS, class IN, ns ns1.canonical.com
        Name: ubuntu.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 164764 (1 day, 21 hours, 46 minutes, 4 seconds)
        Data length: 16
        Name Server: ns1.canonical.com
    ⌄ ubuntu.com: type NS, class IN, ns ns2.canonical.com
        Name: ubuntu.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 164764 (1 day, 21 hours, 46 minutes, 4 seconds)
        Data length: 6
        Name Server: ns2.canonical.com
    ⌄ ubuntu.com: type NS, class IN, ns ns3.canonical.com
        Name: ubuntu.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 164764 (1 day, 21 hours, 46 minutes, 4 seconds)
        Data length: 6
        Name Server: ns3.canonical.com
  [Request In: 81]
  [Time: 0.065362906 seconds]
```