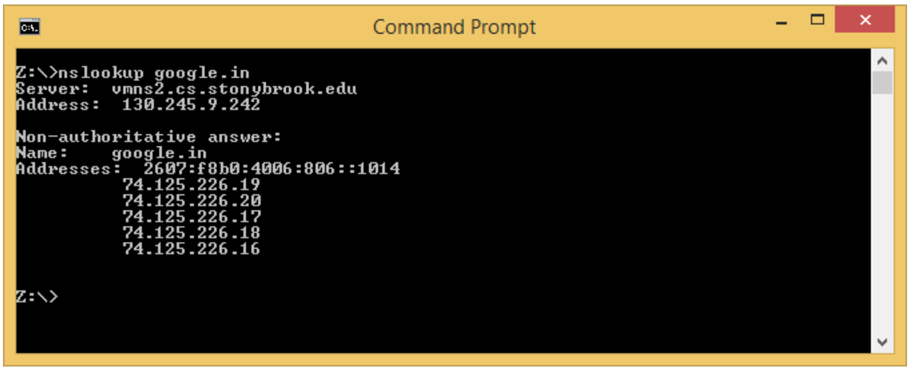
CSE Lab 3

I. WireShark HTTP Lab

Aditya Balwani, SBUID : 109353920

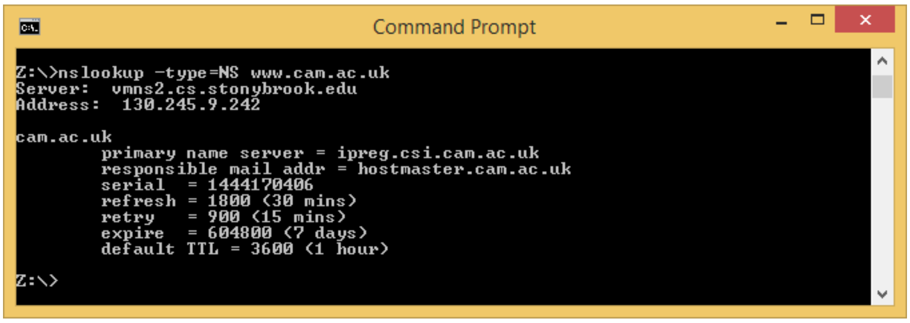
Part 1

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



```
Z:\>nslookup google.in
Server:  vmns2.cs.stonybrook.edu
Address:  130.245.9.242

Non-authoritative answer:
Name:    google.in
Addresses:  2607:f8b0:4006:806::1014
          74.125.226.19
          74.125.226.20
          74.125.226.17
          74.125.226.18
          74.125.226.16


Z:\>
```

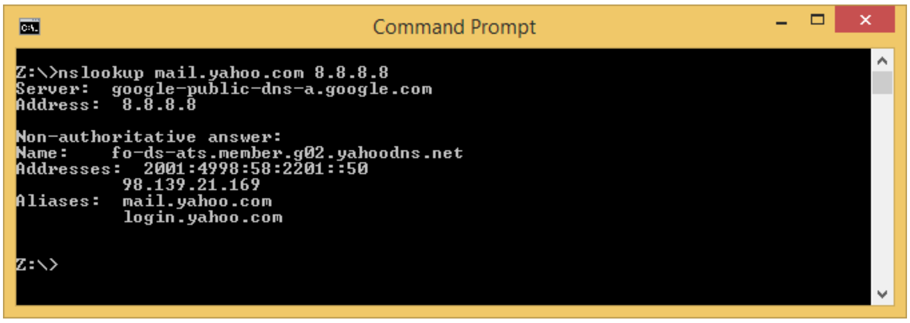
2. **Run nslookup to determine the authoritative DNS servers for a university in Europe.**



```
Z:\>nslookup -type=NS www.cam.ac.uk
Server:  vmns2.cs.stonybrook.edu
Address:  130.245.9.242

cam.ac.uk
        primary name server = ipreg.csi.cam.ac.uk
        responsible mail addr = hostmaster.cam.ac.uk
        serial  = 1444170406
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)

Z:\>
```

3. **Run nslookup so that one of the DNS servers obtained in Question s queried for the mail servers for Yahoo! mail. What is its IP address?**

   The IP address is 98.139.21.169



```
Z:\>nslookup mail.yahoo.com 8.8.8.8
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    fo-ds-ats.member.g02.yahoodns.net
Addresses:  2001:4998:58:2201::50
          98.139.21.169
Aliases:  mail.yahoo.com
          login.yahoo.com


Z:\>
```

4. <

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

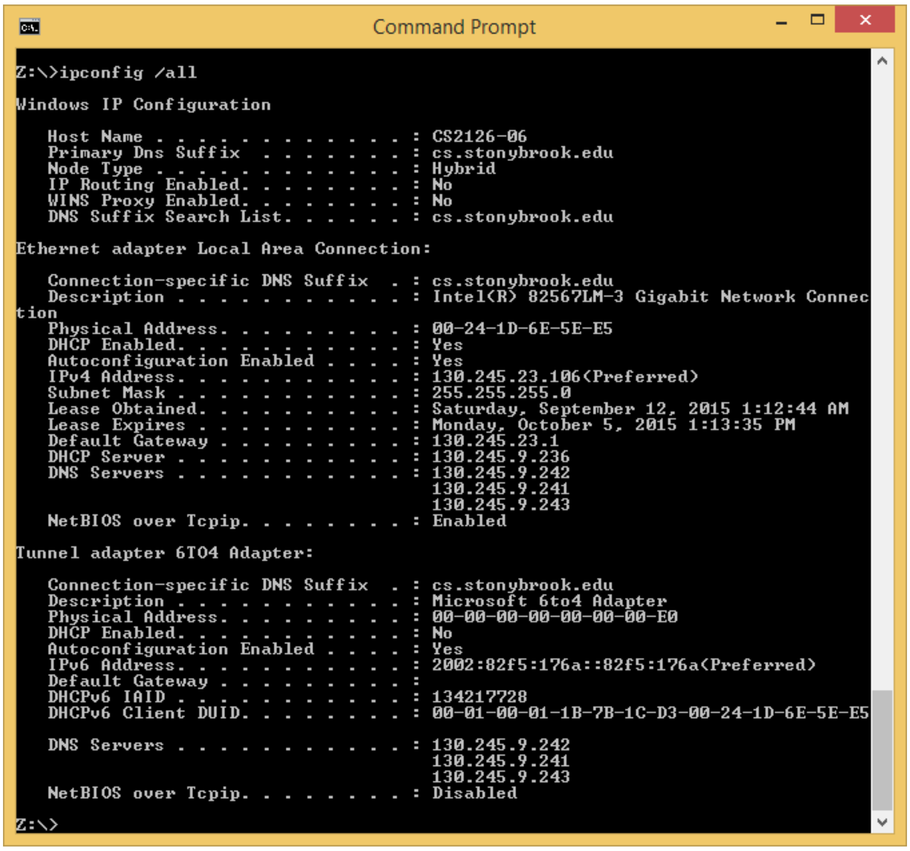
The query and response were sent over UDP.

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

   The destination port of the request is 53. The source port of the response is 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?**

   The DNS query message is sent to 130.245.9.242. Yes this is the address of my local DNS Server as seen in ipconfig :



```
Z:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : CS2126-06
   Primary Dns Suffix  . . . . . . . : cs.stonybrook.edu
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cs.stonybrook.edu

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : cs.stonybrook.edu
   Description . . . . . . . . . . . : Intel(R) 82567LM-3 Gigabit Network Connec
tion
   Physical Address. . . . . . . . . : 00-24-1D-6E-5E-E5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 130.245.23.106(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, September 12, 2015 1:12:44 AM
   Lease Expires . . . . . . . . . . : Monday, October 5, 2015 1:13:35 PM
   Default Gateway . . . . . . . . . : 130.245.23.1
   DHCP Server . . . . . . . . . . . : 130.245.9.236
   DNS Servers . . . . . . . . . . . : 130.245.9.242
                                       130.245.9.241
                                       130.245.9.243
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter 6TO4 Adapter:

   Connection-specific DNS Suffix  . : cs.stonybrook.edu
   Description . . . . . . . . . . . : Microsoft 6to4 Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2002:82f5:176a::82f5:176a(Preferred)
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 134217728
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-7B-1C-D3-00-24-1D-6E-5E-E5

   DNS Servers . . . . . . . . . . . : 130.245.9.242
                                       130.245.9.241
                                       130.245.9.243
   NetBIOS over Tcpip. . . . . . . . : Disabled

Z:\>
```

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

   It is a standard type A query and does not contain any answers

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

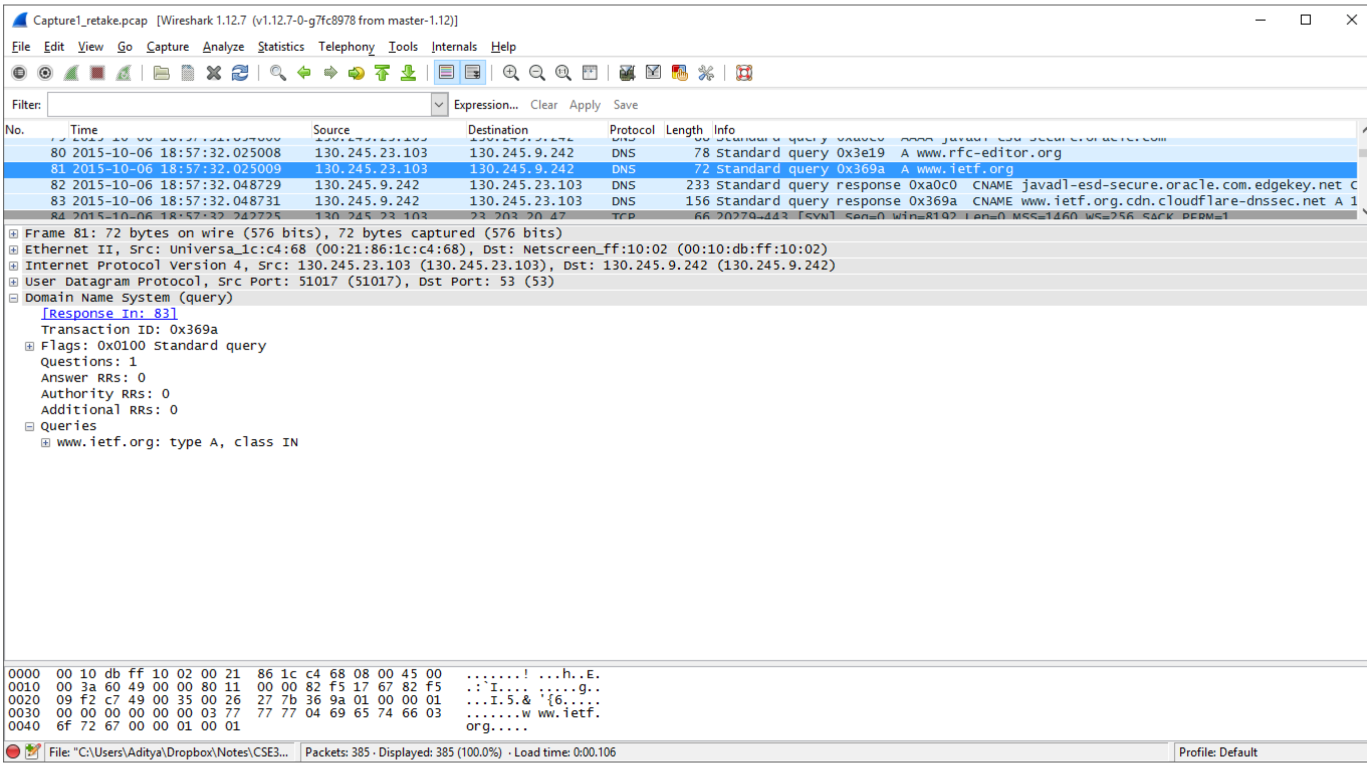
   The response contains 3 answers and each one contains the name, the canonical name, time to live and the data length. One of them also the contains an IP address

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?**

   Yes, the destination of the IP Address of th destination corresponds to one of the IPs provided in the answers of the DNS Response

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

    No, the host does not issue more DNS queries because the images are hosted at the same domain. If the images were hosted somewhere else then it would issue new DNS queries.

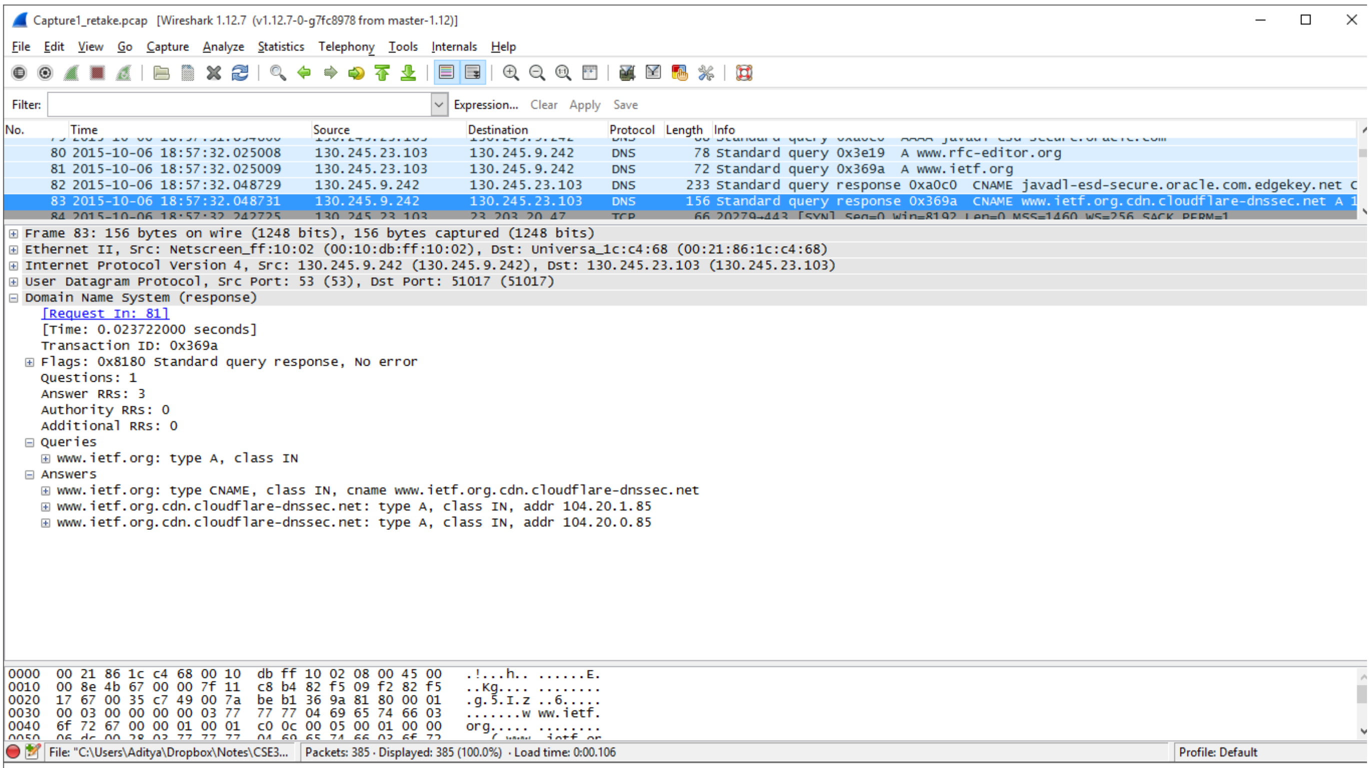

Capture1_retake.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default

```
No.  Time                        Source           Destination      Protocol Length Info
 80 2015-10-06 18:57:32.025008  130.245.23.103   130.245.9.242    DNS       78 Standard query 0x3e19  A www.rfc-editor.org
 81 2015-10-06 18:57:32.025009  130.245.23.103   130.245.9.242    DNS       72 Standard query 0x369a  A www.ietf.org
 82 2015-10-06 18:57:32.048729  130.245.9.242    130.245.23.103   DNS      233 Standard query response 0xa0c0  CNAME javadl-esd-secure.oracle.com.edgekey.net C
 83 2015-10-06 18:57:32.048731  130.245.9.242    130.245.23.103   DNS      156 Standard query response 0x369a  CNAME www.ietf.org.cdn.cloudflare-dnssec.net A 1
 84 2015-10-06 18:57:32.242725  130.245.23.103   23.203.20.47     TCP       66 20279→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
⊞ Frame 81: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
⊞ Ethernet II, Src: Universa_1c:c4:68 (00:21:86:1c:c4:68), Dst: Netscreen_ff:10:02 (00:10:db:ff:10:02)
⊞ Internet Protocol Version 4, Src: 130.245.23.103 (130.245.23.103), Dst: 130.245.9.242 (130.245.9.242)
⊞ User Datagram Protocol, Src Port: 51017 (51017), Dst Port: 53 (53)
⊟ Domain Name System (query)
    [Response In: 83]
    Transaction ID: 0x369a
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊞ www.ietf.org: type A, class IN
```

```
0000  00 10 db ff 10 02 00 21  86 1c c4 68 08 00 45 00   .......! ...h..E.
0010  00 3a 60 49 00 00 80 11  00 00 82 f5 17 67 82 f5   .:`I.... .....g..
0020  09 f2 c7 49 00 35 00 26  27 7b 36 9a 01 00 00 01   ...I.5.& '{6.....
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   .......w ww.ietf.
0040  6f 72 67 00 00 01 00 01                            org.....
```

File: "C:\Users\Aditya\Dropbox\Notes\CSE3... Packets: 385 · Displayed: 385 (100.0%) · Load time: 0:00.106

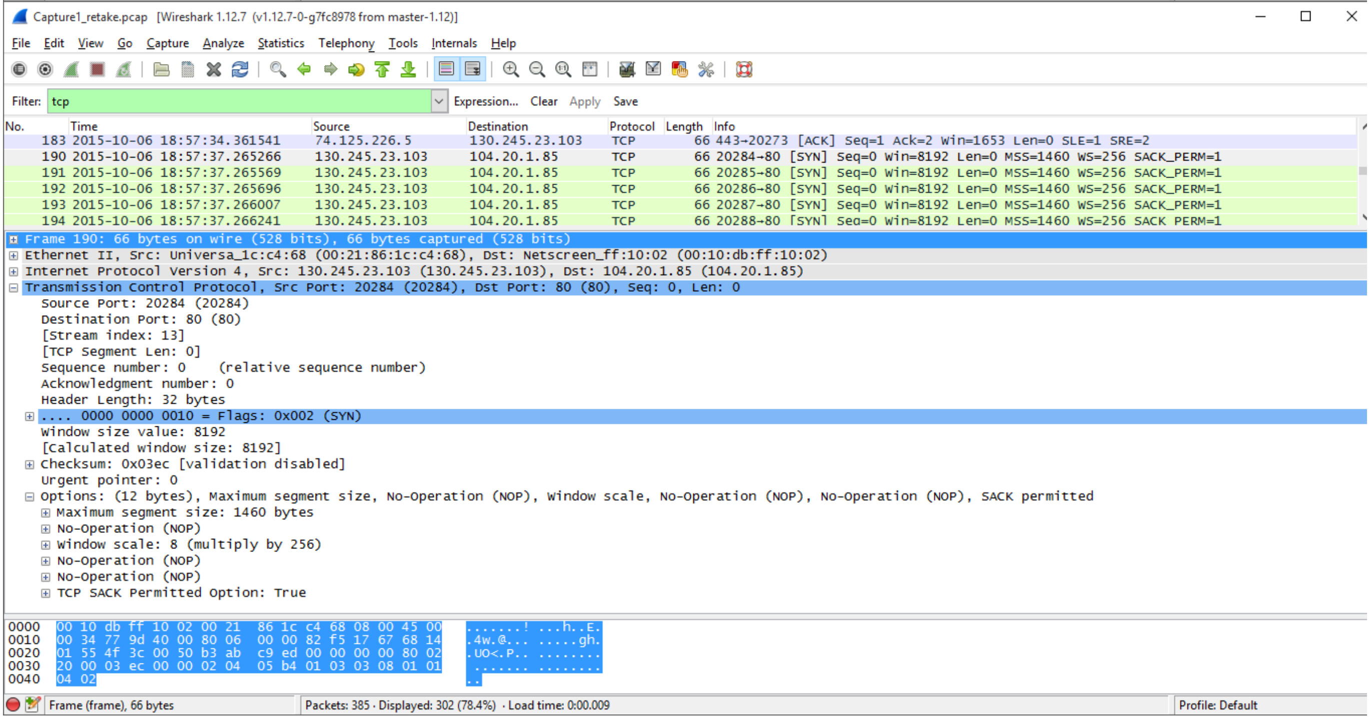

Capture1_retake.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.    Time                        Source            Destination       Protocol Length Info
 79 2015-10-06 18:57:31.894800  130.245.23.103  130.245.9.242    DNS       80 Standard query 0xa0c0  AAAA javadl-esd-secure.oracle.com
 80 2015-10-06 18:57:32.025008  130.245.23.103  130.245.9.242    DNS       78 Standard query 0x3e19  A www.rfc-editor.org
 81 2015-10-06 18:57:32.025009  130.245.23.103  130.245.9.242    DNS       72 Standard query 0x369a  A www.ietf.org
 82 2015-10-06 18:57:32.048729  130.245.9.242   130.245.23.103   DNS      233 Standard query response 0xa0c0  CNAME javadl-esd-secure.oracle.com.edgekey.net C
 83 2015-10-06 18:57:32.048731  130.245.9.242   130.245.23.103   DNS      156 Standard query response 0x369a  CNAME www.ietf.org.cdn.cloudflare-dnssec.net A 1
 84 2015-10-06 18:57:32.242725  130.245.23.103  23.203.20.47     TCP       66 20279→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
⊞ Frame 83: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
⊞ Ethernet II, Src: Netscreen_ff:10:02 (00:10:db:ff:10:02), Dst: Universa_1c:c4:68 (00:21:86:1c:c4:68)
⊞ Internet Protocol Version 4, Src: 130.245.9.242 (130.245.9.242), Dst: 130.245.23.103 (130.245.23.103)
⊞ User Datagram Protocol, Src Port: 53 (53), Dst Port: 51017 (51017)
⊟ Domain Name System (response)
    [Request In: 81]
    [Time: 0.023722000 seconds]
    Transaction ID: 0x369a
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊞ www.ietf.org: type A, class IN
  ⊟ 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 104.20.1.85
    ⊞ www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.0.85
```

```
0000  00 21 86 1c c4 68 00 10  db ff 10 02 08 00 45 00   .!...h.. ......E.
0010  00 8e 4b 67 00 00 7f 11  c8 b4 82 f5 09 f2 82 f5   ..Kg.... ........
0020  17 67 00 35 c7 49 00 7a  be b1 36 9a 81 80 00 01   .g.5.I.z ..6.....
0030  00 03 00 00 00 00 03 77  77 77 04 69 65 74 66 03   .......w ww.ietf.
0040  6f 72 67 00 00 01 00 01  c0 0c 00 05 00 01 00 00   org..... ........
0050  06 dc 00 28 03 77 77 77  04 69 65 74 66 03 6f 72   ...(.www .ietf.or
```

File: "C:\Users\Aditya\Dropbox\Notes\CSE3... | Packets: 385 · Displayed: 385 (100.0%) · Load time: 0:00.106 | Profile: Default


Capture1_retake.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: tcp

```
No.    Time                        Source            Destination       Protocol Length Info
183 2015-10-06 18:57:34.361541  74.125.226.5    130.245.23.103   TCP       66 443→20273 [ACK] Seq=1 Ack=2 Win=1653 Len=0 SLE=1 SRE=2
190 2015-10-06 18:57:37.265266  130.245.23.103  104.20.1.85      TCP       66 20284→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
191 2015-10-06 18:57:37.265569  130.245.23.103  104.20.1.85      TCP       66 20285→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192 2015-10-06 18:57:37.265696  130.245.23.103  104.20.1.85      TCP       66 20286→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
193 2015-10-06 18:57:37.266007  130.245.23.103  104.20.1.85      TCP       66 20287→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
194 2015-10-06 18:57:37.266241  130.245.23.103  104.20.1.85      TCP       66 20288→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
⊞ Frame 190: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
⊞ Ethernet II, Src: Universa_1c:c4:68 (00:21:86:1c:c4:68), Dst: Netscreen_ff:10:02 (00:10:db:ff:10:02)
⊞ Internet Protocol Version 4, Src: 130.245.23.103 (130.245.23.103), Dst: 104.20.1.85 (104.20.1.85)
⊟ Transmission Control Protocol, Src Port: 20284 (20284), Dst Port: 80 (80), Seq: 0, Len: 0
    Source Port: 20284 (20284)
    Destination Port: 80 (80)
    [Stream index: 13]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
  ⊞ .... 0000 0000 0010 = Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
  ⊞ Checksum: 0x03ec [validation disabled]
    Urgent pointer: 0
  ⊟ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    ⊞ Maximum segment size: 1460 bytes
    ⊞ No-Operation (NOP)
    ⊞ Window scale: 8 (multiply by 256)
    ⊞ No-Operation (NOP)
    ⊞ No-Operation (NOP)
    ⊞ TCP SACK Permitted Option: True
```

```
0000  00 10 db ff 10 02 00 21  86 1c c4 68 08 00 45 00   .......! ...h..E.
0010  00 34 77 9d 40 00 80 06  00 00 82 f5 17 67 68 14   .4w.@... .....gh.
0020  01 55 4f 3c 00 50 b3 ab  c9 ed 00 00 00 00 80 02   .UO<.P.. ........
0030  20 00 03 ec 00 00 02 04  05 b4 01 03 03 08 01 01    ....... ........
0040  04 02                                              ..
```

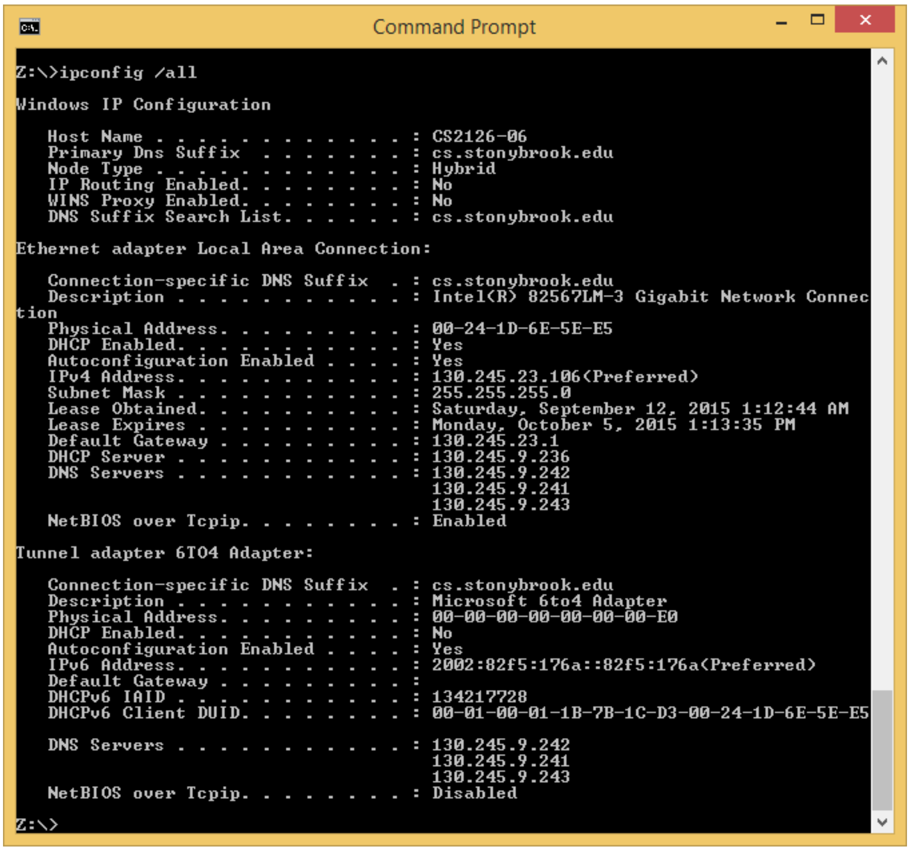
Frame (frame), 66 bytes | Packets: 385 · Displayed: 302 (78.4%) · Load time: 0:00.009 | Profile: Default

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

    The destination port of the request is 53. The source port of the response is 53

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

    The DNS query message is sent to 130.245.9.242. Yes this is the address of my local DNS Server as seen in ipconfig :



```
Z:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : CS2126-06
   Primary Dns Suffix  . . . . . . . : cs.stonybrook.edu
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cs.stonybrook.edu

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : cs.stonybrook.edu
   Description . . . . . . . . . . . : Intel(R) 82567LM-3 Gigabit Network Connec
tion
   Physical Address. . . . . . . . . : 00-24-1D-6E-5E-E5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 130.245.23.106(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, September 12, 2015 1:12:44 AM
   Lease Expires . . . . . . . . . . : Monday, October 5, 2015 1:13:35 PM
   Default Gateway . . . . . . . . . : 130.245.23.1
   DHCP Server . . . . . . . . . . . : 130.245.9.236
   DNS Servers . . . . . . . . . . . : 130.245.9.242
                                       130.245.9.241
                                       130.245.9.243
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter 6TO4 Adapter:

   Connection-specific DNS Suffix  . : cs.stonybrook.edu
   Description . . . . . . . . . . . : Microsoft 6to4 Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2002:82f5:176a::82f5:176a(Preferred)
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 134217728
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-7B-1C-D3-00-24-1D-6E-5E-E5

   DNS Servers . . . . . . . . . . . : 130.245.9.242
                                       130.245.9.241
                                       130.245.9.243
   NetBIOS over Tcpip. . . . . . . . : Disabled

Z:\>
```

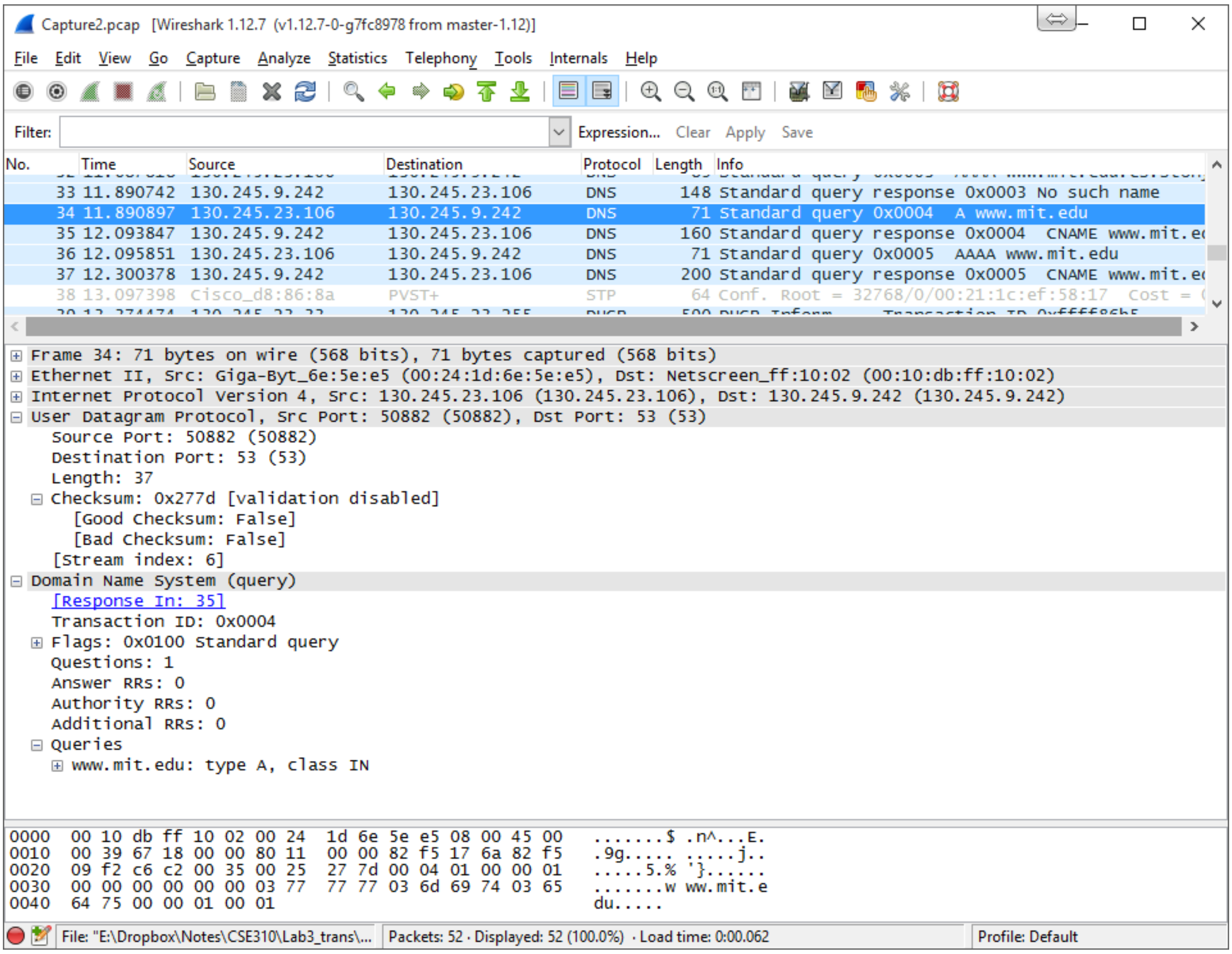
13. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

    It is a type A query and doesn't contain any answers.

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

    The response contains 3 answers and each one contains the name, the canonical name, time to live and the data length. One of them also the contains an IP address

15. **Provide a screenshot. (indicating query and response messages)**

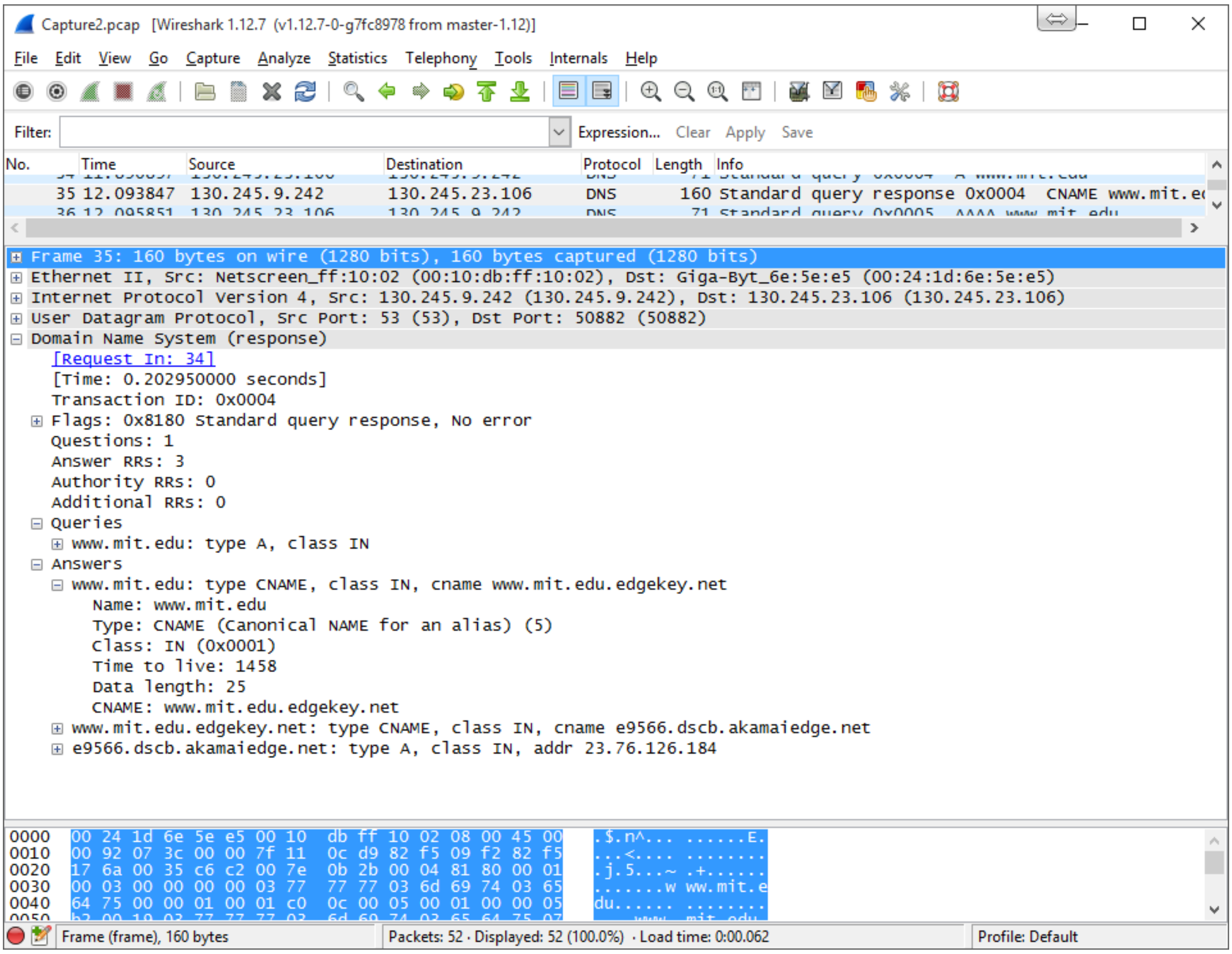

Capture2.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time       Source          Destination     Protocol Length Info
 33 11.890742 130.245.9.242   130.245.23.106  DNS     148 Standard query response 0x0003 No such name
 34 11.890897 130.245.23.106  130.245.9.242   DNS      71 Standard query 0x0004  A www.mit.edu
 35 12.093847 130.245.9.242   130.245.23.106  DNS     160 Standard query response 0x0004  CNAME www.mit.ed
 36 12.095851 130.245.23.106  130.245.9.242   DNS      71 Standard query 0x0005  AAAA www.mit.edu
 37 12.300378 130.245.9.242   130.245.23.106  DNS     200 Standard query response 0x0005  CNAME www.mit.ed
 38 13.097398 Cisco_d8:86:8a  PVST+           STP      64 Conf. Root = 32768/0/00:21:1c:ef:58:17  Cost = (
```

```
⊞ Frame 34: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
⊞ Ethernet II, Src: Giga-Byt_6e:5e:e5 (00:24:1d:6e:5e:e5), Dst: Netscreen_ff:10:02 (00:10:db:ff:10:02)
⊞ Internet Protocol Version 4, Src: 130.245.23.106 (130.245.23.106), Dst: 130.245.9.242 (130.245.9.242)
⊟ User Datagram Protocol, Src Port: 50882 (50882), Dst Port: 53 (53)
    Source Port: 50882 (50882)
    Destination Port: 53 (53)
    Length: 37
  ⊟ Checksum: 0x277d [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
    [Stream index: 6]
⊟ Domain Name System (query)
    [Response In: 35]
    Transaction ID: 0x0004
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊞ www.mit.edu: type A, class IN
```

```
0000  00 10 db ff 10 02 00 24  1d 6e 5e e5 08 00 45 00   .......$ .n^...E.
0010  00 39 67 18 00 00 80 11  00 00 82 f5 17 6a 82 f5   .9g..... .....j..
0020  09 f2 c6 c2 00 35 00 25  27 7d 00 04 01 00 00 01   .....5.% '}......
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
0040  64 75 00 00 01 00 01                               du.....
```

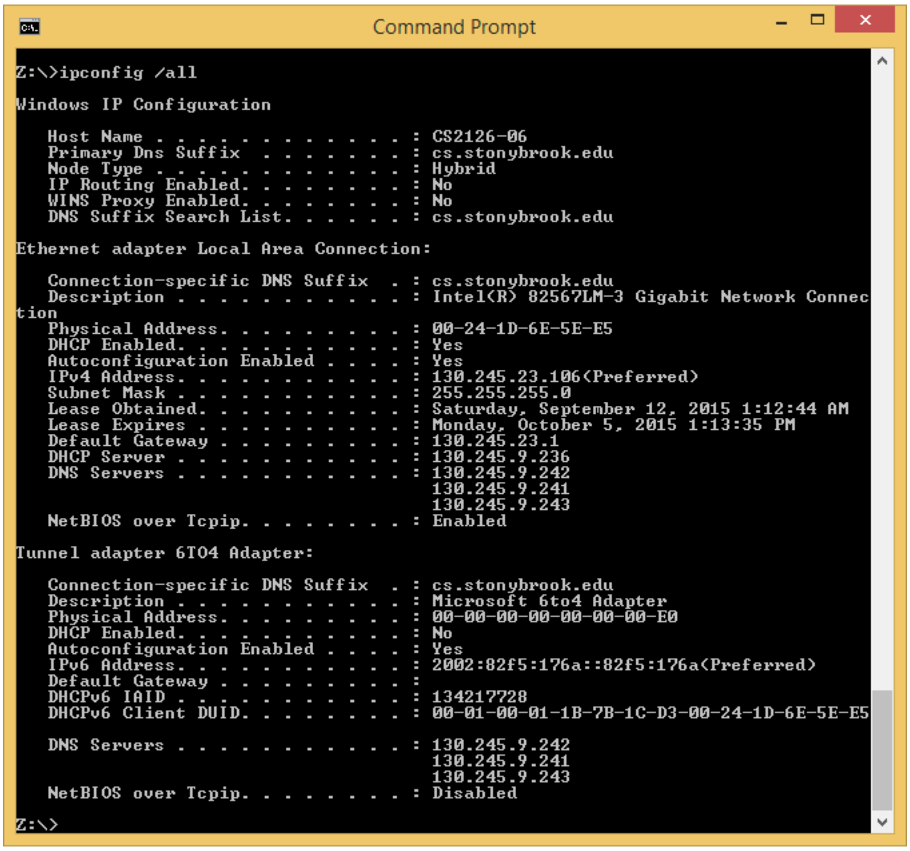
File: "E:\Dropbox\Notes\CSE310\Lab3_trans\... Packets: 52 · Displayed: 52 (100.0%) · Load time: 0:00.062 Profile: Default


Capture2.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time       Source          Destination     Protocol Length Info
   34 [illegible] 130.245.23.106 130.245.9.242   DNS        71 Standard query 0x0004  A www.mit.edu
   35 12.093847  130.245.9.242   130.245.23.106  DNS       160 Standard query response 0x0004  CNAME www.mit.ed
   36 12.095851  130.245.23.106  130.245.9.242   DNS        71 Standard query 0x0005  AAAA www.mit.edu

⊞ Frame 35: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits)
⊞ Ethernet II, Src: Netscreen_ff:10:02 (00:10:db:ff:10:02), Dst: Giga-Byt_6e:5e:e5 (00:24:1d:6e:5e:e5)
⊞ Internet Protocol Version 4, Src: 130.245.9.242 (130.245.9.242), Dst: 130.245.23.106 (130.245.23.106)
⊞ User Datagram Protocol, Src Port: 53 (53), Dst Port: 50882 (50882)
⊟ Domain Name System (response)
    [Request In: 34]
    [Time: 0.202950000 seconds]
    Transaction ID: 0x0004
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊞ www.mit.edu: type A, class IN
  ⊟ 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: 1458
        Data length: 25
        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 A, class IN, addr 23.76.126.184

0000  00 24 1d 6e 5e e5 00 10  db ff 10 02 08 00 45 00   .$.n^... ......E.
0010  00 92 07 3c 00 00 7f 11  0c d9 82 f5 09 f2 82 f5   ...<.... ........
0020  17 6a 00 35 c6 c2 00 7e  0b 2b 00 04 81 80 00 01   .j.5...~ .+......
0030  00 03 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
0040  64 75 00 00 01 00 01 c0  0c 00 05 00 01 00 00 05   du...... ........
0050  b2 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   ....www. mit.edu.

Frame (frame), 160 bytes   Packets: 52 · Displayed: 52 (100.0%) · Load time: 0:00.062   Profile: Default
```

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

The DNS query message is sent to 130.245.9.242. Yes this is the address of my local DNS Server as seen in ipconfig :



```
Z:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : CS2126-06
   Primary Dns Suffix  . . . . . . . : cs.stonybrook.edu
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cs.stonybrook.edu

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : cs.stonybrook.edu
   Description . . . . . . . . . . . : Intel(R) 82567LM-3 Gigabit Network Connec
tion
   Physical Address. . . . . . . . . : 00-24-1D-6E-5E-E5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 130.245.23.106(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, September 12, 2015 1:12:44 AM
   Lease Expires . . . . . . . . . . : Monday, October 5, 2015 1:13:35 PM
   Default Gateway . . . . . . . . . : 130.245.23.1
   DHCP Server . . . . . . . . . . . : 130.245.9.236
   DNS Servers . . . . . . . . . . . : 130.245.9.242
                                       130.245.9.241
                                       130.245.9.243
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter 6TO4 Adapter:

   Connection-specific DNS Suffix  . : cs.stonybrook.edu
   Description . . . . . . . . . . . : Microsoft 6to4 Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2002:82f5:176a::82f5:176a(Preferred)
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 134217728
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-7B-1C-D3-00-24-1D-6E-5E-E5

   DNS Servers . . . . . . . . . . . : 130.245.9.242
                                       130.245.9.241
                                       130.245.9.243
   NetBIOS over Tcpip. . . . . . . . : Disabled

Z:\>
```

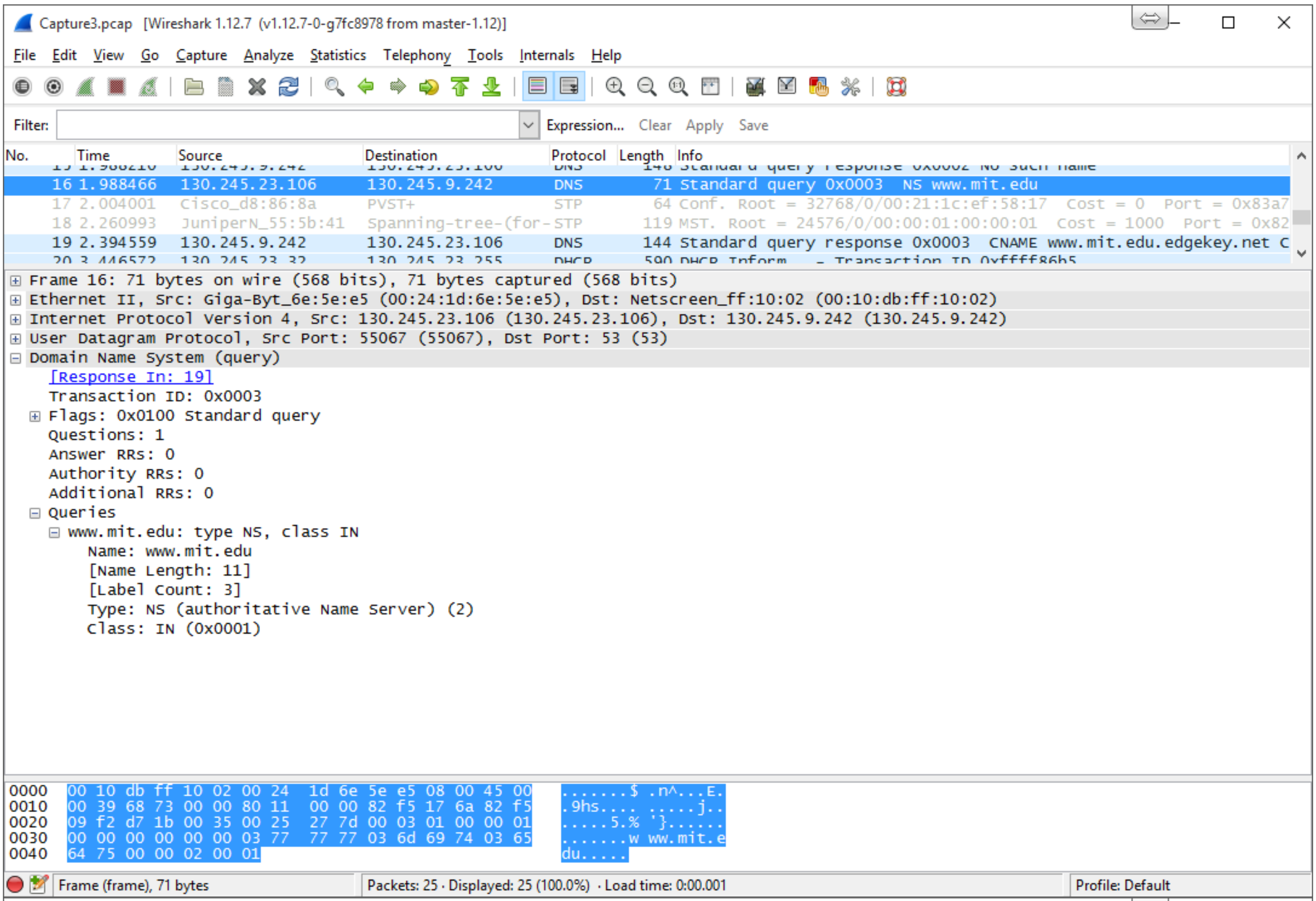
17. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

    It is an NS Type query, and it does not contain any 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?**

    The reponse provides 2 name servers which are www.mit.edu.edgekey.net and e9566.dscb.akamaiedge.net. No it does not provide the IP address for the nameservers.

19. **Provide a screenshot. Indicate query and response messages**

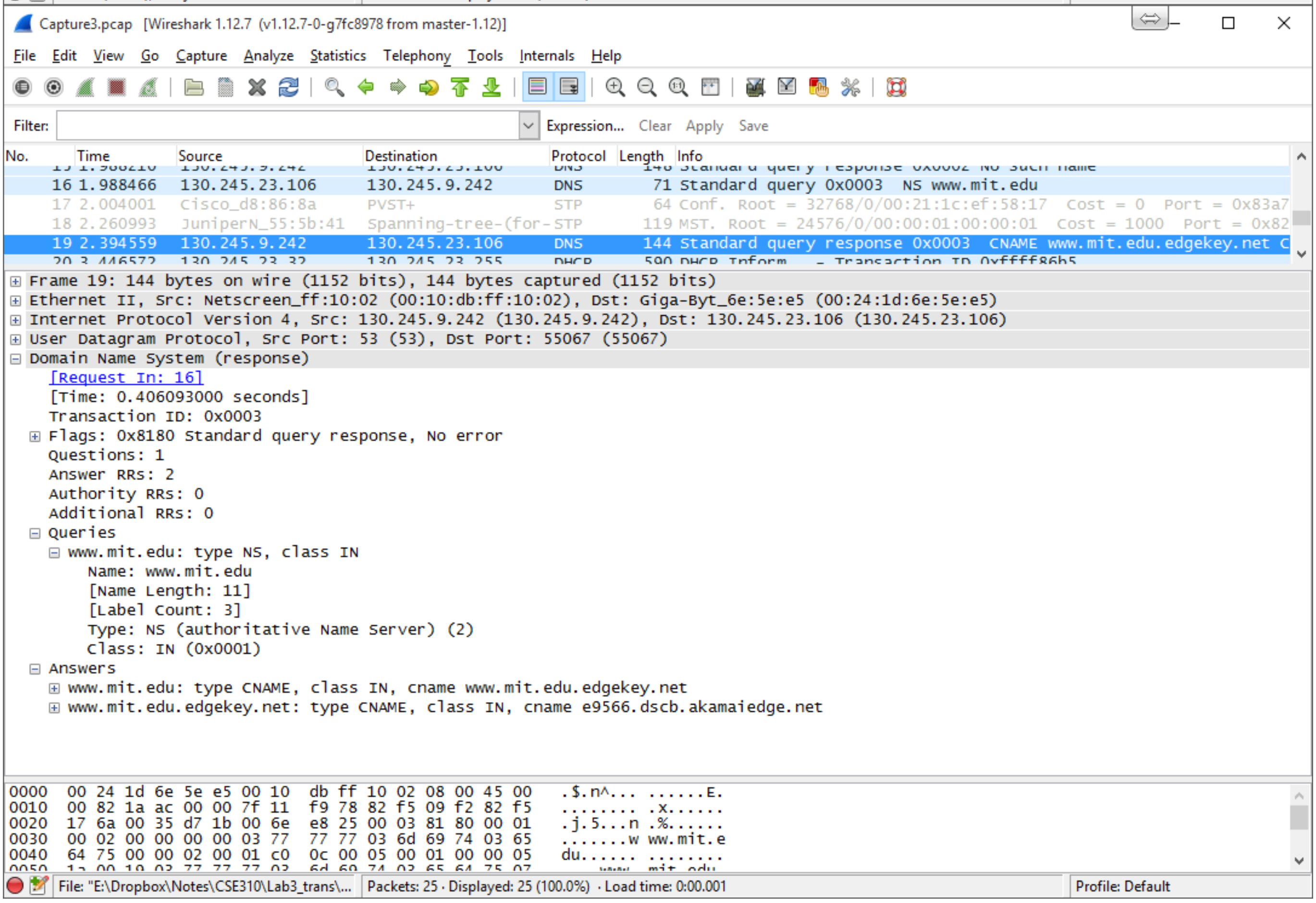


Capture3.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time      Source              Destination         Protocol Length Info
   15 1.988210  130.245.9.242       130.245.23.100      DNS       148 Standard query response 0x0002 No such name
   16 1.988466  130.245.23.106      130.245.9.242       DNS        71 Standard query 0x0003  NS www.mit.edu
   17 2.004001  Cisco_d8:86:8a      PVST+               STP        64 Conf. Root = 32768/0/00:21:1c:ef:58:17  Cost = 0  Port = 0x83a7
   18 2.260993  JuniperN_55:5b:41   Spanning-tree-(for- STP       119 MST. Root = 24576/0/00:00:01:00:00:01  Cost = 1000  Port = 0x82
   19 2.394559  130.245.9.242       130.245.23.106      DNS       144 Standard query response 0x0003  CNAME www.mit.edu.edgekey.net C
   20 3.446572  130.245.23.32       130.245.23.255      DHCP      590 DHCP Inform   - Transaction ID 0xffff86b5

⊞ Frame 16: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
⊞ Ethernet II, Src: Giga-Byt_6e:5e:e5 (00:24:1d:6e:5e:e5), Dst: Netscreen_ff:10:02 (00:10:db:ff:10:02)
⊞ Internet Protocol Version 4, Src: 130.245.23.106 (130.245.23.106), Dst: 130.245.9.242 (130.245.9.242)
⊞ User Datagram Protocol, Src Port: 55067 (55067), Dst Port: 53 (53)
⊟ Domain Name System (query)
    [Response In: 19]
    Transaction ID: 0x0003
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.mit.edu: type NS, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)

0000  00 10 db ff 10 02 00 24  1d 6e 5e e5 08 00 45 00   .......$ .n^...E.
0010  00 39 68 73 00 00 80 11  00 00 82 f5 17 6a 82 f5   .9hs.... .....j..
0020  09 f2 d7 1b 00 35 00 25  27 7d 00 03 01 00 00 01   .....5.% '}......
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
0040  64 75 00 00 02 00 01                               du.....
```

Frame (frame), 71 bytes | Packets: 25 · Displayed: 25 (100.0%) · Load time: 0:00.001 | Profile: Default



Capture3.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time      Source              Destination         Protocol Length Info
   15 1.988210  130.245.9.242       130.245.23.100      DNS       148 Standard query response 0x0002 No such name
   16 1.988466  130.245.23.106      130.245.9.242       DNS        71 Standard query 0x0003  NS www.mit.edu
   17 2.004001  Cisco_d8:86:8a      PVST+               STP        64 Conf. Root = 32768/0/00:21:1c:ef:58:17  Cost = 0  Port = 0x83a7
   18 2.260993  JuniperN_55:5b:41   Spanning-tree-(for- STP       119 MST. Root = 24576/0/00:00:01:00:00:01  Cost = 1000  Port = 0x82
   19 2.394559  130.245.9.242       130.245.23.106      DNS       144 Standard query response 0x0003  CNAME www.mit.edu.edgekey.net C
   20 3.446572  130.245.23.32       130.245.23.255      DHCP      590 DHCP Inform   - Transaction ID 0xffff86b5

⊞ Frame 19: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits)
⊞ Ethernet II, Src: Netscreen_ff:10:02 (00:10:db:ff:10:02), Dst: Giga-Byt_6e:5e:e5 (00:24:1d:6e:5e:e5)
⊞ Internet Protocol Version 4, Src: 130.245.9.242 (130.245.9.242), Dst: 130.245.23.106 (130.245.23.106)
⊞ User Datagram Protocol, Src Port: 53 (53), Dst Port: 55067 (55067)
⊟ Domain Name System (response)
    [Request In: 16]
    [Time: 0.406093000 seconds]
    Transaction ID: 0x0003
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.mit.edu: type NS, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  ⊟ 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

0000  00 24 1d 6e 5e e5 00 10  db ff 10 02 08 00 45 00   .$.n^... ......E.
0010  00 82 1a ac 00 00 7f 11  f9 78 82 f5 09 f2 82 f5   ........ .x......
0020  17 6a 00 35 d7 1b 00 6e  e8 25 00 03 81 80 00 01   .j.5...n .%......
0030  00 02 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
0040  64 75 00 00 02 00 01 c0  0c 00 05 00 01 00 00 05   du...... ........
0050  1a 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   ....www. mit.edu.
```

File: "E:\Dropbox\Notes\CSE310\Lab3_trans\... | Packets: 25 · Displayed: 25 (100.0%) · Load time: 0:00.001 | Profile: Default

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?**

    NOTE : Using the university of Seoul National University domain which is www.snu.ac.kr and using Google DNS (8.8.8.8) as the DNS server

    The DNS Query is sent to 8.8.8.8 which corresponds to Google's DNS. No this is not the default dns.

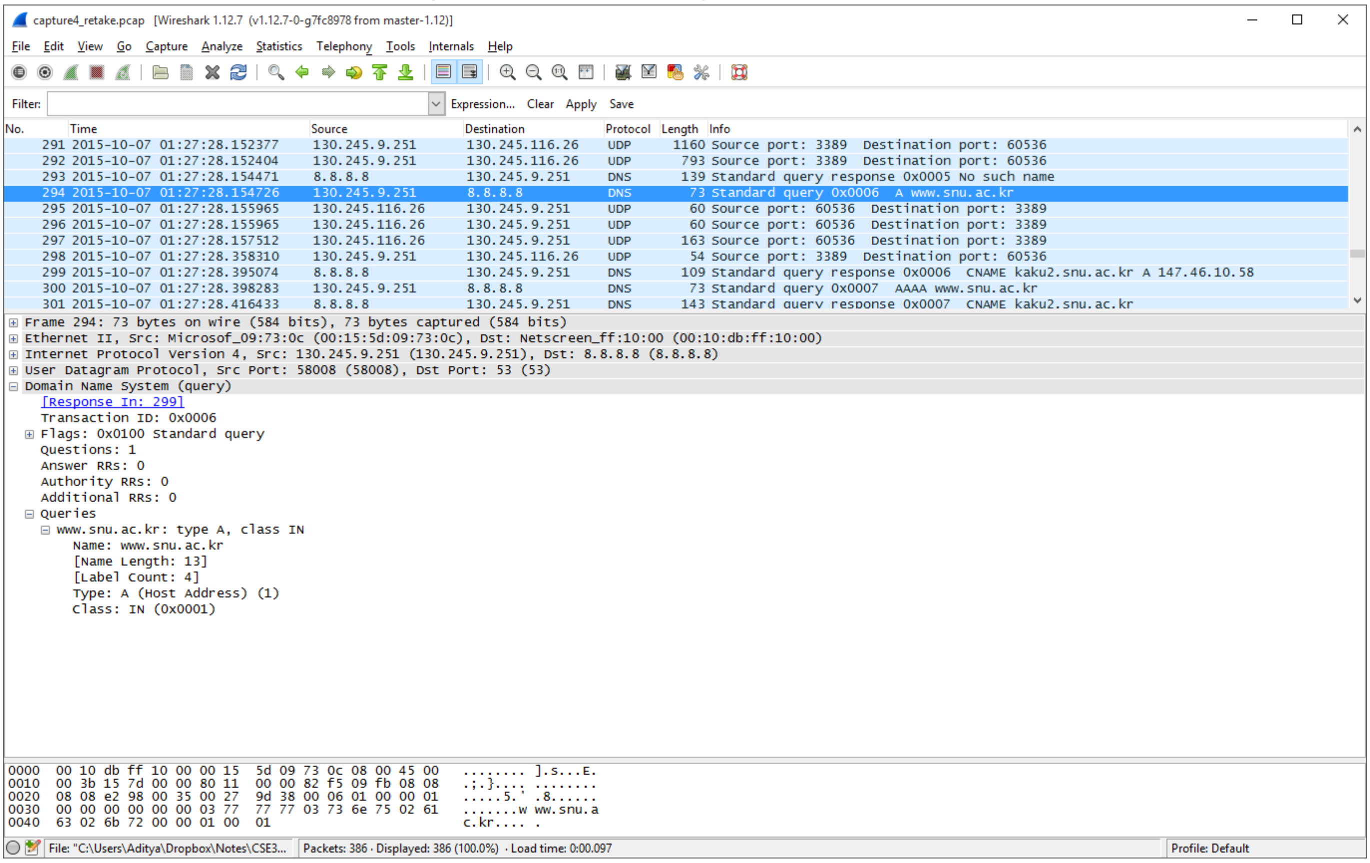
21. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

    It is a standard type A query and does not contain any answers.

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

    There are 2 answers provided the first one is the canonical name and the second has the address.

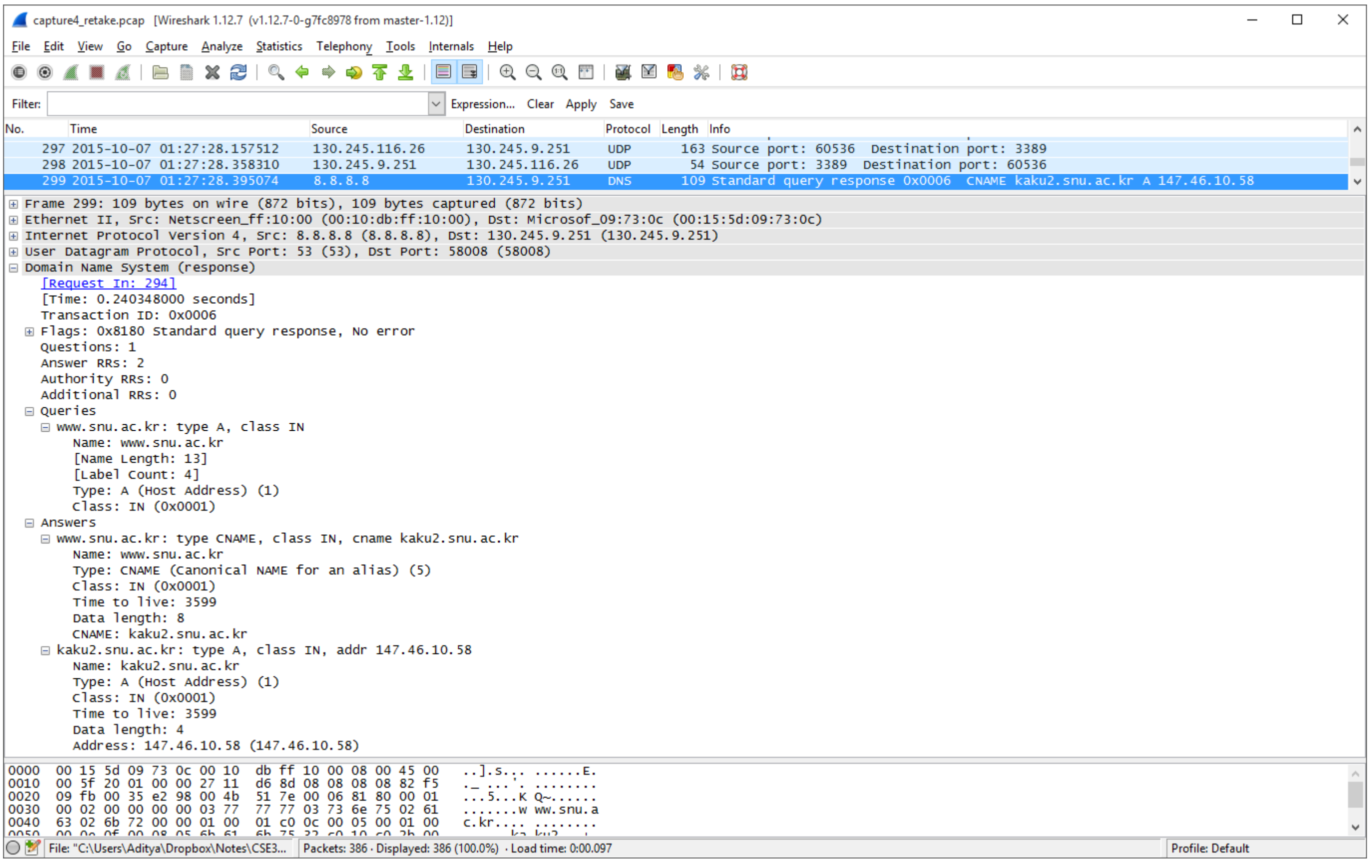
23. **Provide a screenshot. Indicate query and response messages**


capture4_retake.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
File: "C:\Users\Aditya\Dropbox\Notes\CSE3...
Packets: 386 · Displayed: 386 (100.0%) · Load time: 0:00.097
Profile: Default

```
No.   Time                          Source            Destination       Protocol Length Info
  291 2015-10-07 01:27:28.152377    130.245.9.251     130.245.116.26    UDP      1160 Source port: 3389  Destination port: 60536
  292 2015-10-07 01:27:28.152404    130.245.9.251     130.245.116.26    UDP       793 Source port: 3389  Destination port: 60536
  293 2015-10-07 01:27:28.154471    8.8.8.8           130.245.9.251     DNS       139 Standard query response 0x0005 No such name
  294 2015-10-07 01:27:28.154726    130.245.9.251     8.8.8.8           DNS        73 Standard query 0x0006  A www.snu.ac.kr
  295 2015-10-07 01:27:28.155965    130.245.116.26    130.245.9.251     UDP        60 Source port: 60536  Destination port: 3389
  296 2015-10-07 01:27:28.155965    130.245.116.26    130.245.9.251     UDP        60 Source port: 60536  Destination port: 3389
  297 2015-10-07 01:27:28.157512    130.245.116.26    130.245.9.251     UDP       163 Source port: 60536  Destination port: 3389
  298 2015-10-07 01:27:28.358310    130.245.9.251     130.245.116.26    UDP        54 Source port: 3389  Destination port: 60536
  299 2015-10-07 01:27:28.395074    8.8.8.8           130.245.9.251     DNS       109 Standard query response 0x0006  CNAME kaku2.snu.ac.kr A 147.46.10.58
  300 2015-10-07 01:27:28.398283    130.245.9.251     8.8.8.8           DNS        73 Standard query 0x0007  AAAA www.snu.ac.kr
  301 2015-10-07 01:27:28.416433    8.8.8.8           130.245.9.251     DNS       143 Standard query response 0x0007  CNAME kaku2.snu.ac.kr
```

```
⊞ Frame 294: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
⊞ Ethernet II, Src: Microsof_09:73:0c (00:15:5d:09:73:0c), Dst: Netscreen_ff:10:00 (00:10:db:ff:10:00)
⊞ Internet Protocol Version 4, Src: 130.245.9.251 (130.245.9.251), Dst: 8.8.8.8 (8.8.8.8)
⊞ User Datagram Protocol, Src Port: 58008 (58008), Dst Port: 53 (53)
⊟ Domain Name System (query)
    [Response In: 299]
    Transaction ID: 0x0006
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.snu.ac.kr: type A, class IN
        Name: www.snu.ac.kr
        [Name Length: 13]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

```
0000  00 10 db ff 10 00 00 15  5d 09 73 0c 08 00 45 00   ........ ].s...E.
0010  00 3b 15 7d 00 00 80 11  00 00 82 f5 09 fb 08 08   .;.}.... ........
0020  08 08 e2 98 00 35 00 27  9d 38 00 06 01 00 00 01   .....5.' .8......
0030  00 00 00 00 00 00 03 77  77 77 03 73 6e 75 02 61   .......w ww.snu.a
0040  63 02 6b 72 00 00 01 00  01                        c.kr.... .
```


capture4_retake.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time                          Source           Destination      Protocol Length Info
  297 2015-10-07 01:27:28.157512   130.245.116.26   130.245.9.251    UDP      163 Source port: 60536  Destination port: 3389
  298 2015-10-07 01:27:28.358310   130.245.9.251    130.245.116.26   UDP       54 Source port: 3389  Destination port: 60536
  299 2015-10-07 01:27:28.395074   8.8.8.8          130.245.9.251    DNS      109 Standard query response 0x0006  CNAME kaku2.snu.ac.kr A 147.46.10.58

⊞ Frame 299: 109 bytes on wire (872 bits), 109 bytes captured (872 bits)
⊞ Ethernet II, Src: Netscreen_ff:10:00 (00:10:db:ff:10:00), Dst: Microsof_09:73:0c (00:15:5d:09:73:0c)
⊞ Internet Protocol Version 4, Src: 8.8.8.8 (8.8.8.8), Dst: 130.245.9.251 (130.245.9.251)
⊞ User Datagram Protocol, Src Port: 53 (53), Dst Port: 58008 (58008)
⊟ Domain Name System (response)
    [Request In: 294]
    [Time: 0.240348000 seconds]
    Transaction ID: 0x0006
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.snu.ac.kr: type A, class IN
        Name: www.snu.ac.kr
        [Name Length: 13]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ www.snu.ac.kr: type CNAME, class IN, cname kaku2.snu.ac.kr
        Name: www.snu.ac.kr
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 3599
        Data length: 8
        CNAME: kaku2.snu.ac.kr
    ⊟ kaku2.snu.ac.kr: type A, class IN, addr 147.46.10.58
        Name: kaku2.snu.ac.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3599
        Data length: 4
        Address: 147.46.10.58 (147.46.10.58)

0000  00 15 5d 09 73 0c 00 10  db ff 10 00 08 00 45 00   ..].s... ......E.
0010  00 5f 20 01 00 00 27 11  d6 8d 08 08 08 08 82 f5   ._ ...'. ........
0020  09 fb 00 35 e2 98 00 4b  51 7e 00 06 81 80 00 01   ...5...K Q~......
0030  00 02 00 00 00 00 03 77  77 77 03 73 6e 75 02 61   .......w ww.snu.a
0040  63 02 6b 72 00 00 01 00  01 c0 0c 00 05 00 01 00   c.kr.... ........
0050  00 0e 0f 00 08 05 6b 61  6b 75 32 c0 10 c0 2b 00   ......ka ku2...+.
```

File: "C:\Users\Aditya\Dropbox\Notes\CSE3... | Packets: 386 · Displayed: 386 (100.0%) · Load time: 0:00.097 | Profile: Default

Part 2

Documentation

This is a simple HTTP server written in python. It can handle files of type html, rawtext, jpeg and pngs. To execute the server, simply run `python part3server.py` on an allv machine and then visit http://allv24.all.cs.stonybrook.edu:8920/Hello,html

Server code :

```
# pylint: disable=W,C
```

#Aditya Balwani, SBU ID : 109353920

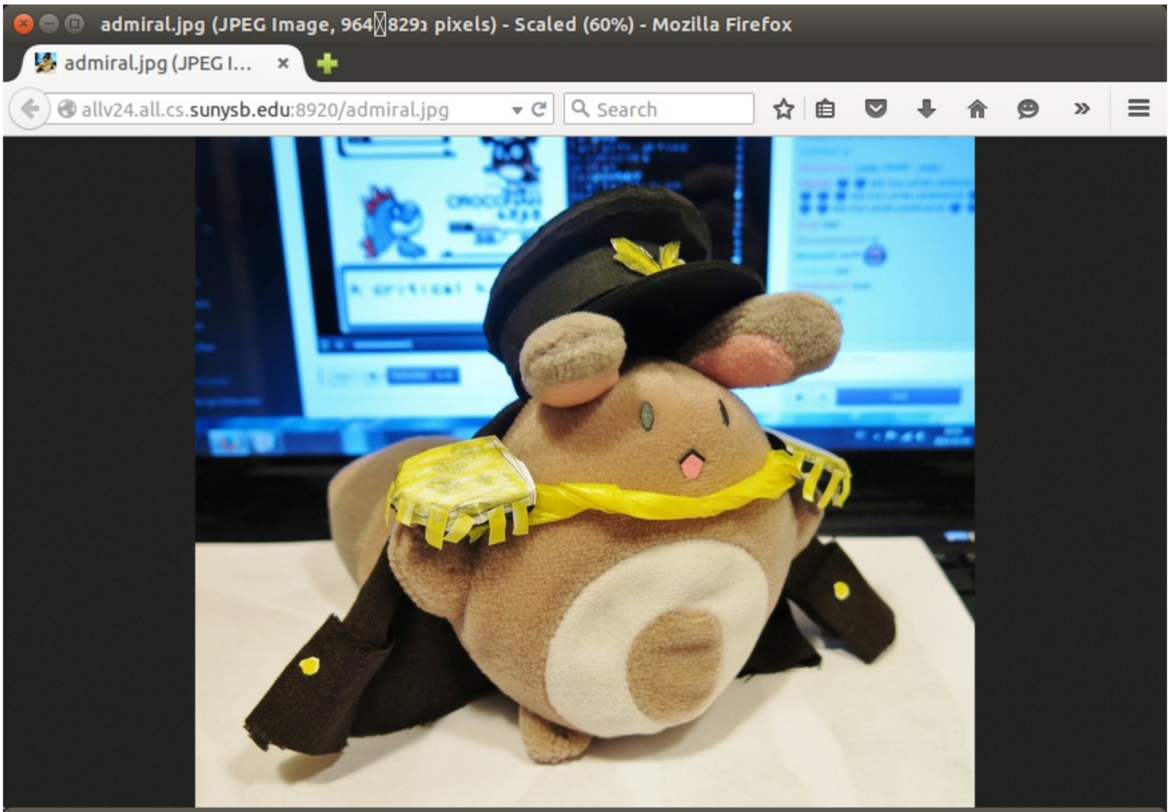
#import socket module from socket import * #Set port number to 8920 serverPort = 8920 serverSocket= socket(AF_INET, SOCK_STREAM) #Prepare a sever socket, bind port serverSocket.bind(('',serverPort)) serverSocket.listen(1) while True: #Establish the connection print 'Ready to serve...'

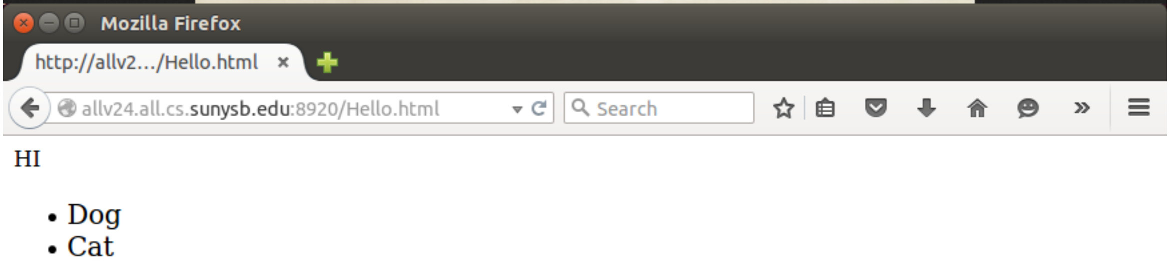
```
<span class="hljs-comment">#Accept a request from a host</span>
connectionSocket, addr = serverSocket.accept()
<span class="hljs-keyword">try</span>:
    <span class="hljs-comment">#On request recieved, parse the message</span>
    message = connectionSocket.recv(<span class="hljs-number">2048</span>)
    <span class="hljs-keyword">print</span> message

    <span class="hljs-comment">#Extract the filename and the filetype</span>
    filename = message.split()[<span class="hljs-number">1</span>]
    <span class="hljs-keyword">print</span> filename

    fileType = filename.split(<span class="hljs-string">"."</span>)[<span class="hljs-number">1</span>].lower()
    <span class="hljs-keyword">print</span> fileType
```

```
        <span class="hljs-comment">#Read file type</span>
        f = open(filename[<span class="hljs-number">1</span>:],<span class="hljs-string">"r"</span>)
        outputdata = f.read()

        <span class="hljs-comment"># Check file types, and define content type header</span>
        <span class="hljs-keyword">if</span> fileType == <span class="hljs-string">'jpg'</span> <span class="hljs-keyword">or</span> fileType == <span class="hljs-string">'jpeg'</spa
            contentType = <span class="hljs-string">'image/jpeg'</span>
        <span class="hljs-keyword">elif</span> fileType == <span class="hljs-string">'png'</span>:
            contentType = <span class="hljs-string">'image/png'</span>
        <span class="hljs-keyword">elif</span> fileType == <span class="hljs-string">'html'</span>:
            contentType = <span class="hljs-string">'text/html'</span>
        <span class="hljs-keyword">else</span>:
            contentType = <span class="hljs-string">'text/plain'</span>

        <span class="hljs-keyword">print</span> contentType

        <span class="hljs-comment"># Send HTTP OK</span>
        connectionSocket.send(<span class="hljs-string">"HTTP/1.1 200 OK\r\nContent-Type: "</span>+contentType+<span class="hljs-string">"; charset=utf-8\r\n\r\n"</span>)

        <span class="hljs-comment">#Send the content of the requested file to the client</span>
        <span class="hljs-keyword">for</span> line <span class="hljs-keyword">in</span> outputdata:
            <span class="hljs-comment">#print line</span>
            connectionSocket.send(line)
        connectionSocket.close()
    <span class="hljs-keyword">except</span> IOError:
        <span class="hljs-comment">#Sendresponse message for file not found</span>
        connectionSocket.send(<span class="hljs-string">"HTTP/1.1 404 NOT FOUND\r\nContent-Type: text/html; charset=utf-8\r\n\r\n"</span>)

        <span class="hljs-comment"># Send a 404 page</span>
        connectionSocket.send(<span class="hljs-string">"&lt;html&gt;&lt;head&gt;&lt;title&gt;Hi&lt;/title&gt;&lt;/head&gt;&lt;body&gt;&lt;h1&gt;404 NOT FOUND&lt;/h1&gt;&lt;/body&gt;&
        <span class="hljs-comment">#Close client socket</span>

        connectionSocket.close()
```

serverSocket.close()

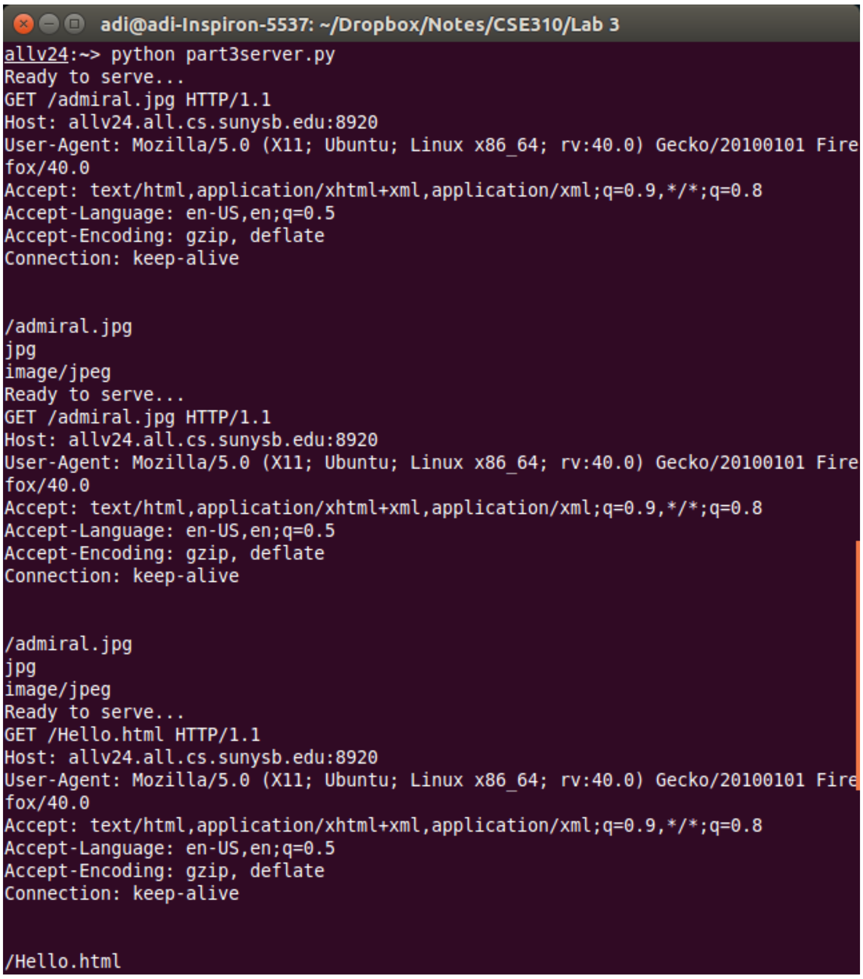
Screenshots


admiral.jpg (JPEG Image, 964▯829ı pixels) - Scaled (60%) - Mozilla Firefox
admiral.jpg (JPEG I...
allv24.all.cs.sunysb.edu:8920/admiral.jpg
Search


Mozilla Firefox
http://allv2.../Hello.html
allv24.all.cs.sunysb.edu:8920/Hello.html
Search

HI

- Dog
- Cat



```
allv24:~> python part3server.py
Ready to serve...
GET /admiral.jpg HTTP/1.1
Host: allv24.all.cs.sunysb.edu:8920
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Fire
fox/40.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive


/admiral.jpg
jpg
image/jpeg
Ready to serve...
GET /admiral.jpg HTTP/1.1
Host: allv24.all.cs.sunysb.edu:8920
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Fire
fox/40.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive


/admiral.jpg
jpg
image/jpeg
Ready to serve...
GET /Hello.html HTTP/1.1
Host: allv24.all.cs.sunysb.edu:8920
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/20100101 Fire
fox/40.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive


/Hello.html
```