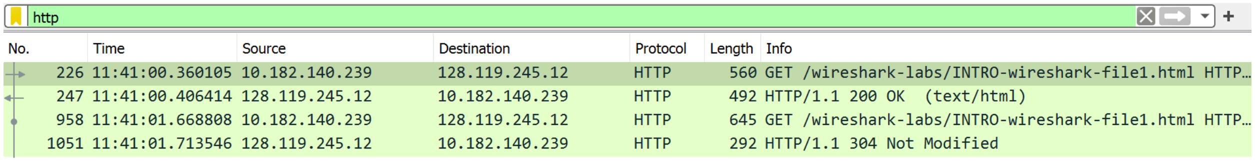
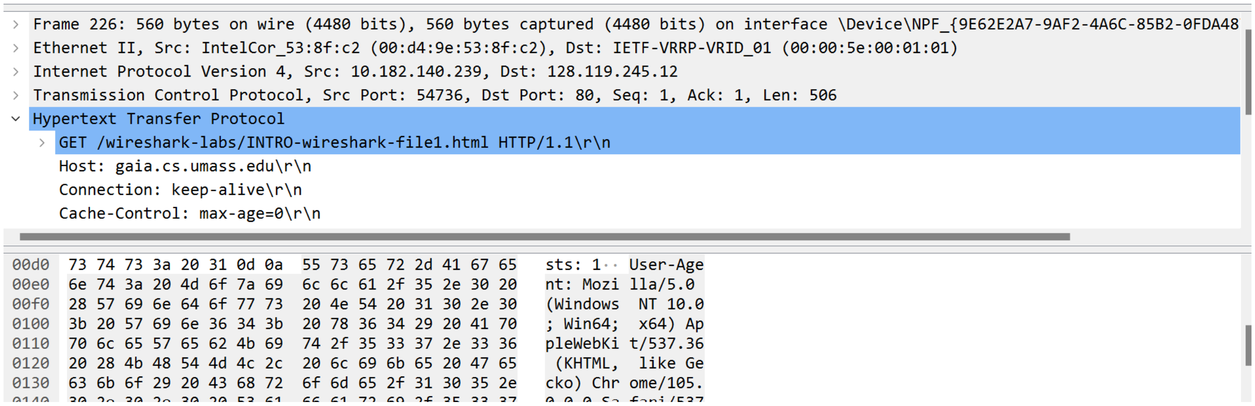
Wireshark Introduction Test Output:



```
http

No.   Time             Source          Destination     Protocol  Length Info
 226 11:41:00.360105 10.182.140.239  128.119.245.12  HTTP       560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP…
 247 11:41:00.406414 128.119.245.12  10.182.140.239  HTTP       492 HTTP/1.1 200 OK  (text/html)
 958 11:41:01.668808 10.182.140.239  128.119.245.12  HTTP       645 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP…
1051 11:41:01.713546 128.119.245.12  10.182.140.239  HTTP       292 HTTP/1.1 304 Not Modified
```

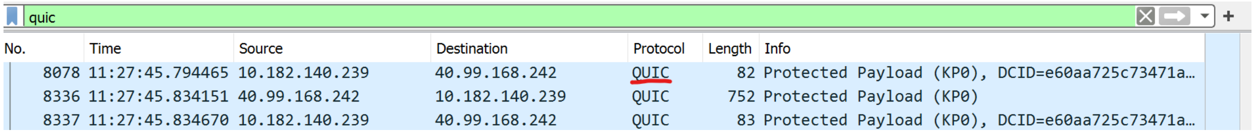


```
> Frame 226: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA48
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54736, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n

00d0  73 74 73 3a 20 31 0d 0a  55 73 65 72 2d 41 67 65   sts: 1·· User-Age
00e0  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0
00f0  28 57 69 6e 64 6f 77 73  20 4e 54 20 31 30 2e 30   (Windows  NT 10.0
0100  3b 20 57 69 6e 36 34 3b  20 78 36 34 29 20 41 70   ; Win64;  x64) Ap
0110  70 6c 65 57 65 62 4b 69  74 2f 35 33 37 2e 33 36   pleWebKi t/537.36
0120  20 28 4b 48 54 4d 4c 2c  20 6c 69 6b 65 20 47 65    (KHTML,  like Ge
0130  63 6b 6f 29 20 43 68 72  6f 6d 65 2f 31 30 35 2e   cko) Chr ome/105.
0140  30 2e 30 2e 30 20 53 61  66 61 72 69 2f 35 33 37   0.0.0 Sa fari/537
```

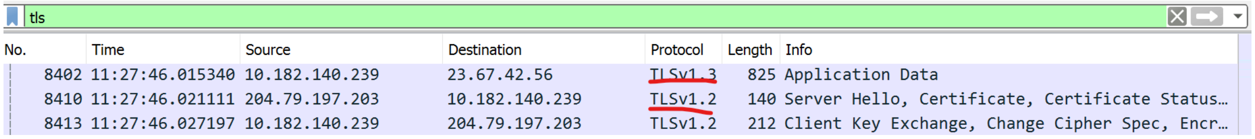
Introduction Lab Questions:

1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark "protocol" column) in your trace file: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

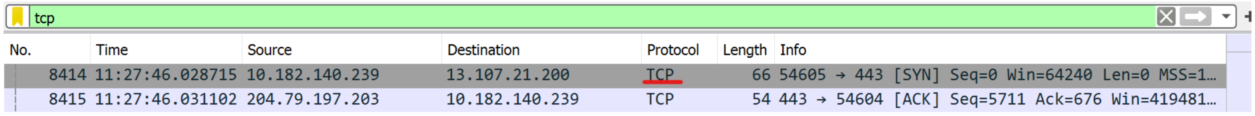
→The following Protocols have appeared: QUIC, TLSv1.3,TLSv1.2, TCP, ICMPv6, HTTP, DNS, UDP. Attached the screenshot of the protocols which appeared in the wireshark.



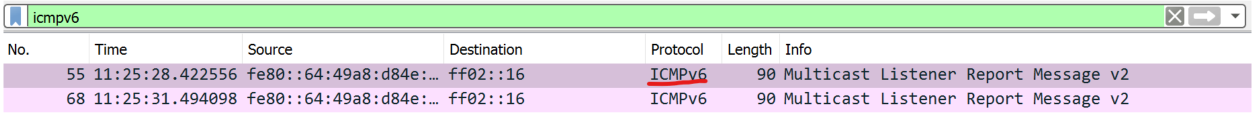
```
quic

No.   Time             Source          Destination     Protocol  Length Info
8078 11:27:45.794465 10.182.140.239  40.99.168.242   QUIC        82 Protected Payload (KP0), DCID=e60aa725c73471a…
8336 11:27:45.834151 40.99.168.242   10.182.140.239  QUIC       752 Protected Payload (KP0)
8337 11:27:45.834670 10.182.140.239  40.99.168.242   QUIC        83 Protected Payload (KP0), DCID=e60aa725c73471a…
```



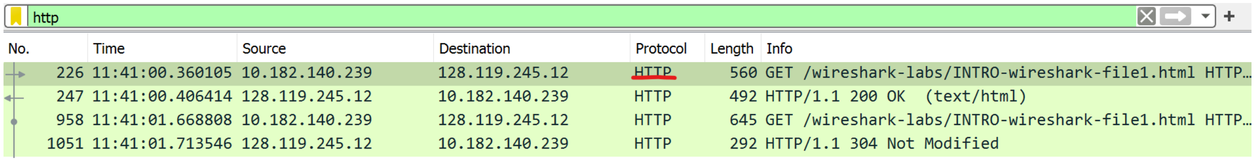
```
tls

No.   Time             Source          Destination     Protocol  Length Info
8402 11:27:46.015340 10.182.140.239  23.67.42.56     TLSv1.3    825 Application Data
8410 11:27:46.021111 204.79.197.203  10.182.140.239  TLSv1.2    140 Server Hello, Certificate, Certificate Status…
8413 11:27:46.027197 10.182.140.239  204.79.197.203  TLSv1.2    212 Client Key Exchange, Change Cipher Spec, Encr…
```



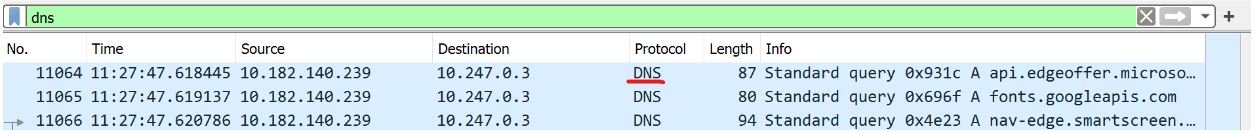
```
tcp

No.   Time             Source          Destination     Protocol  Length Info
8414 11:27:46.028715 10.182.140.239  13.107.21.200   TCP         66 54605 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1…
8415 11:27:46.031102 204.79.197.203  10.182.140.239  TCP         54 443 → 54604 [ACK] Seq=5711 Ack=676 Win=419481…
```



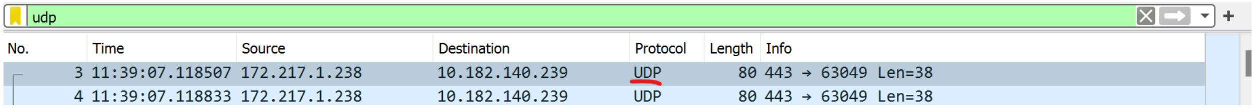
```
icmpv6

No.   Time             Source            Destination  Protocol  Length Info
  55 11:25:28.422556 fe80::64:49a8:d84e:… ff02::16   ICMPv6      90 Multicast Listener Report Message v2
  68 11:25:31.494098 fe80::64:49a8:d84e:… ff02::16   ICMPv6      90 Multicast Listener Report Message v2
```



```
http
No.   Time             Source          Destination     Protocol Length Info
  226 11:41:00.360105 10.182.140.239  128.119.245.12  HTTP      560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP…
  247 11:41:00.406414 128.119.245.12  10.182.140.239  HTTP      492 HTTP/1.1 200 OK  (text/html)
  958 11:41:01.668808 10.182.140.239  128.119.245.12  HTTP      645 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP…
 1051 11:41:01.713546 128.119.245.12  10.182.140.239  HTTP      292 HTTP/1.1 304 Not Modified
```



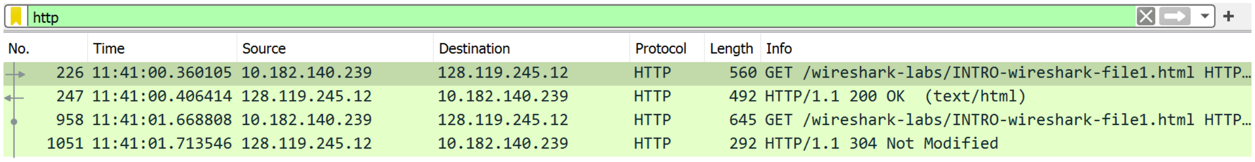
```
dns
No.   Time             Source          Destination     Protocol Length Info
11064 11:27:47.618445 10.182.140.239  10.247.0.3      DNS        87 Standard query 0x931c A api.edgeoffer.microso…
11065 11:27:47.619137 10.182.140.239  10.247.0.3      DNS        80 Standard query 0x696f A fonts.googleapis.com
11066 11:27:47.620786 10.182.140.239  10.247.0.3      DNS        94 Standard query 0x4e23 A nav-edge.smartscreen.…
```



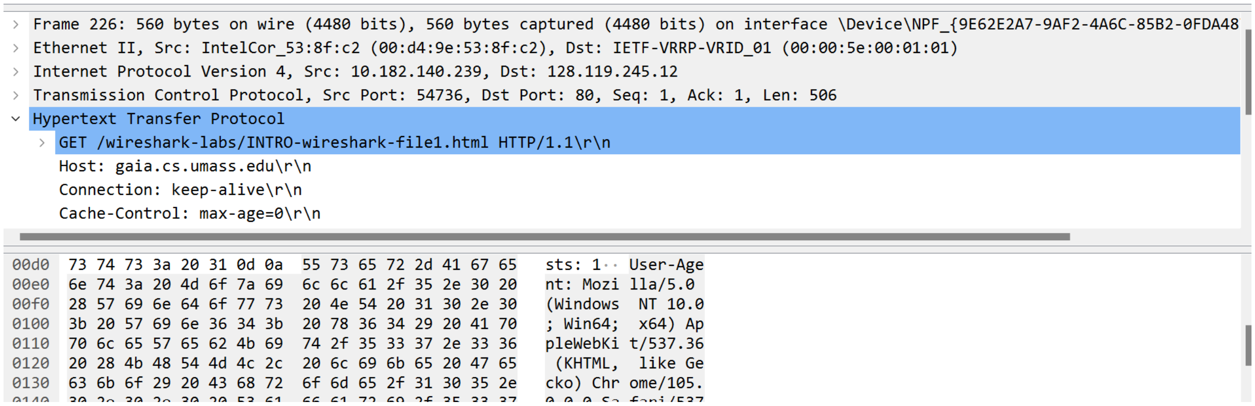
```
udp
No.   Time             Source          Destination     Protocol Length Info
    3 11:39:07.118507 172.217.1.238   10.182.140.239  UDP        80 443 → 63049 Len=38
    4 11:39:07.118833 172.217.1.238   10.182.140.239  UDP        80 443 → 63049 Len=38
```

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

→ It took around 0.046309 seconds (11:41:00.360105 - 11:41:00.406414)



```
http
No.   Time             Source          Destination     Protocol Length Info
  226 11:41:00.360105 10.182.140.239  128.119.245.12  HTTP      560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP…
  247 11:41:00.406414 128.119.245.12  10.182.140.239  HTTP      492 HTTP/1.1 200 OK  (text/html)
  958 11:41:01.668808 10.182.140.239  128.119.245.12  HTTP      645 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP…
 1051 11:41:01.713546 128.119.245.12  10.182.140.239  HTTP      292 HTTP/1.1 304 Not Modified
```

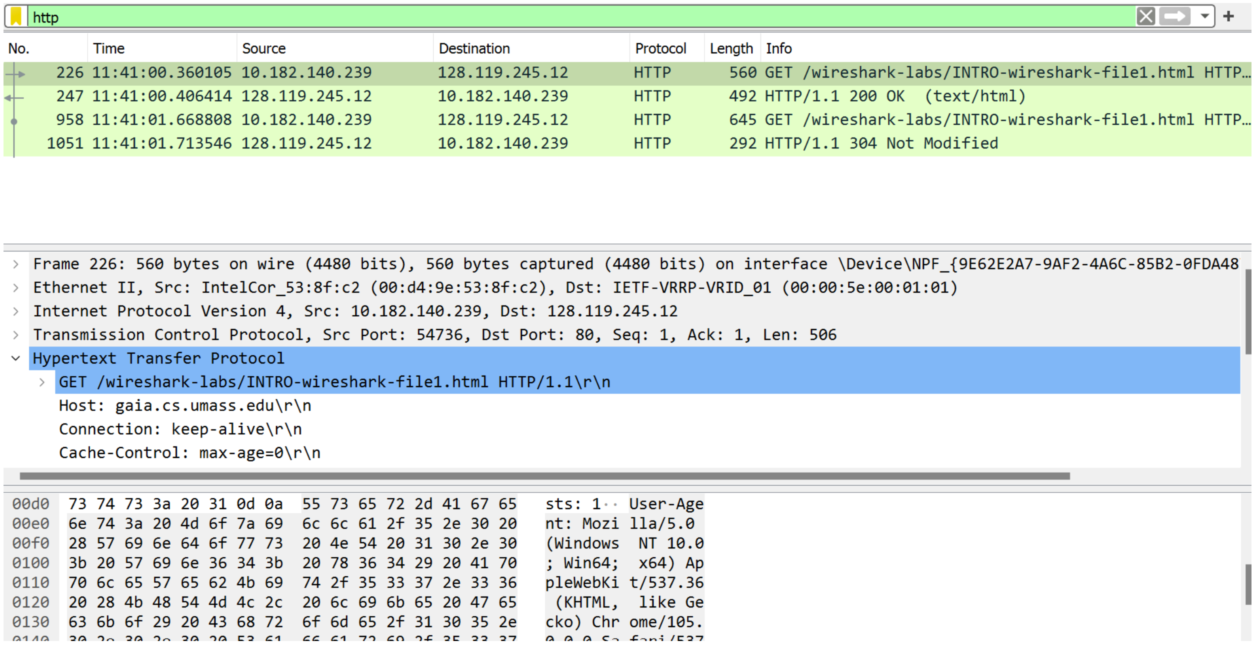


```
> Frame 226: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA48
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54736, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n

00d0  73 74 73 3a 20 31 0d 0a  55 73 65 72 2d 41 67 65   sts: 1·· User-Age
00e0  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0
00f0  28 57 69 6e 64 6f 77 73  20 4e 54 20 31 30 2e 30   (Windows  NT 10.0
0100  3b 20 57 69 6e 36 34 3b  20 78 36 34 29 20 41 70   ; Win64;  x64) Ap
0110  70 6c 65 57 65 62 4b 69  74 2f 35 33 37 2e 33 36   pleWebKi t/537.36
0120  20 28 4b 48 54 4d 4c 2c  20 6c 69 6b 65 20 47 65    (KHTML,  like Ge
0130  63 6b 6f 29 20 43 68 72  6f 6d 65 2f 31 30 35 2e   cko) Chr ome/105.
0140  30 2e 30 2e 30 20 53 61  66 61 72 69 2f 35 33 37   0.0.0 Sa fari/537
```

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer or (if you are using the trace file) the computer that sent the HTTP GET message?

→ The Internet address of gaia.cs.umass.edu is 128.119.245.12

→The Internet address of the computer that sent the HTTP GET message is 10.182.140.239

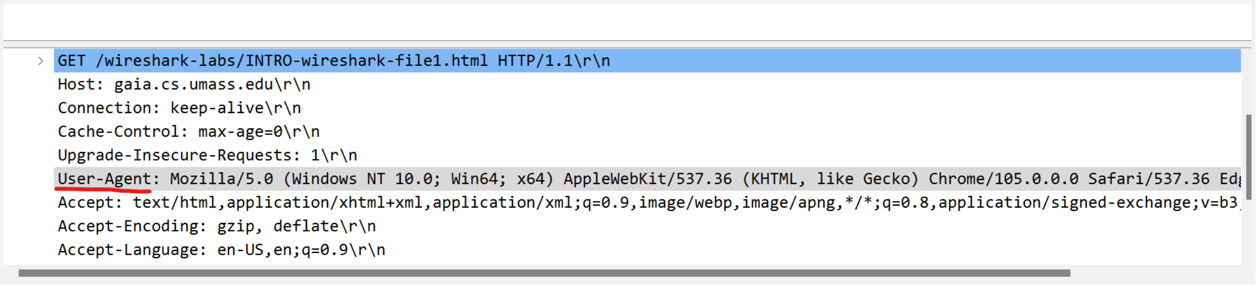


```
http
No.   Time             Source          Destination     Protocol  Length Info
  226 11:41:00.360105 10.182.140.239  128.119.245.12  HTTP       560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP…
  247 11:41:00.406414 128.119.245.12  10.182.140.239  HTTP       492 HTTP/1.1 200 OK  (text/html)
  958 11:41:01.668808 10.182.140.239  128.119.245.12  HTTP       645 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP…
 1051 11:41:01.713546 128.119.245.12  10.182.140.239  HTTP       292 HTTP/1.1 304 Not Modified
```

```
> Frame 226: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA48
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54736, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
```

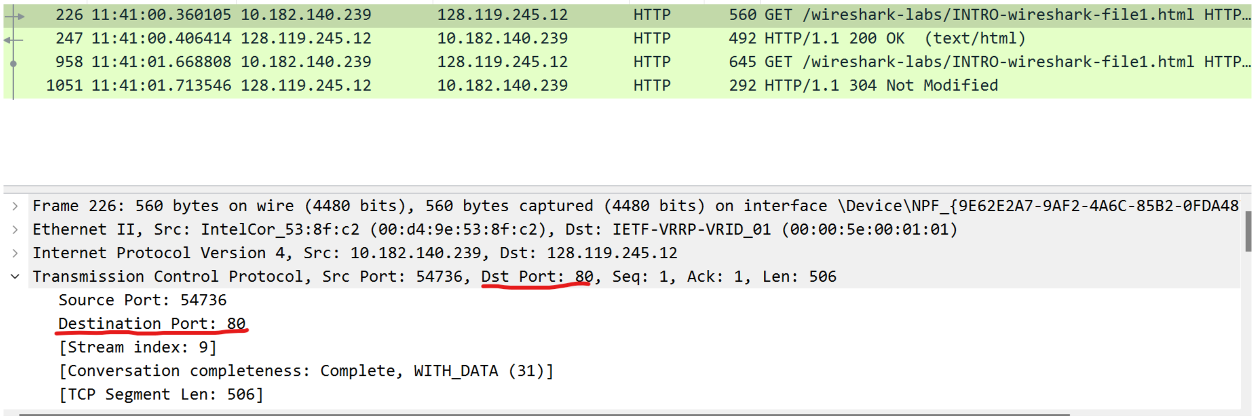
```
00d0  73 74 73 3a 20 31 0d 0a  55 73 65 72 2d 41 67 65   sts: 1·· User-Age
00e0  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0
00f0  28 57 69 6e 64 6f 77 73  20 4e 54 20 31 30 2e 30   (Windows  NT 10.0
0100  3b 20 57 69 6e 36 34 3b  20 78 36 34 29 20 41 70   ; Win64;  x64) Ap
0110  70 6c 65 57 65 62 4b 69  74 2f 35 33 37 2e 33 36   pleWebKi t/537.36
0120  20 28 4b 48 54 4d 4c 2c  20 6c 69 6b 65 20 47 65    (KHTML,  like Ge
0130  63 6b 6f 29 20 43 68 72  6f 6d 65 2f 31 30 35 2e   cko) Chr ome/105.
0140  30 2e 30 2e 30 20 53 61  66 61 72 69 2f 35 33 37   0.0.0 Sa fari/537
```

4. What type of Web browser issued the HTTP request?
→ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.53



```
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Ed
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
```

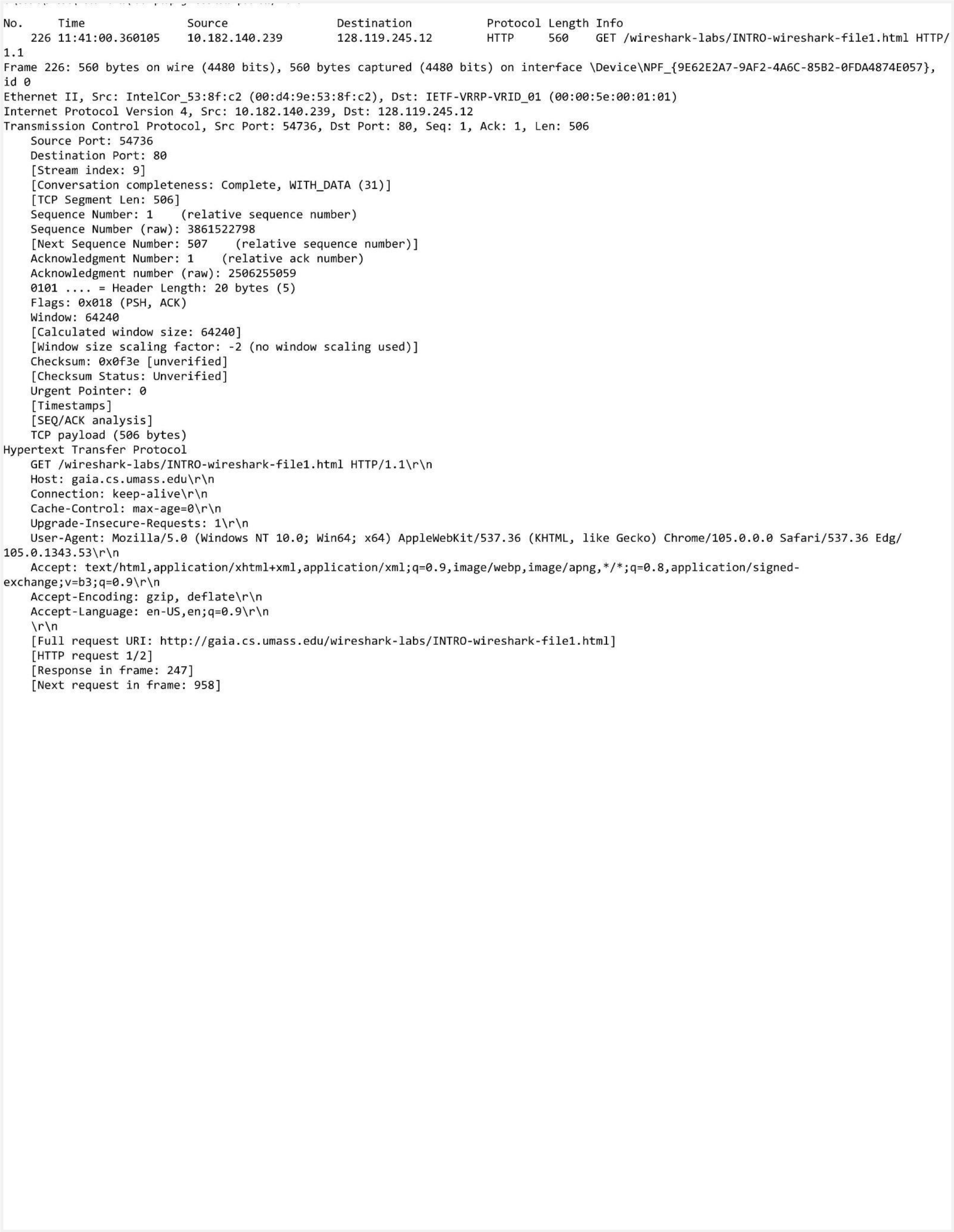
5.What is the destination port number (the number following “Dest Port:” for the TCP segment containing the HTTP request) to which this HTTP request is being sent?
→ The Dest Port is 80



```
  226 11:41:00.360105 10.182.140.239  128.119.245.12  HTTP       560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP…
  247 11:41:00.406414 128.119.245.12  10.182.140.239  HTTP       492 HTTP/1.1 200 OK  (text/html)
  958 11:41:01.668808 10.182.140.239  128.119.245.12  HTTP       645 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP…
 1051 11:41:01.713546 128.119.245.12  10.182.140.239  HTTP       292 HTTP/1.1 304 Not Modified
```

```
> Frame 226: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA48
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 54736, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
    Source Port: 54736
    Destination Port: 80
    [Stream index: 9]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 506]
```

6.Print the two HTTP messages (GET and OK) referred to in question 2 above.



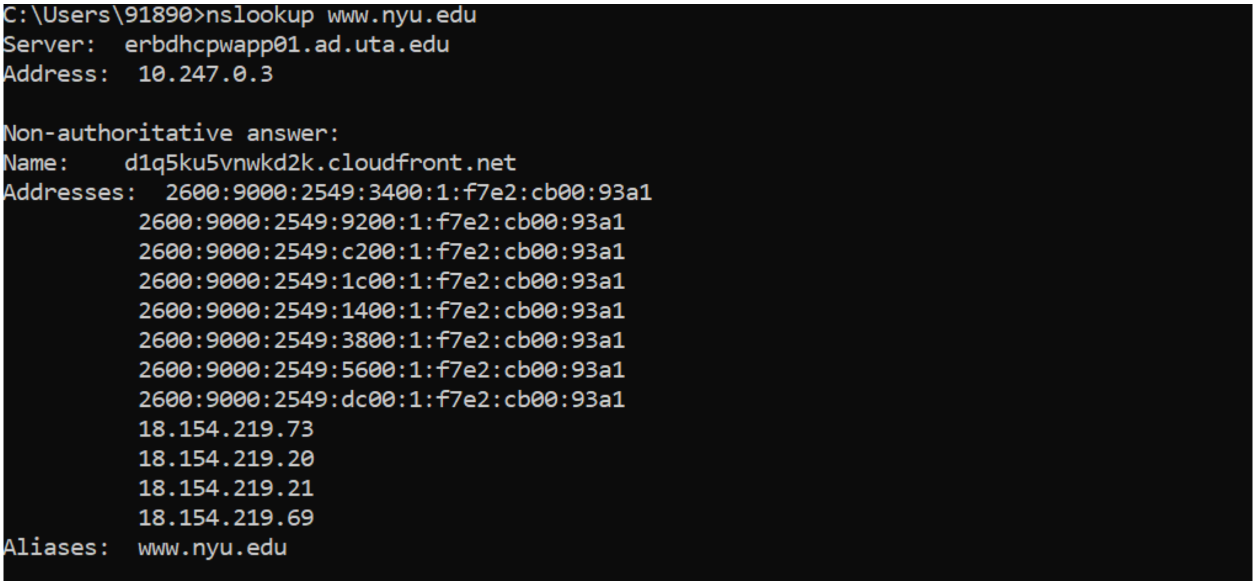
```
No.     Time               Source                Destination           Protocol Length Info
    226 11:41:00.360105    10.182.140.239        128.119.245.12        HTTP     560    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 226: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057},
id 0
Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
Internet Protocol Version 4, Src: 10.182.140.239, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54736, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
    Source Port: 54736
    Destination Port: 80
    [Stream index: 9]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 506]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3861522798
    [Next Sequence Number: 507    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2506255059
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x0f3e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (506 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/
105.0.1343.53\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 247]
    [Next request in frame: 958]
```

```
No.     Time               Source                Destination           Protocol Length Info
    247 11:41:00.406414    128.119.245.12        10.182.140.239        HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 247: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057},
id 0
Ethernet II, Src: JuniperN_27:f3:f0 (d4:04:ff:27:f3:f0), Dst: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.182.140.239
Transmission Control Protocol, Src Port: 80, Dst Port: 54736, Seq: 1, Ack: 507, Len: 438
    Source Port: 80
    Destination Port: 54736
    [Stream index: 9]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2506255059
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 507    (relative ack number)
    Acknowledgment number (raw): 3861523304
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 32120
    [Calculated window size: 32120]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x4b67 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Thu, 29 Sep 2022 16:40:56 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 29 Sep 2022 05:59:01 GMT\r\n
    ETag: "51-5e9ca92f324de"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.046309000 seconds]
    [Request in frame: 226]
    [Next request in frame: 958]
    [Next response in frame: 1051]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

Lab 1 :

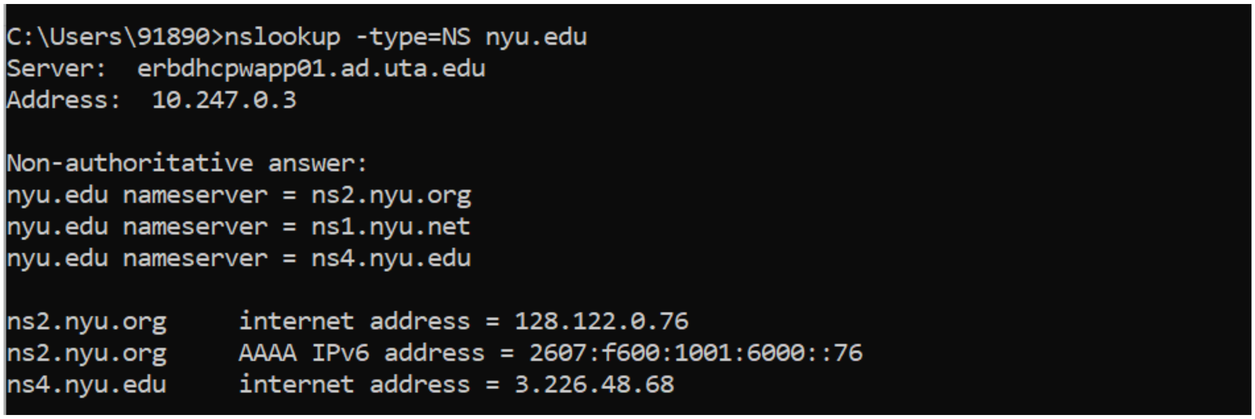
Practice Nslookup Execution

Command 1 : nslookup www.nyu.edu



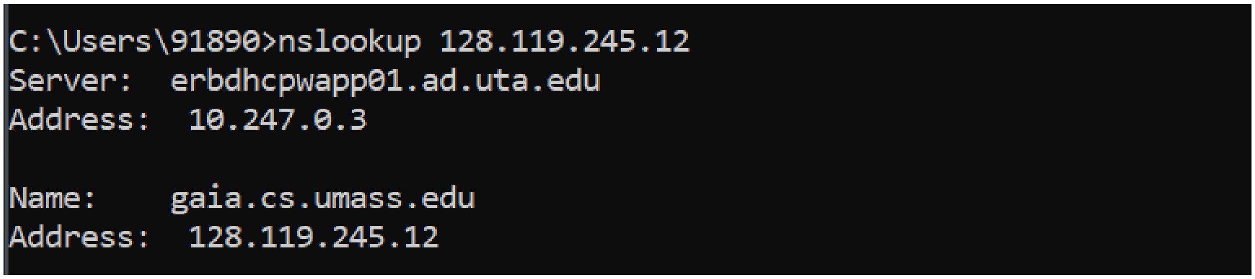
```
C:\Users\91890>nslookup www.nyu.edu
Server:  erbdhcpwapp01.ad.uta.edu
Address:  10.247.0.3

Non-authoritative answer:
Name:    d1q5ku5vnwkd2k.cloudfront.net
Addresses:  2600:9000:2549:3400:1:f7e2:cb00:93a1
          2600:9000:2549:9200:1:f7e2:cb00:93a1
          2600:9000:2549:c200:1:f7e2:cb00:93a1
          2600:9000:2549:1c00:1:f7e2:cb00:93a1
          2600:9000:2549:1400:1:f7e2:cb00:93a1
          2600:9000:2549:3800:1:f7e2:cb00:93a1
          2600:9000:2549:5600:1:f7e2:cb00:93a1
          2600:9000:2549:dc00:1:f7e2:cb00:93a1
          18.154.219.73
          18.154.219.20
          18.154.219.21
          18.154.219.69
Aliases:  www.nyu.edu
```

Command 2 : nslookup -type=NS nyu.edu



```
C:\Users\91890>nslookup -type=NS nyu.edu
Server:  erbdhcpwapp01.ad.uta.edu
Address:  10.247.0.3

Non-authoritative answer:
nyu.edu nameserver = ns2.nyu.org
nyu.edu nameserver = ns1.nyu.net
nyu.edu nameserver = ns4.nyu.edu

ns2.nyu.org     internet address = 128.122.0.76
ns2.nyu.org     AAAA IPv6 address = 2607:f600:1001:6000::76
ns4.nyu.edu     internet address = 3.226.48.68
```

Command 3 : nslookup 128.119.245.12

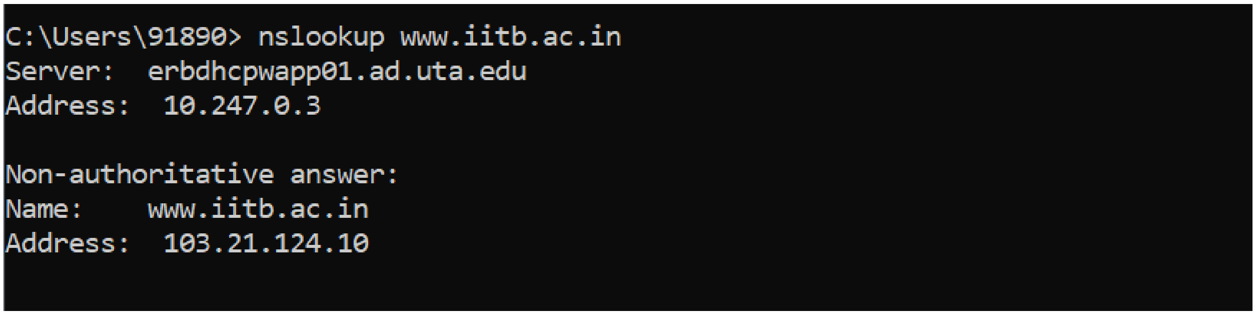


```
C:\Users\91890>nslookup 128.119.245.12
Server:  erbdhcpwapp01.ad.uta.edu
Address:  10.247.0.3

Name:    gaia.cs.umass.edu
Address:  128.119.245.12
```

Lab 1 nslookup execution :

1. What is the IP address of www.iitb.ac.in?

   → The IP address is 103.21.124.10



```
C:\Users\91890> nslookup www.iitb.ac.in
Server:  erbdhcpwapp01.ad.uta.edu
Address:  10.247.0.3

Non-authoritative answer:
Name:    www.iitb.ac.in
Address:  103.21.124.10
```

2. What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above?

   → The IP address for DNS server is 10.247.0.3

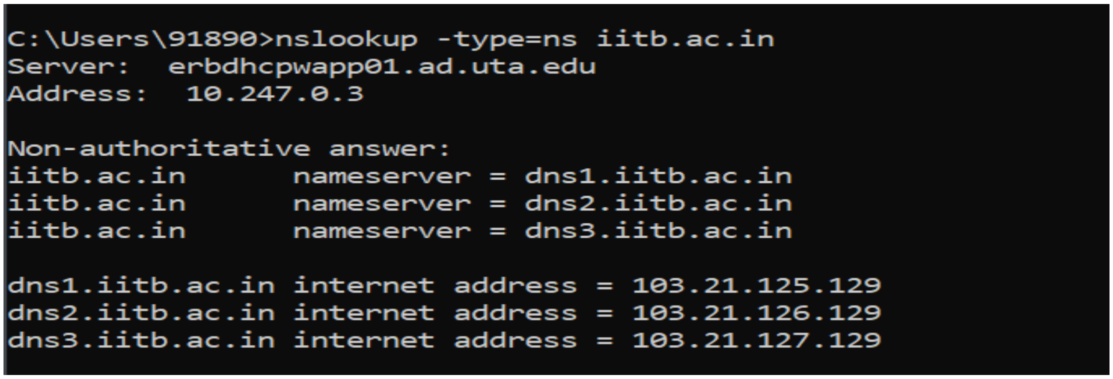
3. Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?

   → The answer came from the Non-authoritative server.

4. Use the nslookup command to determine the name of the authoritative name server for the iit.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative name server, how would you do so?

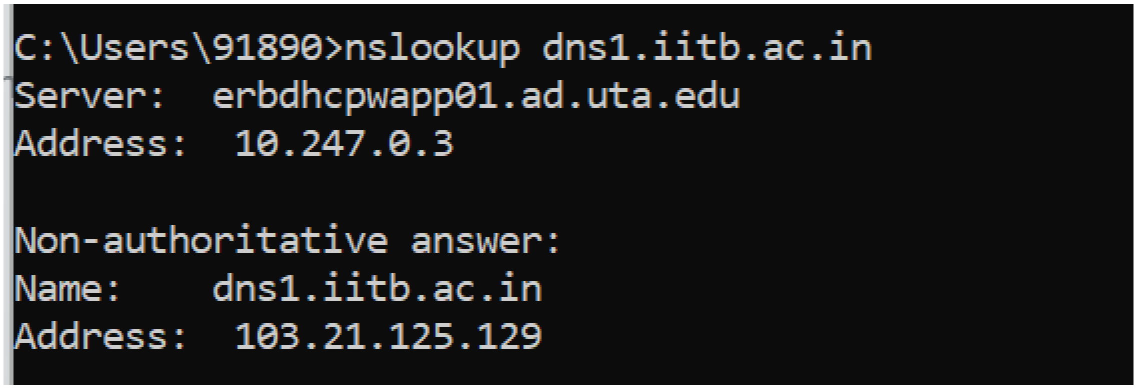
   → The name of the first authoritative server is dns1.iitb.ac.in

   → The IP address of the first authoritative server is 103.21.125.129. it is specified next to the name of the first authoritative server



```
C:\Users\91890>nslookup -type=ns iitb.ac.in
Server:  erbdhcpwapp01.ad.uta.edu
Address:  10.247.0.3

Non-authoritative answer:
iitb.ac.in      nameserver = dns1.iitb.ac.in
iitb.ac.in      nameserver = dns2.iitb.ac.in
iitb.ac.in      nameserver = dns3.iitb.ac.in

dns1.iitb.ac.in internet address = 103.21.125.129
dns2.iitb.ac.in internet address = 103.21.126.129
dns3.iitb.ac.in internet address = 103.21.127.129
```

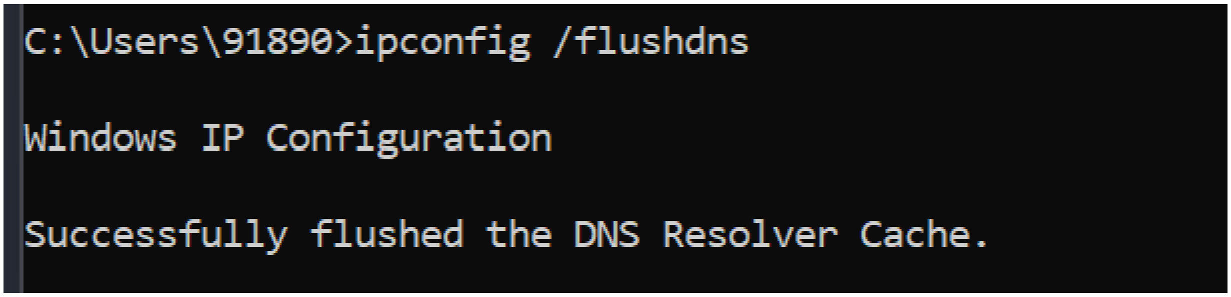
→ The IP address of the first authoritative server can also be found by typing “nslookup dns1.iitb.ac.in “



```
C:\Users\91890>nslookup dns1.iitb.ac.in
Server:  erbdhcpwapp01.ad.uta.edu
Address:  10.247.0.3

Non-authoritative answer:
Name:    dns1.iitb.ac.in
Address:  103.21.125.129
```

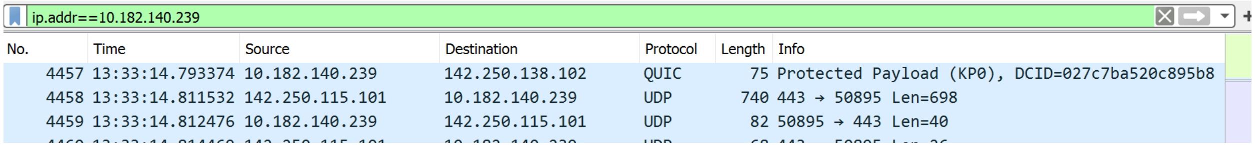
Tracking DNS Execution :

Flush the DNS Resolver cache



```
C:\Users\91890>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

ip.addr == <your_IP_address> filter applied which is displayed in the below screenshot.

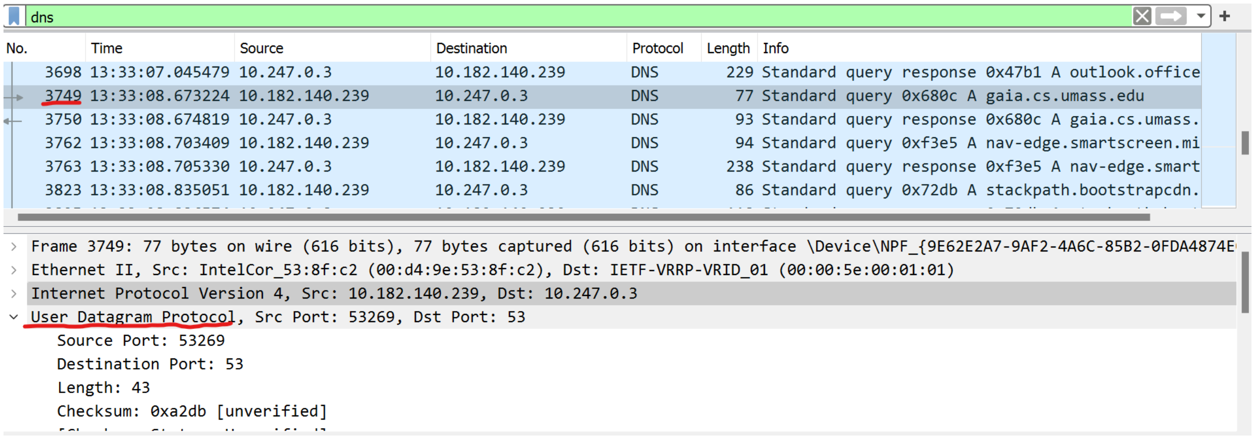


```
ip.addr==10.182.140.239
No.  Time            Source          Destination     Protocol Length Info
4457 13:33:14.793374 10.182.140.239  142.250.138.102 QUIC       75 Protected Payload (KP0), DCID=027c7ba520c895b8
4458 13:33:14.811532 142.250.115.101 10.182.140.239  UDP       740 443 → 50895 Len=698
4459 13:33:14.812476 10.182.140.239  142.250.115.101 UDP        82 50895 → 443 Len=40
```

1. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number in the trace for the DNS query message? Is this query message sent over UDP or TCP?

   → The packet number for the DNS query message is 3749.

   → This query message was sent over UDP - User datagram protocol



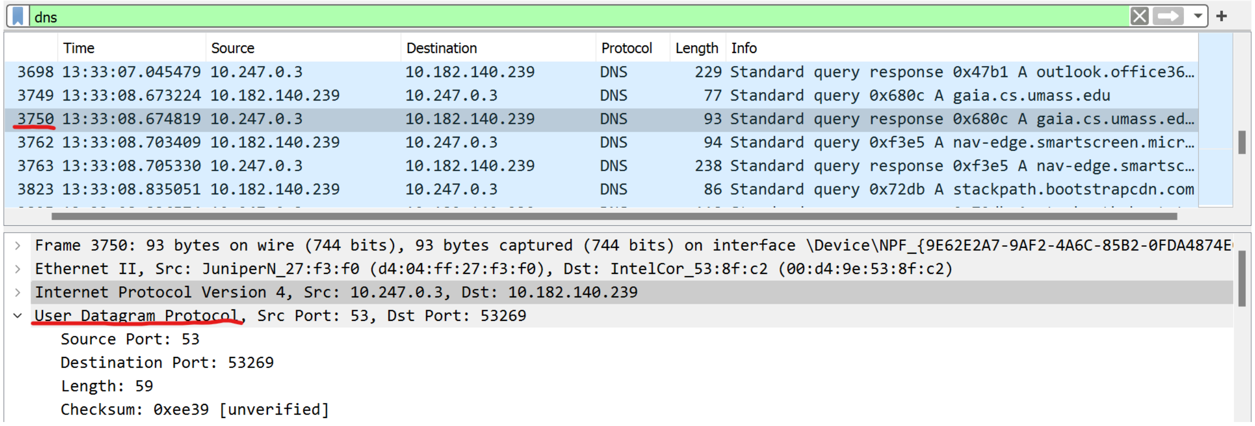
```
No.   Time             Source          Destination     Protocol  Length  Info
 3698 13:33:07.045479 10.247.0.3      10.182.140.239  DNS        229 Standard query response 0x47b1 A outlook.office
 3749 13:33:08.673224 10.182.140.239  10.247.0.3      DNS         77 Standard query 0x680c A gaia.cs.umass.edu
 3750 13:33:08.674819 10.247.0.3      10.182.140.239  DNS         93 Standard query response 0x680c A gaia.cs.umass.
 3762 13:33:08.703409 10.182.140.239  10.247.0.3      DNS         94 Standard query 0xf3e5 A nav-edge.smartscreen.mi
 3763 13:33:08.705330 10.247.0.3      10.182.140.239  DNS        238 Standard query response 0xf3e5 A nav-edge.smart
 3823 13:33:08.835051 10.182.140.239  10.247.0.3      DNS         86 Standard query 0x72db A stackpath.bootstrapcdn.
```

```
> Frame 3749: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 10.247.0.3
v User Datagram Protocol, Src Port: 53269, Dst Port: 53
    Source Port: 53269
    Destination Port: 53
    Length: 43
    Checksum: 0xa2db [unverified]
```

2. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?

→ The packet number for the DNS response message is 3750

→ Response message was sent via UDP - User datagram Protocol.



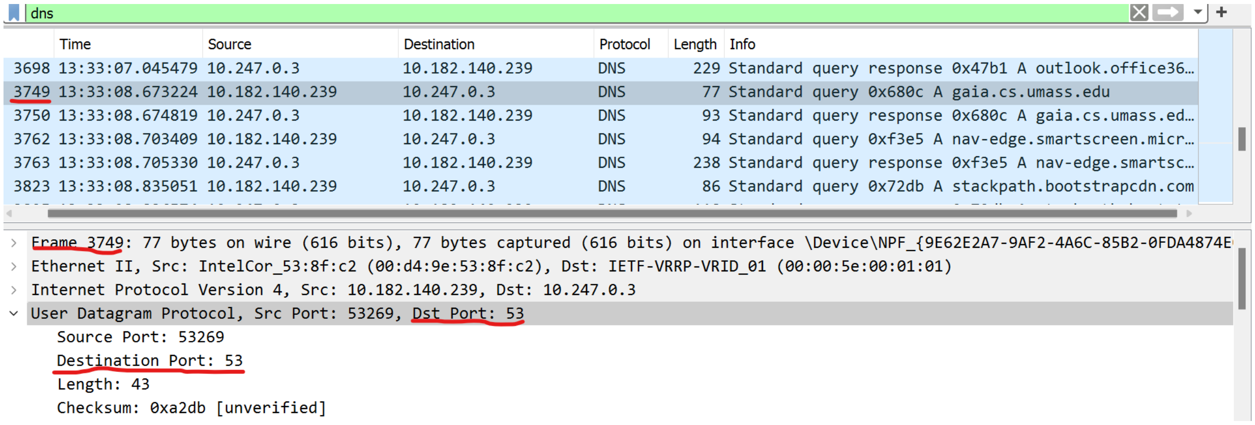
```
      Time             Source          Destination     Protocol  Length  Info
 3698 13:33:07.045479 10.247.0.3      10.182.140.239  DNS        229 Standard query response 0x47b1 A outlook.office36…
 3749 13:33:08.673224 10.182.140.239  10.247.0.3      DNS         77 Standard query 0x680c A gaia.cs.umass.edu
 3750 13:33:08.674819 10.247.0.3      10.182.140.239  DNS         93 Standard query response 0x680c A gaia.cs.umass.ed…
 3762 13:33:08.703409 10.182.140.239  10.247.0.3      DNS         94 Standard query 0xf3e5 A nav-edge.smartscreen.micr…
 3763 13:33:08.705330 10.247.0.3      10.182.140.239  DNS        238 Standard query response 0xf3e5 A nav-edge.smartsc…
 3823 13:33:08.835051 10.182.140.239  10.247.0.3      DNS         86 Standard query 0x72db A stackpath.bootstrapcdn.com
```

```
> Frame 3750: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E
> Ethernet II, Src: JuniperN_27:f3:f0 (d4:04:ff:27:f3:f0), Dst: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2)
> Internet Protocol Version 4, Src: 10.247.0.3, Dst: 10.182.140.239
v User Datagram Protocol, Src Port: 53, Dst Port: 53269
    Source Port: 53
    Destination Port: 53269
    Length: 59
    Checksum: 0xee39 [unverified]
```

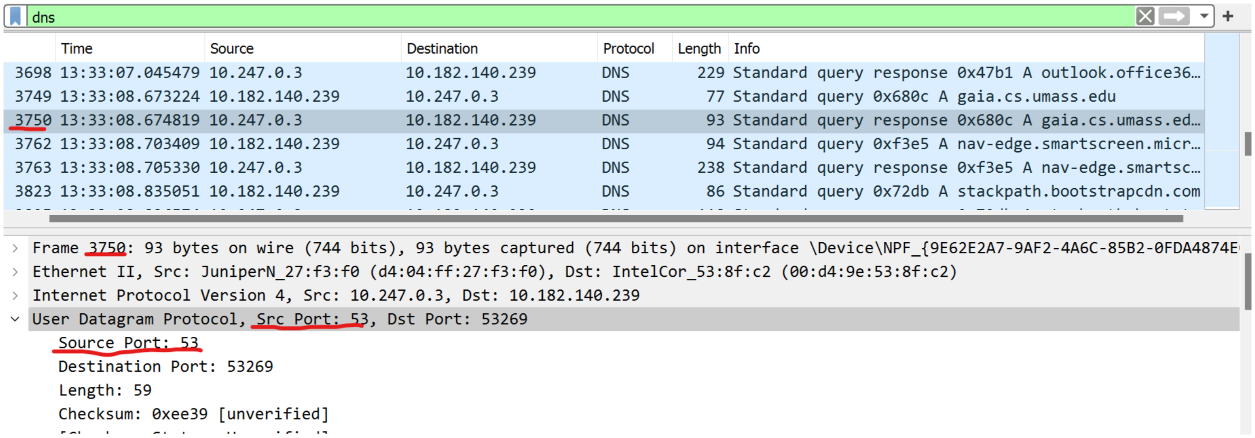
3. What is the destination port for the DNS query message? What is the source port of the DNS response message?

→ The destination port for the DNS query message is 53.

→ The source port of the DNS response message is 53.



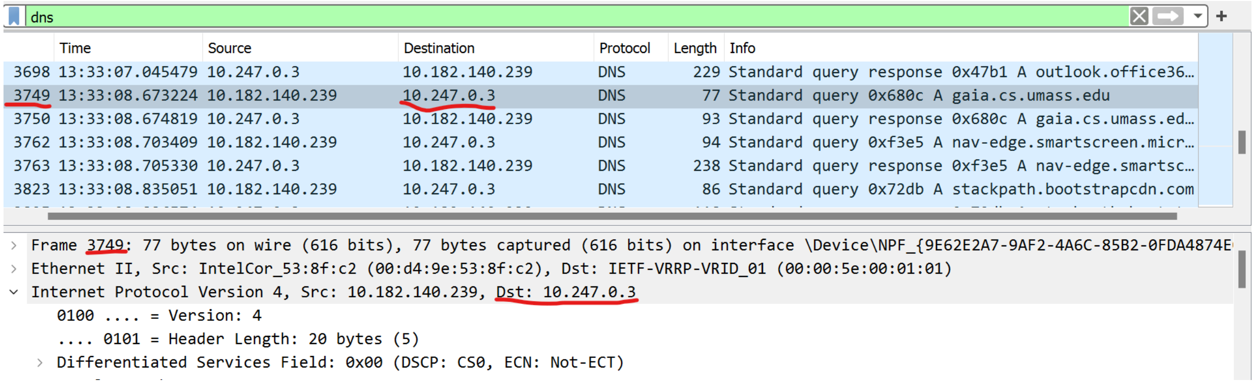
```
dns
     Time            Source          Destination     Protocol Length Info
3698 13:33:07.045479 10.247.0.3      10.182.140.239  DNS      229 Standard query response 0x47b1 A outlook.office36…
3749 13:33:08.673224 10.182.140.239  10.247.0.3      DNS       77 Standard query 0x680c A gaia.cs.umass.edu
3750 13:33:08.674819 10.247.0.3      10.182.140.239  DNS       93 Standard query response 0x680c A gaia.cs.umass.ed…
3762 13:33:08.703409 10.182.140.239  10.247.0.3      DNS       94 Standard query 0xf3e5 A nav-edge.smartscreen.micr…
3763 13:33:08.705330 10.247.0.3      10.182.140.239  DNS      238 Standard query response 0xf3e5 A nav-edge.smartsc…
3823 13:33:08.835051 10.182.140.239  10.247.0.3      DNS       86 Standard query 0x72db A stackpath.bootstrapcdn.com

> Frame 3749: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 10.247.0.3
v User Datagram Protocol, Src Port: 53269, Dst Port: 53
    Source Port: 53269
    Destination Port: 53
    Length: 43
    Checksum: 0xa2db [unverified]
```



```
dns
     Time            Source          Destination     Protocol Length Info
3698 13:33:07.045479 10.247.0.3      10.182.140.239  DNS      229 Standard query response 0x47b1 A outlook.office36…
3749 13:33:08.673224 10.182.140.239  10.247.0.3      DNS       77 Standard query 0x680c A gaia.cs.umass.edu
3750 13:33:08.674819 10.247.0.3      10.182.140.239  DNS       93 Standard query response 0x680c A gaia.cs.umass.ed…
3762 13:33:08.703409 10.182.140.239  10.247.0.3      DNS       94 Standard query 0xf3e5 A nav-edge.smartscreen.micr…
3763 13:33:08.705330 10.247.0.3      10.182.140.239  DNS      238 Standard query response 0xf3e5 A nav-edge.smartsc…
3823 13:33:08.835051 10.182.140.239  10.247.0.3      DNS       86 Standard query 0x72db A stackpath.bootstrapcdn.com

> Frame 3750: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E
> Ethernet II, Src: JuniperN_27:f3:f0 (d4:04:ff:27:f3:f0), Dst: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2)
> Internet Protocol Version 4, Src: 10.247.0.3, Dst: 10.182.140.239
v User Datagram Protocol, Src Port: 53, Dst Port: 53269
    Source Port: 53
    Destination Port: 53269
    Length: 59
    Checksum: 0xee39 [unverified]
```

4. To what IP address is the DNS query message sent?

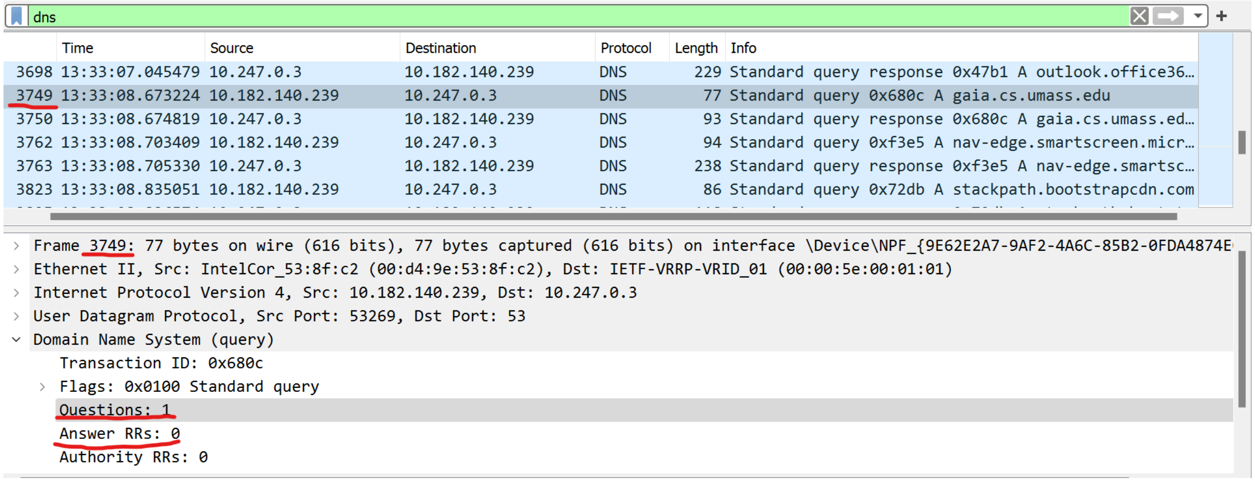
→ The destination IP address of the DNS query message is 10.247.0.3



```
dns
     Time            Source          Destination     Protocol Length Info
3698 13:33:07.045479 10.247.0.3      10.182.140.239  DNS      229 Standard query response 0x47b1 A outlook.office36…
3749 13:33:08.673224 10.182.140.239  10.247.0.3      DNS       77 Standard query 0x680c A gaia.cs.umass.edu
3750 13:33:08.674819 10.247.0.3      10.182.140.239  DNS       93 Standard query response 0x680c A gaia.cs.umass.ed…
3762 13:33:08.703409 10.182.140.239  10.247.0.3      DNS       94 Standard query 0xf3e5 A nav-edge.smartscreen.micr…
3763 13:33:08.705330 10.247.0.3      10.182.140.239  DNS      238 Standard query response 0xf3e5 A nav-edge.smartsc…
3823 13:33:08.835051 10.182.140.239  10.247.0.3      DNS       86 Standard query 0x72db A stackpath.bootstrapcdn.com

> Frame 3749: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
v Internet Protocol Version 4, Src: 10.182.140.239, Dst: 10.247.0.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

5. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

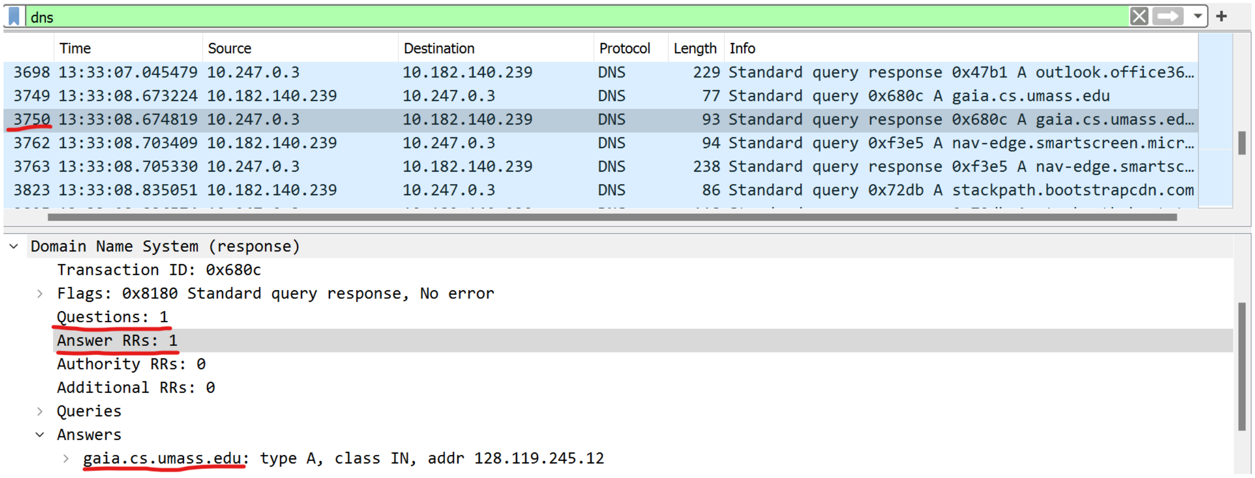
→ DNS query message contains 1 Questions and 0 Answer RRs.



```
dns
No.  Time            Source          Destination     Protocol Length Info
3698 13:33:07.045479 10.247.0.3      10.182.140.239  DNS      229 Standard query response 0x47b1 A outlook.office36…
3749 13:33:08.673224 10.182.140.239  10.247.0.3      DNS       77 Standard query 0x680c A gaia.cs.umass.edu
3750 13:33:08.674819 10.247.0.3      10.182.140.239  DNS       93 Standard query response 0x680c A gaia.cs.umass.ed…
3762 13:33:08.703409 10.182.140.239  10.247.0.3      DNS       94 Standard query 0xf3e5 A nav-edge.smartscreen.micr…
3763 13:33:08.705330 10.247.0.3      10.182.140.239  DNS      238 Standard query response 0xf3e5 A nav-edge.smartsc…
3823 13:33:08.835051 10.182.140.239  10.247.0.3      DNS       86 Standard query 0x72db A stackpath.bootstrapcdn.com

> Frame 3749: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 10.247.0.3
> User Datagram Protocol, Src Port: 53269, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x680c
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

6. Examine the DNS response message to the initial query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

   → The DNS response message has 1 Questions and 1 Answer RRs.

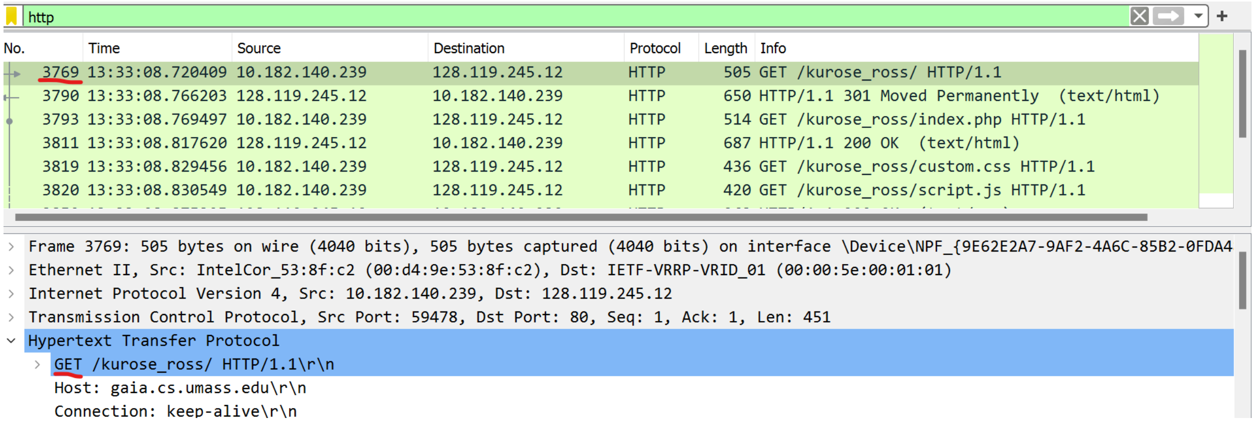


```
dns
No.  Time            Source          Destination     Protocol Length Info
3698 13:33:07.045479 10.247.0.3      10.182.140.239  DNS      229 Standard query response 0x47b1 A outlook.office36…
3749 13:33:08.673224 10.182.140.239  10.247.0.3      DNS       77 Standard query 0x680c A gaia.cs.umass.edu
3750 13:33:08.674819 10.247.0.3      10.182.140.239  DNS       93 Standard query response 0x680c A gaia.cs.umass.ed…
3762 13:33:08.703409 10.182.140.239  10.247.0.3      DNS       94 Standard query 0xf3e5 A nav-edge.smartscreen.micr…
3763 13:33:08.705330 10.247.0.3      10.182.140.239  DNS      238 Standard query response 0xf3e5 A nav-edge.smartsc…
3823 13:33:08.835051 10.182.140.239  10.247.0.3      DNS       86 Standard query 0x72db A stackpath.bootstrapcdn.com

v Domain Name System (response)
    Transaction ID: 0x680c
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > gaia.cs.umass.edu: type A, class IN, addr 128.119.245.12
```

7. The web page for the base file http://gaia.cs.umass.edu/kurose_ross/ references the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg , which, like the base webpage, is on gaia.cs.umass.edu.

   What is the packet number in the trace for the initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose_ross/?

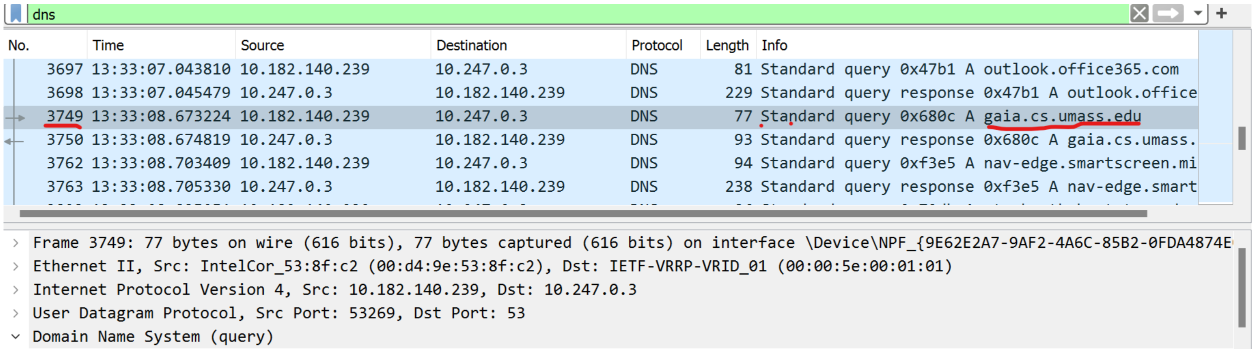
   → The Packet number for initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose_ross/ is 3769



```
http
No.   Time            Source          Destination     Protocol Length Info
3769 13:33:08.720409 10.182.140.239 128.119.245.12  HTTP     505 GET /kurose_ross/ HTTP/1.1
3790 13:33:08.766203 128.119.245.12 10.182.140.239  HTTP     650 HTTP/1.1 301 Moved Permanently  (text/html)
3793 13:33:08.769497 10.182.140.239 128.119.245.12  HTTP     514 GET /kurose_ross/index.php HTTP/1.1
3811 13:33:08.817620 128.119.245.12 10.182.140.239  HTTP     687 HTTP/1.1 200 OK  (text/html)
3819 13:33:08.829456 10.182.140.239 128.119.245.12  HTTP     436 GET /kurose_ross/custom.css HTTP/1.1
3820 13:33:08.830549 10.182.140.239 128.119.245.12  HTTP     420 GET /kurose_ross/script.js HTTP/1.1

> Frame 3769: 505 bytes on wire (4040 bits), 505 bytes captured (4040 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59478, Dst Port: 80, Seq: 1, Ack: 1, Len: 451
v Hypertext Transfer Protocol
  > GET /kurose_ross/ HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
```

What is the packet number in the trace of the DNS query made to resolve gaia.cs.umass.edu so that this initial HTTP request can be sent to the gaia.cs.umass.edu IP address?

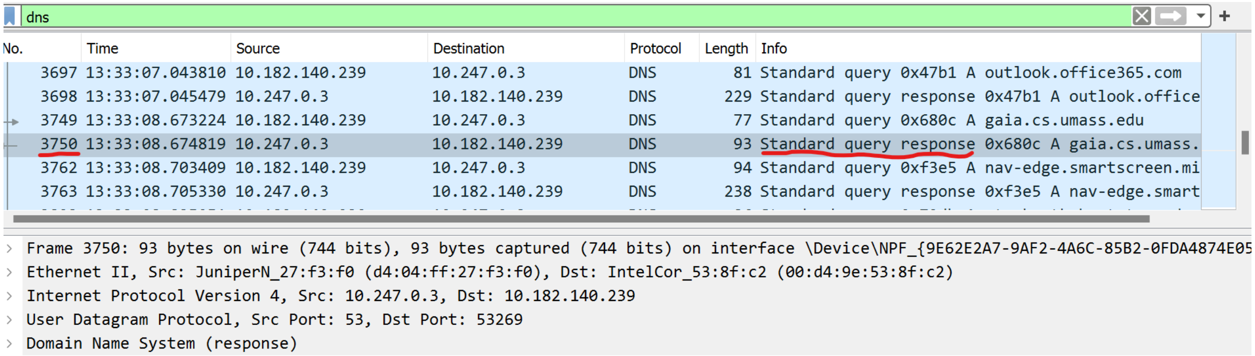
→ The packet number of the DNS query made to resolve gaia.cs.umass.edu is 3749.



```
dns
No.   Time            Source          Destination     Protocol Length Info
3697 13:33:07.043810 10.182.140.239 10.247.0.3      DNS       81 Standard query 0x47b1 A outlook.office365.com
3698 13:33:07.045479 10.247.0.3     10.182.140.239  DNS      229 Standard query response 0x47b1 A outlook.office
3749 13:33:08.673224 10.182.140.239 10.247.0.3      DNS       77 Standard query 0x680c A gaia.cs.umass.edu
3750 13:33:08.674819 10.247.0.3     10.182.140.239  DNS       93 Standard query response 0x680c A gaia.cs.umass.
3762 13:33:08.703409 10.182.140.239 10.247.0.3      DNS       94 Standard query 0xf3e5 A nav-edge.smartscreen.mi
3763 13:33:08.705330 10.247.0.3     10.182.140.239  DNS      238 Standard query response 0xf3e5 A nav-edge.smart

> Frame 3749: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 10.247.0.3
> User Datagram Protocol, Src Port: 53269, Dst Port: 53
v Domain Name System (query)
```

What is the packet number in the trace of the received DNS response?

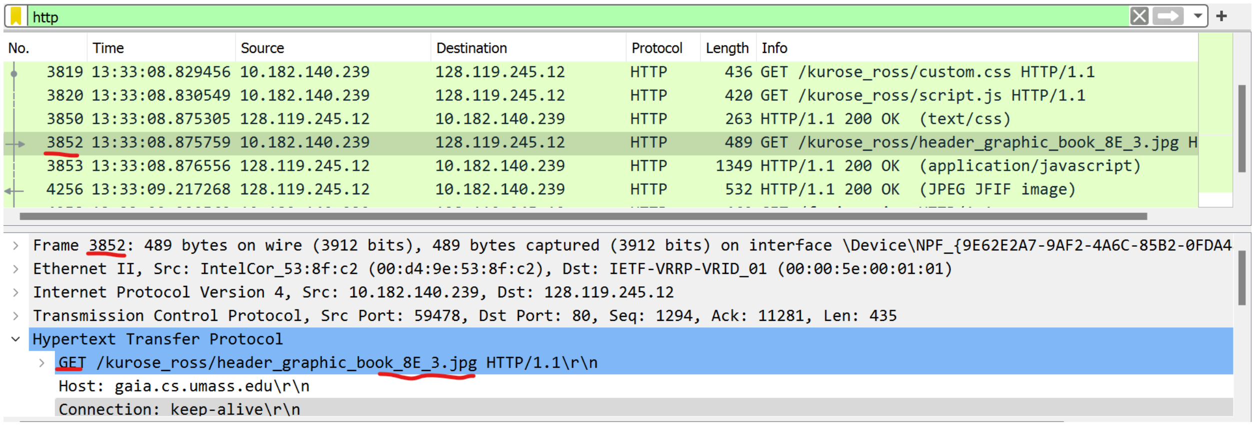
→ The packet number of the DNS response is 3750.



```
dns
No.   Time            Source          Destination     Protocol Length Info
3697 13:33:07.043810 10.182.140.239 10.247.0.3      DNS       81 Standard query 0x47b1 A outlook.office365.com
3698 13:33:07.045479 10.247.0.3     10.182.140.239  DNS      229 Standard query response 0x47b1 A outlook.office
3749 13:33:08.673224 10.182.140.239 10.247.0.3      DNS       77 Standard query 0x680c A gaia.cs.umass.edu
3750 13:33:08.674819 10.247.0.3     10.182.140.239  DNS       93 Standard query response 0x680c A gaia.cs.umass.
3762 13:33:08.703409 10.182.140.239 10.247.0.3      DNS       94 Standard query 0xf3e5 A nav-edge.smartscreen.mi
3763 13:33:08.705330 10.247.0.3     10.182.140.239  DNS      238 Standard query response 0xf3e5 A nav-edge.smart

> Frame 3750: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E05
> Ethernet II, Src: JuniperN_27:f3:f0 (d4:04:ff:27:f3:f0), Dst: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2)
> Internet Protocol Version 4, Src: 10.247.0.3, Dst: 10.182.140.239
> User Datagram Protocol, Src Port: 53, Dst Port: 53269
> Domain Name System (response)
```

What is the packet number in the trace for the HTTP GET request for the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg?

→ The packet number for the HTTP GET Request for the image object is 3852.

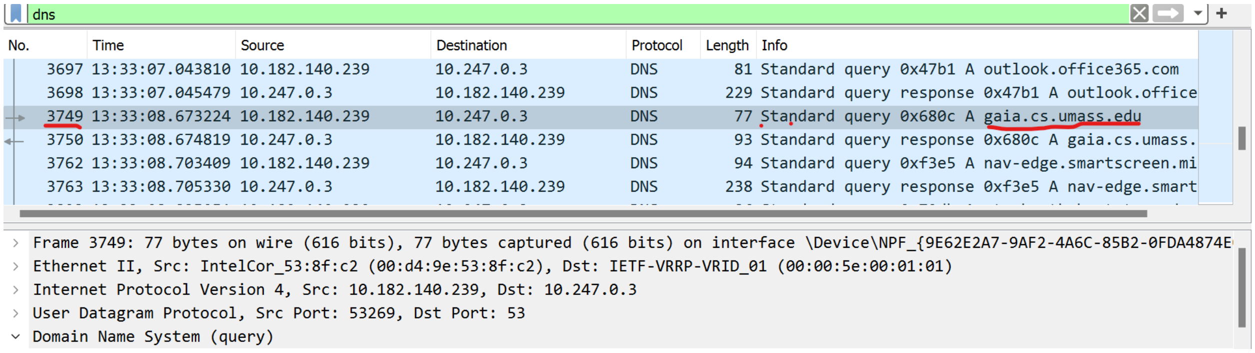


```
http
No.   Time            Source          Destination     Protocol  Length  Info
3819 13:33:08.829456 10.182.140.239  128.119.245.12  HTTP       436 GET /kurose_ross/custom.css HTTP/1.1
3820 13:33:08.830549 10.182.140.239  128.119.245.12  HTTP       420 GET /kurose_ross/script.js HTTP/1.1
3850 13:33:08.875305 128.119.245.12  10.182.140.239  HTTP       263 HTTP/1.1 200 OK  (text/css)
3852 13:33:08.875759 10.182.140.239  128.119.245.12  HTTP       489 GET /kurose_ross/header_graphic_book_8E_3.jpg H
3853 13:33:08.876556 128.119.245.12  10.182.140.239  HTTP      1349 HTTP/1.1 200 OK  (application/javascript)
4256 13:33:09.217268 128.119.245.12  10.182.140.239  HTTP       532 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
> Frame 3852: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59478, Dst Port: 80, Seq: 1294, Ack: 11281, Len: 435
v Hypertext Transfer Protocol
  > GET /kurose_ross/header_graphic_book_8E_3.jpg HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
```

What is the packet number in the DNS query made to resolve gaia.cs.umass.edu so that this second HTTP request can be sent to the gaia.cs.umass.edu IP address? Discuss how DNS caching affects the answer to this last question.

→ The packet number of the DNS query made to resolve gaia.cs.umass.edu is 3749.



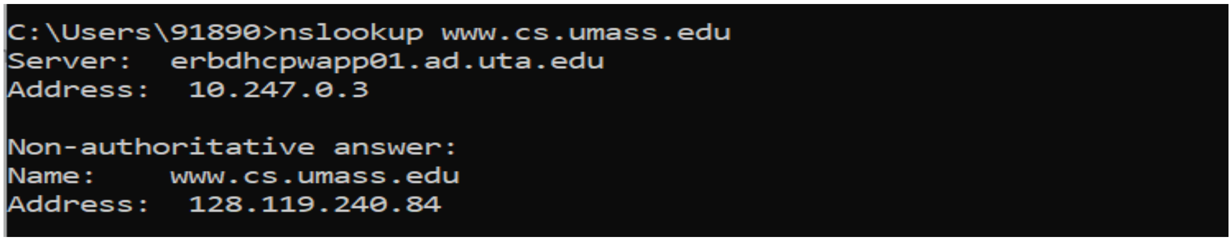
```
dns
No.   Time            Source          Destination     Protocol  Length  Info
3697 13:33:07.043810 10.182.140.239  10.247.0.3      DNS         81 Standard query 0x47b1 A outlook.office365.com
3698 13:33:07.045479 10.247.0.3      10.182.140.239  DNS        229 Standard query response 0x47b1 A outlook.office
3749 13:33:08.673224 10.182.140.239  10.247.0.3      DNS         77 Standard query 0x680c A gaia.cs.umass.edu
3750 13:33:08.674819 10.247.0.3      10.182.140.239  DNS         93 Standard query response 0x680c A gaia.cs.umass.
3762 13:33:08.703409 10.182.140.239  10.247.0.3      DNS         94 Standard query 0xf3e5 A nav-edge.smartscreen.mi
3763 13:33:08.705330 10.247.0.3      10.182.140.239  DNS        238 Standard query response 0xf3e5 A nav-edge.smart
```

```
> Frame 3749: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 10.247.0.3
> User Datagram Protocol, Src Port: 53269, Dst Port: 53
v Domain Name System (query)
```

As soon as we get the IP address of the gaia.cs.umass.edu, the local DNS server caches it, hence when a subsequent HTTP request for the same destination is made, the response to the requested host will be faster because we have already resolved the gaia.cs.umass.edu IP address, which was cached in local DNS server.

Nslookup execution:

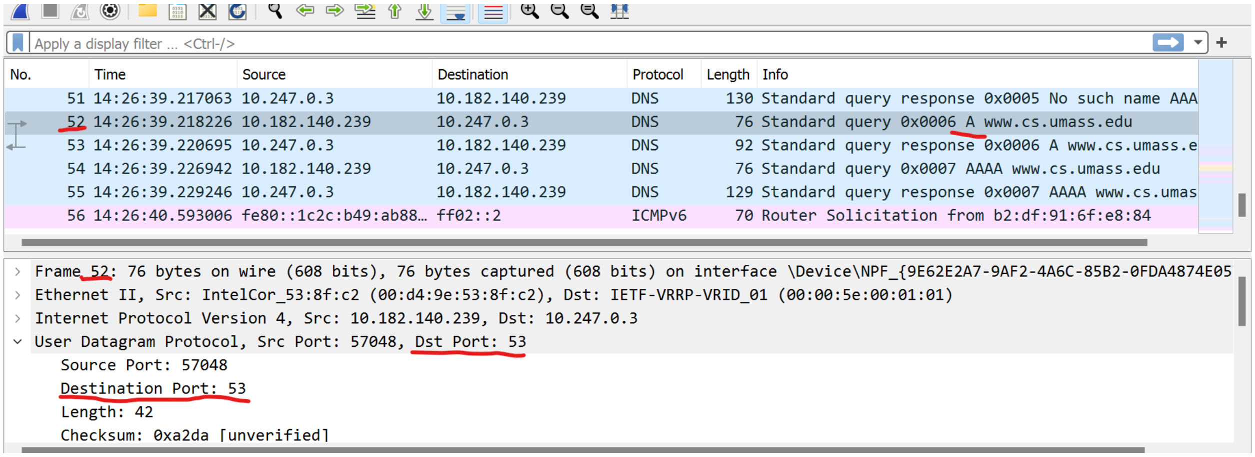
Command : nslookup www.cs.umass.edu



```
C:\Users\91890>nslookup www.cs.umass.edu
Server:   erbdhcpwapp01.ad.uta.edu
Address:   10.247.0.3

Non-authoritative answer:
Name:     www.cs.umass.edu
Address:   128.119.240.84
```

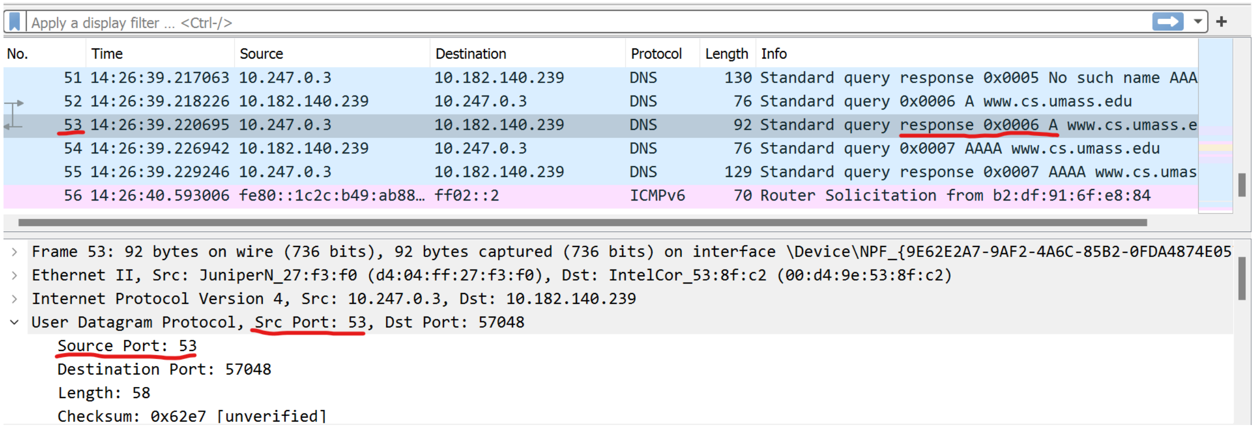
1. What is the destination port for the DNS query message? What is the source port of the DNS response message?

   → The destination port for the DNS query message is 53.



```
Apply a display filter ... <Ctrl-/>

No.  Time             Source                 Destination      Protocol  Length Info
  51 14:26:39.217063 10.247.0.3             10.182.140.239   DNS          130 Standard query response 0x0005 No such name AAA
  52 14:26:39.218226 10.182.140.239         10.247.0.3       DNS           76 Standard query 0x0006 A www.cs.umass.edu
  53 14:26:39.220695 10.247.0.3             10.182.140.239   DNS           92 Standard query response 0x0006 A www.cs.umass.e
  54 14:26:39.226942 10.182.140.239         10.247.0.3       DNS           76 Standard query 0x0007 AAAA www.cs.umass.edu
  55 14:26:39.229246 10.247.0.3             10.182.140.239   DNS          129 Standard query response 0x0007 AAAA www.cs.umas
  56 14:26:40.593006 fe80::1c2c:b49:ab88… ff02::2          ICMPv6        70 Router Solicitation from b2:df:91:6f:e8:84

> Frame 52: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E05
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 10.247.0.3
v User Datagram Protocol, Src Port: 57048, Dst Port: 53
    Source Port: 57048
    Destination Port: 53
    Length: 42
    Checksum: 0xa2da [unverified]
```

   → The Source port of the DNS response message is 53.

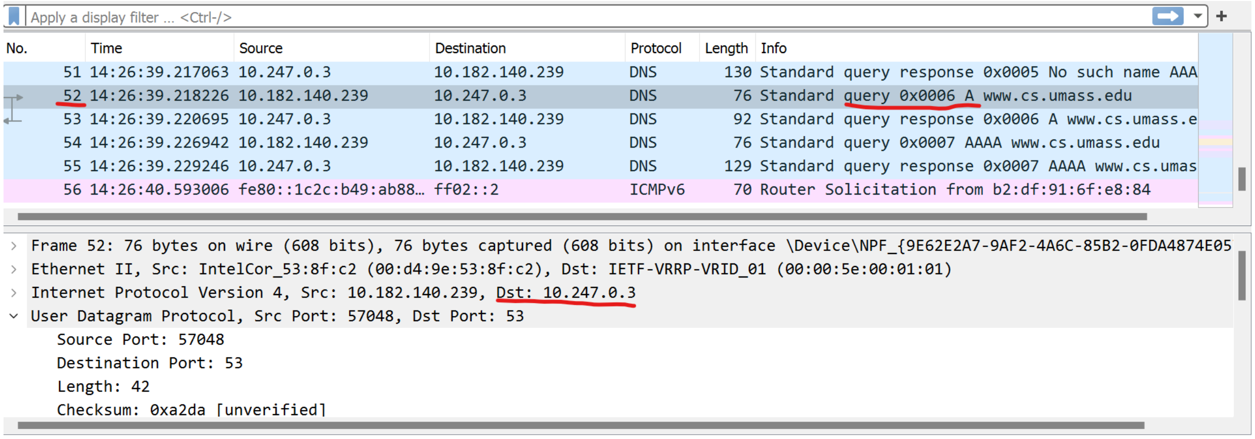


```
Apply a display filter ... <Ctrl-/>

No.  Time             Source                 Destination      Protocol  Length Info
  51 14:26:39.217063 10.247.0.3             10.182.140.239   DNS          130 Standard query response 0x0005 No such name AAA
  52 14:26:39.218226 10.182.140.239         10.247.0.3       DNS           76 Standard query 0x0006 A www.cs.umass.edu
  53 14:26:39.220695 10.247.0.3             10.182.140.239   DNS           92 Standard query response 0x0006 A www.cs.umass.e
  54 14:26:39.226942 10.182.140.239         10.247.0.3       DNS           76 Standard query 0x0007 AAAA www.cs.umass.edu
  55 14:26:39.229246 10.247.0.3             10.182.140.239   DNS          129 Standard query response 0x0007 AAAA www.cs.umas
  56 14:26:40.593006 fe80::1c2c:b49:ab88… ff02::2          ICMPv6        70 Router Solicitation from b2:df:91:6f:e8:84

> Frame 53: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E05
> Ethernet II, Src: JuniperN_27:f3:f0 (d4:04:ff:27:f3:f0), Dst: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2)
> Internet Protocol Version 4, Src: 10.247.0.3, Dst: 10.182.140.239
v User Datagram Protocol, Src Port: 53, Dst Port: 57048
    Source Port: 53
    Destination Port: 57048
    Length: 58
    Checksum: 0x62e7 [unverified]
```

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

   → 10.247.0.3 is the IP address for which the DNS query message was sent.

   → Yes, it is the default local DNS server.

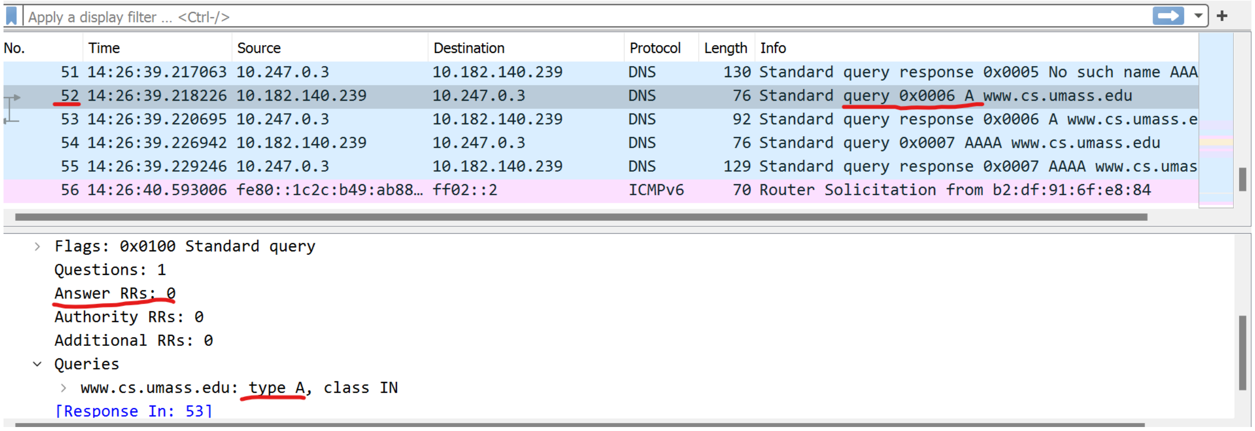


```
No.   Time             Source                 Destination     Protocol  Length  Info
   51 14:26:39.217063 10.247.0.3             10.182.140.239  DNS          130 Standard query response 0x0005 No such name AAA
   52 14:26:39.218226 10.182.140.239         10.247.0.3      DNS           76 Standard query 0x0006 A www.cs.umass.edu
   53 14:26:39.220695 10.247.0.3             10.182.140.239  DNS           92 Standard query response 0x0006 A www.cs.umass.e
   54 14:26:39.226942 10.182.140.239         10.247.0.3      DNS           76 Standard query 0x0007 AAAA www.cs.umass.edu
   55 14:26:39.229246 10.247.0.3             10.182.140.239  DNS          129 Standard query response 0x0007 AAAA www.cs.umas
   56 14:26:40.593006 fe80::1c2c:b49:ab88…   ff02::2         ICMPv6        70 Router Solicitation from b2:df:91:6f:e8:84
```

```
> Frame 52: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E05
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 10.247.0.3
v User Datagram Protocol, Src Port: 57048, Dst Port: 53
    Source Port: 57048
    Destination Port: 53
    Length: 42
    Checksum: 0xa2da [unverified]
```

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

→ The Type of DNS query message is A. There are No Answer RRs in this DNS query message.

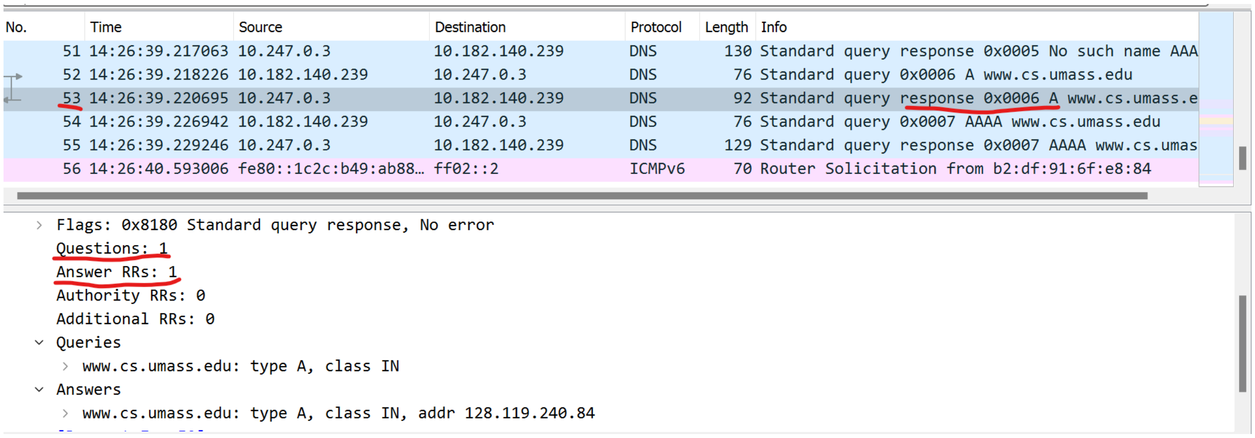


```
No.   Time             Source                 Destination     Protocol  Length  Info
   51 14:26:39.217063 10.247.0.3             10.182.140.239  DNS          130 Standard query response 0x0005 No such name AAA
   52 14:26:39.218226 10.182.140.239         10.247.0.3      DNS           76 Standard query 0x0006 A www.cs.umass.edu
   53 14:26:39.220695 10.247.0.3             10.182.140.239  DNS           92 Standard query response 0x0006 A www.cs.umass.e
   54 14:26:39.226942 10.182.140.239         10.247.0.3      DNS           76 Standard query 0x0007 AAAA www.cs.umass.edu
   55 14:26:39.229246 10.247.0.3             10.182.140.239  DNS          129 Standard query response 0x0007 AAAA www.cs.umas
   56 14:26:40.593006 fe80::1c2c:b49:ab88…   ff02::2         ICMPv6        70 Router Solicitation from b2:df:91:6f:e8:84
```

```
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.cs.umass.edu: type A, class IN
    [Response In: 53]
```

4. Examine the DNS response message to the query message. How many "questions" does this DNS response message contain? How many "answers"?

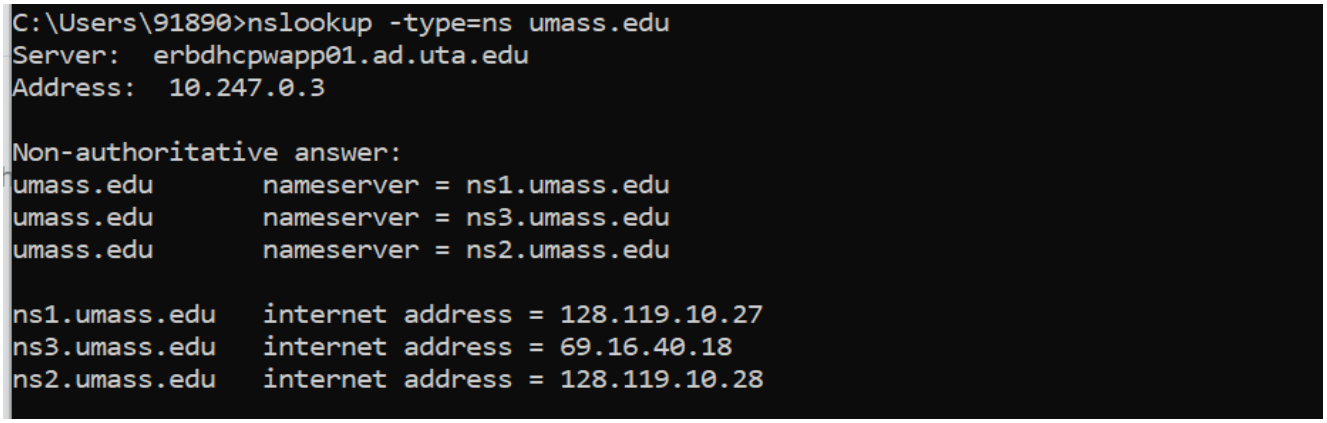
→ The DNS response message has 1 Questions and 1 Answers.



```
No.  Time             Source              Destination     Protocol  Length Info
  51 14:26:39.217063 10.247.0.3          10.182.140.239  DNS          130 Standard query response 0x0005 No such name AAA
  52 14:26:39.218226 10.182.140.239      10.247.0.3      DNS           76 Standard query 0x0006 A www.cs.umass.edu
  53 14:26:39.220695 10.247.0.3          10.182.140.239  DNS           92 Standard query response 0x0006 A www.cs.umass.e
  54 14:26:39.226942 10.182.140.239      10.247.0.3      DNS           76 Standard query 0x0007 AAAA www.cs.umass.edu
  55 14:26:39.229246 10.247.0.3          10.182.140.239  DNS          129 Standard query response 0x0007 AAAA www.cs.umas
  56 14:26:40.593006 fe80::1c2c:b49:ab88… ff02::2        ICMPv6        70 Router Solicitation from b2:df:91:6f:e8:84
```

```
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
      > www.cs.umass.edu: type A, class IN
  v Answers
      > www.cs.umass.edu: type A, class IN, addr 128.119.240.84
```

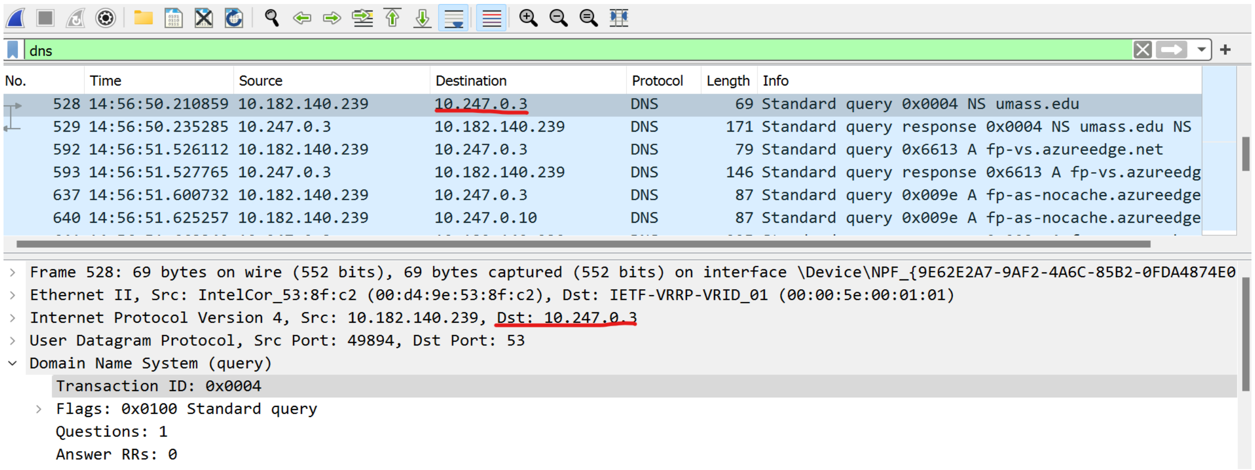
Command : nslookup -type=ns umass.edu



```
C:\Users\91890>nslookup -type=ns umass.edu
Server:  erbdhcpwapp01.ad.uta.edu
Address:  10.247.0.3

Non-authoritative answer:
umass.edu       nameserver = ns1.umass.edu
umass.edu       nameserver = ns3.umass.edu
umass.edu       nameserver = ns2.umass.edu

ns1.umass.edu   internet address = 128.119.10.27
ns3.umass.edu   internet address = 69.16.40.18
ns2.umass.edu   internet address = 128.119.10.28
```

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

   → The IP address for the DNS query message sent is 10.247.0.3. Yes it is my default local DNS server.



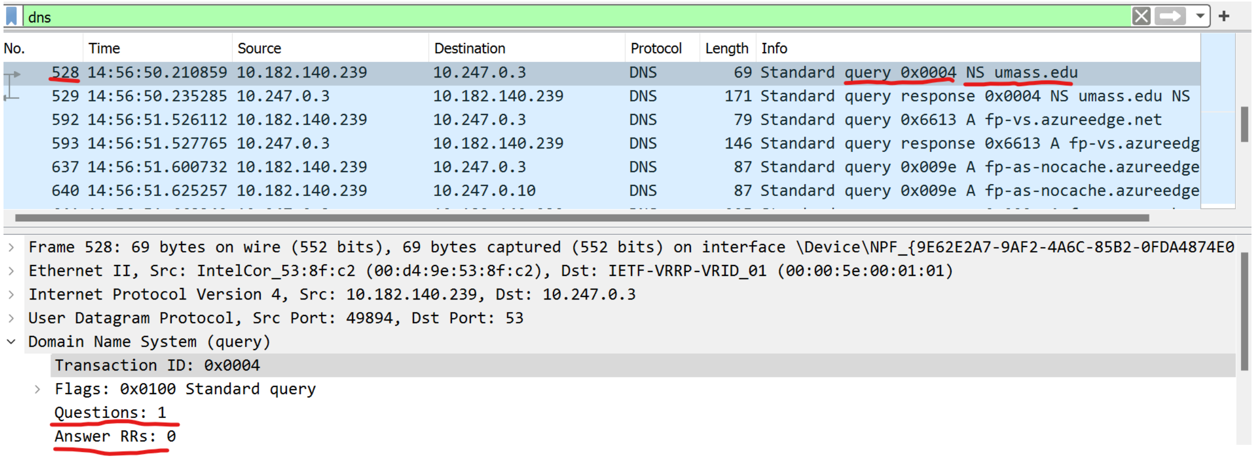
```
dns
```

```
No.  Time             Source          Destination     Protocol  Length Info
 528 14:56:50.210859 10.182.140.239  10.247.0.3      DNS           69 Standard query 0x0004 NS umass.edu
 529 14:56:50.235285 10.247.0.3      10.182.140.239  DNS          171 Standard query response 0x0004 NS umass.edu NS
 592 14:56:51.526112 10.182.140.239  10.247.0.3      DNS           79 Standard query 0x6613 A fp-vs.azureedge.net
 593 14:56:51.527765 10.247.0.3      10.182.140.239  DNS          146 Standard query response 0x6613 A fp-vs.azureedg
 637 14:56:51.600732 10.182.140.239  10.247.0.3      DNS           87 Standard query 0x009e A fp-as-nocache.azureedge
 640 14:56:51.625257 10.182.140.239  10.247.0.10     DNS           87 Standard query 0x009e A fp-as-nocache.azureedge
```

```
> Frame 528: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E0
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 10.247.0.3
> User Datagram Protocol, Src Port: 49894, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
```

2. Examine the DNS query message. How many questions does the query have? Does the query message contain any “answers”?

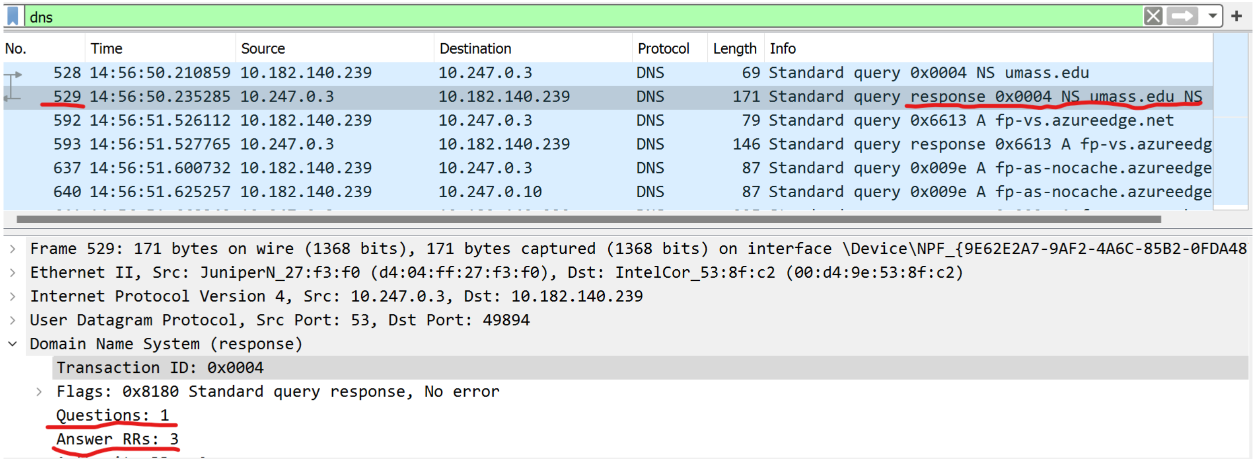
→ The DNS query message has 1 Questions and 0 Answer RRs



```
dns
No.   Time             Source          Destination     Protocol  Length  Info
  528 14:56:50.210859  10.182.140.239  10.247.0.3      DNS           69  Standard query 0x0004 NS umass.edu
  529 14:56:50.235285  10.247.0.3      10.182.140.239  DNS          171  Standard query response 0x0004 NS umass.edu NS
  592 14:56:51.526112  10.182.140.239  10.247.0.3      DNS           79  Standard query 0x6613 A fp-vs.azureedge.net
  593 14:56:51.527765  10.247.0.3      10.182.140.239  DNS          146  Standard query response 0x6613 A fp-vs.azureedg
  637 14:56:51.600732  10.182.140.239  10.247.0.3      DNS           87  Standard query 0x009e A fp-as-nocache.azureedge
  640 14:56:51.625257  10.182.140.239  10.247.0.10     DNS           87  Standard query 0x009e A fp-as-nocache.azureedge

> Frame 528: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E0
> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.140.239, Dst: 10.247.0.3
> User Datagram Protocol, Src Port: 49894, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
```

3. Examine the DNS response message. How many answers does the response have? What information is contained in the answers? How many additional resource records are returned? What additional information is included in these additional resource records?

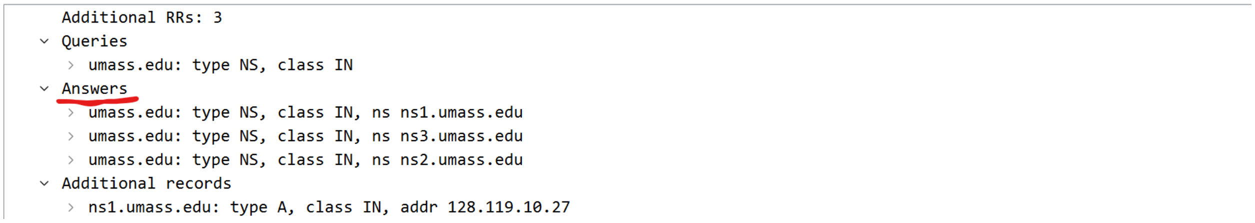
→ This Response message has 3 Answer RRs



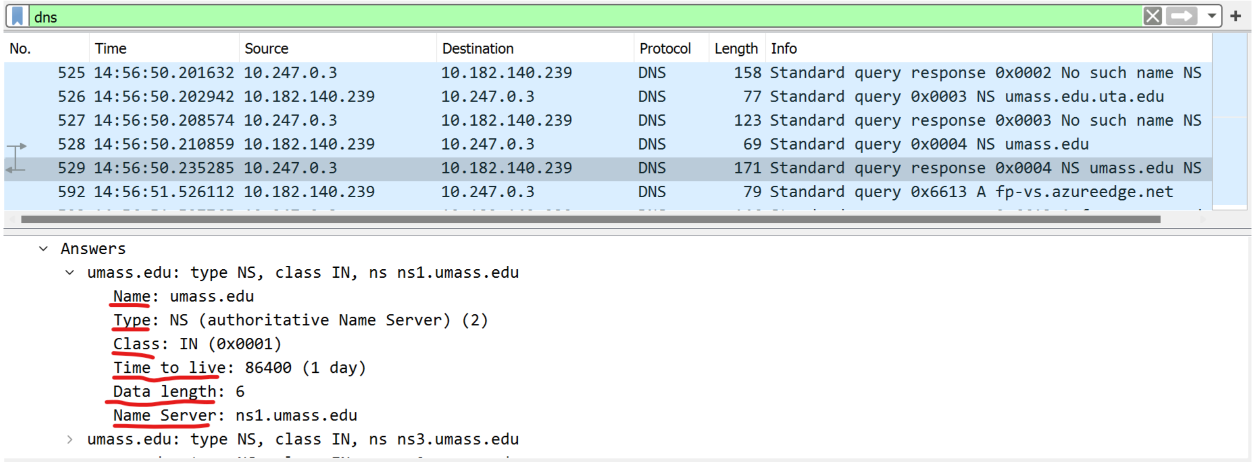
```
dns
No.   Time             Source          Destination     Protocol  Length  Info
  528 14:56:50.210859  10.182.140.239  10.247.0.3      DNS           69  Standard query 0x0004 NS umass.edu
  529 14:56:50.235285  10.247.0.3      10.182.140.239  DNS          171  Standard query response 0x0004 NS umass.edu NS
  592 14:56:51.526112  10.182.140.239  10.247.0.3      DNS           79  Standard query 0x6613 A fp-vs.azureedge.net
  593 14:56:51.527765  10.247.0.3      10.182.140.239  DNS          146  Standard query response 0x6613 A fp-vs.azureedg
  637 14:56:51.600732  10.182.140.239  10.247.0.3      DNS           87  Standard query 0x009e A fp-as-nocache.azureedge
  640 14:56:51.625257  10.182.140.239  10.247.0.10     DNS           87  Standard query 0x009e A fp-as-nocache.azureedge

> Frame 529: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA48
> Ethernet II, Src: JuniperN_27:f3:f0 (d4:04:ff:27:f3:f0), Dst: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2)
> Internet Protocol Version 4, Src: 10.247.0.3, Dst: 10.182.140.239
> User Datagram Protocol, Src Port: 53, Dst Port: 49894
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
```

→ Information in the Answers is as follows:

It gives the 3 DNS Non Authoritative servers names. Where each non authoritative server contains Name,Type, Class, Time to Live, Data Length, and Name server .Screenshot attached below.

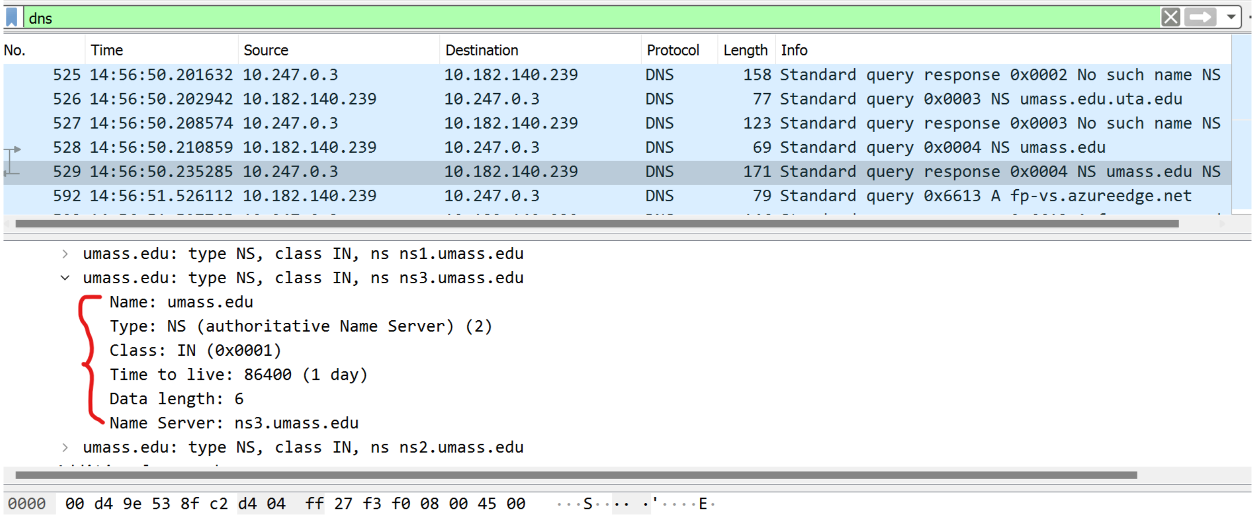


```
  Additional RRs: 3
v Queries
  > umass.edu: type NS, class IN
v Answers
  > umass.edu: type NS, class IN, ns ns1.umass.edu
  > umass.edu: type NS, class IN, ns ns3.umass.edu
  > umass.edu: type NS, class IN, ns ns2.umass.edu
v Additional records
  > ns1.umass.edu: type A, class IN, addr 128.119.10.27
```



```
No.  Time            Source          Destination     Protocol Length Info
 525 14:56:50.201632 10.247.0.3      10.182.140.239  DNS      158 Standard query response 0x0002 No such name NS
 526 14:56:50.202942 10.182.140.239  10.247.0.3      DNS       77 Standard query 0x0003 NS umass.edu.uta.edu
 527 14:56:50.208574 10.247.0.3      10.182.140.239  DNS      123 Standard query response 0x0003 No such name NS
 528 14:56:50.210859 10.182.140.239  10.247.0.3      DNS       69 Standard query 0x0004 NS umass.edu
 529 14:56:50.235285 10.247.0.3      10.182.140.239  DNS      171 Standard query response 0x0004 NS umass.edu NS
 592 14:56:51.526112 10.182.140.239  10.247.0.3      DNS       79 Standard query 0x6613 A fp-vs.azureedge.net
```

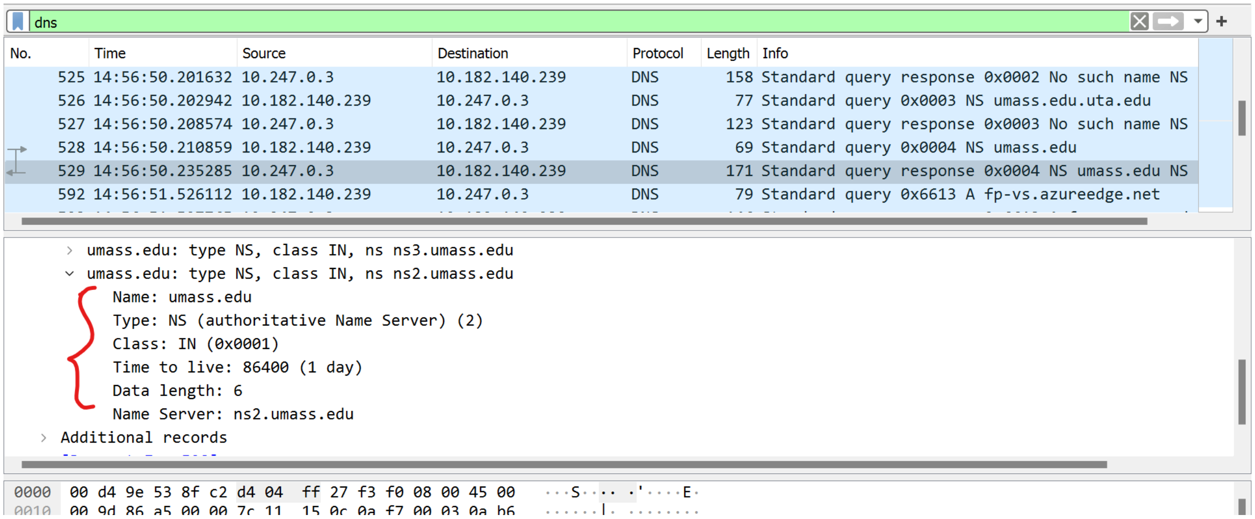
```
v Answers
  v umass.edu: type NS, class IN, ns ns1.umass.edu
      Name: umass.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 6
      Name Server: ns1.umass.edu
  > umass.edu: type NS, class IN, ns ns3.umass.edu
```



```
No.  Time            Source          Destination     Protocol Length Info
 525 14:56:50.201632 10.247.0.3      10.182.140.239  DNS      158 Standard query response 0x0002 No such name NS
 526 14:56:50.202942 10.182.140.239  10.247.0.3      DNS       77 Standard query 0x0003 NS umass.edu.uta.edu
 527 14:56:50.208574 10.247.0.3      10.182.140.239  DNS      123 Standard query response 0x0003 No such name NS
 528 14:56:50.210859 10.182.140.239  10.247.0.3      DNS       69 Standard query 0x0004 NS umass.edu
 529 14:56:50.235285 10.247.0.3      10.182.140.239  DNS      171 Standard query response 0x0004 NS umass.edu NS
 592 14:56:51.526112 10.182.140.239  10.247.0.3      DNS       79 Standard query 0x6613 A fp-vs.azureedge.net
```

```
  > umass.edu: type NS, class IN, ns ns1.umass.edu
  v umass.edu: type NS, class IN, ns ns3.umass.edu
      Name: umass.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 6
      Name Server: ns3.umass.edu
  > umass.edu: type NS, class IN, ns ns2.umass.edu
```

```
0000  00 d4 9e 53 8f c2 d4 04  ff 27 f3 f0 08 00 45 00   ···S····'····E·
```



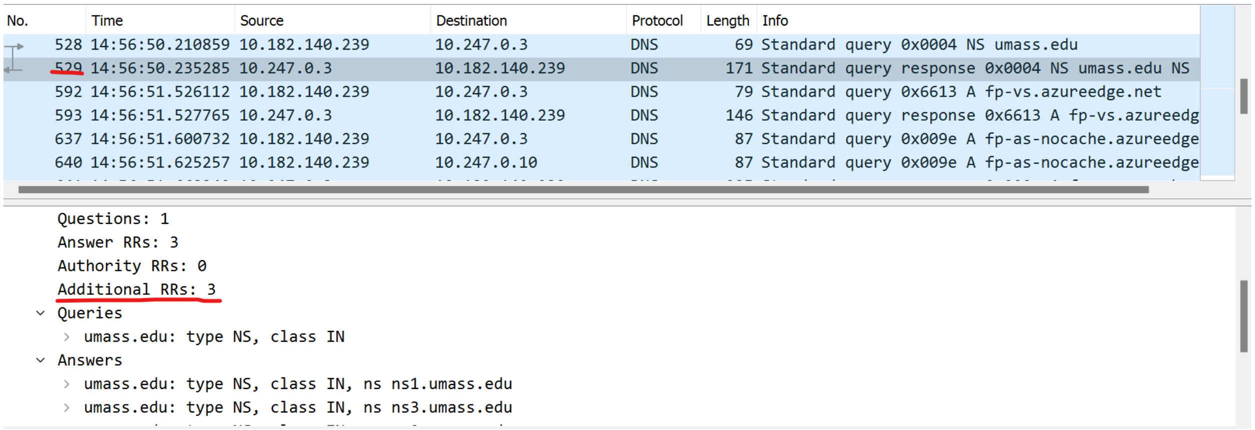
dns

No.	Time	Source	Destination	Protocol	Length	Info
525	14:56:50.201632	10.247.0.3	10.182.140.239	DNS	158	Standard query response 0x0002 No such name NS
526	14:56:50.202942	10.182.140.239	10.247.0.3	DNS	77	Standard query 0x0003 NS umass.edu.uta.edu
527	14:56:50.208574	10.247.0.3	10.182.140.239	DNS	123	Standard query response 0x0003 No such name NS
528	14:56:50.210859	10.182.140.239	10.247.0.3	DNS	69	Standard query 0x0004 NS umass.edu
529	14:56:50.235285	10.247.0.3	10.182.140.239	DNS	171	Standard query response 0x0004 NS umass.edu NS
592	14:56:51.526112	10.182.140.239	10.247.0.3	DNS	79	Standard query 0x6613 A fp-vs.azureedge.net

```
    > umass.edu: type NS, class IN, ns ns3.umass.edu
    v umass.edu: type NS, class IN, ns ns2.umass.edu
        Name: umass.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 86400 (1 day)
        Data length: 6
        Name Server: ns2.umass.edu
  > Additional records
```

```
0000  00 d4 9e 53 8f c2 d4 04  ff 27 f3 f0 08 00 45 00   ···S··· ·'····E·
0010  00 9d 86 a5 00 00 7c 11  15 0c 0a f7 00 03 0a b6   ······|· ········
```

→ 3 Additional RRs are returned

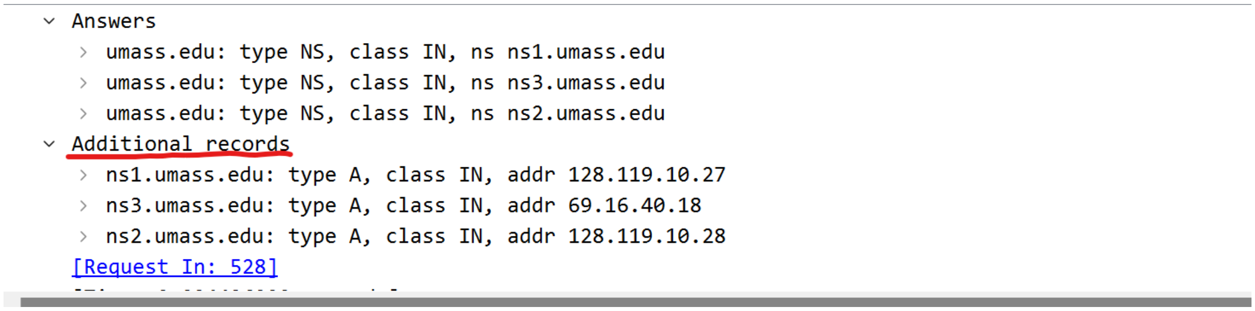


No.	Time	Source	Destination	Protocol	Length	Info
528	14:56:50.210859	10.182.140.239	10.247.0.3	DNS	69	Standard query 0x0004 NS umass.edu
529	14:56:50.235285	10.247.0.3	10.182.140.239	DNS	171	Standard query response 0x0004 NS umass.edu NS
592	14:56:51.526112	10.182.140.239	10.247.0.3	DNS	79	Standard query 0x6613 A fp-vs.azureedge.net
593	14:56:51.527765	10.247.0.3	10.182.140.239	DNS	146	Standard query response 0x6613 A fp-vs.azureedg
637	14:56:51.600732	10.182.140.239	10.247.0.3	DNS	87	Standard query 0x009e A fp-as-nocache.azureedge
640	14:56:51.625257	10.182.140.239	10.247.0.10	DNS	87	Standard query 0x009e A fp-as-nocache.azureedge

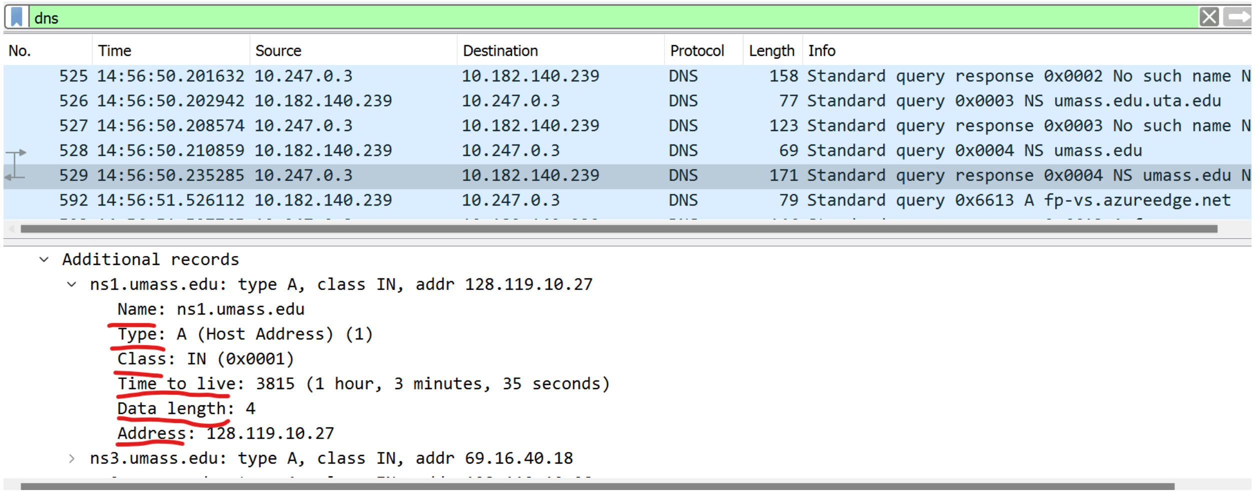
```
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 3
  v Queries
    > umass.edu: type NS, class IN
  v Answers
    > umass.edu: type NS, class IN, ns ns1.umass.edu
    > umass.edu: type NS, class IN, ns ns3.umass.edu
```

→ Information in the Additional RRs is as follows:

It contains the IP address of the 3 non authoritative DNS servers. Where each non authoritative server contains Name,Type, Class, Time to Live, Data Length, and IP address. Screenshot attached below with details.

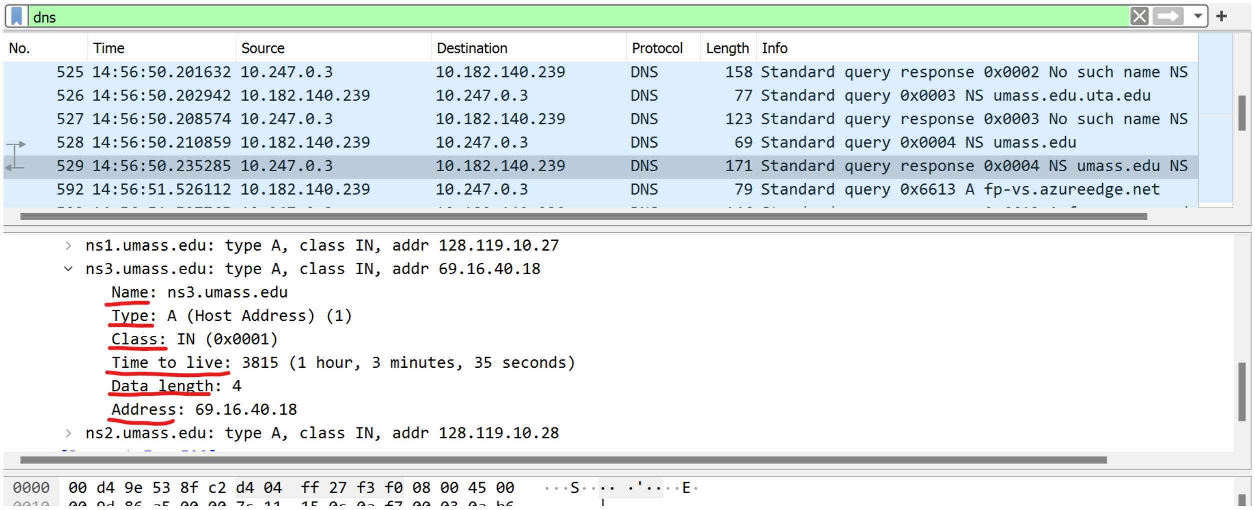


```
  v Answers
    > umass.edu: type NS, class IN, ns ns1.umass.edu
    > umass.edu: type NS, class IN, ns ns3.umass.edu
    > umass.edu: type NS, class IN, ns ns2.umass.edu
  v Additional records
    > ns1.umass.edu: type A, class IN, addr 128.119.10.27
    > ns3.umass.edu: type A, class IN, addr 69.16.40.18
    > ns2.umass.edu: type A, class IN, addr 128.119.10.28
  [Request In: 528]
```



```
No.   Time             Source          Destination     Protocol Length Info
  525 14:56:50.201632 10.247.0.3      10.182.140.239  DNS       158 Standard query response 0x0002 No such name N
  526 14:56:50.202942 10.182.140.239  10.247.0.3      DNS        77 Standard query 0x0003 NS umass.edu.uta.edu
  527 14:56:50.208574 10.247.0.3      10.182.140.239  DNS       123 Standard query response 0x0003 No such name N
  528 14:56:50.210859 10.182.140.239  10.247.0.3      DNS        69 Standard query 0x0004 NS umass.edu
  529 14:56:50.235285 10.247.0.3      10.182.140.239  DNS       171 Standard query response 0x0004 NS umass.edu N
  592 14:56:51.526112 10.182.140.239  10.247.0.3      DNS        79 Standard query 0x6613 A fp-vs.azureedge.net
```

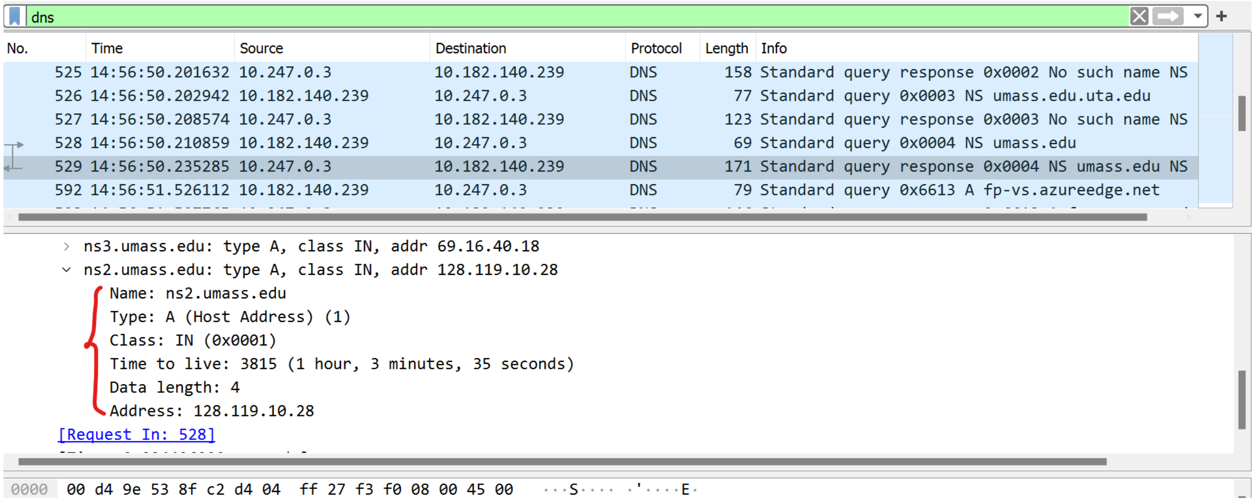
```
  Additional records
    ns1.umass.edu: type A, class IN, addr 128.119.10.27
        Name: ns1.umass.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3815 (1 hour, 3 minutes, 35 seconds)
        Data length: 4
        Address: 128.119.10.27
    ns3.umass.edu: type A, class IN, addr 69.16.40.18
```



```
No.   Time            Source          Destination     Protocol Length Info
  525 14:56:50.201632 10.247.0.3      10.182.140.239  DNS       158 Standard query response 0x0002 No such name NS
  526 14:56:50.202942 10.182.140.239  10.247.0.3      DNS        77 Standard query 0x0003 NS umass.edu.uta.edu
  527 14:56:50.208574 10.247.0.3      10.182.140.239  DNS       123 Standard query response 0x0003 No such name NS
  528 14:56:50.210859 10.182.140.239  10.247.0.3      DNS        69 Standard query 0x0004 NS umass.edu
  529 14:56:50.235285 10.247.0.3      10.182.140.239  DNS       171 Standard query response 0x0004 NS umass.edu NS
  592 14:56:51.526112 10.182.140.239  10.247.0.3      DNS        79 Standard query 0x6613 A fp-vs.azureedge.net
```

```
    ns1.umass.edu: type A, class IN, addr 128.119.10.27
    ns3.umass.edu: type A, class IN, addr 69.16.40.18
        Name: ns3.umass.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3815 (1 hour, 3 minutes, 35 seconds)
        Data length: 4
        Address: 69.16.40.18
    ns2.umass.edu: type A, class IN, addr 128.119.10.28
```

```
0000  00 d4 9e 53 8f c2 d4 04  ff 27 f3 f0 08 00 45 00   ···S···· ·'····E·
```



```
No.   Time            Source          Destination     Protocol Length Info
  525 14:56:50.201632 10.247.0.3      10.182.140.239  DNS       158 Standard query response 0x0002 No such name NS
  526 14:56:50.202942 10.182.140.239  10.247.0.3      DNS        77 Standard query 0x0003 NS umass.edu.uta.edu
  527 14:56:50.208574 10.247.0.3      10.182.140.239  DNS       123 Standard query response 0x0003 No such name NS
  528 14:56:50.210859 10.182.140.239  10.247.0.3      DNS        69 Standard query 0x0004 NS umass.edu
  529 14:56:50.235285 10.247.0.3      10.182.140.239  DNS       171 Standard query response 0x0004 NS umass.edu NS
  592 14:56:51.526112 10.182.140.239  10.247.0.3      DNS        79 Standard query 0x6613 A fp-vs.azureedge.net
```

```
    ns3.umass.edu: type A, class IN, addr 69.16.40.18
    ns2.umass.edu: type A, class IN, addr 128.119.10.28
        Name: ns2.umass.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3815 (1 hour, 3 minutes, 35 seconds)
        Data length: 4
        Address: 128.119.10.28
  [Request In: 528]
```

```
0000  00 d4 9e 53 8f c2 d4 04  ff 27 f3 f0 08 00 45 00   ···S···· ·'····E·
```