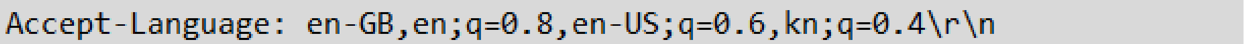
MIS 543 – Homework Assignment #1

Application Layer Protocols (Based on Wireshark Labs from Kurose and Ross 6th Edition)

NAME: Akshay A Nayak

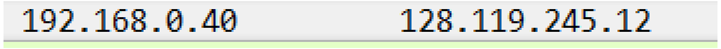
PART 1: HTTP (20 Points)

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   Browser and Server are both running HTTP version 1.1
2. What languages (if any) does your browser indicate that it can accept to the server?



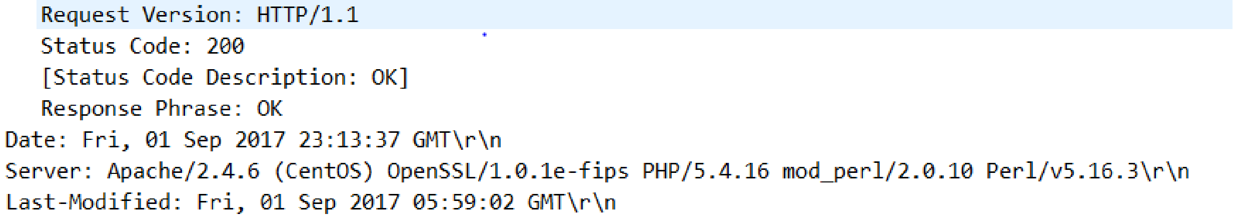
```
Accept-Language: en-GB,en;q=0.8,en-US;q=0.6,kn;q=0.4\r\n
```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?



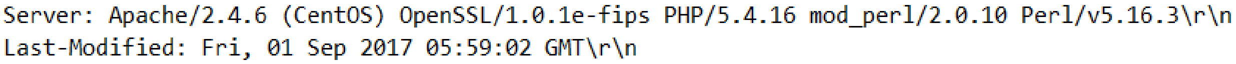
```
192.168.0.40        128.119.245.12
```

   IP address of computer and server respectively
4. What is the status code returned from the server to your browser?



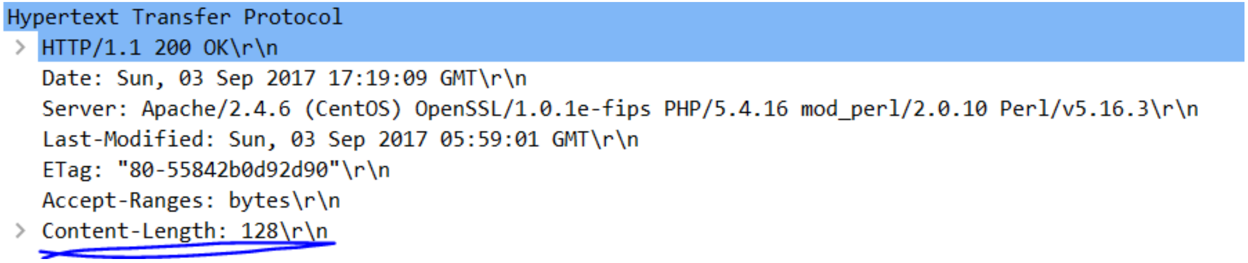
```
    Request Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
Date: Fri, 01 Sep 2017 23:13:37 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Fri, 01 Sep 2017 05:59:02 GMT\r\n
```

5. When was the HTML file that you are retrieving last modified at the server?



```
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Fri, 01 Sep 2017 05:59:02 GMT\r\n
```

6. How many bytes of content are being returned to your browser?

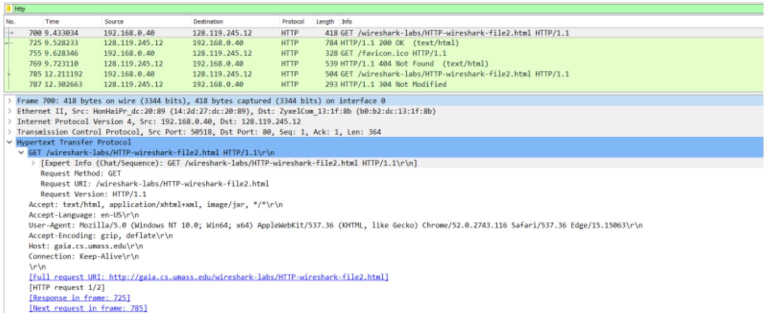


```
Hypertext Transfer Protocol
 > HTTP/1.1 200 OK\r\n
   Date: Sun, 03 Sep 2017 17:19:09 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
   Last-Modified: Sun, 03 Sep 2017 05:59:01 GMT\r\n
   ETag: "80-55842b0d92d90"\r\n
   Accept-Ranges: bytes\r\n
 > Content-Length: 128\r\n
```

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
   No all the headers can be found in the raw data.

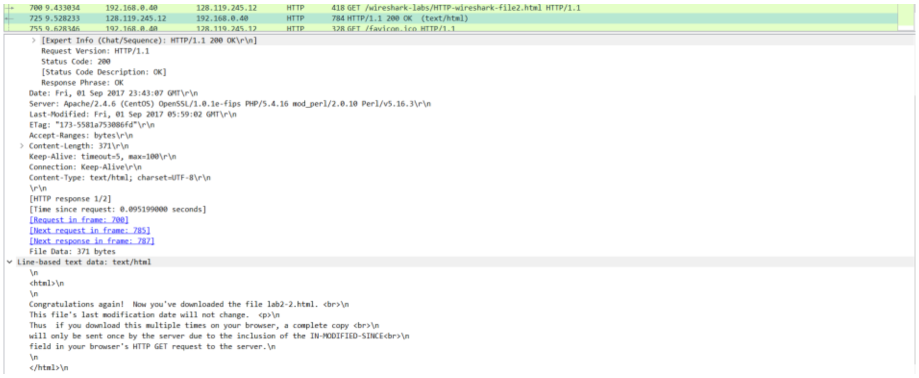
2. The HTTP CONDITIONAL GET/response interaction

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?
   No I did not find any "IF-MODIFIED-SINCE "



```
http
No.   Time        Source           Destination      Protocol  Length  Info
  700 9.433034    192.168.0.40     128.119.245.12   HTTP      418 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  725 9.528233    128.119.245.12   192.168.0.40     HTTP      784 HTTP/1.1 200 OK  (text/html)
  755 9.628346    192.168.0.40     128.119.245.12   HTTP      328 GET /favicon.ico HTTP/1.1
  769 9.723110    128.119.245.12   192.168.0.40     HTTP      539 HTTP/1.1 404 Not Found  (text/html)
  785 12.211192   192.168.0.40     128.119.245.12   HTTP      504 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  787 12.302663   128.119.245.12   192.168.0.40     HTTP      293 HTTP/1.1 304 Not Modified

> Frame 700: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface 0
> Ethernet II, Src: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89), Dst: ZyxelCom_13:1f:8b (b0:b2:dc:13:1f:8b)
> Internet Protocol Version 4, Src: 192.168.0.40, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50518, Dst Port: 80, Seq: 1, Ack: 1, Len: 364
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Edge/15.15063\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 725]
    [Next request in frame: 785]
```

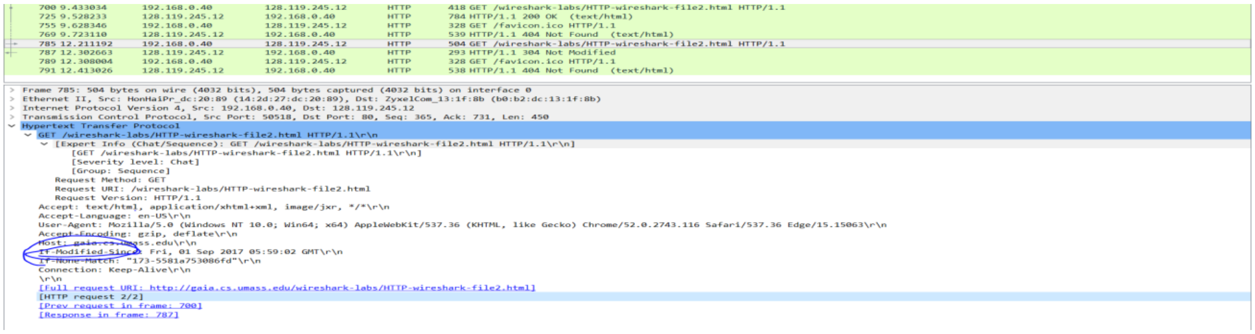
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?



```
  700 9.433034    192.168.0.40     128.119.245.12   HTTP      418 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  725 9.528233    128.119.245.12   192.168.0.40     HTTP      784 HTTP/1.1 200 OK  (text/html)
  755 9.628346    192.168.0.40     128.119.245.12   HTTP      328 GET /favicon.ico HTTP/1.1
      > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Request Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Fri, 01 Sep 2017 23:43:07 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Fri, 01 Sep 2017 05:59:02 GMT\r\n
    ETag: "173-5581a753086fd"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 371\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: 0.095199000 seconds]
    [Request in frame: 700]
    [Next request in frame: 785]
    [Next response in frame: 787]
    File Data: 371 bytes
v Line-based text data: text/html
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

Yes the server explicitly returned the contents, we can know this as we have line based text data and the Status code description status as “ OK”.

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

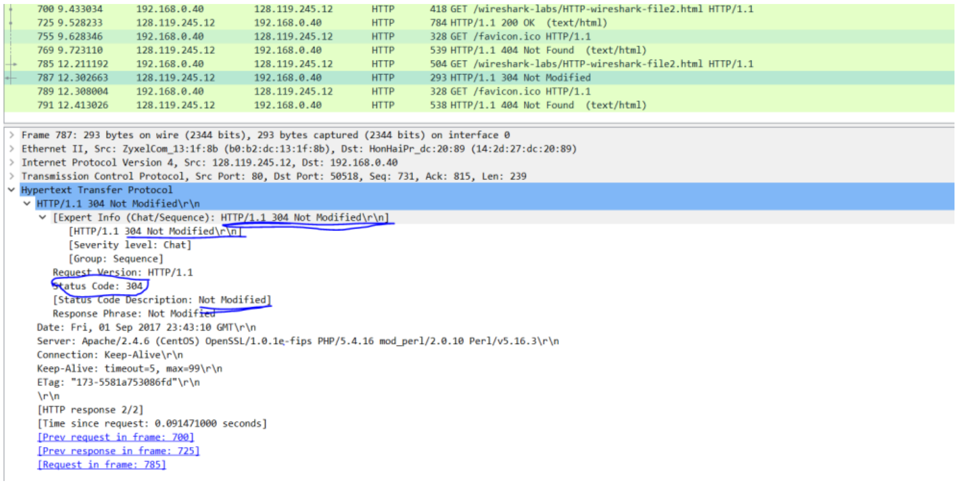


```
  700 9.433034    192.168.0.40     128.119.245.12   HTTP   418 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  725 9.528233    128.119.245.12   192.168.0.40     HTTP   784 HTTP/1.1 200 OK  (text/html)
  755 9.628346    192.168.0.40     128.119.245.12   HTTP   328 GET /favicon.ico HTTP/1.1
  769 9.723110    128.119.245.12   192.168.0.40     HTTP   539 HTTP/1.1 404 Not Found  (text/html)
  785 12.211192   192.168.0.40     128.119.245.12   HTTP   504 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  787 12.302663   128.119.245.12   192.168.0.40     HTTP   293 HTTP/1.1 304 Not Modified
  789 12.308004   192.168.0.40     128.119.245.12   HTTP   328 GET /favicon.ico HTTP/1.1
  791 12.413026   128.119.245.12   192.168.0.40     HTTP   538 HTTP/1.1 404 Not Found  (text/html)

> Frame 785: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface 0
> Ethernet II, Src: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89), Dst: ZyxelCom_13:1f:8b (b0:b2:dc:13:1f:8b)
> Internet Protocol Version 4, Src: 192.168.0.40, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50518, Dst Port: 80, Seq: 365, Ack: 731, Len: 450
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Edge/15.15063\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    If-Modified-Since: Fri, 01 Sep 2017 05:59:02 GMT\r\n
    If-None-Match: "173-5581a753086fd"\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 700]
    [Response in frame: 787]
```

The information followed is Fri ,01 sep 2017 05:9:02 GMT\r\n which is the date of the last modification of the file from previous get request.

11.

What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file?   Explain.

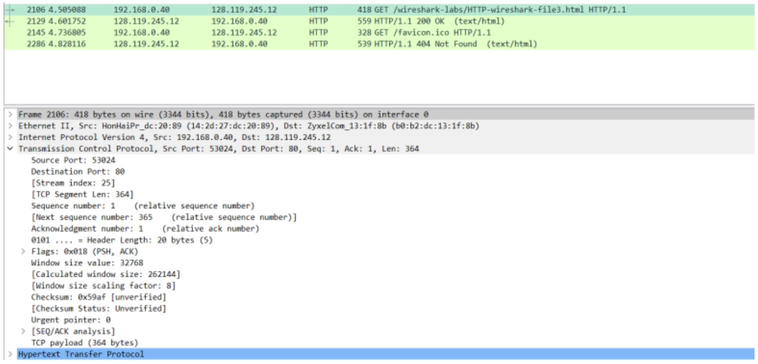


```
   700 9.433034    192.168.0.40      128.119.245.12    HTTP     418 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   725 9.528233    128.119.245.12    192.168.0.40      HTTP     784 HTTP/1.1 200 OK  (text/html)
   755 9.628346    192.168.0.40      128.119.245.12    HTTP     328 GET /favicon.ico HTTP/1.1
   769 9.723110    128.119.245.12    192.168.0.40      HTTP     539 HTTP/1.1 404 Not Found  (text/html)
   785 12.211192   192.168.0.40      128.119.245.12    HTTP     504 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   787 12.302663   128.119.245.12    192.168.0.40      HTTP     293 HTTP/1.1 304 Not Modified
   789 12.308004   192.168.0.40      128.119.245.12    HTTP     328 GET /favicon.ico HTTP/1.1
   791 12.413026   128.119.245.12    192.168.0.40      HTTP     538 HTTP/1.1 404 Not Found  (text/html)

> Frame 787: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0
> Ethernet II, Src: ZyxelCom_13:1f:8b (b0:b2:dc:13:1f:8b), Dst: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.40
> Transmission Control Protocol, Src Port: 80, Dst Port: 50518, Seq: 731, Ack: 815, Len: 239
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Fri, 01 Sep 2017 23:43:10 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5581a753086fd"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.091471000 seconds]
    [Prev request in frame: 700]
    [Prev response in frame: 725]
    [Request in frame: 785]
```

The status code and phrase returned from server is HTTP/1.1 304 not modified. The server explicitly did not return the contents of the file, since we the browser loaded from its cache.

3. Retrieving Long Documents

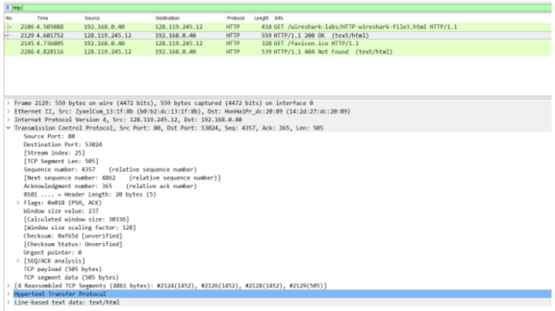
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?



```
   2106 4.505088   192.168.0.40     128.119.245.12   HTTP     418 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   2129 4.601752   128.119.245.12   192.168.0.40     HTTP     559 HTTP/1.1 200 OK  (text/html)
   2145 4.736805   192.168.0.40     128.119.245.12   HTTP     328 GET /favicon.ico HTTP/1.1
   2286 4.828116   128.119.245.12   192.168.0.40     HTTP     539 HTTP/1.1 404 Not Found  (text/html)

> Frame 2106: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface 0
> Ethernet II, Src: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89), Dst: ZyxelCom_13:1f:8b (b0:b2:dc:13:1f:8b)
> Internet Protocol Version 4, Src: 192.168.0.40, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 53024, Dst Port: 80, Seq: 1, Ack: 1, Len: 364
    Source Port: 53024
    Destination Port: 80
    [Stream index: 25]
    [TCP Segment Len: 364]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 365    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 32768
    [Calculated window size: 262144]
    [Window size scaling factor: 8]
    Checksum: 0x59af [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
    TCP payload (364 bytes)
> Hypertext Transfer Protocol
```

The browser sent only one HTTP GET request message and the packet number is 2106

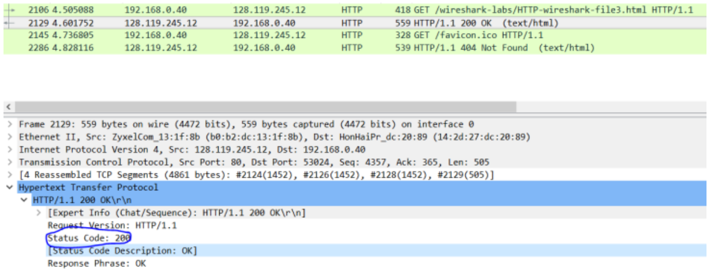
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?



```
http
No.         Time       Source           Destination      Protocol  Length  Info
   2106 4.505088   192.168.0.40     128.119.245.12   HTTP     418 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   2129 4.601752   128.119.245.12   192.168.0.40     HTTP     559 HTTP/1.1 200 OK  (text/html)
   2145 4.736805   192.168.0.40     128.119.245.12   HTTP     328 GET /favicon.ico HTTP/1.1
   2286 4.828116   128.119.245.12   192.168.0.40     HTTP     539 HTTP/1.1 404 Not Found  (text/html)

> Frame 2129: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface 0
> Ethernet II, Src: ZyxelCom_13:1f:8b (b0:b2:dc:13:1f:8b), Dst: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.40
v Transmission Control Protocol, Src Port: 80, Dst Port: 53024, Seq: 4357, Ack: 365, Len: 505
    Source Port: 80
    Destination Port: 53024
    [Stream index: 25]
    [TCP Segment Len: 505]
    Sequence number: 4357    (relative sequence number)
    [Next sequence number: 4862    (relative sequence number)]
    Acknowledgment number: 365    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xf65d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
    TCP payload (505 bytes)
    TCP segment data (505 bytes)
> [4 Reassembled TCP Segments (4861 bytes): #2124(1452), #2126(1452), #2128(1452), #2129(505)]
> Hypertext Transfer Protocol
> Line-based text data: text/html
```

Packet number 2129 in the trace contains the status code and phrase associated with the response to the HTTP GET request

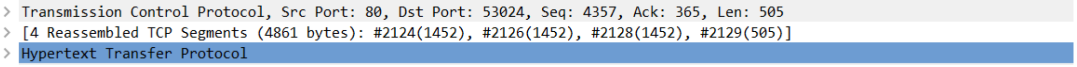
14. What is the status code and phrase in the response?



```
2106 4.505088   192.168.0.40     128.119.245.12   HTTP   418 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2129 4.601752   128.119.245.12   192.168.0.40     HTTP   559 HTTP/1.1 200 OK  (text/html)
2145 4.736805   192.168.0.40     128.119.245.12   HTTP   328 GET /favicon.ico HTTP/1.1
2286 4.828116   128.119.245.12   192.168.0.40     HTTP   539 HTTP/1.1 404 Not Found  (text/html)

> Frame 2129: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface 0
> Ethernet II, Src: ZyxelCom_13:1f:8b (b0:b2:dc:13:1f:8b), Dst: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.40
> Transmission Control Protocol, Src Port: 80, Dst Port: 53024, Seq: 4357, Ack: 365, Len: 505
> [4 Reassembled TCP Segments (4861 bytes): #2124(1452), #2126(1452), #2128(1452), #2129(505)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
```

The status code is 200 and response phrase is ok

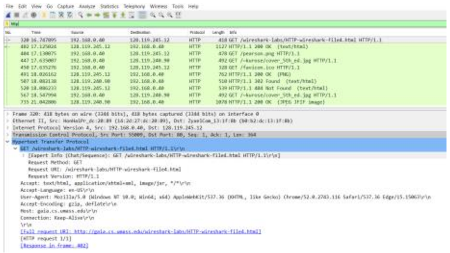
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?



```
> Transmission Control Protocol, Src Port: 80, Dst Port: 53024, Seq: 4357, Ack: 365, Len: 505
> [4 Reassembled TCP Segments (4861 bytes): #2124(1452), #2126(1452), #2128(1452), #2129(505)]
> Hypertext Transfer Protocol
```

There were 4 TCP segments needed to carry a single HTTP response carrying a total of 4861 bytes.

4. HTML Documents with Embedded Objects



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time        Source           Destination      Protocol  Length Info
320 16.747895    192.168.0.40     128.119.245.12   HTTP     418 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
402 17.125026    128.119.245.12   192.168.0.40     HTTP    1127 HTTP/1.1 200 OK  (text/html)
404 17.130075    192.168.0.40     128.119.245.12   HTTP     478 GET /pearson.png HTTP/1.1
447 17.635087    192.168.0.40     128.119.240.90   HTTP     492 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
450 17.635276    192.168.0.40     128.119.245.12   HTTP     328 GET /favicon.ico HTTP/1.1
491 18.026162    128.119.245.12   192.168.0.40     HTTP     762 HTTP/1.1 200 OK  (PNG)
507 18.082138    128.119.240.90   192.168.0.40     HTTP     510 HTTP/1.1 302 Found  (text/html)
520 18.086233    128.119.245.12   192.168.0.40     HTTP     539 HTTP/1.1 404 Not Found  (text/html)
567 18.547994    192.168.0.40     128.119.240.90   HTTP     492 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
735 21.042806    128.119.240.90   192.168.0.40     HTTP    1078 HTTP/1.1 200 OK  (JPEG JFIF image)

> Frame 320: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface 0
> Ethernet II, Src: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89), Dst: ZyxelCom_13:1f:8b (b0:b2:dc:13:1f:8b)
> Internet Protocol Version 4, Src: 192.168.0.40, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55009, Dst Port: 80, Seq: 1, Ack: 1, Len: 364
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file4.html
      Request Version: HTTP/1.1
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Edge/15.15063\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
    [HTTP request 1/1]
    [Response in frame: 402]
```

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

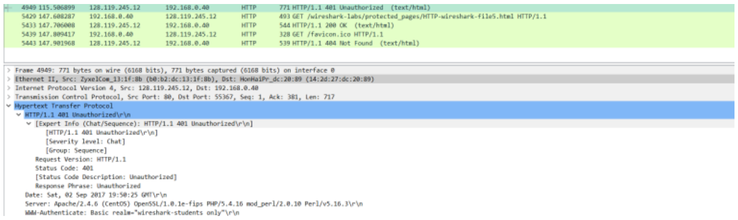
    Our browser sent 4 HTTP GET request messages. The GET request were sent to
    128.119.245.12 – GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
    128.119.245.12 - GET / pearson.png HTTP/ 1.1
    128.119.240.90 – GET /~kurose/cover_5th_ed.jpg HTTP/1.1
    128.119.240.90 - GET /~kurose/cover_5th_ed.jpg HTTP/1.1

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

    From the looks of it, it would appear they are downloaded serially. In this case the two images were transmitted over two TCP connections therefore they were downloaded serially.

5. HTTP Authentication

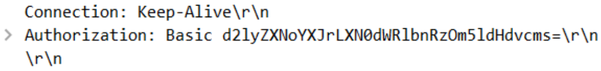
18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?



```
4949 115.506899  128.119.245.12   192.168.0.40     HTTP   771 HTTP/1.1 401 Unauthorized  (text/html)
5429 147.608287  192.168.0.40     128.119.245.12   HTTP   493 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
5433 147.706008  128.119.245.12   192.168.0.40     HTTP   544 HTTP/1.1 200 OK  (text/html)
5439 147.809417  192.168.0.40     128.119.245.12   HTTP   328 GET /favicon.ico HTTP/1.1
5443 147.901968  128.119.245.12   192.168.0.40     HTTP   539 HTTP/1.1 404 Not Found  (text/html)

> Frame 4949: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface 0
> Ethernet II, Src: ZyxelCom_13:1f:8b (b0:b2:dc:13:1f:8b), Dst: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.40
> Transmission Control Protocol, Src Port: 80, Dst Port: 55367, Seq: 1, Ack: 381, Len: 717
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
        [HTTP/1.1 401 Unauthorized\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
    Date: Sat, 02 Sep 2017 19:50:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
```

Status code is 401 and response phrase is unauthorized

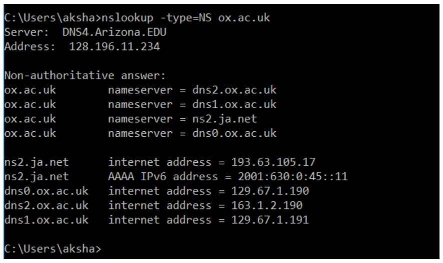
19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?



```
   Connection: Keep-Alive\r\n
 > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
   \r\n
```

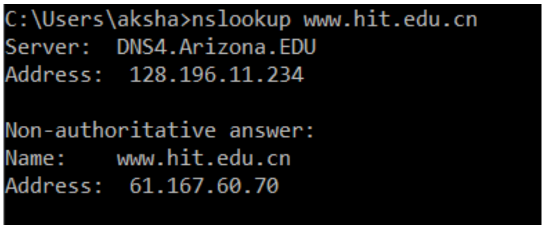
Authorization is included

PART 2: DNS (15 Points)



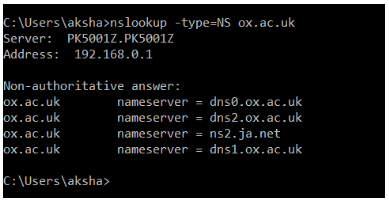
```
C:\Users\aksha>nslookup -type=NS ox.ac.uk
Server:  DNS4.Arizona.EDU
Address:  128.196.11.234

Non-authoritative answer:
ox.ac.uk        nameserver = dns2.ox.ac.uk
ox.ac.uk        nameserver = dns1.ox.ac.uk
ox.ac.uk        nameserver = ns2.ja.net
ox.ac.uk        nameserver = dns0.ox.ac.uk

ns2.ja.net      internet address = 193.63.105.17
ns2.ja.net      AAAA IPv6 address = 2001:630:0:45::11
dns0.ox.ac.uk   internet address = 129.67.1.190
dns2.ox.ac.uk   internet address = 163.1.2.190
dns1.ox.ac.uk   internet address = 129.67.1.191

C:\Users\aksha>
```

1. Run *nslookup* to obtain the IP address of a www.hit.edu.cn.



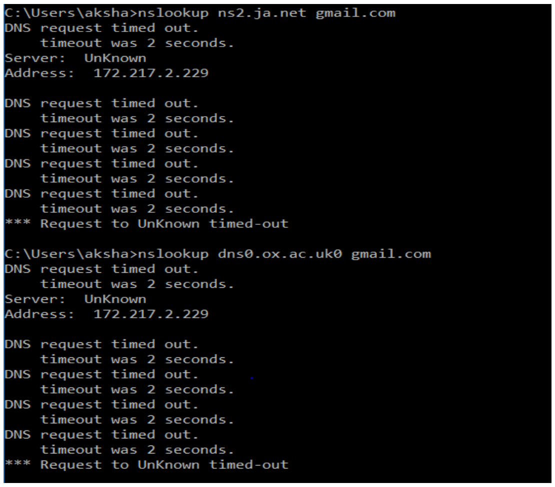
```
C:\Users\aksha>nslookup www.hit.edu.cn
Server:  DNS4.Arizona.EDU
Address:  128.196.11.234

Non-authoritative answer:
Name:    www.hit.edu.cn
Address:  61.167.60.70
```

2. Run *nslookup* to determine the authoritative DNS servers for ox.ac.uk, University of Oxford.

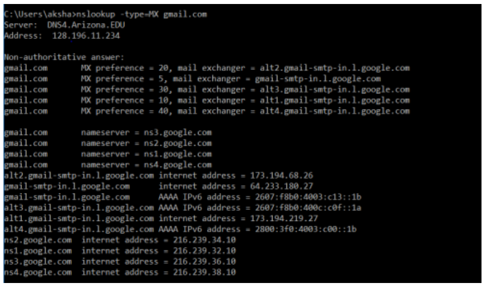


```
C:\Users\aksha>nslookup -type=NS ox.ac.uk
Server:  PK5001Z.PK5001Z
Address:  192.168.0.1

Non-authoritative answer:
ox.ac.uk        nameserver = dns0.ox.ac.uk
ox.ac.uk        nameserver = dns2.ox.ac.uk
ox.ac.uk        nameserver = ns2.ja.net
ox.ac.uk        nameserver = dns1.ox.ac.uk

C:\Users\aksha>
```

3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for gmail.com. What happens when you do it? Then do not query from the DNS servers obtained in Question 2. What are the mail servers?



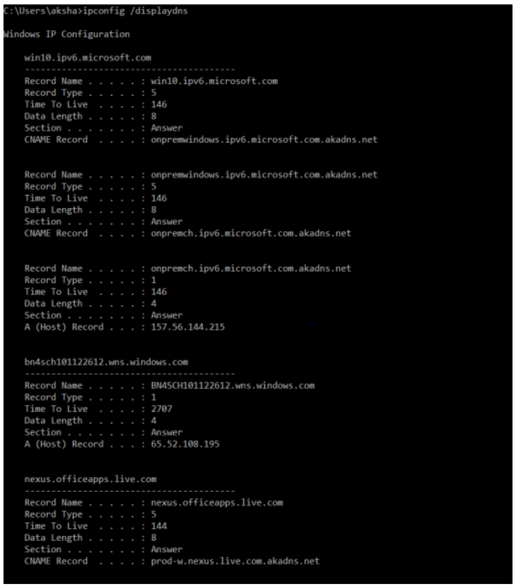
```
C:\Users\aksha>nslookup ns2.ja.net gmail.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  172.217.2.229

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\aksha>nslookup dns0.ox.ac.uk0 gmail.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  172.217.2.229

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```



```
C:\Users\aksha>nslookup -type=MX gmail.com
Server:  DNS4.Arizona.EDU
Address:  128.196.11.234

Non-authoritative answer:
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com

gmail.com       nameserver = ns3.google.com
gmail.com       nameserver = ns2.google.com
gmail.com       nameserver = ns1.google.com
gmail.com       nameserver = ns4.google.com
alt2.gmail-smtp-in.l.google.com internet address = 173.194.68.26
gmail-smtp-in.l.google.com      internet address = 64.233.180.27
gmail-smtp-in.l.google.com      AAAA IPv6 address = 2607:f8b0:4003:c13::1b
alt3.gmail-smtp-in.l.google.com AAAA IPv6 address = 2607:f8b0:400c:c0f::1a
alt1.gmail-smtp-in.l.google.com internet address = 173.194.219.27
alt4.gmail-smtp-in.l.google.com AAAA IPv6 address = 2800:3f0:4003:c00::1b
ns2.google.com  internet address = 216.239.34.10
ns1.google.com  internet address = 216.239.32.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
```

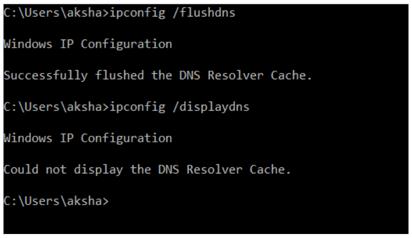
2. ipconfig

Using ipconfig / displaydns



```
C:\Users\aksha>ipconfig /displaydns

Windows IP Configuration

    win10.ipv6.microsoft.com
    ----------------------------------------
    Record Name . . . . . : win10.ipv6.microsoft.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 146
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : onpremwindows.ipv6.microsoft.com.akadns.net


    Record Name . . . . . : onpremwindows.ipv6.microsoft.com.akadns.net
    Record Type . . . . . : 5
    Time To Live  . . . . : 146
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : onpremch.ipv6.microsoft.com.akadns.net


    Record Name . . . . . : onpremch.ipv6.microsoft.com.akadns.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 146
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 157.56.144.215


    bn4sch101122612.wns.windows.com
    ----------------------------------------
    Record Name . . . . . : BN4SCH101122612.wns.windows.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 2707
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 65.52.108.195


    nexus.officeapps.live.com
    ----------------------------------------
    Record Name . . . . . : nexus.officeapps.live.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 144
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : prod-w.nexus.live.com.akadns.net
```

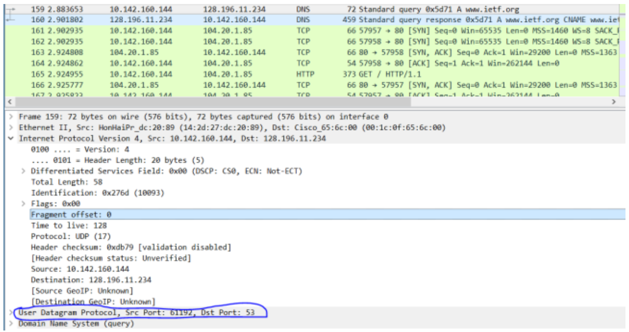
Using ipconfig/ flushdns



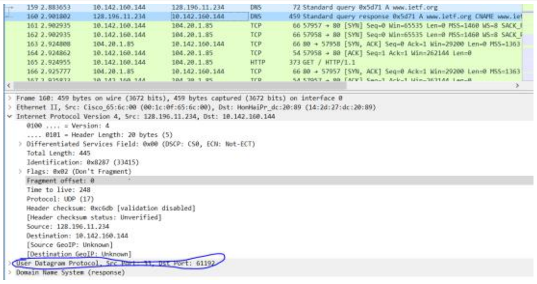
```
C:\Users\aksha>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\aksha>ipconfig /displaydns

Windows IP Configuration

Could not display the DNS Resolver Cache.

C:\Users\aksha>
```

3. Tracing DNS with Wireshark

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



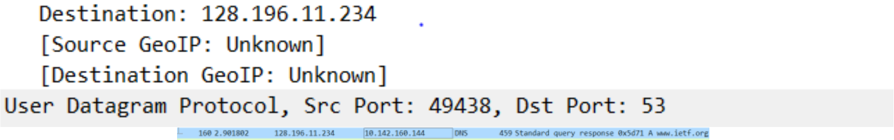
```
159 2.883653  10.142.160.144  128.196.11.234  DNS   72 Standard query 0x5d71 A www.ietf.org
160 2.901802  128.196.11.234  10.142.160.144  DNS  459 Standard query response 0x5d71 A www.ietf.org CNAME www.iet
161 2.902935  10.142.160.144  104.20.1.85     TCP   66 57957 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_
162 2.902935  10.142.160.144  104.20.1.85     TCP   66 57958 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_
163 2.924808  104.20.1.85     10.142.160.144  TCP   66 80 → 57958 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1363
164 2.924862  10.142.160.144  104.20.1.85     TCP   54 57958 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
165 2.924955  10.142.160.144  104.20.1.85     HTTP 373 GET / HTTP/1.1
166 2.925777  104.20.1.85     10.142.160.144  TCP   66 80 → 57957 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1363

> Frame 159: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89), Dst: Cisco_65:6c:00 (00:1c:0f:65:6c:00)
v Internet Protocol Version 4, Src: 10.142.160.144, Dst: 128.196.11.234
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0x276d (10093)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xdb79 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.142.160.144
    Destination: 128.196.11.234
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
> User Datagram Protocol, Src Port: 61192, Dst Port: 53
> Domain Name System (query)
```



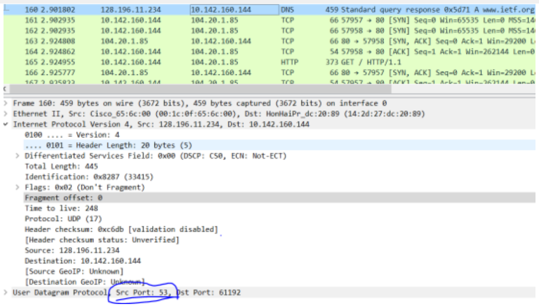
```
159 2.883653  10.142.160.144  128.196.11.234  DNS   72 Standard query 0x5d71 A www.ietf.org
160 2.901802  128.196.11.234  10.142.160.144  DNS  459 Standard query response 0x5d71 A www.ietf.org CNAME www.iet
161 2.902935  10.142.160.144  104.20.1.85     TCP   66 57957 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_
162 2.902935  10.142.160.144  104.20.1.85     TCP   66 57958 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_
163 2.924808  104.20.1.85     10.142.160.144  TCP   66 80 → 57958 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1363
164 2.924862  10.142.160.144  104.20.1.85     TCP   54 57958 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
165 2.924955  10.142.160.144  104.20.1.85     HTTP 373 GET / HTTP/1.1
166 2.925777  104.20.1.85     10.142.160.144  TCP   66 80 → 57957 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1363

> Frame 160: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface 0
> Ethernet II, Src: Cisco_65:6c:00 (00:1c:0f:65:6c:00), Dst: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89)
v Internet Protocol Version 4, Src: 128.196.11.234, Dst: 10.142.160.144
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 445
    Identification: 0x8287 (33415)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 248
    Protocol: UDP (17)
    Header checksum: 0xc6db [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.196.11.234
    Destination: 10.142.160.144
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
> User Datagram Protocol, Src Port: 53, Dst Port: 61192
> Domain Name System (response)
```

The DNS query message is sent over UDP.

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



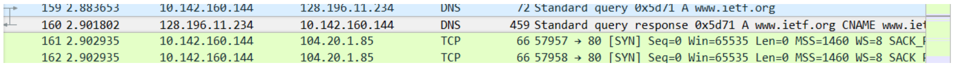
```
    Destination: 128.196.11.234
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 49438, Dst Port: 53
```



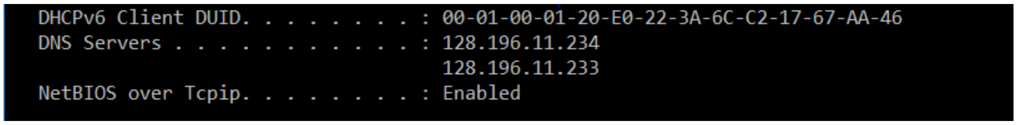
```
160 2.901802  128.196.11.234  10.142.160.144  DNS  459 Standard query response 0x5d71 A www.ietf.org
161 2.902935  10.142.160.144  104.20.1.85     TCP   66 57957 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=14
162 2.902935  10.142.160.144  104.20.1.85     TCP   66 57958 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=14
163 2.924808  104.20.1.85     10.142.160.144  TCP   66 80 → 57958 [SYN, ACK] Seq=0 Ack=1 Win=29200 L
164 2.924862  10.142.160.144  104.20.1.85     TCP   54 57958 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
165 2.924955  10.142.160.144  104.20.1.85     HTTP 373 GET / HTTP/1.1
166 2.925777  104.20.1.85     10.142.160.144  TCP   66 80 → 57957 [SYN, ACK] Seq=0 Ack=1 Win=29200 L

> Frame 160: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface 0
> Ethernet II, Src: Cisco_65:6c:00 (00:1c:0f:65:6c:00), Dst: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89)
v Internet Protocol Version 4, Src: 128.196.11.234, Dst: 10.142.160.144
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 445
    Identification: 0x8287 (33415)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 248
    Protocol: UDP (17)
    Header checksum: 0xc6db [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.196.11.234
    Destination: 10.142.160.144
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
> User Datagram Protocol, Src Port: 53, Dst Port: 61192
```

The destination port of DNS query message and source port of DNS response message 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?



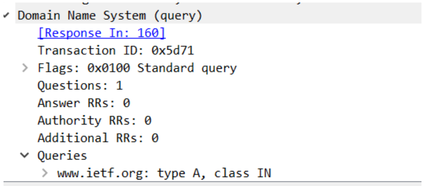
```
159 2.883653  10.142.160.144  128.196.11.234  DNS   72 Standard query 0x5d71 A www.ietf.org
160 2.901802  128.196.11.234  10.142.160.144  DNS  459 Standard query response 0x5d71 A www.ietf.org CNAME www.iet
161 2.902935  10.142.160.144  104.20.1.85     TCP   66 57957 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_
162 2.902935  10.142.160.144  104.20.1.85     TCP   66 57958 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_
```



```
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-E0-22-3A-6C-C2-17-67-AA-46
   DNS Servers . . . . . . . . . . . : 128.196.11.234
                                       128.196.11.233
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

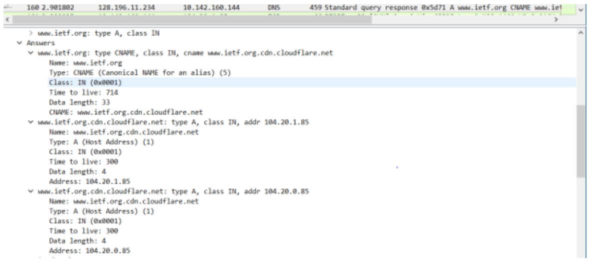
Yes, they are the same

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
   It is a standard Query of type A, it does not contain any answer



```
✓ Domain Name System (query)
    [Response In: 160]
    Transaction ID: 0x5d71
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    > www.ietf.org: type A, class IN
```

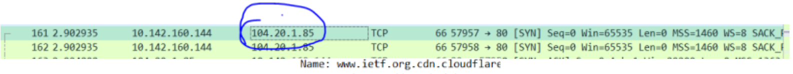
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



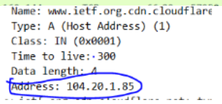
```
160 2.901802    128.196.11.234    10.142.160.144    DNS    459 Standard query response 0x5d71 A www.ietf.org CNAME www.iet

  > www.ietf.org: type A, class IN
⌄ Answers
  ⌄ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 714
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  ⌄ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300
      Data length: 4
      Address: 104.20.1.85
  ⌄ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300
      Data length: 4
      Address: 104.20.0.85
```

Three answers are provided, the answer contain TTL, data length Type and the NAME.

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?



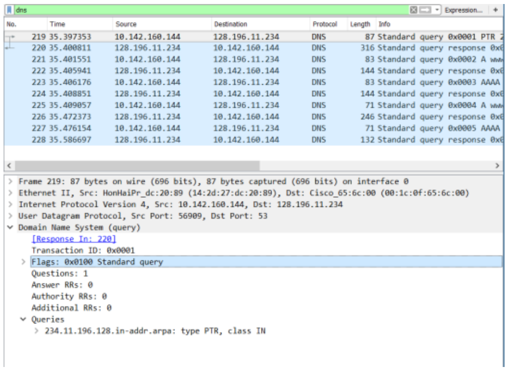
```
161 2.902935    10.142.160.144    104.20.1.85    TCP    66 57957 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_P
162 2.902935    10.142.160.144    104.20.1.85    TCP    66 57958 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_P
```



```
Name: www.ietf.org.cdn.cloudflare
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.20.1.85
```

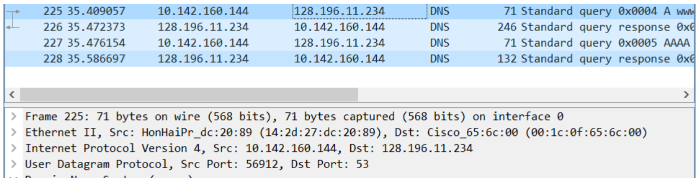
The first SYN packet was sent to address 104.20.1.85 which is also the address of the First DNS response message.

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
    NO

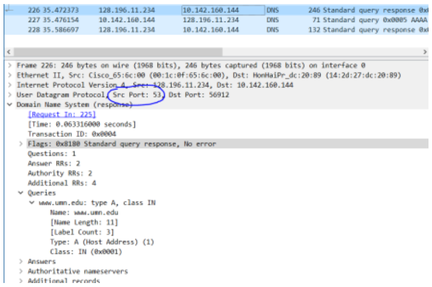


```
dns                                                                          Expression...  +
No.   Time        Source            Destination       Protocol  Length  Info
  219 35.397353   10.142.160.144    128.196.11.234    DNS          87 Standard query 0x0001 PTR 2
  220 35.400811   128.196.11.234    10.142.160.144    DNS         316 Standard query response 0x0
  221 35.401551   10.142.160.144    128.196.11.234    DNS          83 Standard query 0x0002 A www
  222 35.405941   128.196.11.234    10.142.160.144    DNS         144 Standard query response 0x0
  223 35.406176   10.142.160.144    128.196.11.234    DNS          83 Standard query 0x0003 AAAA
  224 35.408851   128.196.11.234    10.142.160.144    DNS         144 Standard query response 0x0
  225 35.409057   10.142.160.144    128.196.11.234    DNS          71 Standard query 0x0004 A www
  226 35.472373   128.196.11.234    10.142.160.144    DNS         246 Standard query response 0x0
  227 35.476154   10.142.160.144    128.196.11.234    DNS          71 Standard query 0x0005 AAAA
  228 35.586697   128.196.11.234    10.142.160.144    DNS         132 Standard query response 0x0

> Frame 219: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
> Ethernet II, Src: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89), Dst: Cisco_65:6c:00 (00:1c:0f:65:6c:00)
> Internet Protocol Version 4, Src: 10.142.160.144, Dst: 128.196.11.234
> User Datagram Protocol, Src Port: 56909, Dst Port: 53
⌄ Domain Name System (query)
    [Response In: 220]
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    > 234.11.196.128.in-addr.arpa: type PTR, class IN
```

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



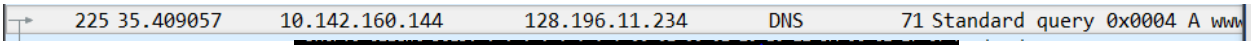
```
  225 35.409057   10.142.160.144    128.196.11.234    DNS     71 Standard query 0x0004 A www
  226 35.472373   128.196.11.234    10.142.160.144    DNS    246 Standard query response 0x0
  227 35.476154   10.142.160.144    128.196.11.234    DNS     71 Standard query 0x0005 AAAA
  228 35.586697   128.196.11.234    10.142.160.144    DNS    132 Standard query response 0x0

> Frame 225: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89), Dst: Cisco_65:6c:00 (00:1c:0f:65:6c:00)
> Internet Protocol Version 4, Src: 10.142.160.144, Dst: 128.196.11.234
> User Datagram Protocol, Src Port: 56912, Dst Port: 53
```



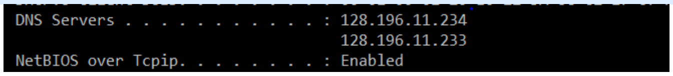
```
226 35.472373   128.196.11.234   10.142.160.144   DNS   246 Standard query response 0x
227 35.476154   10.142.160.144   128.196.11.234   DNS    71 Standard query 0x0005 AAAA
228 35.586697   128.196.11.234   10.142.160.144   DNS   132 Standard query response 0x

> Frame 226: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits) on interface 0
> Ethernet II, Src: Cisco_65:6c:00 (00:1c:0f:65:6c:00), Dst: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89)
> Internet Protocol Version 4, Src: 128.196.11.234, Dst: 10.142.160.144
> User Datagram Protocol, Src Port: 53, Dst Port: 56912
v Domain Name System (response)
    [Request In: 225]
    [Time: 0.063316000 seconds]
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 2
    Additional RRs: 4
  v Queries
    v www.umn.edu: type A, class IN
        Name: www.umn.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  > Answers
  > Authoritative nameservers
  > Additional records
```

destination port for the DNS query message and source port of DNS response message is 53

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



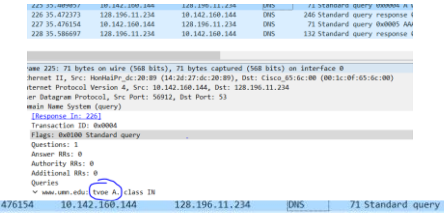
```
225 35.409057   10.142.160.144   128.196.11.234   DNS   71 Standard query 0x0004 A www
```



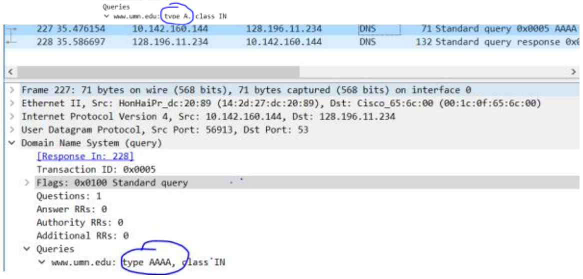
```
DNS Servers . . . . . . . . . . . : 128.196.11.234
                                    128.196.11.233
NetBIOS over Tcpip. . . . . . . . : Enabled
```

The IP address is 128.196.11.234

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



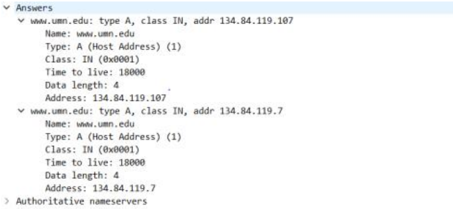
```
225 35.409057   10.142.160.144   128.196.11.234   DNS    71 Standard query 0x0004 A
226 35.472373   128.196.11.234   10.142.160.144   DNS   246 Standard query response
227 35.476154   10.142.160.144   128.196.11.234   DNS    71 Standard query 0x0005 AA
228 35.586697   128.196.11.234   10.142.160.144   DNS   132 Standard query response

ame 225: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
hernet II, Src: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89), Dst: Cisco_65:6c:00 (00:1c:0f:65:6c:00)
ternet Protocol Version 4, Src: 10.142.160.144, Dst: 128.196.11.234
er Datagram Protocol, Src Port: 56912, Dst Port: 53
main Name System (query)
 [Response In: 226]
 Transaction ID: 0x0004
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 v www.umn.edu: type A, class IN
```



```
227 35.476154   10.142.160.144   128.196.11.234   DNS    71 Standard query 0x0005 AAAA
228 35.586697   128.196.11.234   10.142.160.144   DNS   132 Standard query response 0x0

> Frame 227: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89), Dst: Cisco_65:6c:00 (00:1c:0f:65:6c:00)
> Internet Protocol Version 4, Src: 10.142.160.144, Dst: 128.196.11.234
> User Datagram Protocol, Src Port: 56913, Dst Port: 53
v Domain Name System (query)
    [Response In: 228]
    Transaction ID: 0x0005
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.umn.edu: type AAAA, class IN
```

Last but one query is of type A and last query is of type AAAA(Specifies IPV6 address for given host), there are no answers in query message.

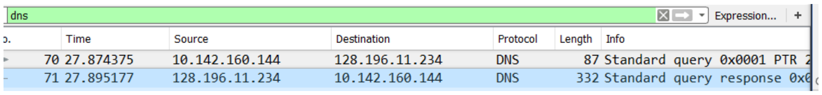
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



```
v Answers
  v www.umn.edu: type A, class IN, addr 134.84.119.107
      Name: www.umn.edu
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 18000
      Data length: 4
      Address: 134.84.119.107
  v www.umn.edu: type A, class IN, addr 134.84.119.7
      Name: www.umn.edu
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 18000
      Data length: 4
      Address: 134.84.119.7
> Authoritative nameservers
```

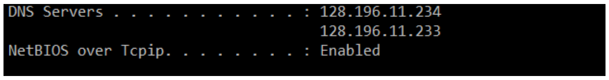
There are two answers, it contains Type , Class ,TTL ,Data length and the address.

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



dns

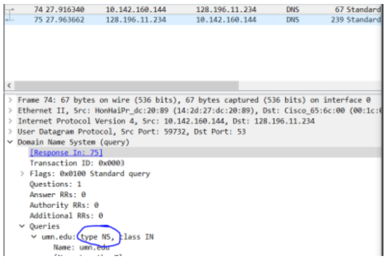
```
o.   Time        Source           Destination      Protocol  Length  Info
  70 27.874375   10.142.160.144   128.196.11.234   DNS          87 Standard query 0x0001 PTR 2
  71 27.895177   128.196.11.234   10.142.160.144   DNS         332 Standard query response 0x0
```



```
DNS Servers . . . . . . . . . . . : 128.196.11.234
                                    128.196.11.233
NetBIOS over Tcpip. . . . . . . . : Enabled
```

The DNS query message is sent to 128.196.11.234 which is the IP address of my local DNS server.

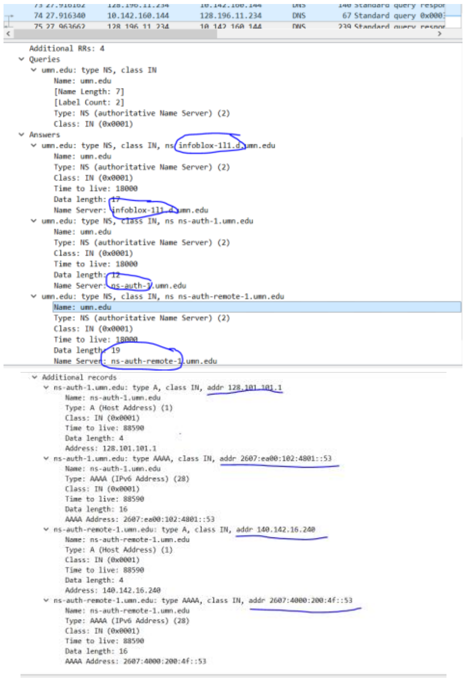
16. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
74 27.916340   10.142.160.144   128.196.11.234   DNS    67 Standard
75 27.963662   128.196.11.234   10.142.160.144   DNS   239 Standard

> Frame 74: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
> Ethernet II, Src: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89), Dst: Cisco_65:6c:00 (00:1c:0
> Internet Protocol Version 4, Src: 10.142.160.144, Dst: 128.196.11.234
> User Datagram Protocol, Src Port: 59732, Dst Port: 53
v Domain Name System (query)
    [Response In: 75]
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v umn.edu: type NS, class IN
        Name: umn.edu
```

The type of query is NS ,it does not contain any answer.

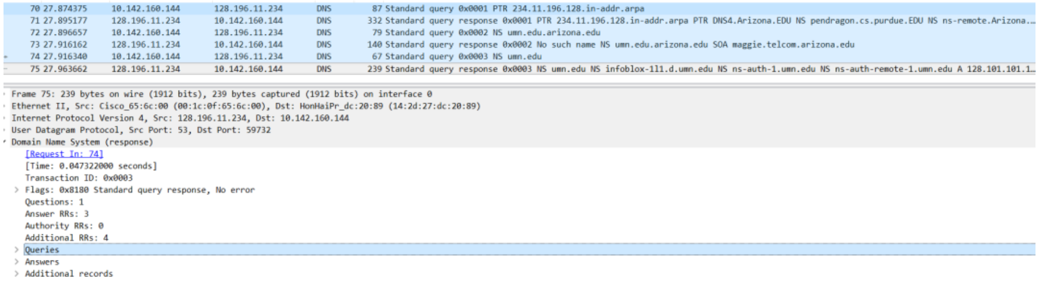
17. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?
The name servers are
Infoblox-111.d , ns-auth and ns-auth-remote.1



```
73 27.916162   128.196.11.234   10.142.160.144   DNS   140 Standard query respon
74 27.916340   10.142.160.144   128.196.11.234   DNS    67 Standard query 0x000
75 27.963662   128.196.11.234   10.142.160.144   DNS   239 Standard query respon

    Additional RRs: 4
  v Queries
    v umn.edu: type NS, class IN
        Name: umn.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  v Answers
    v umn.edu: type NS, class IN, ns infoblox-111.d.umn.edu
        Name: umn.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 18000
        Data length: 17
        Name Server: infoblox-111.d.umn.edu
    v umn.edu: type NS, class IN, ns ns-auth-1.umn.edu
        Name: umn.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 18000
        Data length: 12
        Name Server: ns-auth-1.umn.edu
    v umn.edu: type NS, class IN, ns ns-auth-remote-1.umn.edu
        Name: umn.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 18000
        Data length: 19
        Name Server: ns-auth-remote-1.umn.edu

  v Additional records
    v ns-auth-1.umn.edu: type A, class IN, addr 128.101.101.1
        Name: ns-auth-1.umn.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 88590
        Data length: 4
        Address: 128.101.101.1
    v ns-auth-1.umn.edu: type AAAA, class IN, addr 2607:ea00:102:4801::53
        Name: ns-auth-1.umn.edu
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 88590
        Data length: 16
        AAAA Address: 2607:ea00:102:4801::53
    v ns-auth-remote-1.umn.edu: type A, class IN, addr 140.142.16.240
        Name: ns-auth-remote-1.umn.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 88590
        Data length: 4
        Address: 140.142.16.240
    v ns-auth-remote-1.umn.edu: type AAAA, class IN, addr 2607:4000:200:4f::53
        Name: ns-auth-remote-1.umn.edu
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 88590
        Data length: 16
        AAAA Address: 2607:4000:200:4f::53
```

The IP address are found in additional section.

18. Provide a screenshot.



```
70 27.874375   10.142.160.144   128.196.11.234   DNS    87 Standard query 0x0001 PTR 234.11.196.128.in-addr.arpa
71 27.895177   128.196.11.234   10.142.160.144   DNS   332 Standard query response 0x0001 PTR 234.11.196.128.in-addr.arpa PTR DNS4.Arizona.EDU NS pendragon.cs.purdue.EDU NS ns-remote.Arizona...
72 27.896657   10.142.160.144   128.196.11.234   DNS    79 Standard query 0x0002 NS umn.edu.arizona.edu
73 27.916162   128.196.11.234   10.142.160.144   DNS   140 Standard query response 0x0002 No such name NS umn.edu.arizona.edu SOA maggie.telcom.arizona.edu
74 27.916340   10.142.160.144   128.196.11.234   DNS    67 Standard query 0x0003 NS umn.edu
75 27.963662   128.196.11.234   10.142.160.144   DNS   239 Standard query response 0x0003 NS umn.edu NS infoblox-111.d.umn.edu NS ns-auth-1.umn.edu NS ns-auth-remote-1.umn.edu A 128.101.101.1...

> Frame 75: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface 0
> Ethernet II, Src: Cisco_65:6c:00 (00:1c:0f:65:6c:00), Dst: HonHaiPr_dc:20:89 (14:2d:27:dc:20:89)
> Internet Protocol Version 4, Src: 128.196.11.234, Dst: 10.142.160.144
> User Datagram Protocol, Src Port: 53, Dst Port: 59732
v Domain Name System (response)
    [Request In: 74]
    [Time: 0.047322000 seconds]
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 4
  > Queries
  > Answers
  > Additional records
```