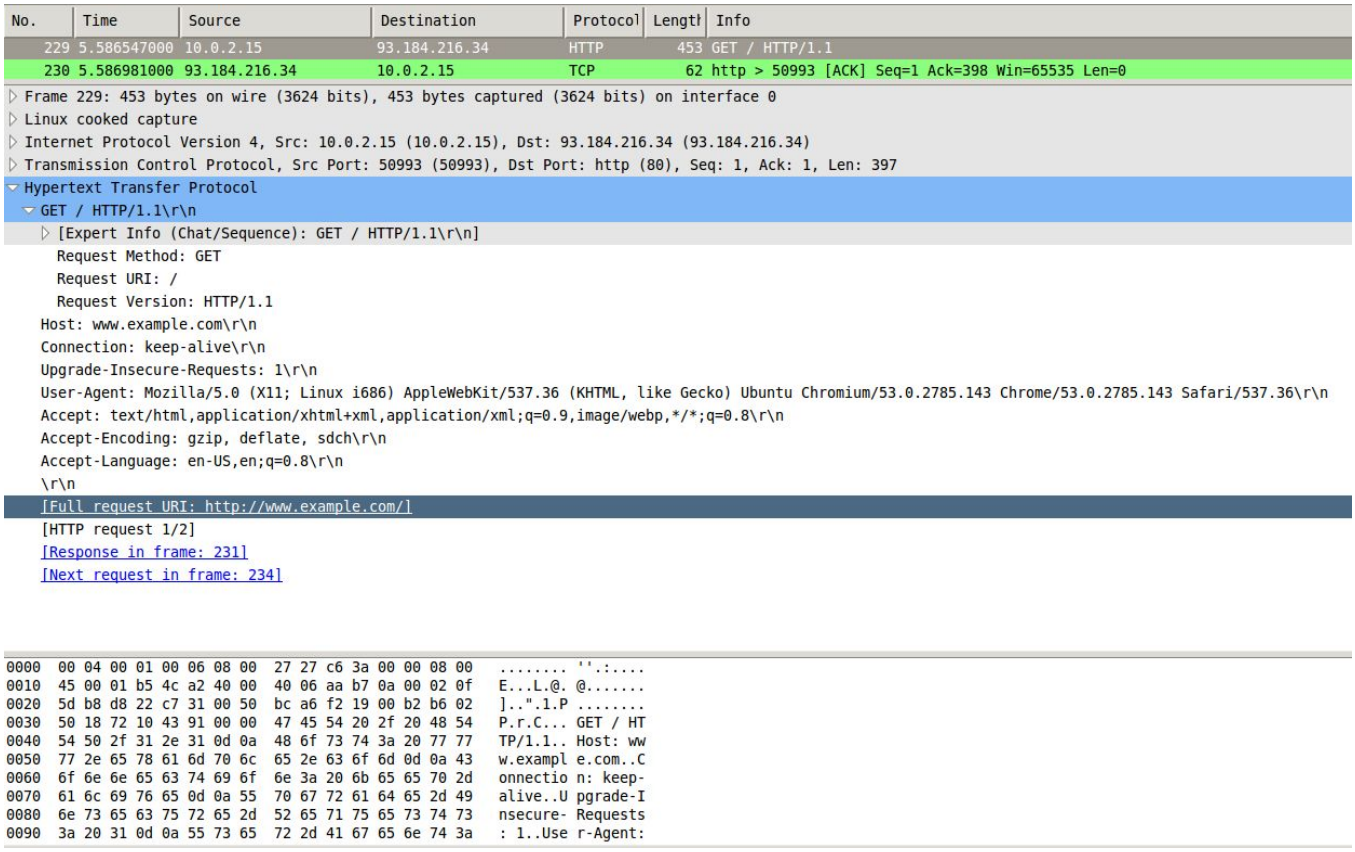
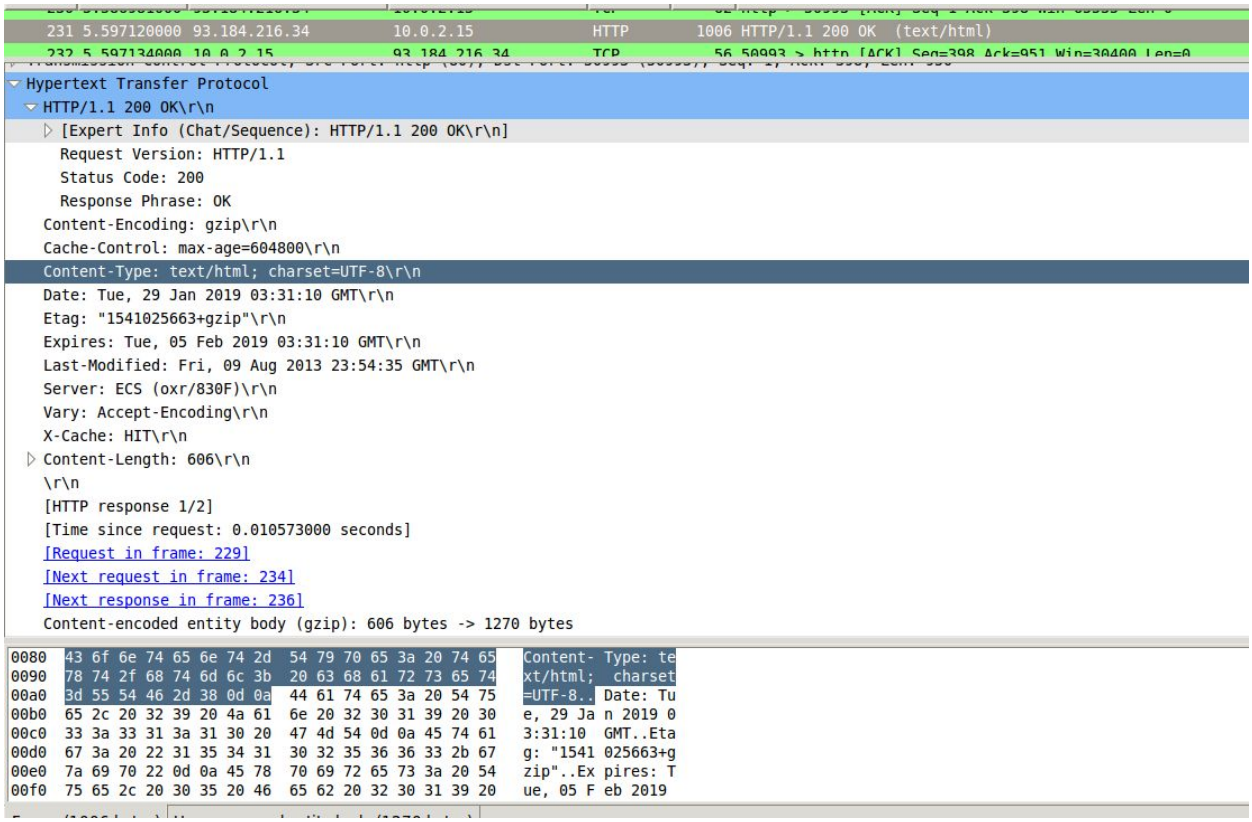
Part 1: HTTP

1. Find the packet that corresponds to the initial HTTP request that your computer issued. Take a screenshot of this packet. What HTTP method did your computer use to make this request? What URI did your computer request from the server, as present in the HTTP request? (note: NOT the URL). Explain.



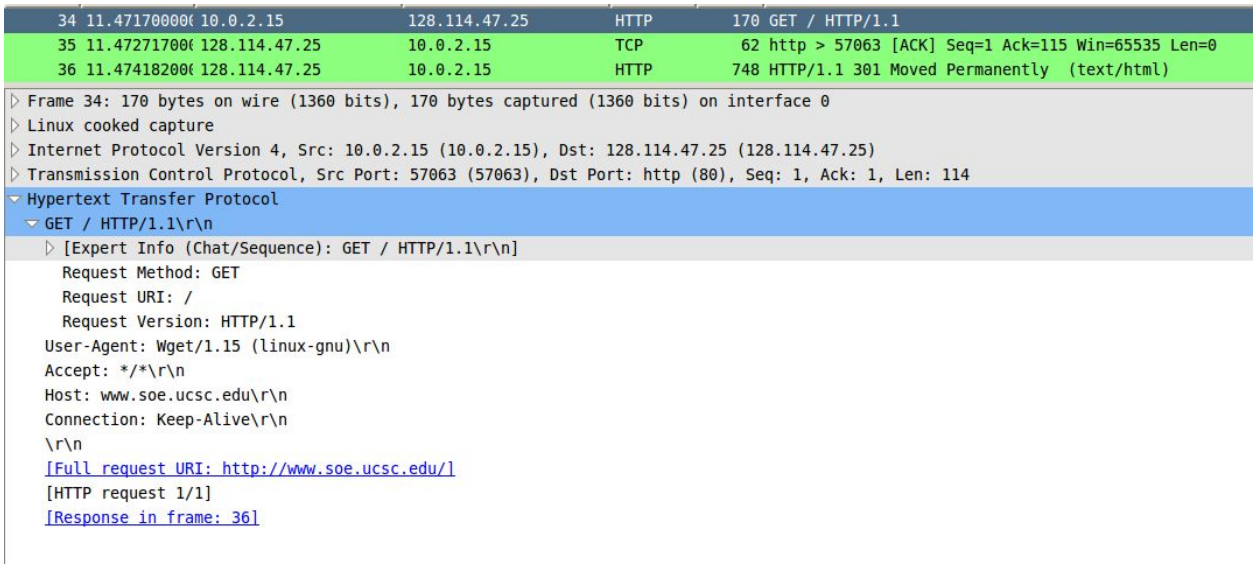
The HTTP method that my computer used to make this request is GET, and the URI that the computer requested from the server is “http://www.example.com”

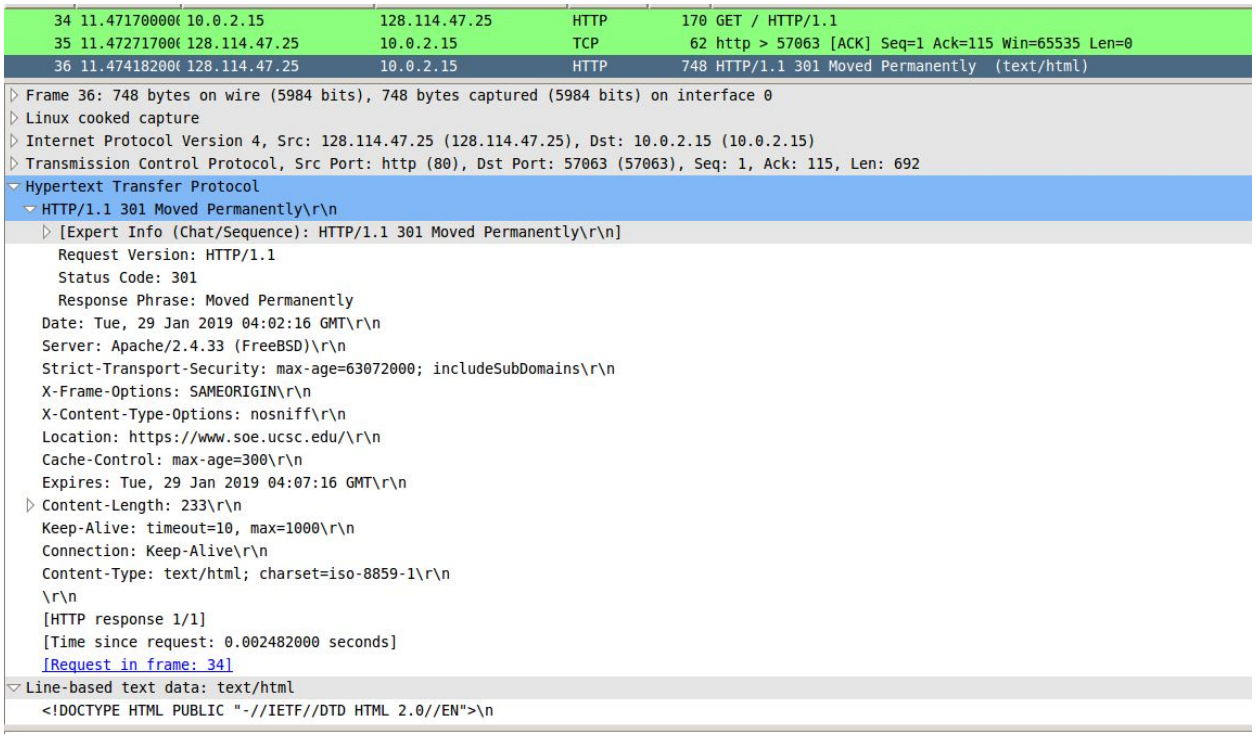
2. Find the packet that corresponds to the initial HTTP response the server issued in response to your request. Take a screenshot of this packet. What HTTP status code did the server return? What is the content type of the response the server is sending back? Explain.



The Status Code given for the response is 200, the Content Type is text/html

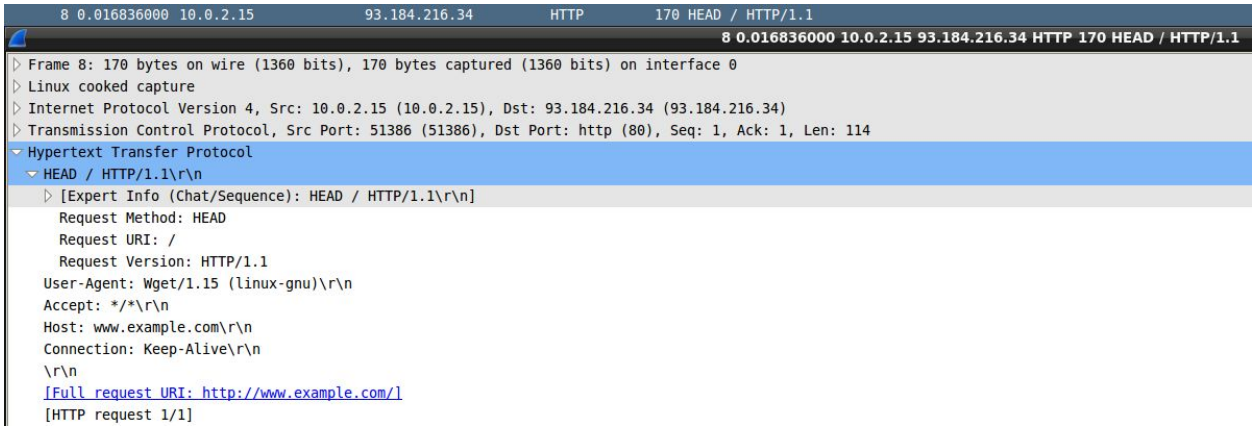
3. Find the packets that correspond to the initial HTTP request and response that your computer issued/received. Take a screenshot of these packets. What's different? Explain.

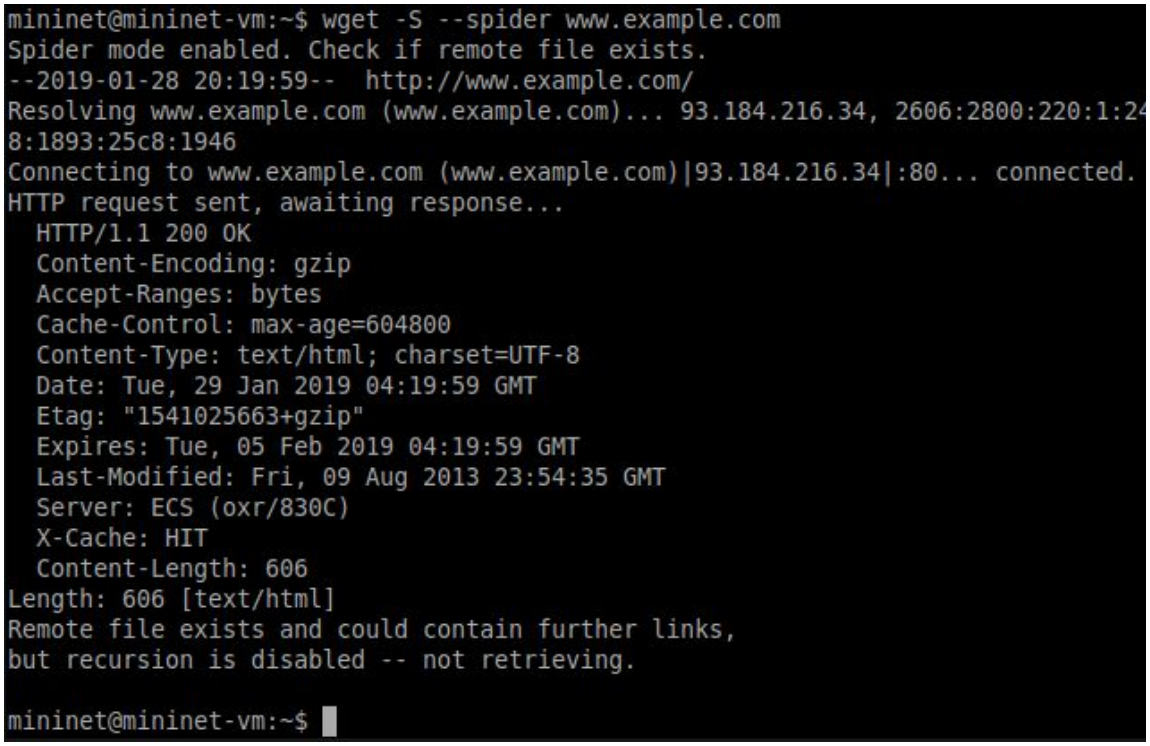




The request method was the same, which was “GET”, however the Response code was different, the Status Code is “301”

4. Take a screenshot of your packet and explain what you did to create it.

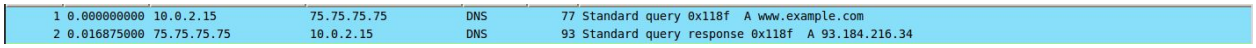


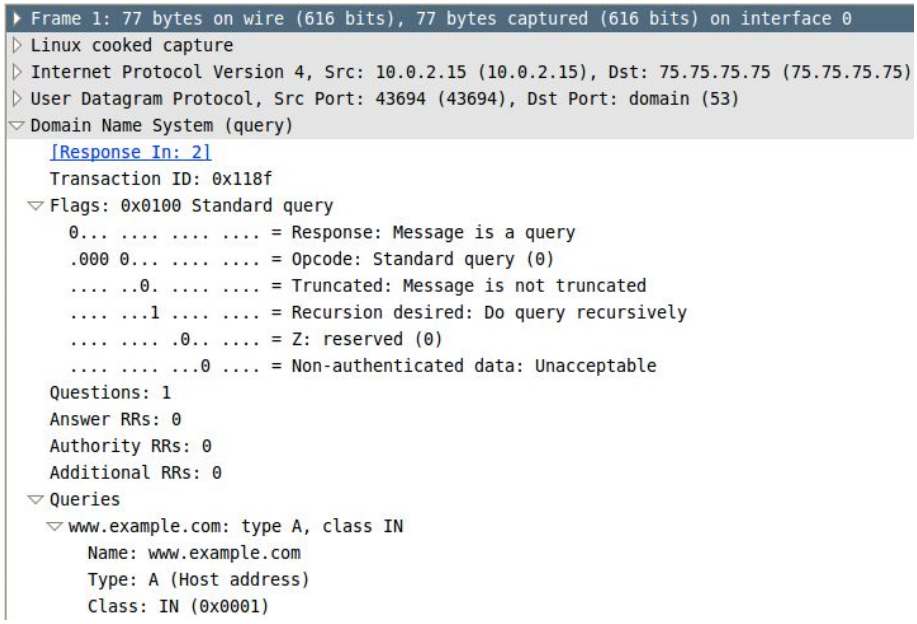


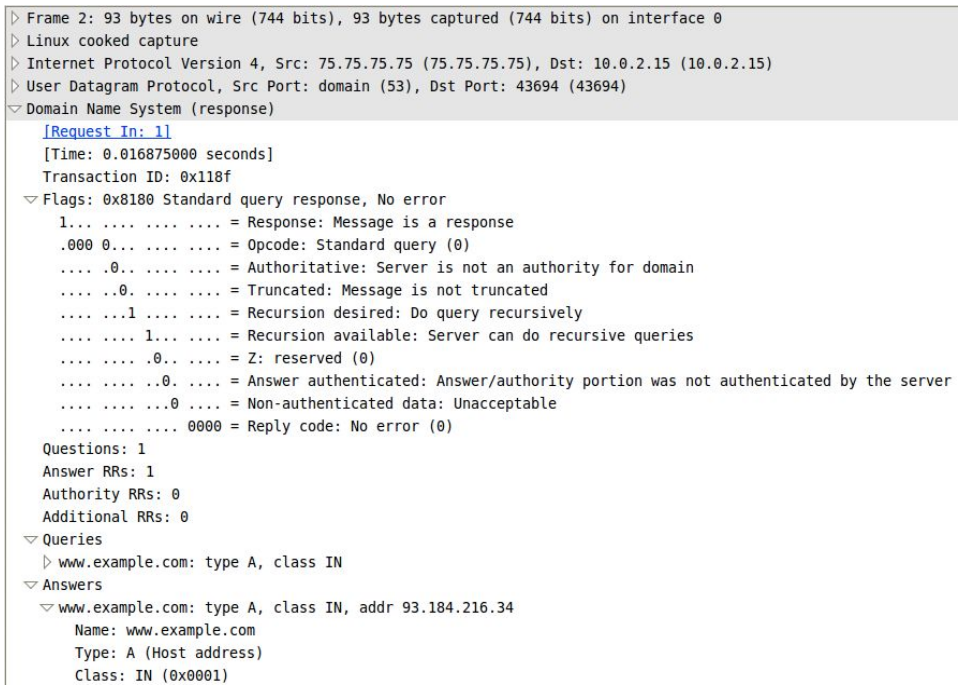
To create this packet, I went into Mininet and used the command “wget -S --spider www.exmple.com” which then gave me a Request Method of “Head” for the packet.

Part 2: DNS

5. Were any steps taken by your computer before the web page was loaded? If so, using your captured packets in Wireshark, find the packets that allowed your computer to successfully load http://www.example.com. Take a screenshot of these packets, and explain why you think these are the correct packets. If not, explain why your computer did not need to take these steps.







6. Were any steps taken by your computer before the web page was loaded? If so, using your captured packets in Wireshark, find the packets that allowed your computer to successfully load http://216.58.193.68. Take a screenshot of these packets, and explain why you think these are the correct packets. If not, explain why your computer did not need to take these steps.

```
    66 3.079019000 10.0.2.15        128.114.142.6    DNS         79 Standard query 0xe9f6  A fonts.gstatic.com
    67 3.080769000 128.114.142.6    10.0.2.15        DNS        134 Standard query response 0xe9f6  CNAME gstaticadssl.l.google.com A 172.217.5.99
```

7. Take a screenshot of the packets corresponding to your request, and the response from the server. If the request was resolved, what is the IP address you were given for www.google.com?

```
    23 9.983497000 10.0.2.15        128.114.142.6    DNS         76 Standard query 0x530e  A www.google.com
    24 9.986096000 128.114.142.6    10.0.2.15        DNS         92 Standard query response 0x530e  A 172.217.5.100
```

The IP address given for is 172.217.5.100

8. Did your computer want to complete the request recursively? How do you know? Take a screenshot proving your answer.

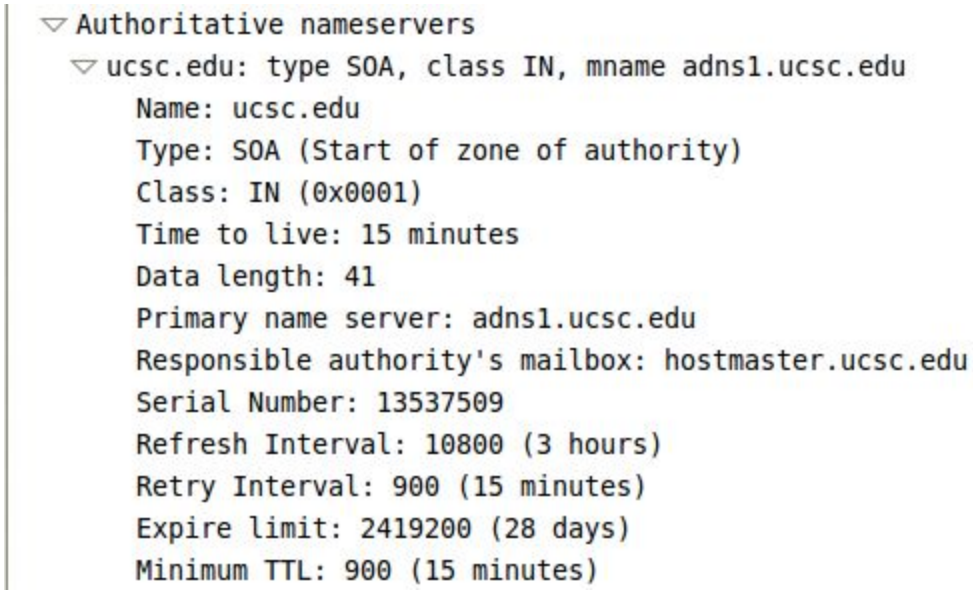
```
▷ Frame 23: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
▷ Linux cooked capture
▷ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 128.114.142.6 (128.114.142.6)
▷ User Datagram Protocol, Src Port: 51297 (51297), Dst Port: domain (53)
▽ Domain Name System (query)
    [Response In: 24]
    Transaction ID: 0x530e
  ▽ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▷ www.google.com: type A, class IN
```

In the packet file, the recursion flag is set on.

9. Take a screenshot of the packets corresponding to your request, and the response from the server. If the request was resolved, what is the IP address you were given for cmpe150.ucsc.edu?

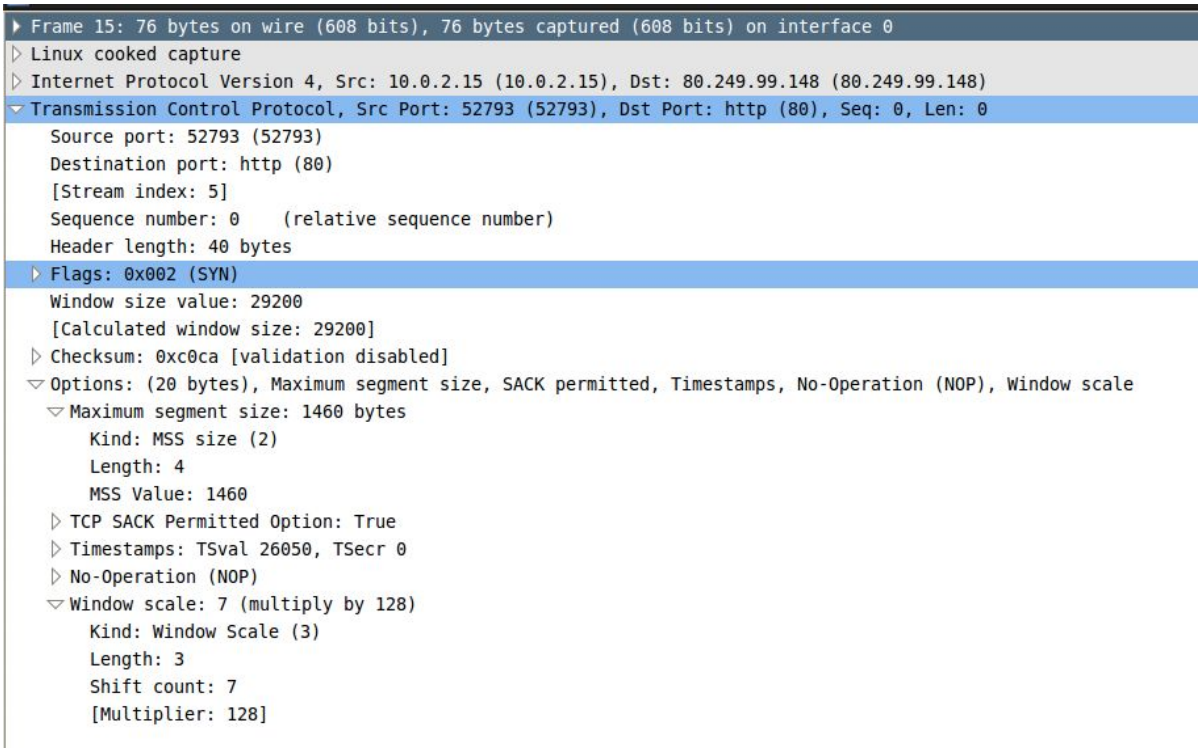
7	2.427641000	10.0.2.15	128.114.142.6	DNS	89 Standard query 0x9aff A cmpe150.ucsc.edu
8	2.430205000	128.114.142.6	10.0.2.15	DNS	142 Standard query response 0x9aff No such name

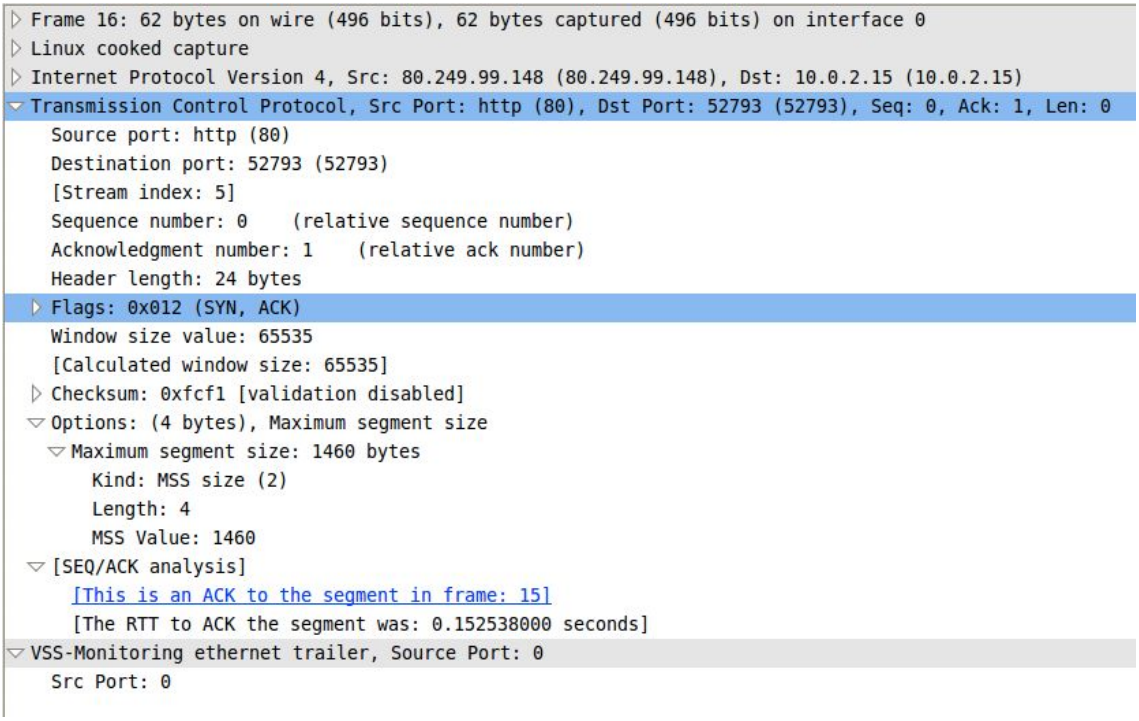
10. What is the authoritative name server for the ucsc.edu domain? How do you know? Take a screenshot proving your answer.



Part 3: TCP

11. Find the packets corresponding to the SYN, SYN-ACK, and ACK that initiated the TCP connection for this file transfer. Take a screenshot of these packets. What was the initial window size that your computer advertised to the server? What was the initial window size that the server advertised to you?



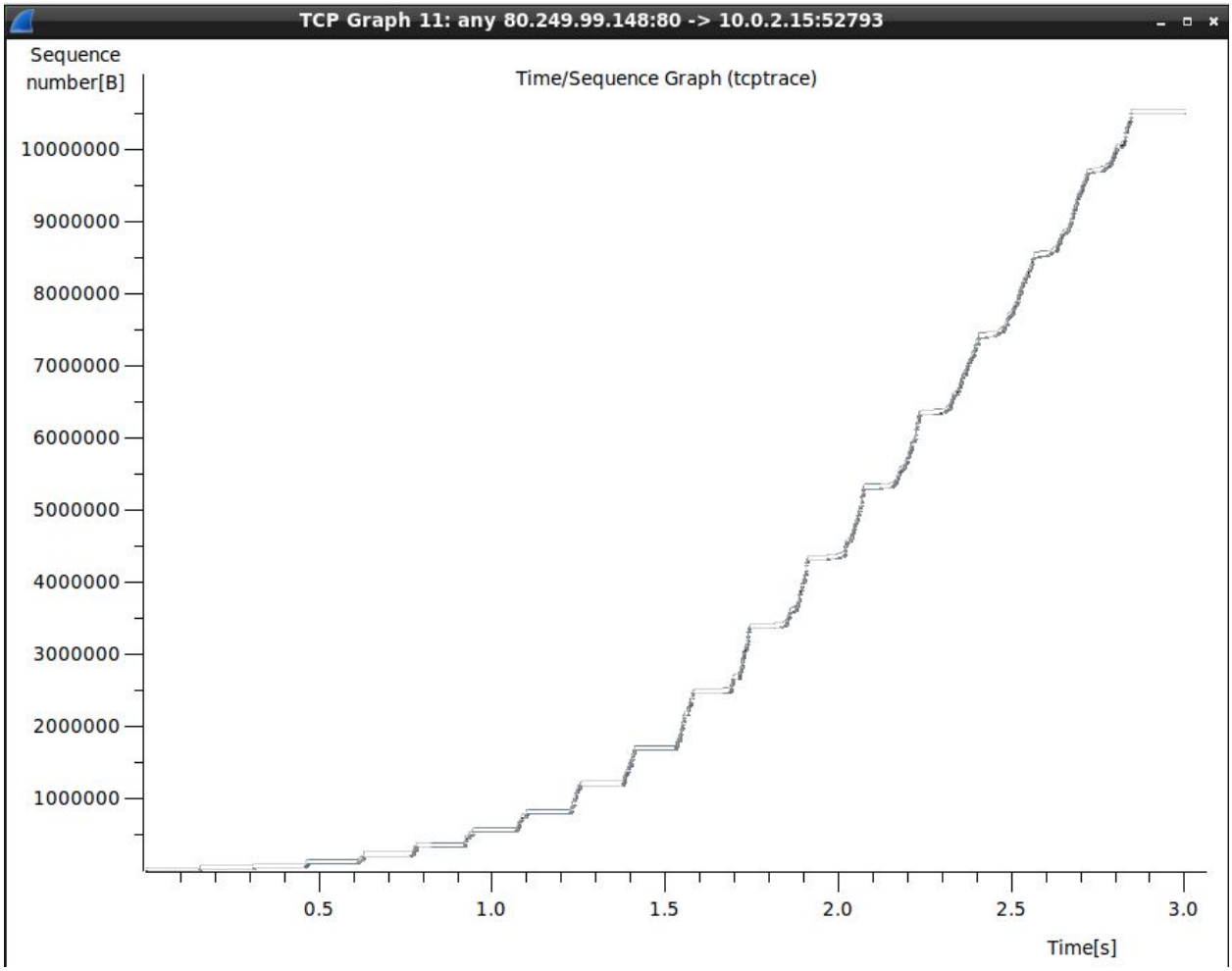


```
▸ Frame 17: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
▷ Linux cooked capture
▷ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 80.249.99.148 (80.249.99.148)
▽ Transmission Control Protocol, Src Port: 52793 (52793), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
    Source port: 52793 (52793)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header length: 20 bytes
  ▽ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
    Window size value: 29200
    [Calculated window size: 29200]
    [Window size scaling factor: -2 (no window scaling used)]
  ▷ Checksum: 0xc0b6 [validation disabled]
  ▽ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 16]
      [The RTT to ACK the segment was: 0.000042000 seconds]
```

```
    13 4.196545000 128.114.142.6    10.0.2.15       DNS      157 Standard query response 0x317c  CNAME ipv4.download1.thinkbroadband.com A 80.249.99.148
    14 4.196575000 128.114.142.6    10.0.2.15       DNS      218 Standard query response 0xaf09  CNAME ipv4.download1.thinkbroadband.com
    15 4.197015000 10.0.2.15        80.249.99.148   TCP       76 52793 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=26050 TSecr=0 WS=128
    16 4.349553000 80.249.99.148    10.0.2.15       TCP       62 http > 52793 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
    17 4.349595000 10.0.2.15        80.249.99.148   TCP       56 52793 > http [ACK] Seq=1 Ack=1 Win=29200 Len=0
    18 4.352841000 10.0.2.15        80.249.99.148   HTTP     194 GET /10MB.zip HTTP/1.1
    19 4.353952000 80.249.99.148    10.0.2.15       TCP       62 http > 52793 [ACK] Seq=1 Ack=139 Win=65535 Len=0
    20 4.505244000 80.249.99.148    10.0.2.15       TCP     2694 [TCP segment of a reassembled PDU]
    21 4.505278000 10.0.2.15        80.249.99.148   TCP       56 52793 > http [ACK] Seq=139 Ack=2639 Win=34080 Len=0
    22 4.505812000 80.249.99.148    10.0.2.15       TCP     4316 [TCP segment of a reassembled PDU]
    23 4.505837000 10.0.2.15        80.249.99.148   TCP       56 52793 > http [ACK] Seq=139 Ack=6899 Win=42600 Len=0
    24 4.506278000 80.249.99.148    10.0.2.15       TCP     5736 [TCP segment of a reassembled PDU]
    25 4.506294000 10.0.2.15        80.249.99.148   TCP       56 52793 > http [ACK] Seq=139 Ack=12579 Win=53960 Len=0
```

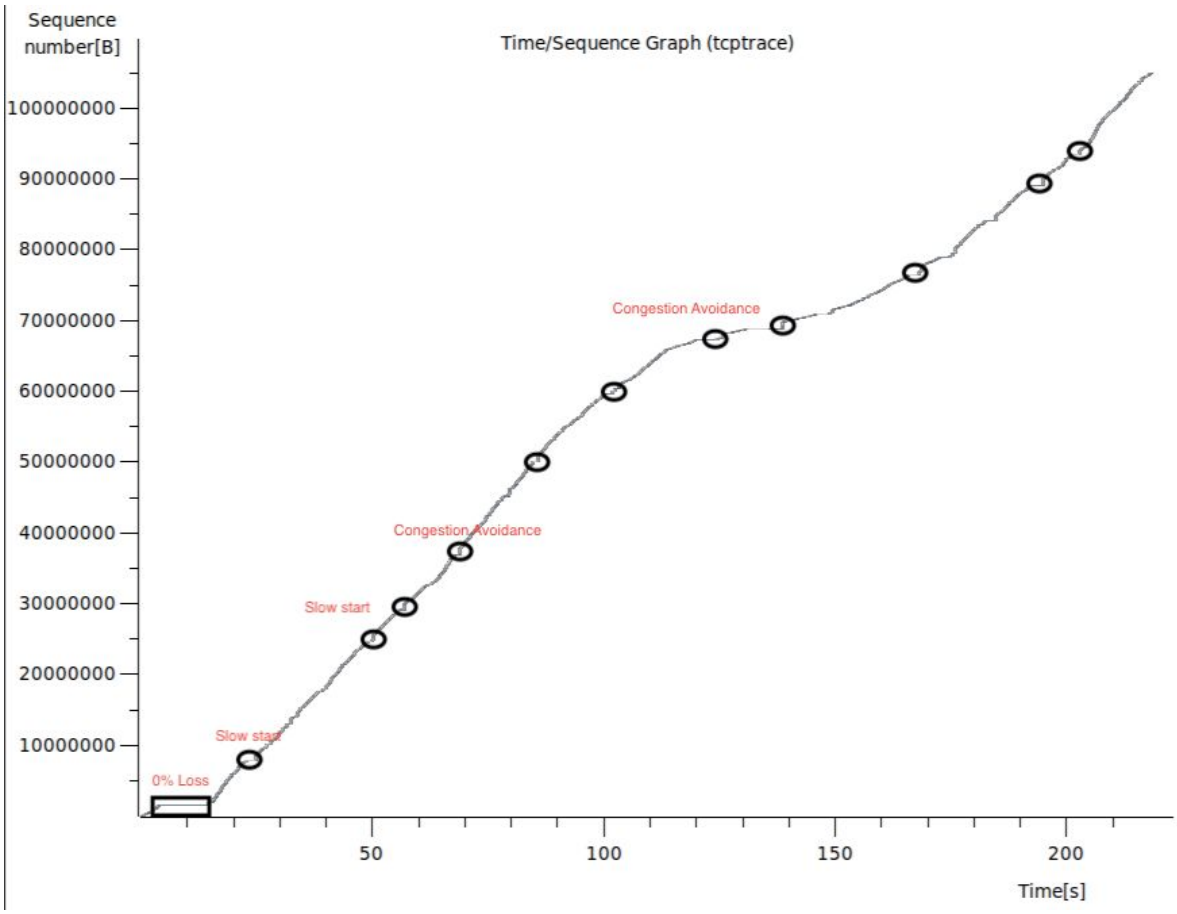
The initial window size the computer advertised to the server is 29200, the initial window size the server advertise to me is 65535.

12. Find a packet from the download whose source address is the server's address and the destination address is your computer's address. Using Wireshark, create a tcptrace graph with this packet selected. Take a screenshot of the graph and explain what it is showing. **Look into the Wireshark documentation if you need assistance making this graph.**



The graph is showing the receive window, the amount of bytes being sent, the TCP segments, and ACKs with the amount of bytes being sent over time.

13. Find a packet from the download whose source address is the address of the server and destination address is your computer's address. Create a tcptrace graph with this packet selected. Take a screenshot of the graph and explain what it is showing. Using an image editing program, circle the areas where the 0% loss is shown, as well as where TCP is in slow-start and congestion-avoidance.



The graph is showing the receive window, the amount of bytes being sent, the TCP segments, and ACKs with the amount of bytes being sent over time.