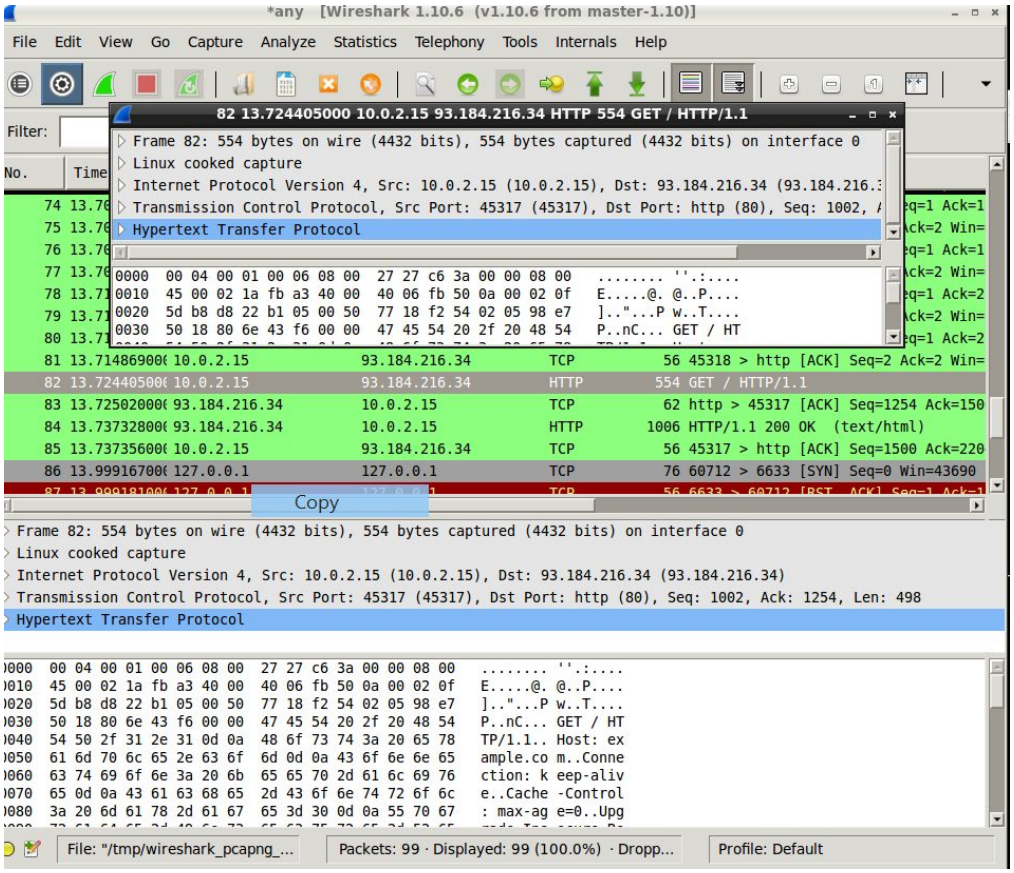
Peter Jiang
2/10/2019
CMPE150

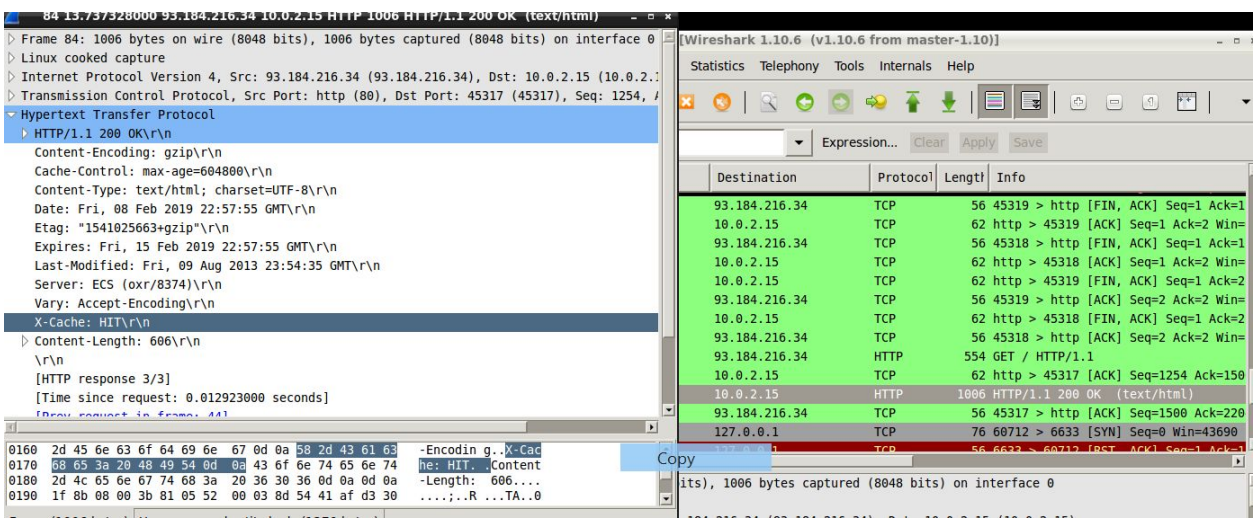
Lab 2

1.



The method HTTP method used is GET request. The URI is:
[Full request URI: http: //example.com]

2.

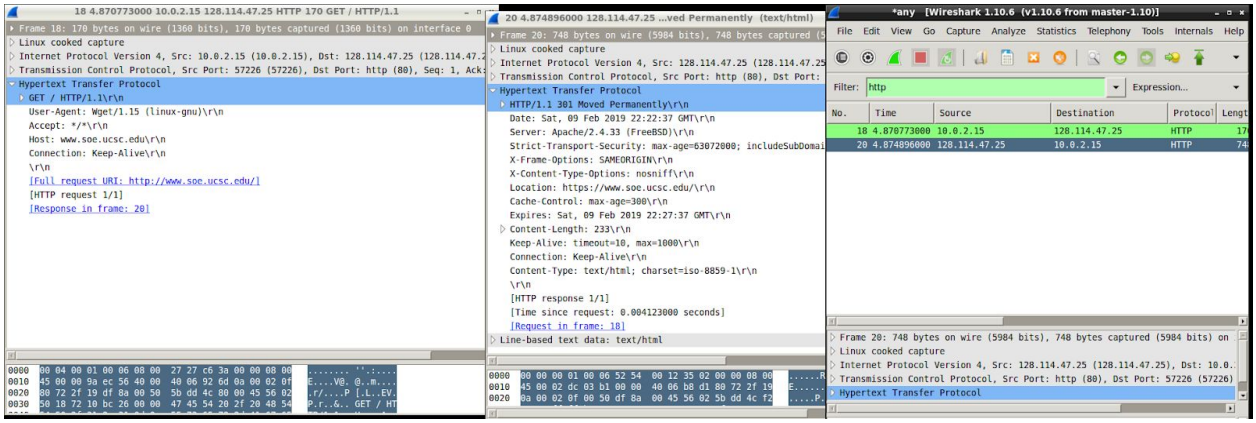


The HTTP status code is: HTTP/1.1.2.00 OK\r\n

Peter Jiang
2/10/2019
CMPE150

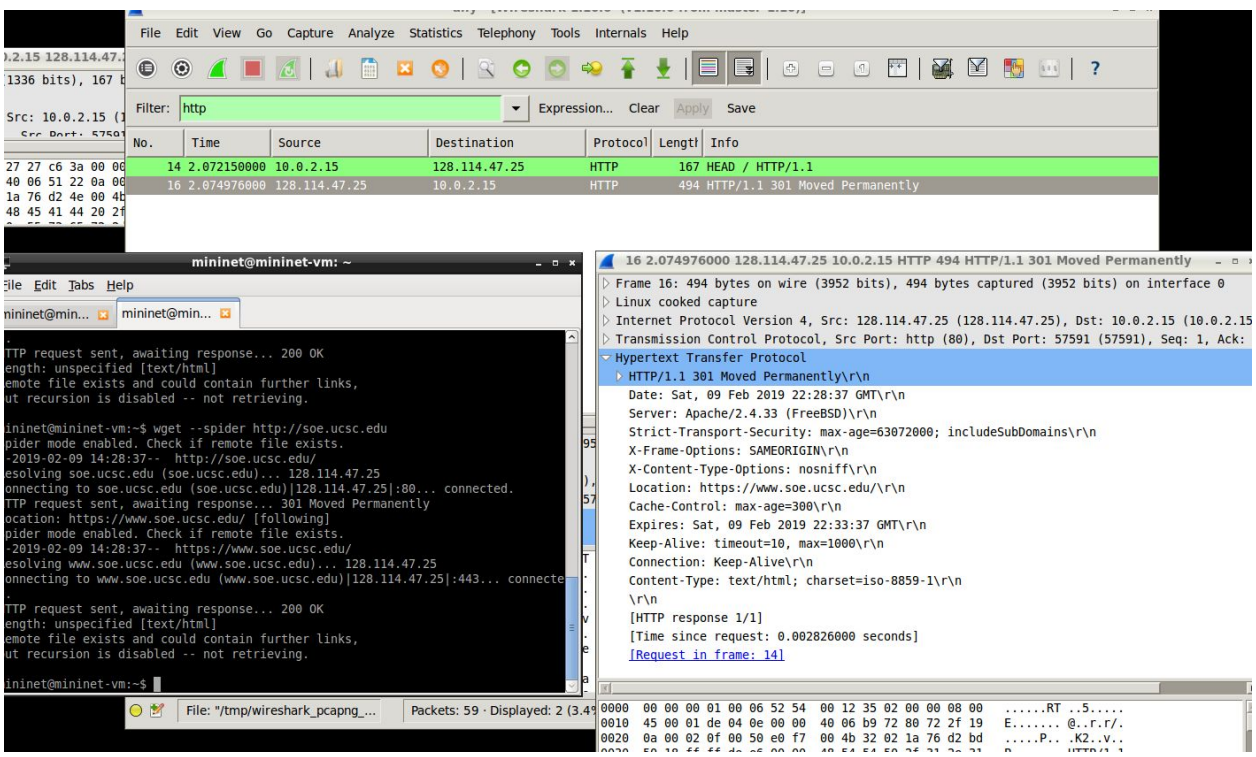
The Content Type is: text/html; charset=UTF8\r\n

3.



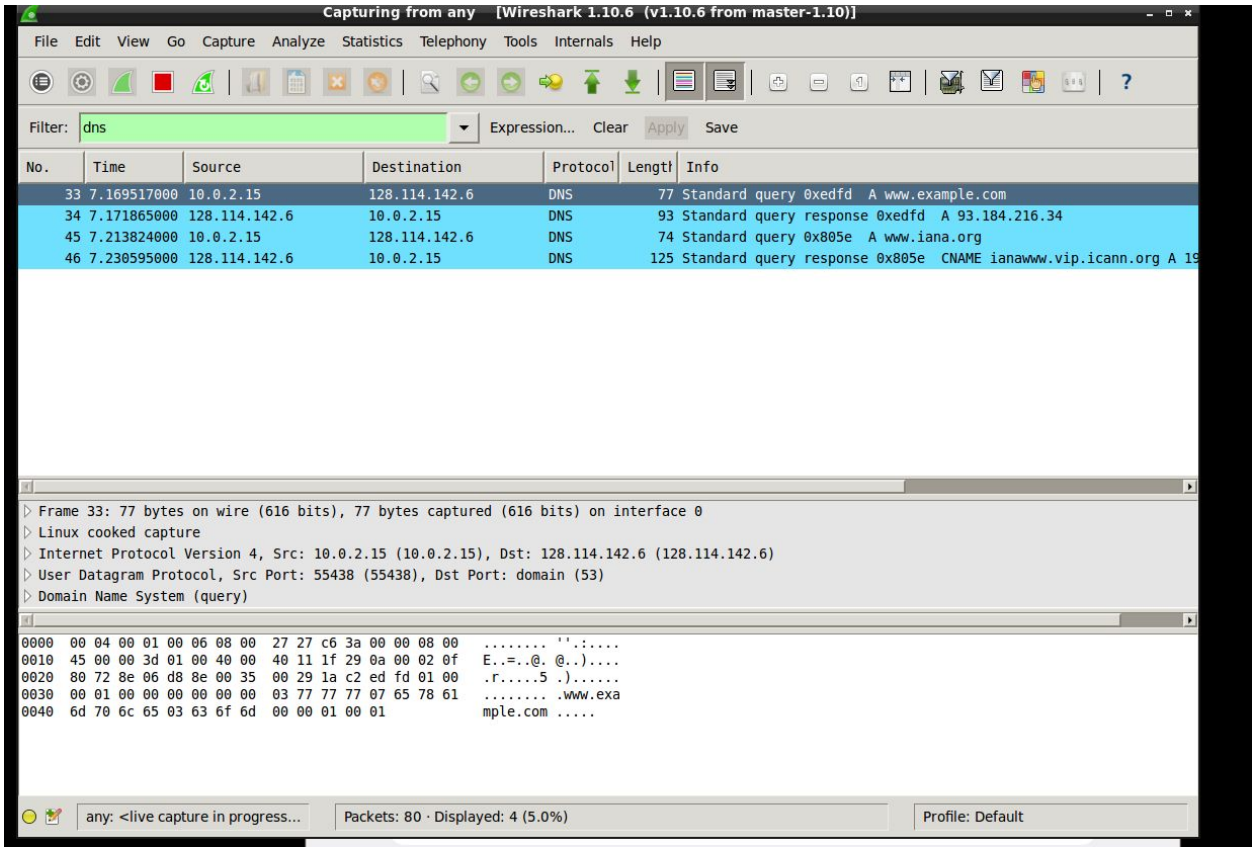
These packets are different because there is only one request and one response. The status code is 1.1.301 Moved Permanent.

4. Using the wget --spider command will create the HTTP request. Instead of using GET request it uses HEAD.



Peter Jiang
2/10/2019
CMPE150

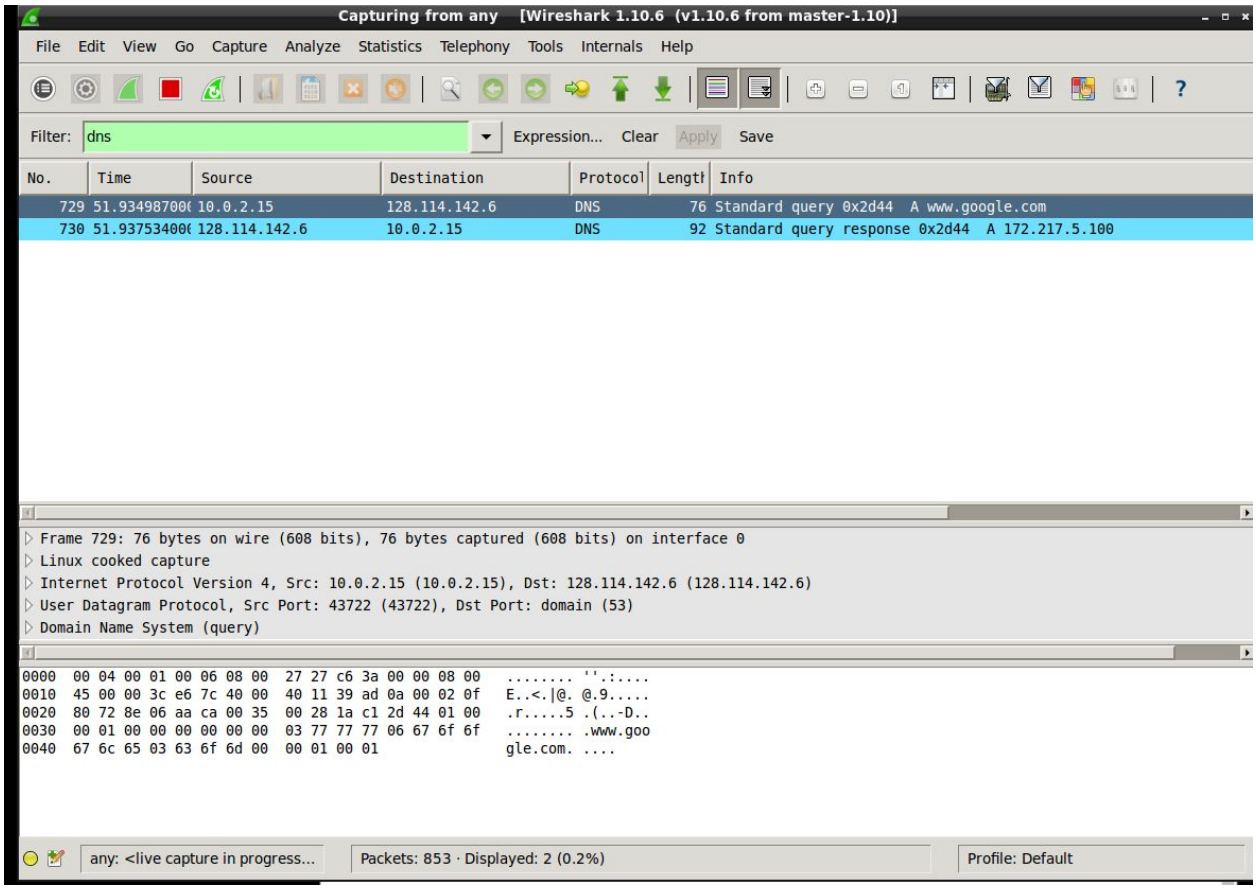
5.



These packets allow my computer to get to www.example.com
There is a Standard query and response, which allows the computer to direct to the correct site.

Peter Jiang
2/10/2019
CMPE150

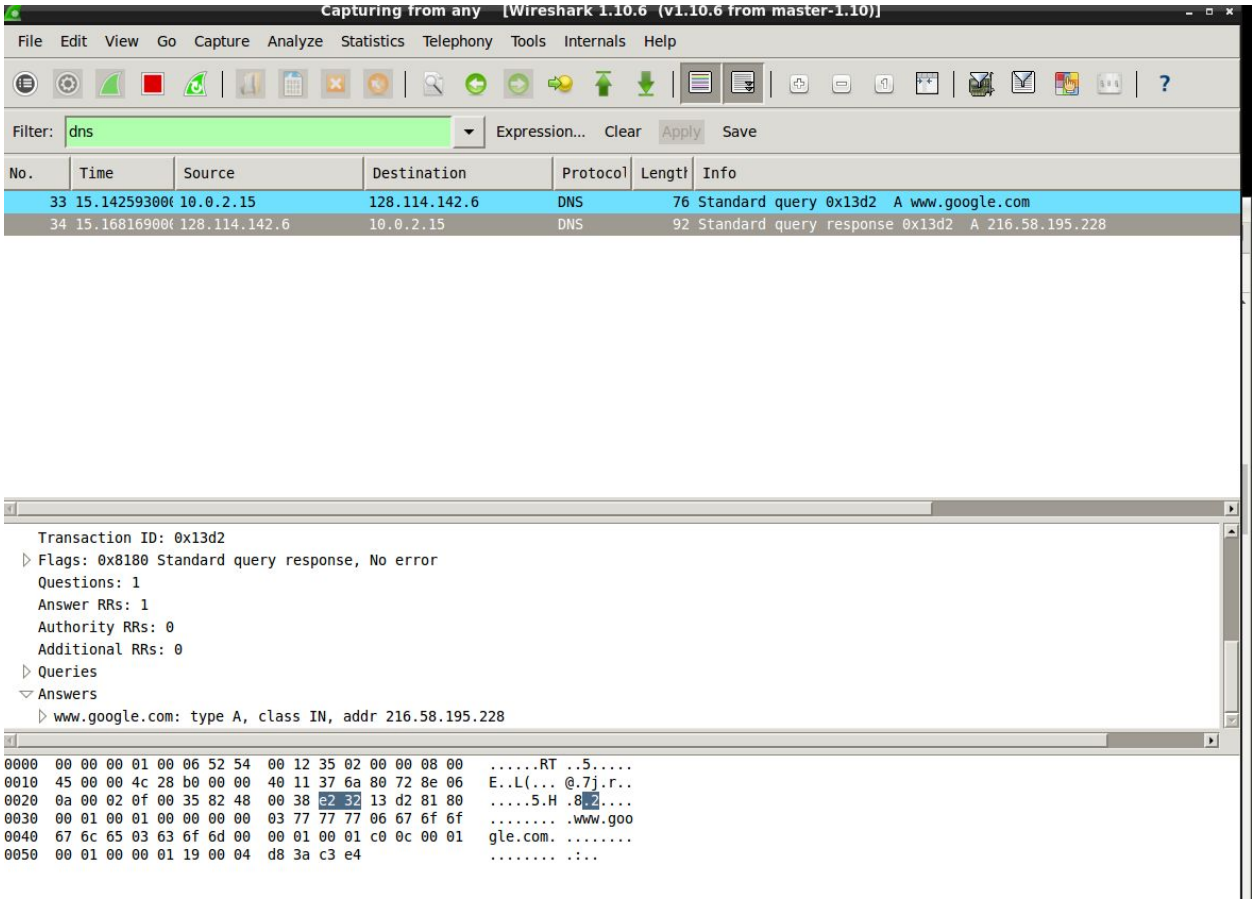
6.



Navigating to http://216.58.193.68. Will show these two packets. These are the correct packets because there is a single standard query and one standard query response.

Peter Jiang
2/10/2019
CMPE150

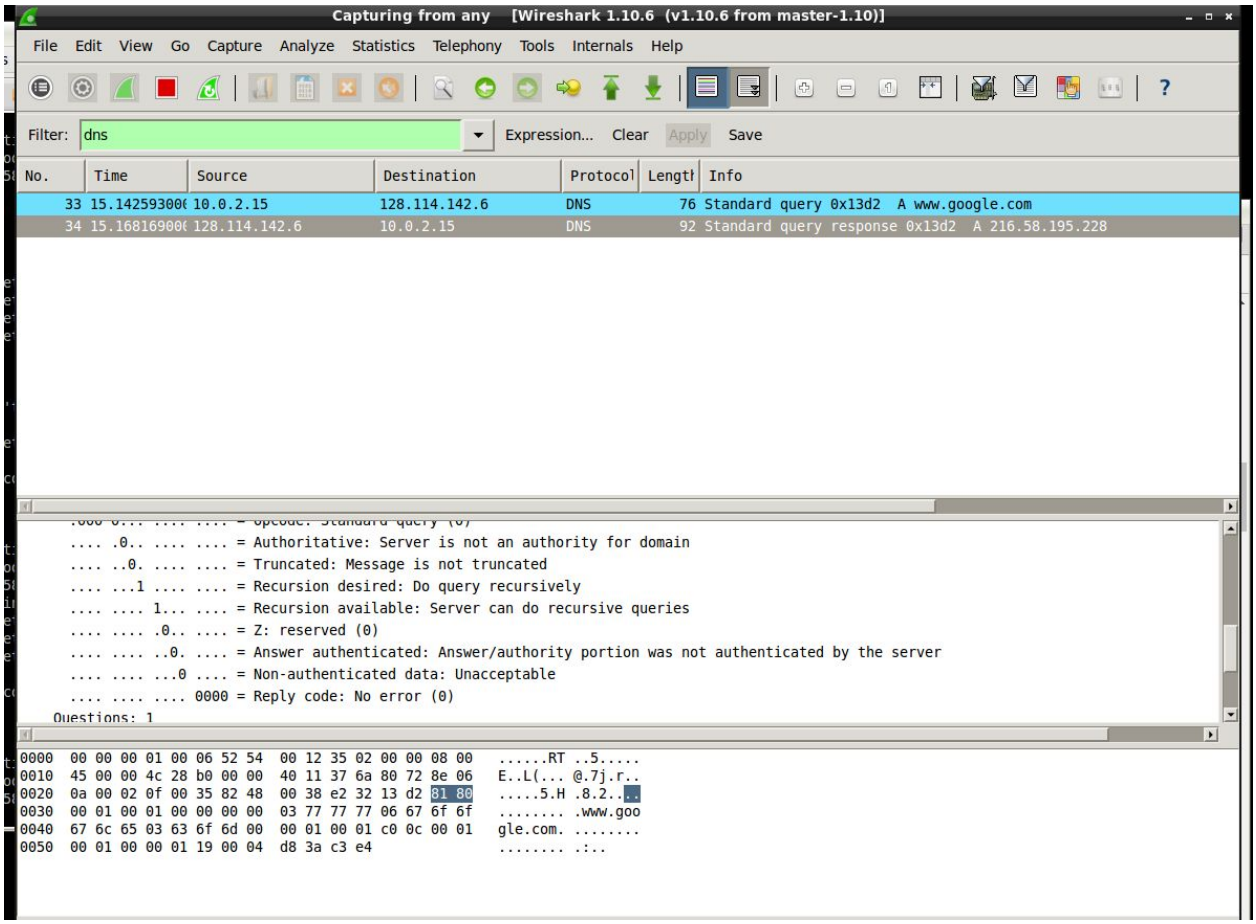
7.



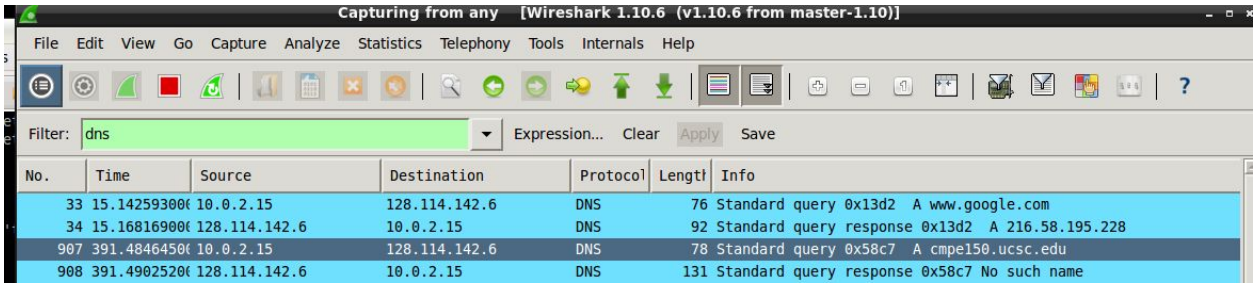
The IP address given is 216.58.195.228

Peter Jiang
2/10/2019
CMPE150

8. The computer wanted to complete the request recursively. I know this because under Flags, it states that Recursion is Desired: Do query recursively.



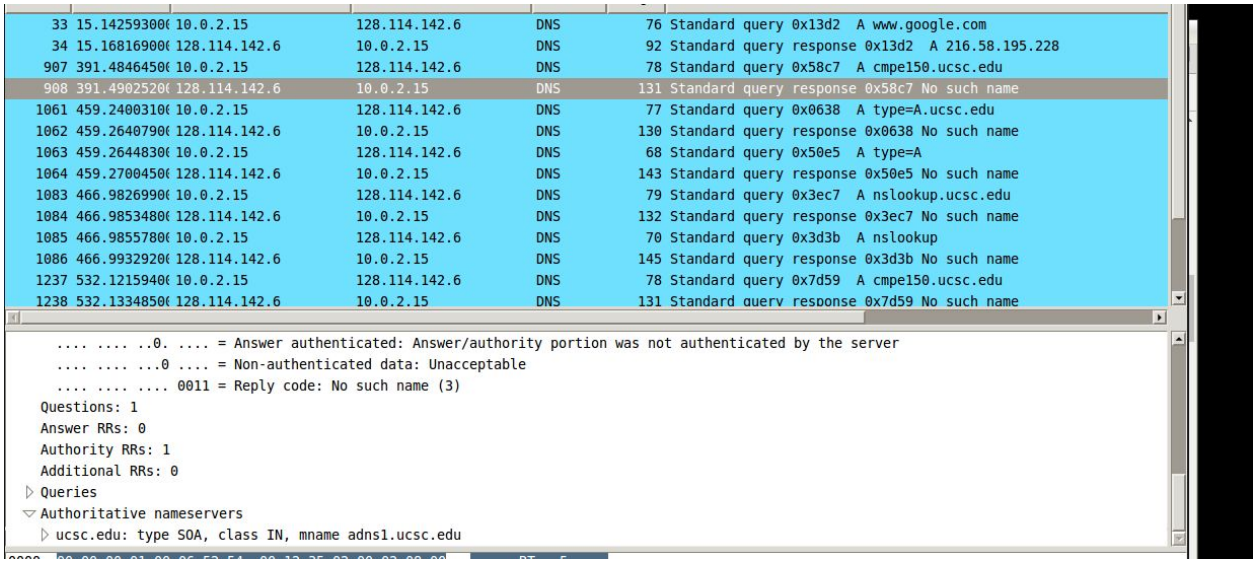
9.



The response to the Standard query is No such name. The server cannot get an IP address.

Peter Jiang
2/10/2019
CMPE150

10.

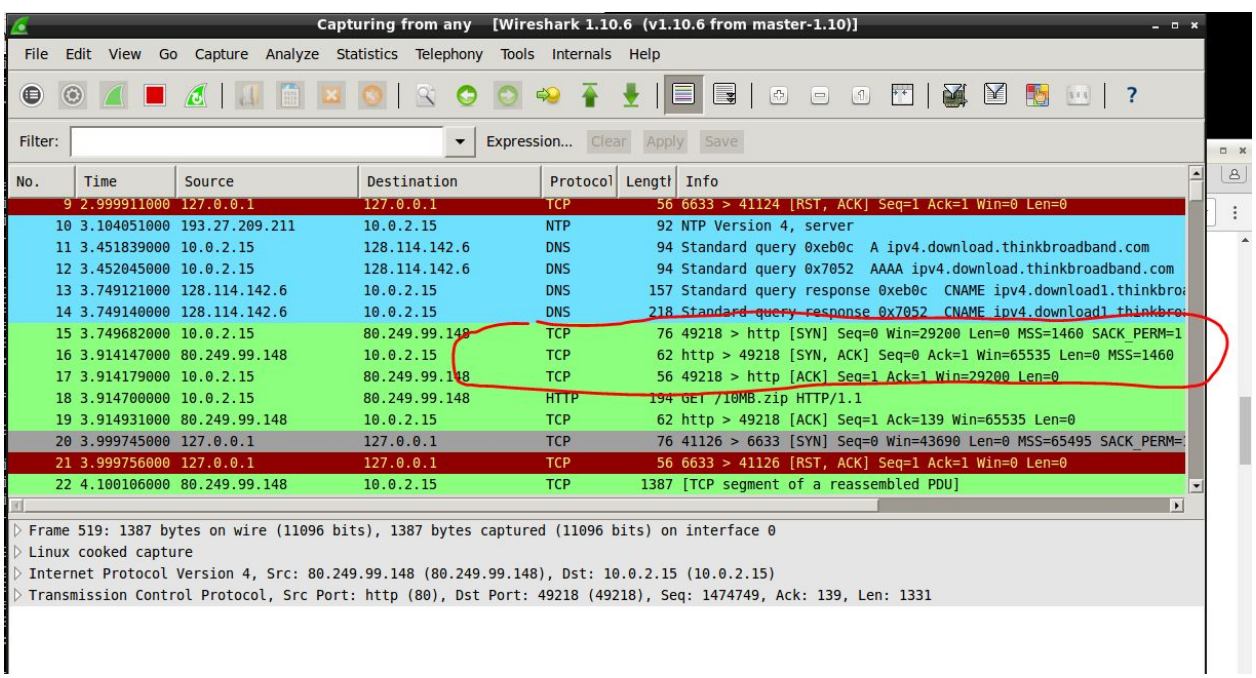


33	15.14259300(	10.0.2.15	128.114.142.6	DNS	76	Standard query 0x13d2 A www.google.com
34	15.16816900(	128.114.142.6	10.0.2.15	DNS	92	Standard query response 0x13d2 A 216.58.195.228
907	391.4846450(	10.0.2.15	128.114.142.6	DNS	78	Standard query 0x58c7 A cmpe150.ucsc.edu
908	391.4902520(	128.114.142.6	10.0.2.15	DNS	131	Standard query response 0x58c7 No such name
1061	459.2400310(	10.0.2.15	128.114.142.6	DNS	77	Standard query 0x0638 A type=A.ucsc.edu
1062	459.2640790(	128.114.142.6	10.0.2.15	DNS	130	Standard query response 0x0638 No such name
1063	459.2644830(	10.0.2.15	128.114.142.6	DNS	68	Standard query 0x50e5 A type=A
1064	459.2700450(	128.114.142.6	10.0.2.15	DNS	143	Standard query response 0x50e5 No such name
1083	466.9826990(	10.0.2.15	128.114.142.6	DNS	79	Standard query 0x3ec7 A nslookup.ucsc.edu
1084	466.9853480(	128.114.142.6	10.0.2.15	DNS	132	Standard query response 0x3ec7 No such name
1085	466.9855780(	10.0.2.15	128.114.142.6	DNS	70	Standard query 0x3d3b A nslookup
1086	466.9932920(	128.114.142.6	10.0.2.15	DNS	145	Standard query response 0x3d3b No such name
1237	532.1215940(	10.0.2.15	128.114.142.6	DNS	78	Standard query 0x7d59 A cmpe150.ucsc.edu
1238	532.1334850(	128.114.142.6	10.0.2.15	DNS	131	Standard query response 0x7d59 No such name

```
.... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
.... .... ...0 .... = Non-authenticated data: Unacceptable
.... .... .... 0011 = Reply code: No such name (3)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
▷ Queries
▽ Authoritative nameservers
  ▷ ucsc.edu: type SOA, class IN, mname adns1.ucsc.edu
```

The authoritative name server is ucsc.edu: type SOA, class IN, mname adns1.ucsc.edu
This is under the response query information.

11.



Capturing from any [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

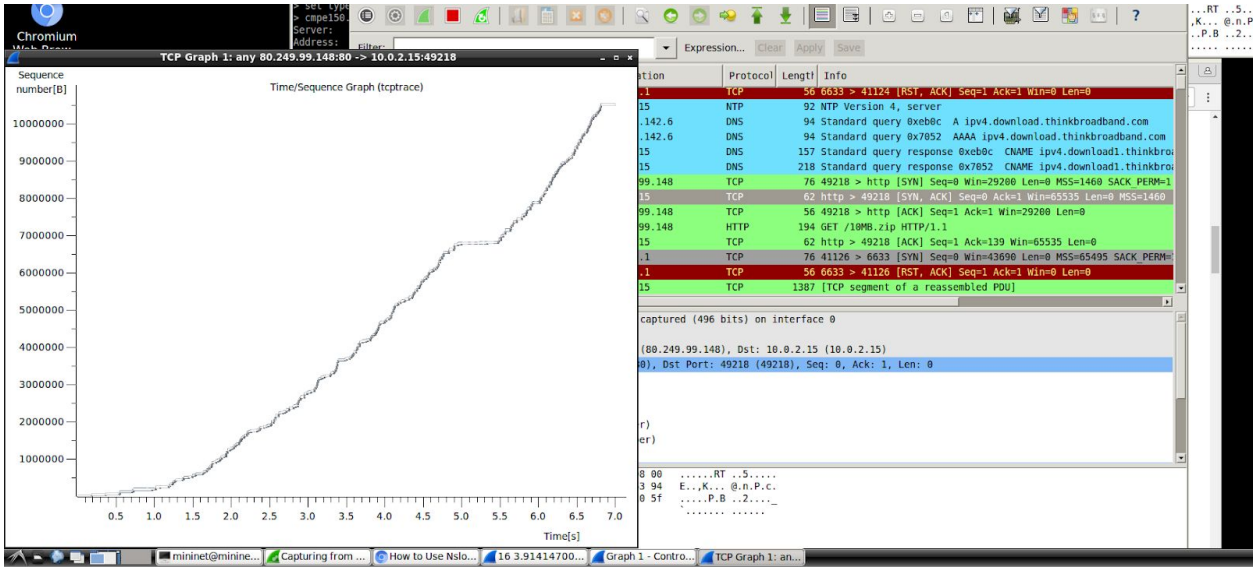
No.	Time	Source	Destination	Protocol	Length	Info
9	2.999911000	127.0.0.1	127.0.0.1	TCP	56	6633 > 41124 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	3.104051000	193.27.209.211	10.0.2.15	NTP	92	NTP Version 4, server
11	3.451839000	10.0.2.15	128.114.142.6	DNS	94	Standard query 0xeb0c A ipv4.download.thinkbroadband.com
12	3.452045000	10.0.2.15	128.114.142.6	DNS	94	Standard query 0x7052 AAAA ipv4.download.thinkbroadband.com
13	3.749121000	128.114.142.6	10.0.2.15	DNS	157	Standard query response 0xeb0c CNAME ipv4.download1.thinkbroa
14	3.749140000	128.114.142.6	10.0.2.15	DNS	218	Standard query response 0x7052 CNAME ipv4.download1.thinkbro
15	3.749682000	10.0.2.15	80.249.99.148	TCP	76	49218 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
16	3.914147000	80.249.99.148	10.0.2.15	TCP	62	http > 49218 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
17	3.914179000	10.0.2.15	80.249.99.148	TCP	56	49218 > http [ACK] Seq=1 Ack=1 Win=29200 Len=0
18	3.914700000	10.0.2.15	80.249.99.148	HTTP	194	GET /10MB.zip HTTP/1.1
19	3.914931000	80.249.99.148	10.0.2.15	TCP	62	http > 49218 [ACK] Seq=1 Ack=139 Win=65535 Len=0
20	3.999745000	127.0.0.1	127.0.0.1	TCP	76	41126 > 6633 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=
21	3.999756000	127.0.0.1	127.0.0.1	TCP	56	6633 > 41126 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	4.100106000	80.249.99.148	10.0.2.15	TCP	1387	[TCP segment of a reassembled PDU]

```
▷ Frame 519: 1387 bytes on wire (11096 bits), 1387 bytes captured (11096 bits) on interface 0
▷ Linux cooked capture
▷ Internet Protocol Version 4, Src: 80.249.99.148 (80.249.99.148), Dst: 10.0.2.15 (10.0.2.15)
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: 49218 (49218), Seq: 1474749, Ack: 139, Len: 1331
```

The original window size stated by my computer is : 29200
The initial window size the server advertised is: 65535

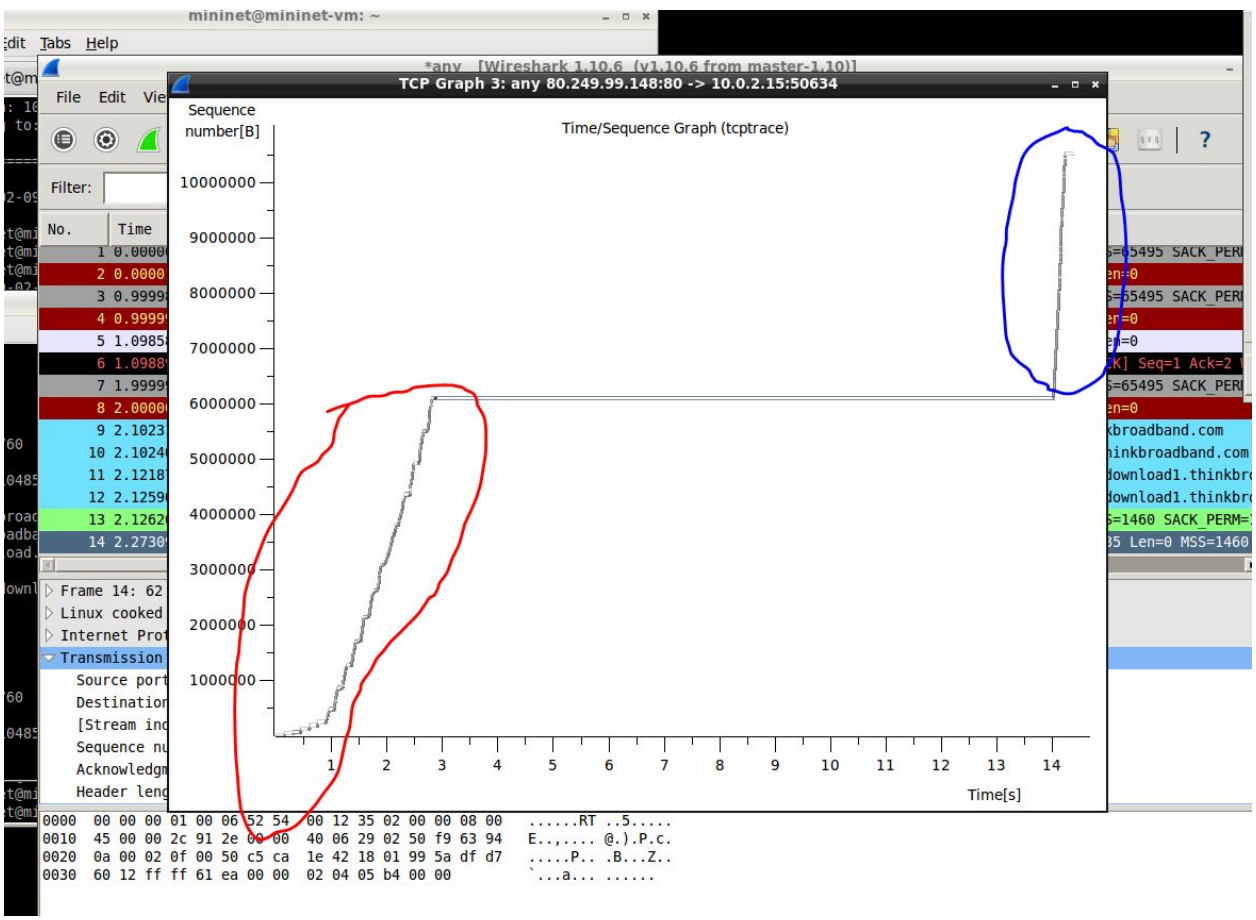
Peter Jiang
2/10/2019
CMPE150

12.



This graph represents slow start, which means only one packet is sent with each acknowledgement. It is showing sequence numbers compared to time.

13.



Peter Jiang
2/10/2019
CMPE150

This graph is showing three parts: First shows the slow start curved part sloping up. The horizontal part of the graph is where the 100% loss occurs because no packets are being sent. Then the last part of the graph is the congestion where the line is straight up.
Red Circle is 0% Loss and Slow Start
Blue Circle is congestion avoidance