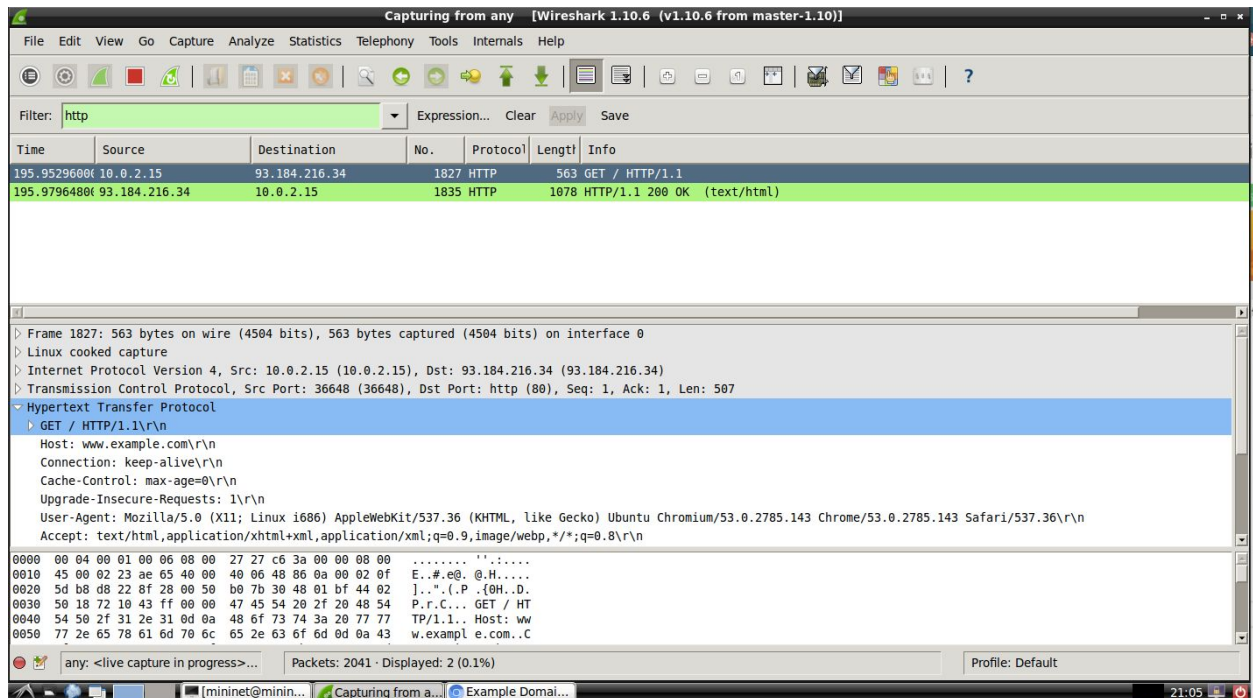


Part 1: HTTP

1.



The method that my computer used was GET

The URI used was www.example.com

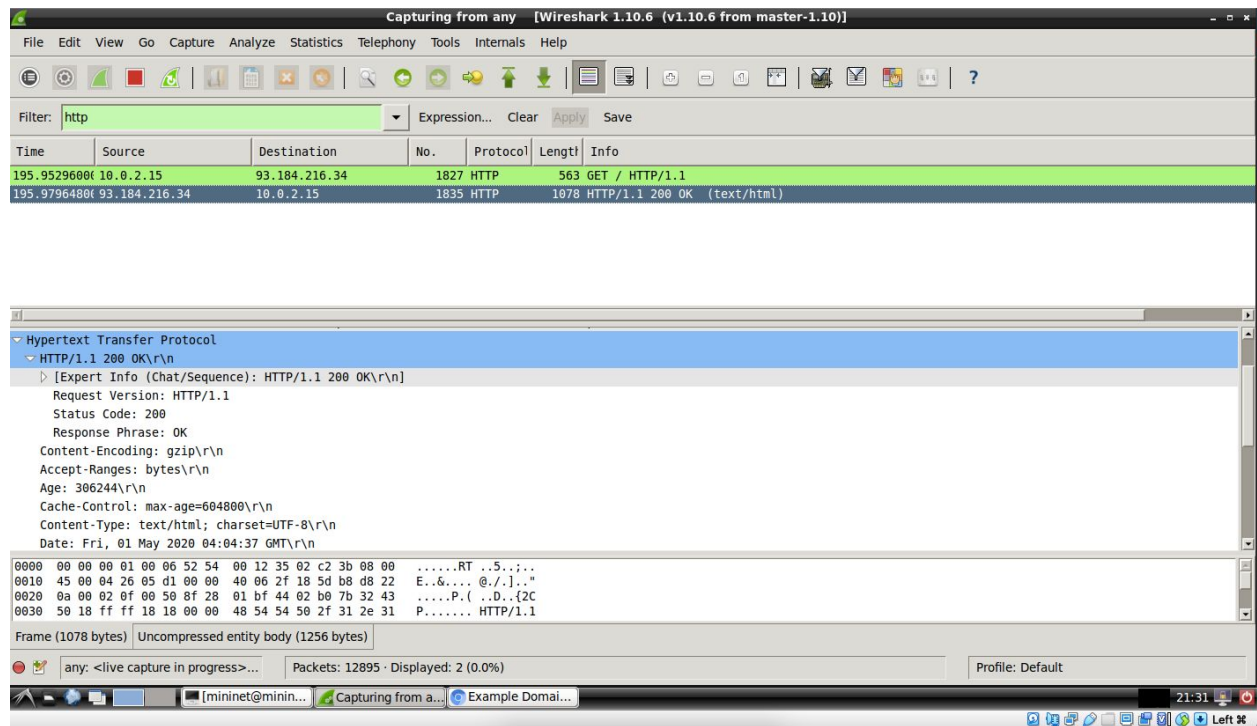
Request URI: /

URI = uniform resource identifier

Can be a name, locator, or both for an online recourse, but a URL is just the locator.

URL = uniform resource locator

2.

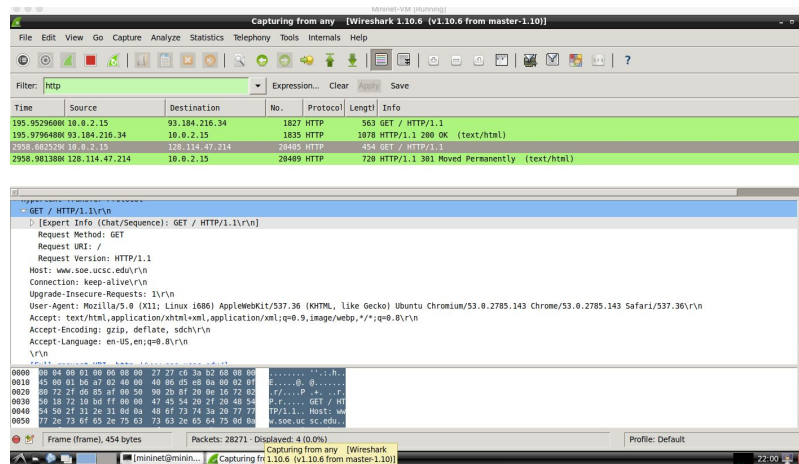


It returned status code: 200

The content type is: text/html; charset=UTF-8

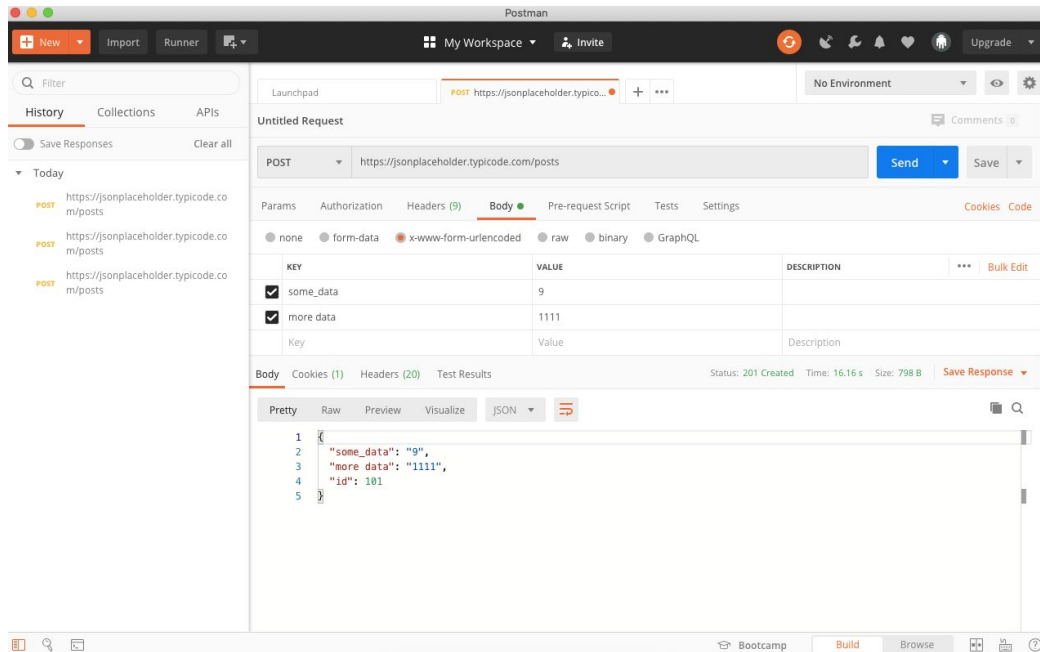
The status code 200 means: standard response for successful HTTP requests

3.

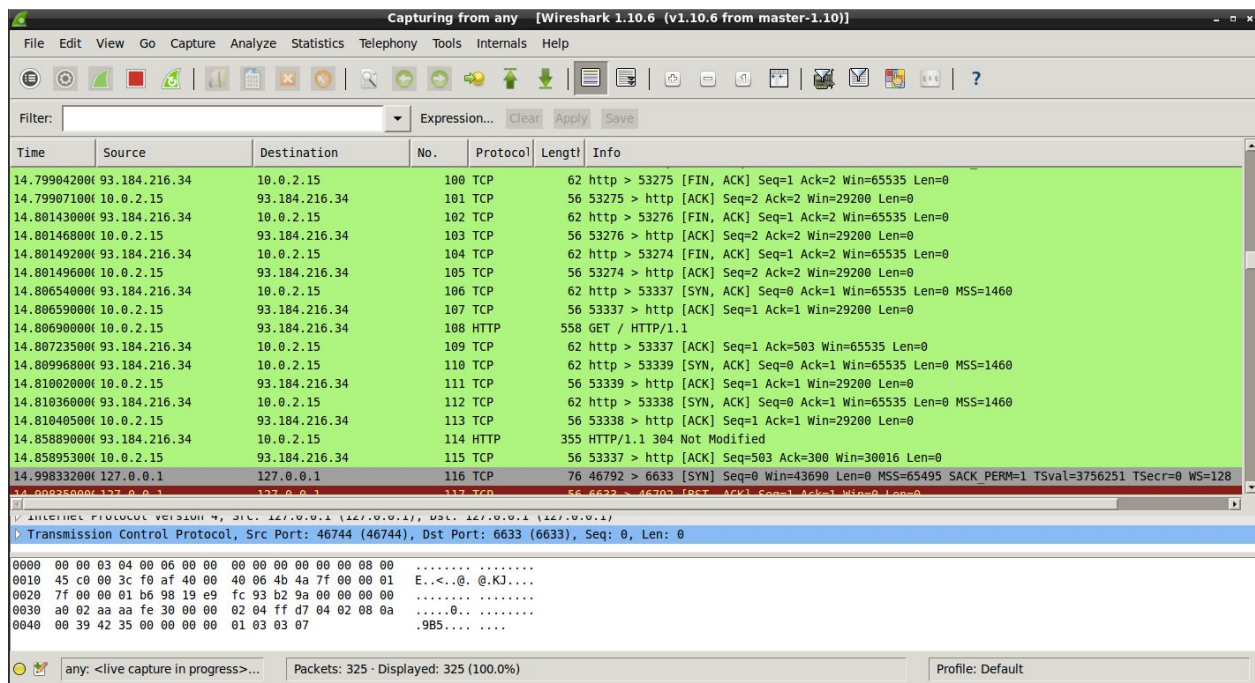


Here are the screenshots for the initial http request and response. The difference is that the hypertext transfer protocol was moved permanently and its status code is 301

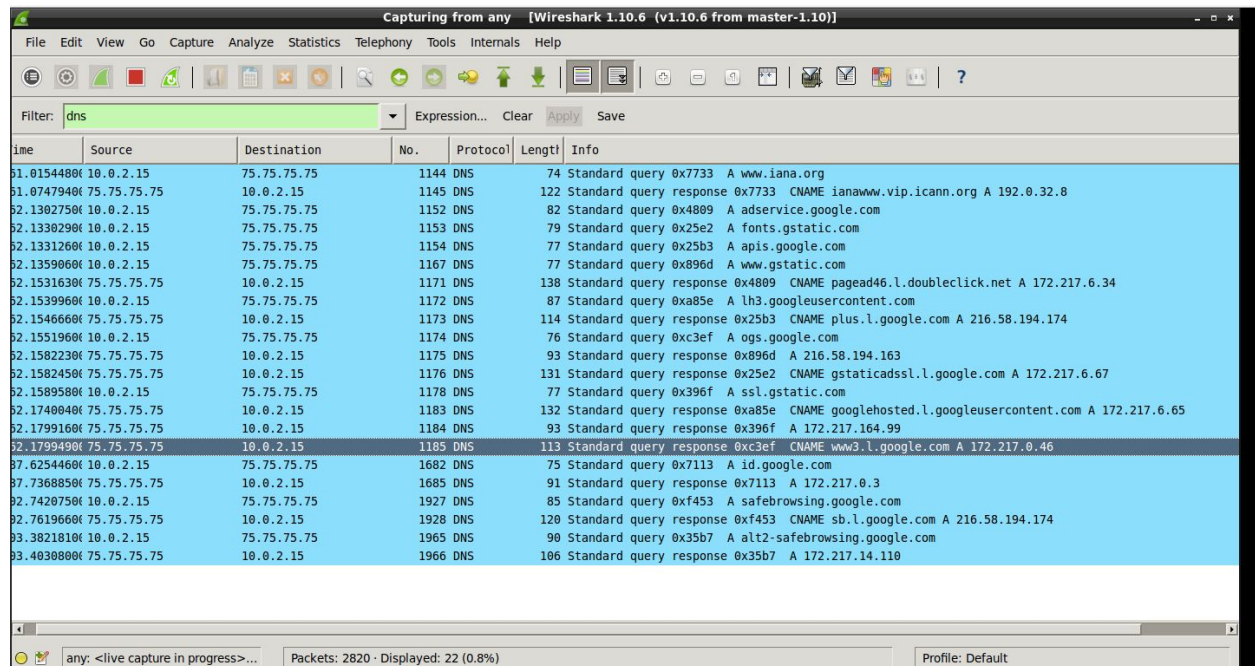
4. I figured out how to get postman to work and then I created an account. I then set the drop down bar to “POST” and then entered the URL: <https://jsonplaceholder.typicode.com/posts> into the URL slot. I then clicked on Body and then x-www-form-urlencoded and inserted a key with a value. I then sent the message and created a HTTP post message.



5. Several steps were taken the web page was loaded. The browser has to extract the domain name from the URL. The browser then queries DNS for the IP address. Then the first servers that the query interacts with are recursive resolvers. If the request was successful then the client machine now has an IP address. These are some of the steps taken before the page was loaded

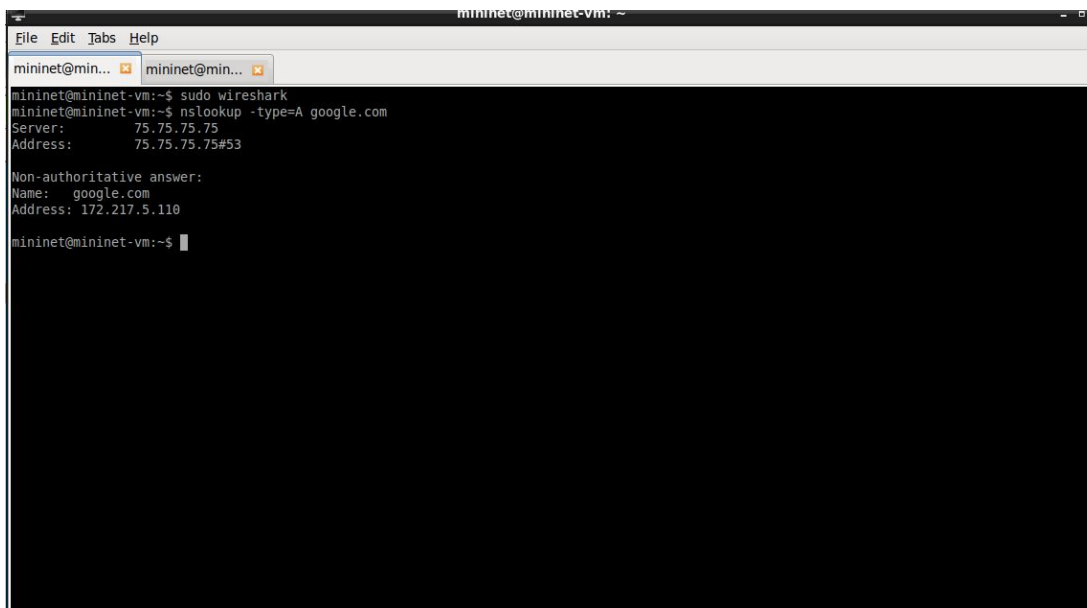


6. The computer already has the IP address so it will have a successful DNS request.



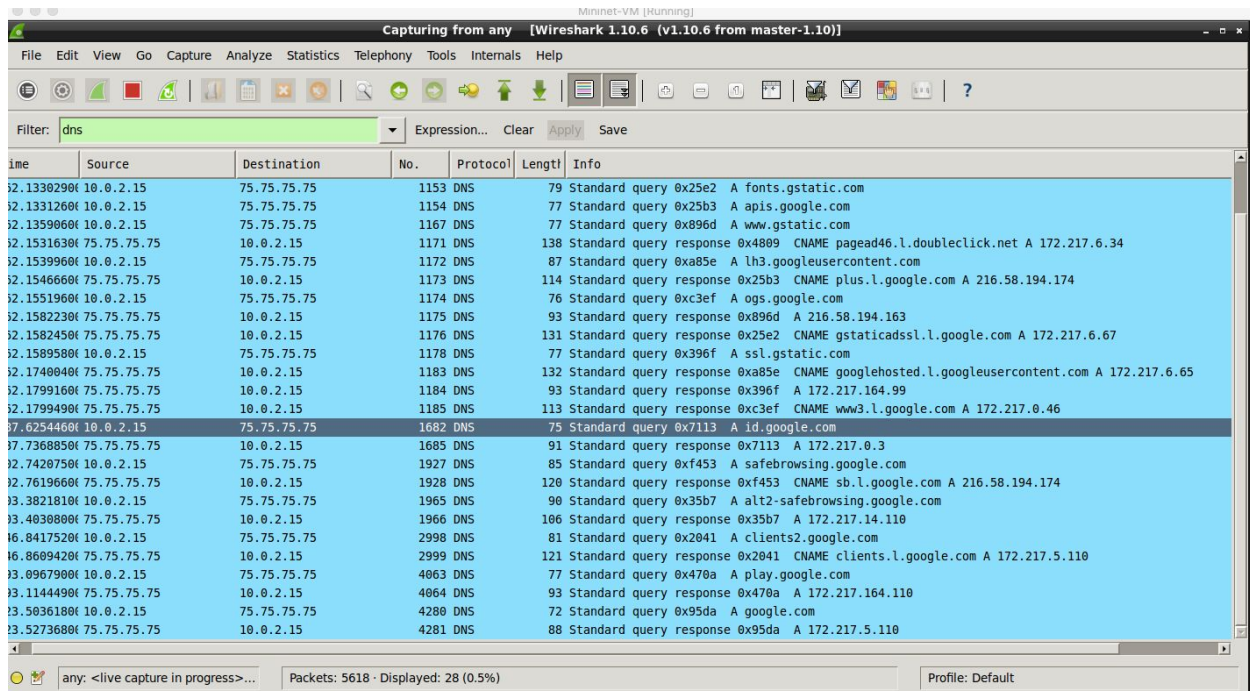
Time	Source	Destination	No.	Protocol	Length	Info
01.01544800	10.0.2.15	75.75.75.75	1144	DNS	74	Standard query 0x7733 A www.iana.org
01.07479400	75.75.75.75	10.0.2.15	1145	DNS	122	Standard query response 0x7733 CNAME ianawww.vip.icann.org A 192.0.32.8
02.13027500	10.0.2.15	75.75.75.75	1152	DNS	82	Standard query 0x4809 A adservice.google.com
02.13302900	10.0.2.15	75.75.75.75	1153	DNS	79	Standard query 0x25e2 A fonts.gstatic.com
02.13312600	10.0.2.15	75.75.75.75	1154	DNS	77	Standard query 0x25b3 A apis.google.com
02.13590600	10.0.2.15	75.75.75.75	1167	DNS	77	Standard query 0x896d A www.gstatic.com
02.15316300	75.75.75.75	10.0.2.15	1171	DNS	138	Standard query response 0x4809 CNAME pagead46.l.doubleclick.net A 172.217.6.34
02.15399600	10.0.2.15	75.75.75.75	1172	DNS	87	Standard query 0xa85e A lh3.googleusercontent.com
02.15466600	75.75.75.75	10.0.2.15	1173	DNS	114	Standard query response 0x25b3 CNAME plus.l.google.com A 216.58.194.174
02.15519600	10.0.2.15	75.75.75.75	1174	DNS	76	Standard query 0xc3ef A ogs.google.com
02.15822300	75.75.75.75	10.0.2.15	1175	DNS	93	Standard query response 0x896d A 216.58.194.163
02.15824500	75.75.75.75	10.0.2.15	1176	DNS	131	Standard query response 0x25e2 CNAME gstaticadssl.l.google.com A 172.217.6.67
02.15895800	10.0.2.15	75.75.75.75	1178	DNS	77	Standard query 0x396f A ssl.gstatic.com
02.17400400	75.75.75.75	10.0.2.15	1183	DNS	132	Standard query response 0xa85e CNAME googlehosted.l.googleusercontent.com A 172.217.6.65
02.17991600	75.75.75.75	10.0.2.15	1184	DNS	93	Standard query response 0x396f A 172.217.164.99
02.17994900	75.75.75.75	10.0.2.15	1185	DNS	113	Standard query response 0xc3ef CNAME www3.l.google.com A 172.217.0.46
07.62544600	10.0.2.15	75.75.75.75	1682	DNS	75	Standard query 0x7113 A id.google.com
07.73688500	75.75.75.75	10.0.2.15	1685	DNS	91	Standard query response 0x7113 A 172.217.0.3
02.74207500	10.0.2.15	75.75.75.75	1927	DNS	85	Standard query 0xf453 A safebrowsing.google.com
02.76196600	75.75.75.75	10.0.2.15	1928	DNS	120	Standard query response 0xf453 CNAME sb.l.google.com A 216.58.194.174
03.38218100	10.0.2.15	75.75.75.75	1965	DNS	90	Standard query 0x35b7 A alt2-safebrowsing.google.com
03.40308000	75.75.75.75	10.0.2.15	1966	DNS	106	Standard query response 0x35b7 A 172.217.14.110

7.
IP Address: 172.217.5.110



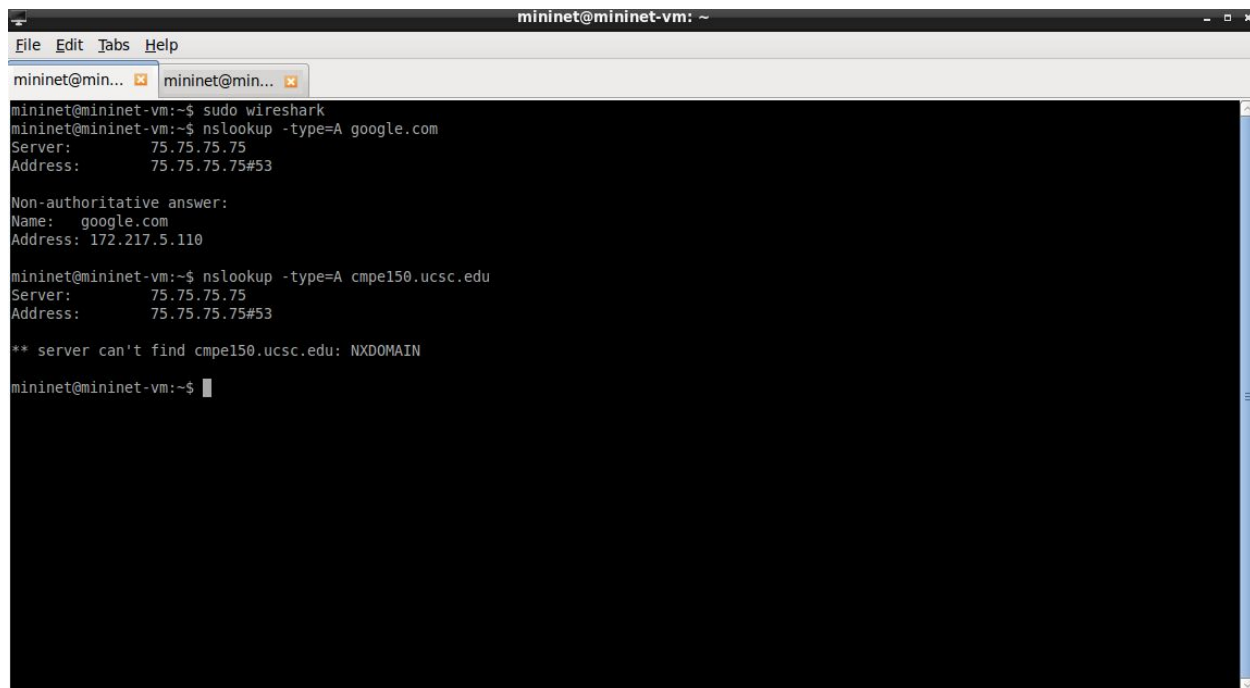
```
mininet@mininet-vm: ~  
File Edit Tabs Help  
mininet@mininet-vm:~$ sudo wireshark  
mininet@mininet-vm:~$ nslookup -type=A google.com  
Server: 75.75.75.75  
Address: 75.75.75.75#53  
  
Non-authoritative answer:  
Name: google.com  
Address: 172.217.5.110  
  
mininet@mininet-vm:~$
```


8.yes it is being solved recursively with server 75.75.75.75



Time	Source	Destination	No.	Protocol	Length	Info
32.13302900	10.0.2.15	75.75.75.75	1153	DNS	79	Standard query 0x25e2 A fonts.gstatic.com
32.13312600	10.0.2.15	75.75.75.75	1154	DNS	77	Standard query 0x25b3 A apis.google.com
32.13590600	10.0.2.15	75.75.75.75	1167	DNS	77	Standard query 0x896d A www.gstatic.com
32.15316300	75.75.75.75	10.0.2.15	1171	DNS	138	Standard query response 0x4809 CNAME pagead46.l.doubleclick.net A 172.217.6.34
32.15399600	10.0.2.15	75.75.75.75	1172	DNS	87	Standard query 0xa85e A lh3.googleusercontent.com
32.15466600	75.75.75.75	10.0.2.15	1173	DNS	114	Standard query response 0x25b3 CNAME plus.l.google.com A 216.58.194.174
32.15519600	10.0.2.15	75.75.75.75	1174	DNS	76	Standard query 0xc3ef A ogs.google.com
32.15822300	75.75.75.75	10.0.2.15	1175	DNS	93	Standard query response 0x896d A 216.58.194.163
32.15824500	75.75.75.75	10.0.2.15	1176	DNS	131	Standard query response 0x25e2 CNAME gstaticadssl.l.google.com A 172.217.6.67
32.15895800	10.0.2.15	75.75.75.75	1178	DNS	77	Standard query 0x396f A ssl.gstatic.com
32.17409400	75.75.75.75	10.0.2.15	1183	DNS	132	Standard query response 0xa85e CNAME googlehosted.l.googleusercontent.com A 172.217.6.65
32.17991600	75.75.75.75	10.0.2.15	1184	DNS	93	Standard query response 0x396f A 172.217.164.99
32.17994900	75.75.75.75	10.0.2.15	1185	DNS	113	Standard query response 0xc3ef CNAME www3.l.google.com A 172.217.0.46
37.62544600	10.0.2.15	75.75.75.75	1682	DNS	75	Standard query 0x7113 A id.google.com
37.73688500	75.75.75.75	10.0.2.15	1685	DNS	91	Standard query response 0x7113 A 172.217.0.3
37.74207500	10.0.2.15	75.75.75.75	1927	DNS	85	Standard query 0xf453 A safebrowsing.google.com
37.76196600	75.75.75.75	10.0.2.15	1928	DNS	120	Standard query response 0xf453 CNAME sb.l.google.com A 216.58.194.174
37.38218100	10.0.2.15	75.75.75.75	1965	DNS	90	Standard query 0x35b7 A alt2-safebrowsing.google.com
37.40308000	75.75.75.75	10.0.2.15	1966	DNS	106	Standard query response 0x35b7 A 172.217.14.110
37.84175200	10.0.2.15	75.75.75.75	2998	DNS	81	Standard query 0x2041 A clients2.google.com
37.86094200	75.75.75.75	10.0.2.15	2999	DNS	121	Standard query response 0x2041 CNAME clients.l.google.com A 172.217.5.110
37.09679000	10.0.2.15	75.75.75.75	4063	DNS	77	Standard query 0x470a A play.google.com
37.11444900	75.75.75.75	10.0.2.15	4064	DNS	93	Standard query response 0x470a A 172.217.164.110
37.50361800	10.0.2.15	75.75.75.75	4280	DNS	72	Standard query 0x95da A google.com
37.52736800	75.75.75.75	10.0.2.15	4281	DNS	88	Standard query response 0x95da A 172.217.5.110

9.It is not getting resolved



```
mininet@mininet-vm: ~  
File Edit Tabs Help  
mininet@min... mininet@min...  
mininet@mininet-vm:~$ sudo wireshark  
mininet@mininet-vm:~$ nslookup -type=A google.com  
Server: 75.75.75.75  
Address: 75.75.75.75#53  
  
Non-authoritative answer:  
Name: google.com  
Address: 172.217.5.110  
  
mininet@mininet-vm:~$ nslookup -type=A cmpe150.ucsc.edu  
Server: 75.75.75.75  
Address: 75.75.75.75#53  
  
** server can't find cmpe150.ucsc.edu: NXDOMAIN  
mininet@mininet-vm:~$
```

10. typing `nslookup -type=soa ucsc.edu` produces the solution: `adns1.ucsc.edu`

```
mininet@mininet-vm: ~  
File Edit Tabs Help  
mininet@min... mininet@min...  
  
mininet@mininet-vm:~$ nslookup -type=A cmpe150.ucsc.edu  
Server:      75.75.75.75  
Address:     75.75.75.75#53  
  
** server can't find cmpe150.ucsc.edu: NXDOMAIN  
  
mininet@mininet-vm:~$ nslookup -type=A ucsc.edu  
Server:      75.75.75.75  
Address:     75.75.75.75#53  
  
Non-authoritative answer:  
Name:   ucsc.edu  
Address: 128.114.109.5  
  
mininet@mininet-vm:~$ nslookup -type=soa ucsc.edu  
Server:      75.75.75.75  
Address:     75.75.75.75#53  
  
Non-authoritative answer:  
ucsc.edu  
    origin = adns1.ucsc.edu  
    mail addr = hostmaster.ucsc.edu  
    serial = 18622360  
    refresh = 10800  
    retry = 900  
    expire = 2419200  
    minimum = 900  
  
Authoritative answers can be found from:  
  
mininet@mininet-vm:~$
```

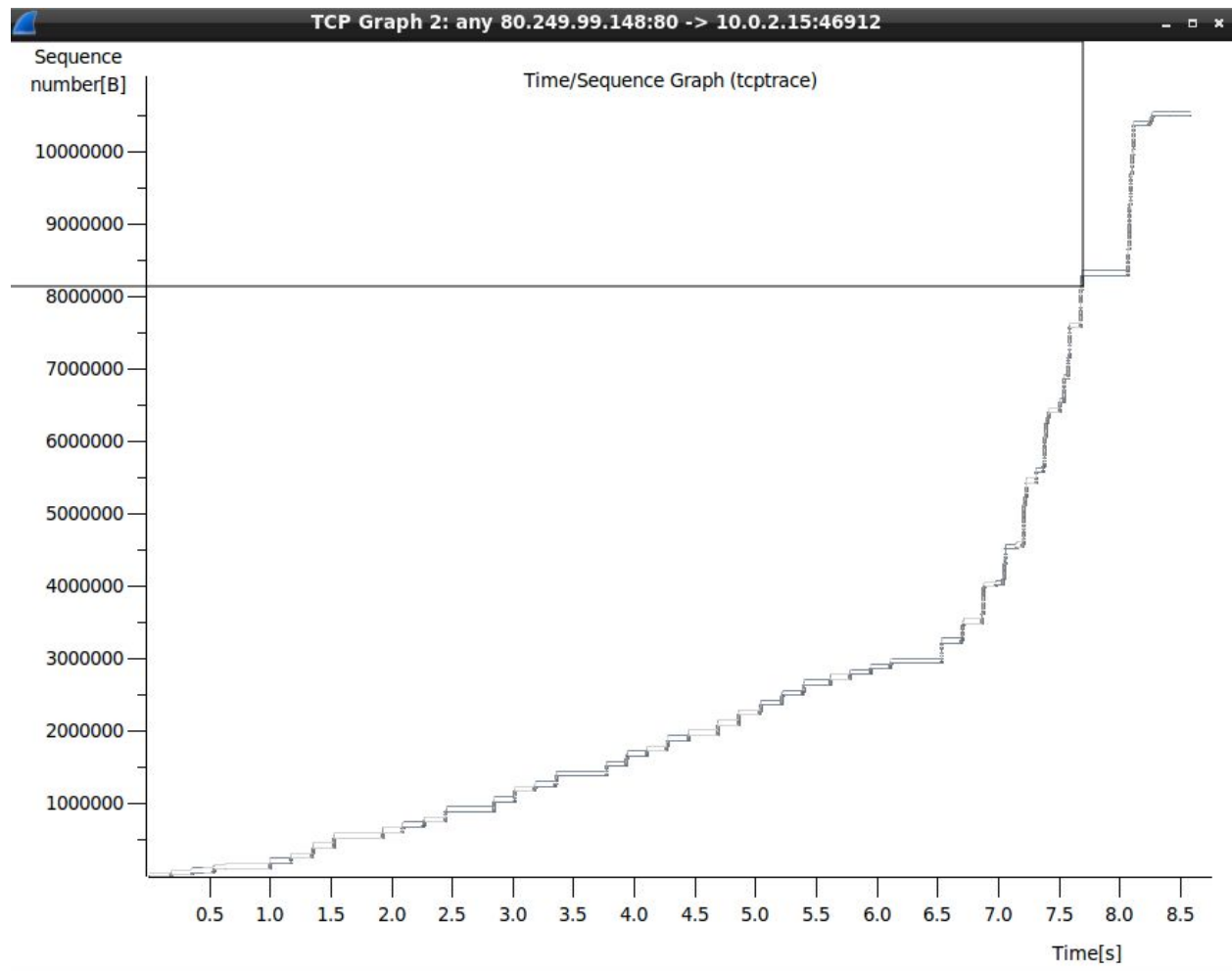
11.

The image shows a Wireshark packet capture of an HTTP transaction. The filter is set to 'any'. The capture shows a sequence of packets from source 10.0.2.15 to destination 80.249.99.148. The transaction starts with a GET request for 'http' and is followed by several 'ACK' packets. The final packet in the sequence is a 200 OK response from the server to the client, with a status code of 200 and a content type of 'application/zip'. The 'Info' column for this packet shows '56 42178 > http [ACK] Seq=139 Ack=10486038 Win=65535 Len=0'.

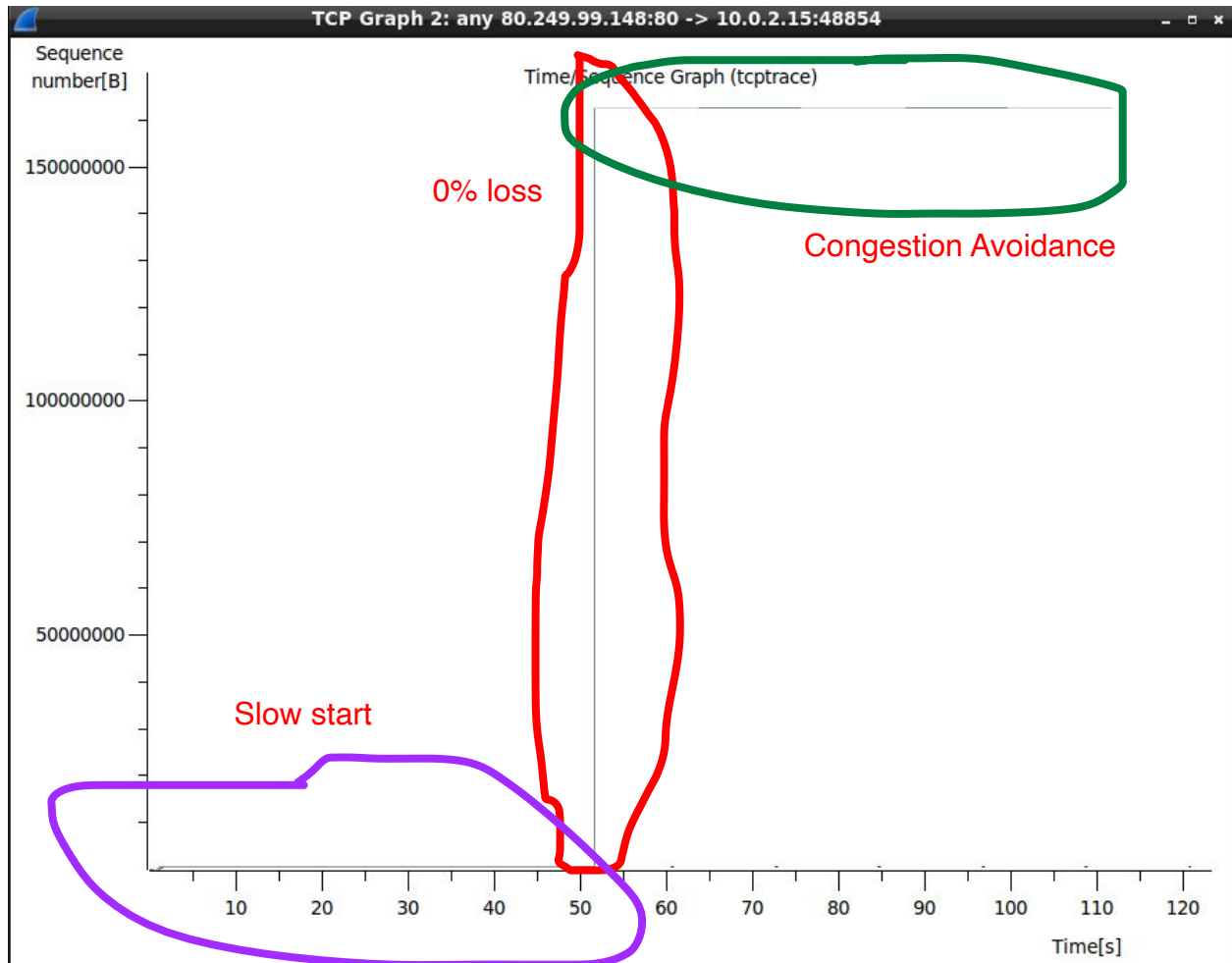
Time	Source	Destination	No.	Protocol	Length	Info
11.45980700	80.249.99.148	10.0.2.15	1417	TCP	9348	[TCP segment of a reassembled PDU]
11.45987200	10.0.2.15	80.249.99.148	1418	TCP	56	42178 > http [ACK] Seq=139 Ack=10363337 Win=65535 Len=0
11.46213400	80.249.99.148	10.0.2.15	1419	TCP	17432	[TCP segment of a reassembled PDU]
11.46217600	10.0.2.15	80.249.99.148	1420	TCP	56	42178 > http [ACK] Seq=139 Ack=10380713 Win=65535 Len=0
11.46262200	80.249.99.148	10.0.2.15	1421	TCP	34808	[TCP segment of a reassembled PDU]
11.46264000	10.0.2.15	80.249.99.148	1422	TCP	56	42178 > http [ACK] Seq=139 Ack=10415465 Win=65535 Len=0
11.46290800	80.249.99.148	10.0.2.15	1423	TCP	29876	[TCP segment of a reassembled PDU]
11.46292400	10.0.2.15	80.249.99.148	1424	TCP	56	42178 > http [ACK] Seq=139 Ack=10445285 Win=65535 Len=0
11.46300800	80.249.99.148	10.0.2.15	1425	TCP	3540	[TCP segment of a reassembled PDU]
11.46301300	10.0.2.15	80.249.99.148	1426	TCP	56	42178 > http [ACK] Seq=139 Ack=10448769 Win=65535 Len=0
11.46340600	80.249.99.148	10.0.2.15	1427	TCP	4400	[TCP segment of a reassembled PDU]
11.46346600	10.0.2.15	80.249.99.148	1428	TCP	56	42178 > http [ACK] Seq=139 Ack=10453113 Win=65535 Len=0
11.46353100	80.249.99.148	10.0.2.15	1429	TCP	13088	[TCP segment of a reassembled PDU]
11.46368500	80.249.99.148	10.0.2.15	1430	TCP	9996	[TCP segment of a reassembled PDU]
11.46373100	80.249.99.148	10.0.2.15	1431	TCP	252	[TCP segment of a reassembled PDU]
11.46373900	80.249.99.148	10.0.2.15	1432	TCP	8744	[TCP segment of a reassembled PDU]
11.46612400	10.0.2.15	80.249.99.148	1433	TCP	56	42178 > http [ACK] Seq=139 Ack=10484969 Win=65535 Len=0
11.63731200	80.249.99.148	10.0.2.15	1434	HTTP	1125	HTTP/1.1 200 OK (application/zip)
11.63746900	10.0.2.15	80.249.99.148	1435	TCP	56	42178 > http [ACK] Seq=139 Ack=10486038 Win=65535 Len=0
11.63818200	10.0.2.15	80.249.99.148	1436	TCP	56	42178 > http [FIN, ACK] Seq=139 Ack=10486038 Win=65535 Len=0
11.63841000	80.249.99.148	10.0.2.15	1437	TCP	62	http > 42178 [ACK] Seq=10486038 Ack=140 Win=65535 Len=0
11.81222600	80.249.99.148	10.0.2.15	1438	TCP	62	http > 42178 [FIN, ACK] Seq=10486038 Ack=140 Win=65535 Len=0
11.81225900	10.0.2.15	80.249.99.148	1439	TCP	56	42178 > http [ACK] Seq=140 Ack=10486039 Win=40256 Len=0
11.99999900	127.0.0.1	127.0.0.1	1440	TCP	76	52475 > 6633 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=4228251 TSecr=0 WS=128
12.00000700	127.0.0.1	127.0.0.1	1441	TCP	56	6633 > 52475 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Win= 43690

12. The graph shows the download vs. time. The server sending over information to my computer



13. When the packet loss was at 100% there was no download at all, but as soon as there was 0% packet loss there was a complete download.



Special thanks to for the info:

<https://dev.to/flippedcoding/what-is-the-difference-between-a-uri-and-a-url-4455>

https://en.wikipedia.org/wiki/List_of_HTTP_status_codes