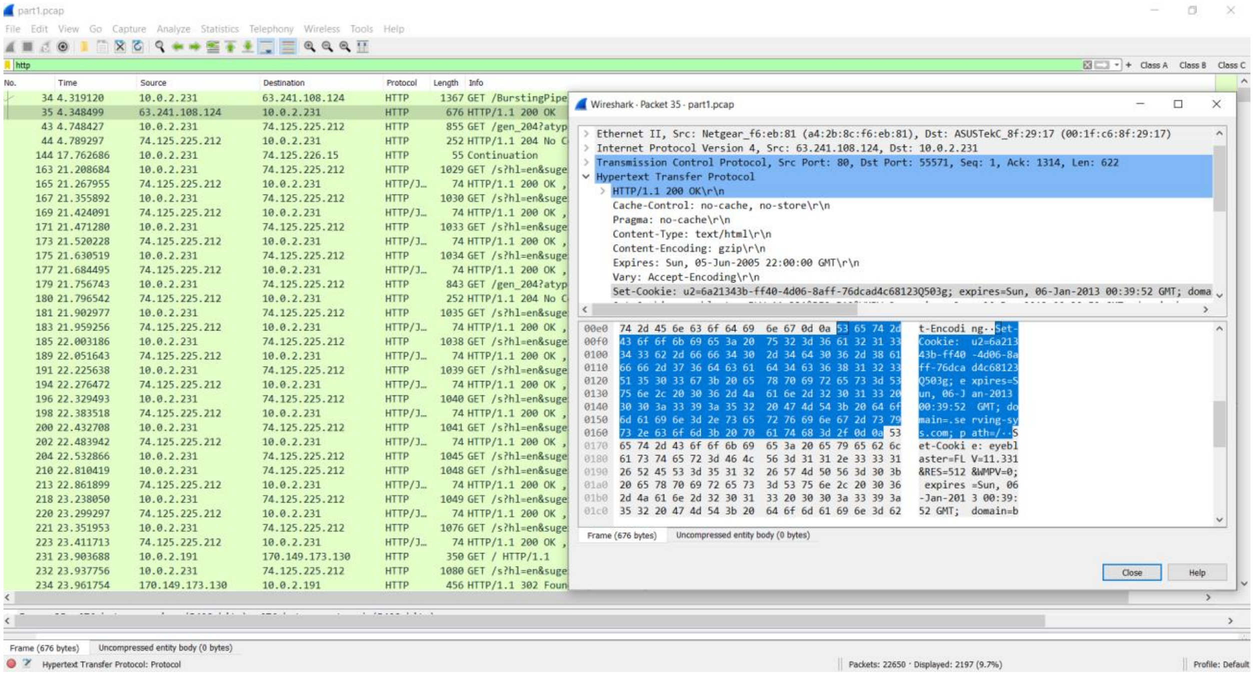
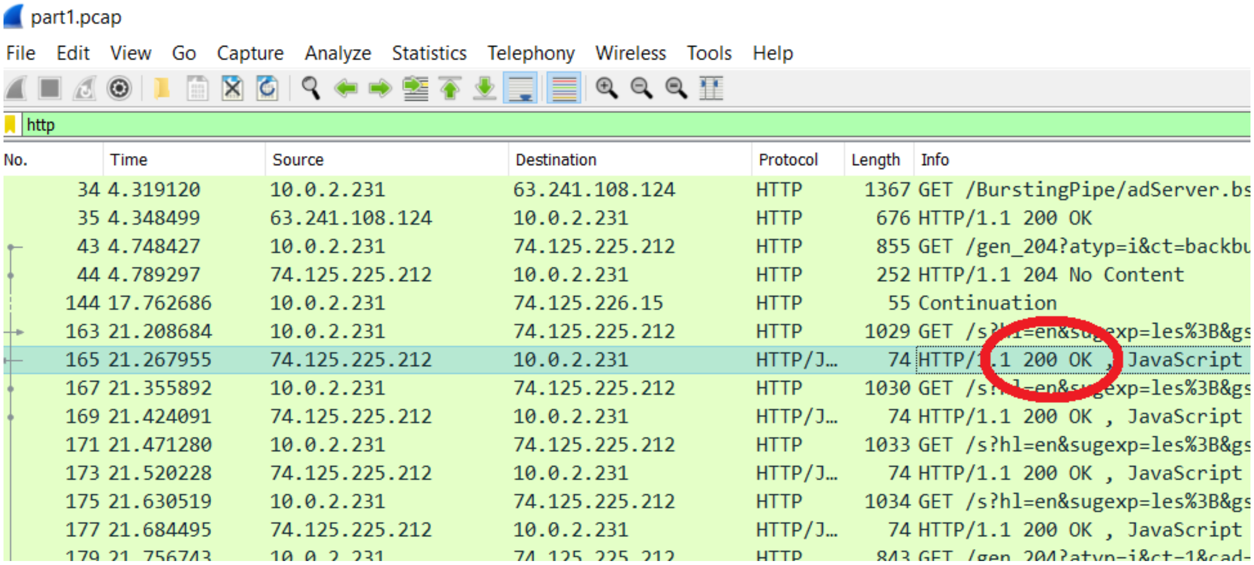


```
part1.pcap
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
http                                                                       + Class A  Class B  Class C
No.   Time        Source           Destination      Protocol  Length Info
   34 4.319120    10.0.2.231       63.241.108.124   HTTP       1367 GET /BurstingPipe
   35 4.348499    63.241.108.124   10.0.2.231       HTTP        676 HTTP/1.1 200 OK
   43 4.748427    10.0.2.231       74.125.225.212   HTTP        855 GET /gen_204?atyp
   44 4.789297    74.125.225.212   10.0.2.231       HTTP        252 HTTP/1.1 204 No C
  144 17.762686   10.0.2.231       74.125.226.15    HTTP         55 Continuation
  163 21.208684   10.0.2.231       74.125.225.212   HTTP       1029 GET /s?hl=en&suge
  165 21.267955   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  167 21.355892   10.0.2.231       74.125.225.212   HTTP       1030 GET /s?hl=en&suge
  169 21.424091   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  171 21.471280   10.0.2.231       74.125.225.212   HTTP       1033 GET /s?hl=en&suge
  173 21.520228   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  175 21.630519   10.0.2.231       74.125.225.212   HTTP       1034 GET /s?hl=en&suge
  177 21.684495   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  179 21.756743   10.0.2.231       74.125.225.212   HTTP        843 GET /gen_204?atyp
  180 21.796542   74.125.225.212   10.0.2.231       HTTP        252 HTTP/1.1 204 No C
  181 21.902977   10.0.2.231       74.125.225.212   HTTP       1035 GET /s?hl=en&suge
  183 21.959256   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  185 22.003186   10.0.2.231       74.125.225.212   HTTP       1038 GET /s?hl=en&suge
  189 22.051643   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  191 22.225638   10.0.2.231       74.125.225.212   HTTP       1039 GET /s?hl=en&suge
  194 22.276472   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  196 22.329493   10.0.2.231       74.125.225.212   HTTP       1040 GET /s?hl=en&suge
  198 22.383518   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  200 22.432708   10.0.2.231       74.125.225.212   HTTP       1041 GET /s?hl=en&suge
  202 22.483942   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  204 22.532866   10.0.2.231       74.125.225.212   HTTP       1045 GET /s?hl=en&suge
  210 22.810419   10.0.2.231       74.125.225.212   HTTP       1048 GET /s?hl=en&suge
  213 22.861899   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  218 23.238050   10.0.2.231       74.125.225.212   HTTP       1049 GET /s?hl=en&suge
  220 23.299297   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  221 23.351953   10.0.2.231       74.125.225.212   HTTP       1076 GET /s?hl=en&suge
  223 23.411713   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK ,
  231 23.903688   10.0.2.191       170.149.173.130  HTTP        350 GET / HTTP/1.1
  232 23.937756   10.0.2.231       74.125.225.212   HTTP       1080 GET /s?hl=en&suge
  234 23.961754   170.149.173.130  10.0.2.191       HTTP        456 HTTP/1.1 302 Foun

Frame (676 bytes)   Uncompressed entity body (0 bytes)
Hypertext Transfer Protocol: Protocol                     Packets: 22650 · Displayed: 2197 (9.7%)   Profile: Default
```

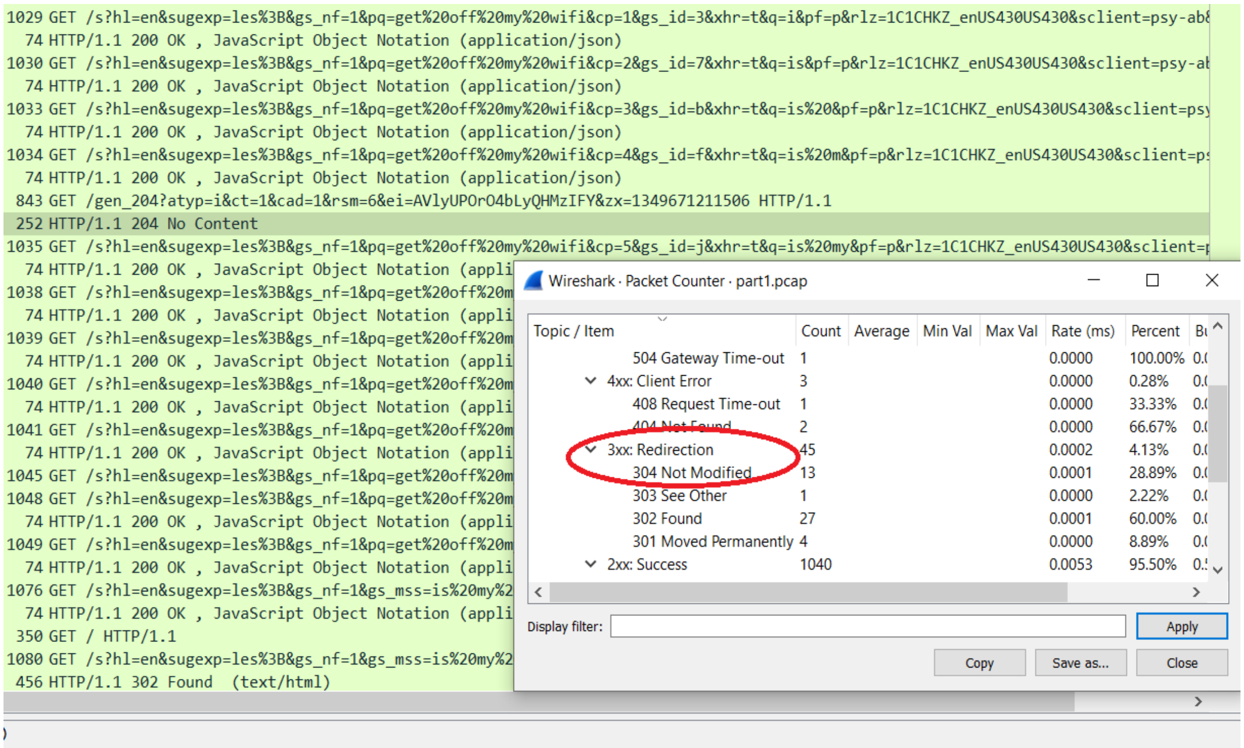
```
Wireshark · Packet 35 · part1.pcap

> Ethernet II, Src: Netgear_f6:eb:81 (a4:2b:8c:f6:eb:81), Dst: ASUSTekC_8f:29:17 (00:1f:c6:8f:29:17)
> Internet Protocol Version 4, Src: 63.241.108.124, Dst: 10.0.2.231
> Transmission Control Protocol, Src Port: 80, Dst Port: 55571, Seq: 1, Ack: 1314, Len: 622
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Cache-Control: no-cache, no-store\r\n
    Pragma: no-cache\r\n
    Content-Type: text/html\r\n
    Content-Encoding: gzip\r\n
    Expires: Sun, 05-Jun-2005 22:00:00 GMT\r\n
    Vary: Accept-Encoding\r\n
    Set-Cookie: u2=6a21343b-ff40-4d06-8aff-76dcad4c68123Q503g; expires=Sun, 06-Jan-2013 00:39:52 GMT; doma

00e0  74 2d 45 6e 63 6f 64 69  6e 67 0d 0a 53 65 74 2d   t-Encodi ng··Set-
00f0  43 6f 6f 6b 69 65 3a 20  75 32 3d 36 61 32 31 33   Cookie:  u2=6a213
0100  34 33 62 2d 66 66 34 30  2d 34 64 30 36 2d 38 61   43b-ff40 -4d06-8a
0110  66 66 2d 37 36 64 63 61  64 34 63 36 38 31 32 33   ff-76dca d4c68123
0120  51 35 30 33 67 3b 20 65  78 70 69 72 65 73 3d 53   Q503g; e xpires=S
0130  75 6e 2c 20 30 36 2d 4a  61 6e 2d 32 30 31 33 20   un, 06-J an-2013
0140  30 30 3a 33 39 3a 35 32  20 47 4d 54 3b 20 64 6f   00:39:52  GMT; do
0150  6d 61 69 6e 3d 2e 73 65  72 76 69 6e 67 2d 73 79   main=.se rving-sy
0160  73 2e 63 6f 6d 3b 20 70  61 74 68 3d 2f 0d 0a 53   s.com; p ath=/··S
0170  65 74 2d 43 6f 6f 6b 69  65 3a 20 65 79 65 62 6c   et-Cooki e: eyebl
0180  61 73 74 65 72 3d 46 4c  56 3d 31 31 2e 33 33 31   aster=FL V=11.331
0190  26 52 45 53 3d 35 31 32  26 57 4d 50 56 3d 30 3b   &RES=512 &WMPV=0;
01a0  20 65 78 70 69 72 65 73  3d 53 75 6e 2c 20 30 36    expires =Sun, 06
01b0  2d 4a 61 6e 2d 32 30 31  33 20 30 30 3a 33 39 3a   -Jan-201 3 00:39:
01c0  35 32 20 47 4d 54 3b 20  64 6f 6d 61 69 6e 3d 62   52 GMT;  domain=b

Frame (676 bytes)   Uncompressed entity body (0 bytes)
```

When you type HTTP on the filter's bar will cause only HTTP message to be displayed in the packet-listing window. This screenshot after the http filter has been applied. That called HTTP packet sniffing. Also, that in the Selected packet details window, we've chosen to show detailed content for the Hypertext Transfer Protocol application message that was found within the TCP segment, that was inside the IPv4 datagram that was inside the Ethernet II wifi frame.



```
part1.pcap
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
http
No.   Time        Source           Destination      Protocol  Length Info
   34 4.319120    10.0.2.231       63.241.108.124   HTTP       1367 GET /BurstingPipe/adServer.bs
   35 4.348499    63.241.108.124   10.0.2.231       HTTP        676 HTTP/1.1 200 OK
   43 4.748427    10.0.2.231       74.125.225.212   HTTP        855 GET /gen_204?atyp=i&ct=backbu
   44 4.789297    74.125.225.212   10.0.2.231       HTTP        252 HTTP/1.1 204 No Content
  144 17.762686   10.0.2.231       74.125.226.15    HTTP         55 Continuation
  163 21.208684   10.0.2.231       74.125.225.212   HTTP       1029 GET /s?hl=en&sugexp=les%3B&gs
  165 21.267955   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK , JavaScript
  167 21.355892   10.0.2.231       74.125.225.212   HTTP       1030 GET /s?hl=en&sugexp=les%3B&gs
  169 21.424091   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK , JavaScript
  171 21.471280   10.0.2.231       74.125.225.212   HTTP       1033 GET /s?hl=en&sugexp=les%3B&gs
  173 21.520228   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK , JavaScript
  175 21.630519   10.0.2.231       74.125.225.212   HTTP       1034 GET /s?hl=en&sugexp=les%3B&gs
  177 21.684495   74.125.225.212   10.0.2.231       HTTP/J…      74 HTTP/1.1 200 OK , JavaScript
  179 21.756743   10.0.2.231       74.125.225.212   HTTP        843 GET /gen_204?atyp=i&ct=1&cad=
```

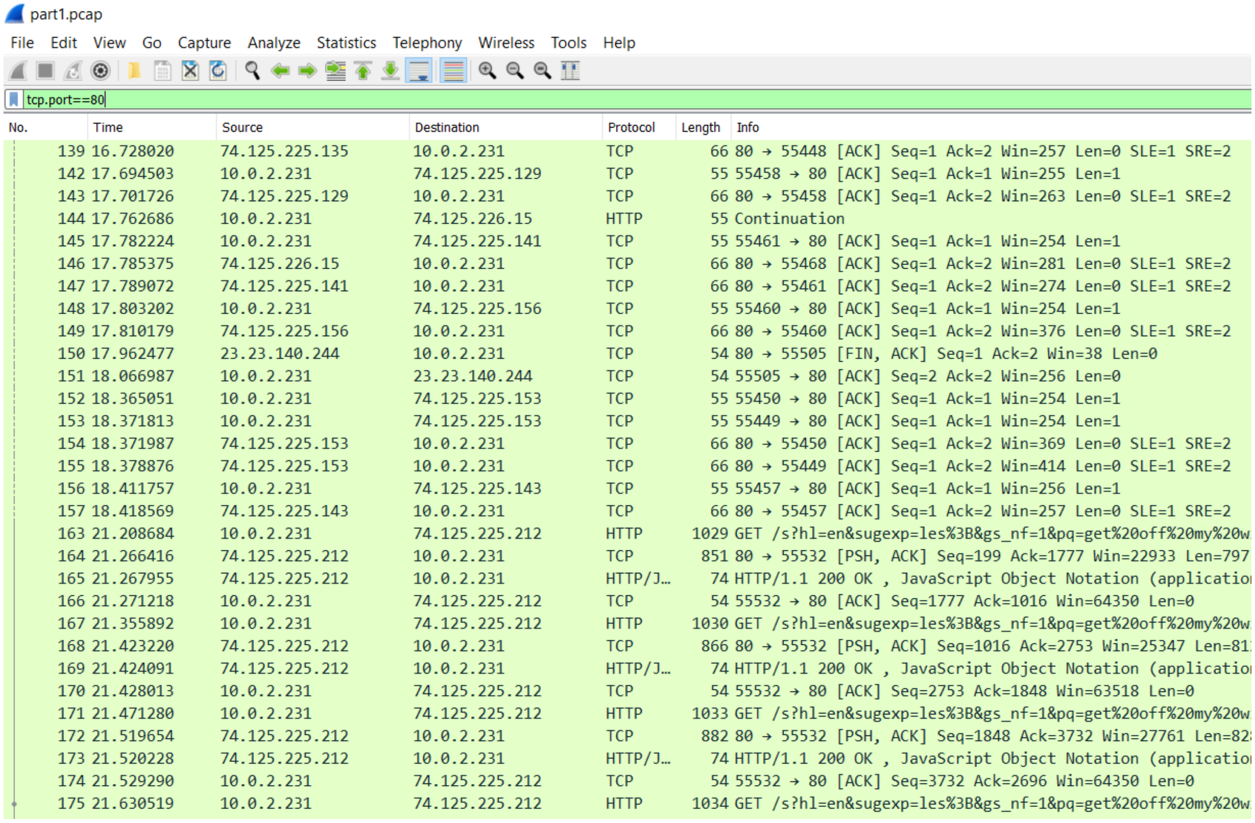
The Info for this packet will indicate “200 OK” in the case of a normal, successful transfer. You will see that the response is similar to the request, with a series of headers that follow the “200 OK” status code.



```
1029 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20my%20wifi&cp=1&gs_id=3&xhr=t&q=i&pf=p&rlz=1C1CHKZ_enUS430US430&sclient=psy-ab
  74 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
1030 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20my%20wifi&cp=2&gs_id=7&xhr=t&q=is&pf=p&rlz=1C1CHKZ_enUS430US430&sclient=psy-ab
  74 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
1033 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20my%20wifi&cp=3&gs_id=b&xhr=t&q=is%20&pf=p&rlz=1C1CHKZ_enUS430US430&sclient=psy
  74 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
1034 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20my%20wifi&cp=4&gs_id=f&xhr=t&q=is%20m&pf=p&rlz=1C1CHKZ_enUS430US430&sclient=p
  74 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
 843 GET /gen_204?atyp=i&ct=1&cad=1&rsm=6&ei=AVlyUPOrO4bLyQHMzIFY&zx=1349671211506 HTTP/1.1
 252 HTTP/1.1 204 No Content
1035 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20my%20wifi&cp=5&gs_id=j&xhr=t&q=is%20my&pf=p&rlz=1C1CHKZ_enUS430US430&sclient=
  74 HTTP/1.1 200 OK , JavaScript Object Notation (appli
1038 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20m
  74 HTTP/1.1 200 OK , JavaScript Object Notation (appli
1039 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20m
  74 HTTP/1.1 200 OK , JavaScript Object Notation (appli
1040 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20m
  74 HTTP/1.1 200 OK , JavaScript Object Notation (appli
1041 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20m
  74 HTTP/1.1 200 OK , JavaScript Object Notation (appli
1045 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20m
1048 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20m
  74 HTTP/1.1 200 OK , JavaScript Object Notation (appli
1049 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20m
  74 HTTP/1.1 200 OK , JavaScript Object Notation (appli
1076 GET /s?hl=en&sugexp=les%3B&gs_nf=1&gs_mss=is%20my%2
  74 HTTP/1.1 200 OK , JavaScript Object Notation (appli
 350 GET / HTTP/1.1
1080 GET /s?hl=en&sugexp=les%3B&gs_nf=1&gs_mss=is%20my%2
 456 HTTP/1.1 302 Found  (text/html)
```

| Topic / Item | Count | Average | Min Val | Max Val | Rate (ms) | Percent | Bu |
|---|---|---|---|---|---|---|---|
| 504 Gateway Time-out | 1 | | | | 0.0000 | 100.00% | 0.0 |
| 4xx: Client Error | 3 | | | | 0.0000 | 0.28% | 0.0 |
| 408 Request Time-out | 1 | | | | 0.0000 | 33.33% | 0.0 |
| 404 Not Found | 2 | | | | 0.0000 | 66.67% | 0.0 |
| 3xx: Redirection | 45 | | | | 0.0002 | 4.13% | 0.0 |
| 304 Not Modified | 13 | | | | 0.0001 | 28.89% | 0.0 |
| 303 See Other | 1 | | | | 0.0000 | 2.22% | 0.0 |
| 302 Found | 27 | | | | 0.0001 | 60.00% | 0.0 |
| 301 Moved Permanently | 4 | | | | 0.0000 | 8.89% | 0.0 |
| 2xx: Success | 1040 | | | | 0.0053 | 95.50% | 0.5 |

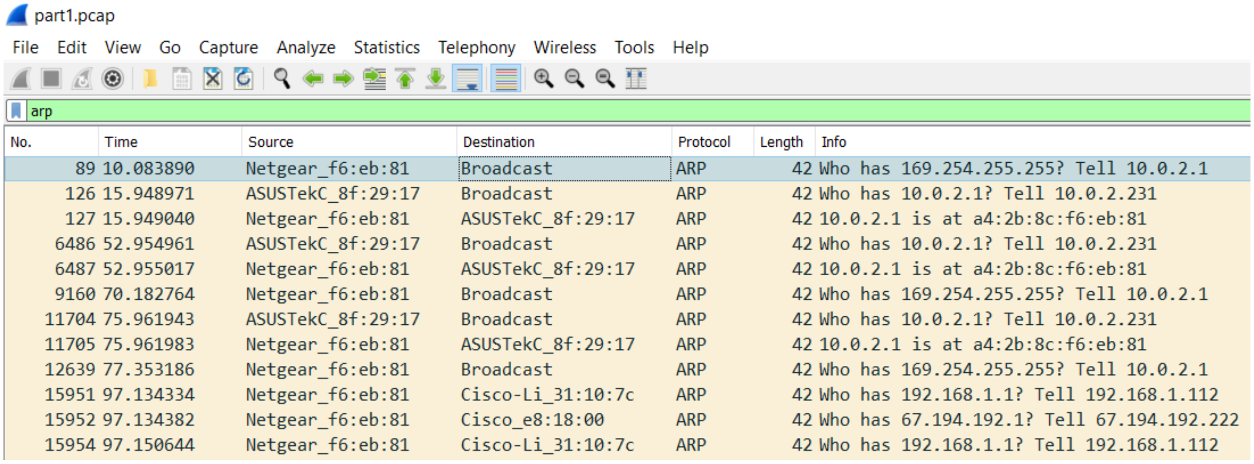
You will also find this panel under “Statistics” and “HTTP”, and you should filter for the packets that are part of the fetch as before. This panel will tell you the kinds of request and responses. Our panel is shown in the figure below. You can see that it consists of GET requests that are matched by 200 OK responses and 304 Not Modified.



tcp.port==80

```
No.     Time       Source           Destination      Protocol  Length Info
    139 16.728020  74.125.225.135   10.0.2.231       TCP         66 80 → 55448 [ACK] Seq=1 Ack=2 Win=257 Len=0 SLE=1 SRE=2
    142 17.694503  10.0.2.231       74.125.225.129   TCP         55 55458 → 80 [ACK] Seq=1 Ack=1 Win=255 Len=1
    143 17.701726  74.125.225.129   10.0.2.231       TCP         66 80 → 55458 [ACK] Seq=1 Ack=2 Win=263 Len=0 SLE=1 SRE=2
    144 17.762686  10.0.2.231       74.125.226.15    HTTP        55 Continuation
    145 17.782224  10.0.2.231       74.125.225.141   TCP         55 55461 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
    146 17.785375  74.125.226.15    10.0.2.231       TCP         66 80 → 55468 [ACK] Seq=1 Ack=2 Win=281 Len=0 SLE=1 SRE=2
    147 17.789072  74.125.225.141   10.0.2.231       TCP         66 80 → 55461 [ACK] Seq=1 Ack=2 Win=274 Len=0 SLE=1 SRE=2
    148 17.803202  10.0.2.231       74.125.225.156   TCP         55 55460 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
    149 17.810179  74.125.225.156   10.0.2.231       TCP         66 80 → 55460 [ACK] Seq=1 Ack=2 Win=376 Len=0 SLE=1 SRE=2
    150 17.962477  23.23.140.244    10.0.2.231       TCP         54 80 → 55505 [FIN, ACK] Seq=1 Ack=2 Win=38 Len=0
    151 18.066987  10.0.2.231       23.23.140.244    TCP         54 55505 → 80 [ACK] Seq=2 Ack=2 Win=256 Len=0
    152 18.365051  10.0.2.231       74.125.225.153   TCP         55 55450 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
    153 18.371813  10.0.2.231       74.125.225.153   TCP         55 55449 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
    154 18.371987  74.125.225.153   10.0.2.231       TCP         66 80 → 55450 [ACK] Seq=1 Ack=2 Win=369 Len=0 SLE=1 SRE=2
    155 18.378876  74.125.225.153   10.0.2.231       TCP         66 80 → 55449 [ACK] Seq=1 Ack=2 Win=414 Len=0 SLE=1 SRE=2
    156 18.411757  10.0.2.231       74.125.225.143   TCP         55 55457 → 80 [ACK] Seq=1 Ack=1 Win=256 Len=1
    157 18.418569  74.125.225.143   10.0.2.231       TCP         66 80 → 55457 [ACK] Seq=1 Ack=2 Win=257 Len=0 SLE=1 SRE=2
    163 21.208684  10.0.2.231       74.125.225.212   HTTP      1029 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20my%20w
    164 21.266416  74.125.225.212   10.0.2.231       TCP        851 80 → 55532 [PSH, ACK] Seq=199 Ack=1777 Win=22933 Len=797
    165 21.267955  74.125.225.212   10.0.2.231       HTTP/J…     74 HTTP/1.1 200 OK , JavaScript Object Notation (applicatio
    166 21.271218  10.0.2.231       74.125.225.212   TCP         54 55532 → 80 [ACK] Seq=1777 Ack=1016 Win=64350 Len=0
    167 21.355892  10.0.2.231       74.125.225.212   HTTP      1030 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20my%20w
    168 21.423220  74.125.225.212   10.0.2.231       TCP        866 80 → 55532 [PSH, ACK] Seq=1016 Ack=2753 Win=25347 Len=81
    169 21.424091  74.125.225.212   10.0.2.231       HTTP/J…     74 HTTP/1.1 200 OK , JavaScript Object Notation (applicatio
    170 21.428013  10.0.2.231       74.125.225.212   TCP         54 55532 → 80 [ACK] Seq=2753 Ack=1848 Win=63518 Len=0
    171 21.471280  10.0.2.231       74.125.225.212   HTTP      1033 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20my%20w
    172 21.519654  74.125.225.212   10.0.2.231       TCP        882 80 → 55532 [PSH, ACK] Seq=1848 Ack=3732 Win=27761 Len=82
    173 21.520228  74.125.225.212   10.0.2.231       HTTP/J…     74 HTTP/1.1 200 OK , JavaScript Object Notation (applicatio
    174 21.529290  10.0.2.231       74.125.225.212   TCP         54 55532 → 80 [ACK] Seq=3732 Ack=2696 Win=64350 Len=0
    175 21.630519  10.0.2.231       74.125.225.212   HTTP      1034 GET /s?hl=en&sugexp=les%3B&gs_nf=1&pq=get%20off%20my%20w
```

This filter will record only standard web traffic and not other kinds of packets that your computer may send. The checking will translate the addresses of the computers sending and receiving packets into names, which should help you to recognize whether the packets are going to or from your computer.



arp

```
No.     Time        Source              Destination         Protocol  Length Info
     89 10.083890   Netgear_f6:eb:81    Broadcast           ARP         42 Who has 169.254.255.255? Tell 10.0.2.1
    126 15.948971   ASUSTekC_8f:29:17   Broadcast           ARP         42 Who has 10.0.2.1? Tell 10.0.2.231
    127 15.949040   Netgear_f6:eb:81    ASUSTekC_8f:29:17   ARP         42 10.0.2.1 is at a4:2b:8c:f6:eb:81
   6486 52.954961   ASUSTekC_8f:29:17   Broadcast           ARP         42 Who has 10.0.2.1? Tell 10.0.2.231
   6487 52.955017   Netgear_f6:eb:81    ASUSTekC_8f:29:17   ARP         42 10.0.2.1 is at a4:2b:8c:f6:eb:81
   9160 70.182764   Netgear_f6:eb:81    Broadcast           ARP         42 Who has 169.254.255.255? Tell 10.0.2.1
  11704 75.961943   ASUSTekC_8f:29:17   Broadcast           ARP         42 Who has 10.0.2.1? Tell 10.0.2.231
  11705 75.961983   Netgear_f6:eb:81    ASUSTekC_8f:29:17   ARP         42 10.0.2.1 is at a4:2b:8c:f6:eb:81
  12639 77.353186   Netgear_f6:eb:81    Broadcast           ARP         42 Who has 169.254.255.255? Tell 10.0.2.1
  15951 97.134334   Netgear_f6:eb:81    Cisco-Li_31:10:7c   ARP         42 Who has 192.168.1.1? Tell 192.168.1.112
  15952 97.134382   Netgear_f6:eb:81    Cisco_e8:18:00      ARP         42 Who has 67.194.192.1? Tell 67.194.192.222
  15954 97.150644   Netgear_f6:eb:81    Cisco-Li_31:10:7c   ARP         42 Who has 192.168.1.1? Tell 192.168.1.112
```

The Address Resolution Protocol is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

To capture ARP traffic:

1- Start Wireshark, but do not yet start a capture.

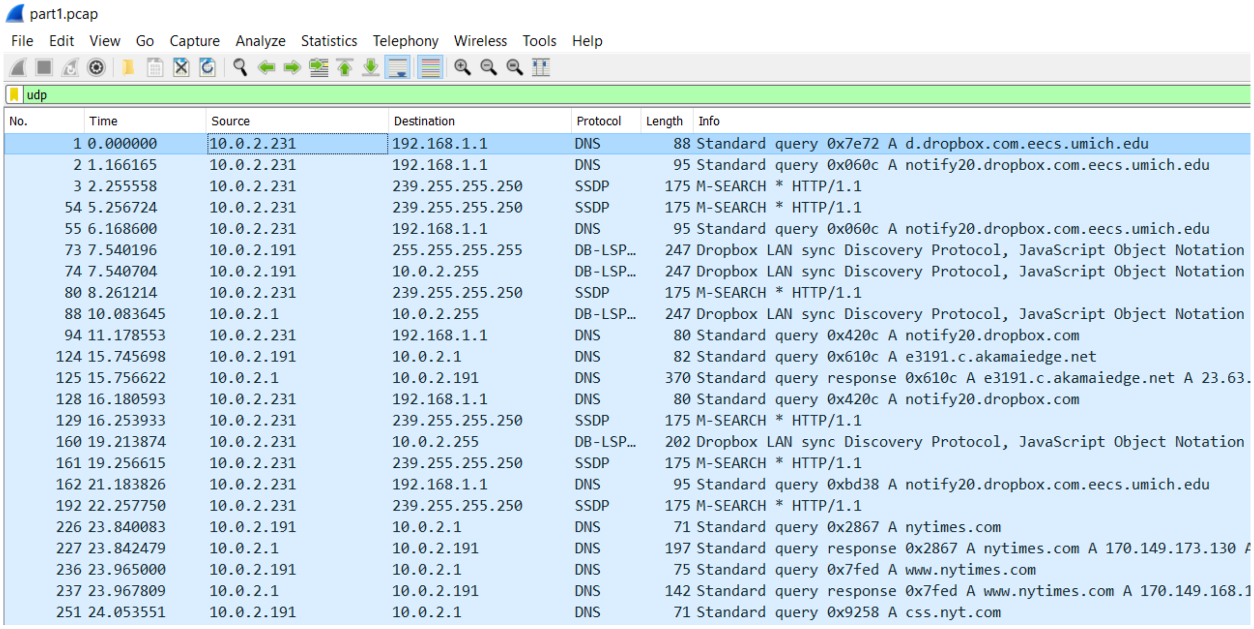
2- Open an elevated/administrator command prompt.

3- Use ipconfig to display the default gateway address. ...

4- Start a Wireshark capture.

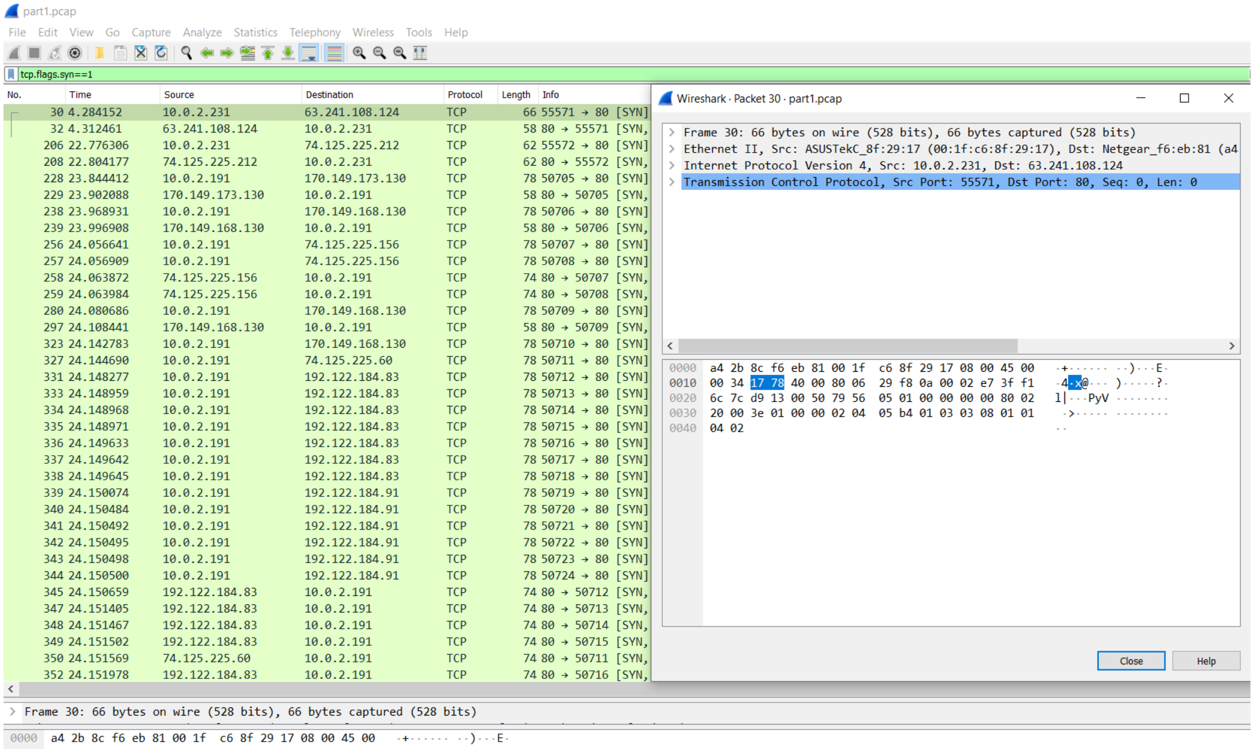
5- Use arp -d to clear the ARP cache.

6- Use ping <default gateway address> to ping the default gateway address.


part1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 10.0.2.231 | 192.168.1.1 | DNS | 88 | Standard query 0x7e72 A d.dropbox.com.eecs.umich.edu |
| 2 | 1.166165 | 10.0.2.231 | 192.168.1.1 | DNS | 95 | Standard query 0x060c A notify20.dropbox.com.eecs.umich.edu |
| 3 | 2.255558 | 10.0.2.231 | 239.255.255.250 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 54 | 5.256724 | 10.0.2.231 | 239.255.255.250 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 55 | 6.168600 | 10.0.2.231 | 192.168.1.1 | DNS | 95 | Standard query 0x060c A notify20.dropbox.com.eecs.umich.edu |
| 73 | 7.540196 | 10.0.2.191 | 255.255.255.255 | DB-LSP… | 247 | Dropbox LAN sync Discovery Protocol, JavaScript Object Notation |
| 74 | 7.540704 | 10.0.2.191 | 10.0.2.255 | DB-LSP… | 247 | Dropbox LAN sync Discovery Protocol, JavaScript Object Notation |
| 80 | 8.261214 | 10.0.2.231 | 239.255.255.250 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 88 | 10.083645 | 10.0.2.1 | 10.0.2.255 | DB-LSP… | 247 | Dropbox LAN sync Discovery Protocol, JavaScript Object Notation |
| 94 | 11.178553 | 10.0.2.231 | 192.168.1.1 | DNS | 80 | Standard query 0x420c A notify20.dropbox.com |
| 124 | 15.745698 | 10.0.2.191 | 10.0.2.1 | DNS | 82 | Standard query 0x610c A e3191.c.akamaiedge.net |
| 125 | 15.756622 | 10.0.2.1 | 10.0.2.191 | DNS | 370 | Standard query response 0x610c A e3191.c.akamaiedge.net A 23.63. |
| 128 | 16.180593 | 10.0.2.231 | 192.168.1.1 | DNS | 80 | Standard query 0x420c A notify20.dropbox.com |
| 129 | 16.253933 | 10.0.2.231 | 239.255.255.250 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 160 | 19.213874 | 10.0.2.231 | 10.0.2.255 | DB-LSP… | 202 | Dropbox LAN sync Discovery Protocol, JavaScript Object Notation |
| 161 | 19.256615 | 10.0.2.231 | 239.255.255.250 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 162 | 21.183826 | 10.0.2.231 | 192.168.1.1 | DNS | 95 | Standard query 0xbd38 A notify20.dropbox.com.eecs.umich.edu |
| 192 | 22.257750 | 10.0.2.231 | 239.255.255.250 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 226 | 23.840083 | 10.0.2.191 | 10.0.2.1 | DNS | 71 | Standard query 0x2867 A nytimes.com |
| 227 | 23.842479 | 10.0.2.1 | 10.0.2.191 | DNS | 197 | Standard query response 0x2867 A nytimes.com A 170.149.173.130 A |
| 236 | 23.965000 | 10.0.2.191 | 10.0.2.1 | DNS | 75 | Standard query 0x7fed A www.nytimes.com |
| 237 | 23.967809 | 10.0.2.1 | 10.0.2.191 | DNS | 142 | Standard query response 0x7fed A www.nytimes.com A 170.149.168.1 |
| 251 | 24.053551 | 10.0.2.191 | 10.0.2.1 | DNS | 71 | Standard query 0x9258 A css.nyt.com |

The UDP layer provides datagram based connectionless transport layer (layer 4) functionality in the Internet Protocol Family. UDP is only a thin layer, and provides not much more than the described UDP port multiplexing.


part1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

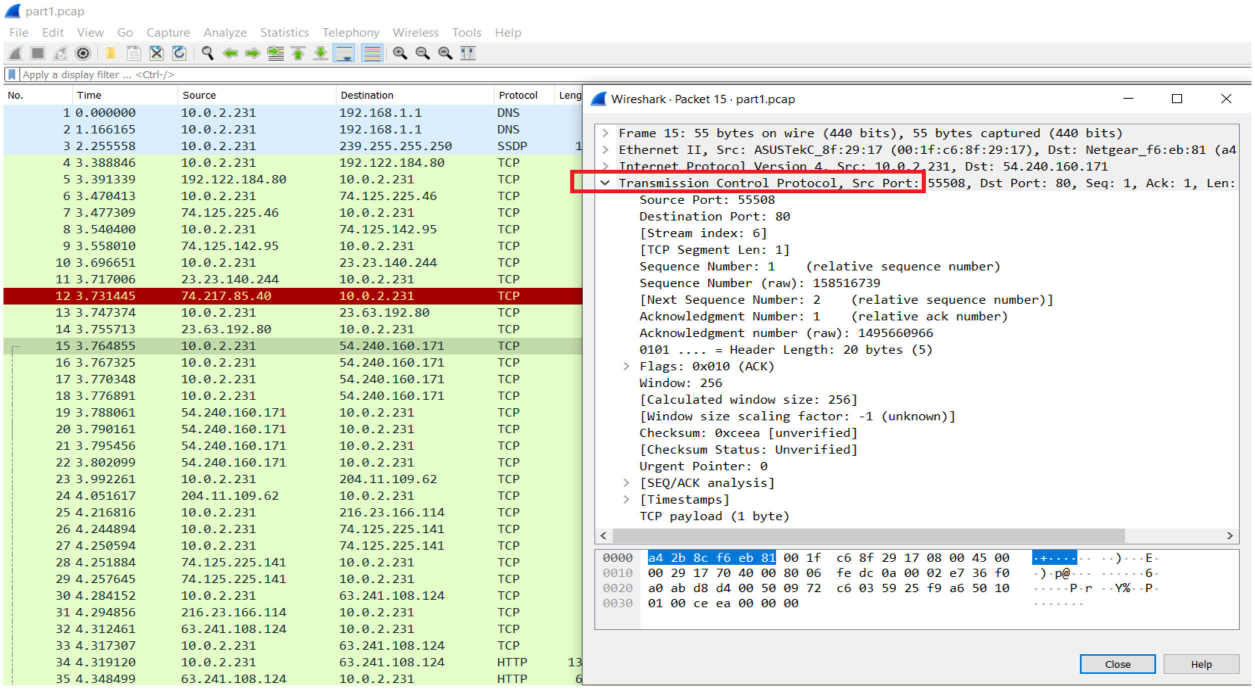
```
tcp.flags.syn==1
```

```
No.   Time         Source            Destination       Protocol  Length  Info
   30 4.284152     10.0.2.231        63.241.108.124    TCP       66 55571 → 80 [SYN]
   32 4.312461     63.241.108.124    10.0.2.231        TCP       58 80 → 55571 [SYN,
  206 22.776306    10.0.2.231        74.125.225.212    TCP       62 55572 → 80 [SYN]
  208 22.804177    74.125.225.212    10.0.2.231        TCP       62 80 → 55572 [SYN,
  228 23.844412    10.0.2.191        170.149.173.130   TCP       78 50705 → 80 [SYN]
  229 23.902088    170.149.173.130   10.0.2.191        TCP       58 80 → 50705 [SYN,
  238 23.968931    10.0.2.191        170.149.168.130   TCP       78 50706 → 80 [SYN]
  239 23.996908    170.149.168.130   10.0.2.191        TCP       58 80 → 50706 [SYN,
  256 24.056641    10.0.2.191        74.125.225.156    TCP       78 50707 → 80 [SYN]
  257 24.056909    10.0.2.191        74.125.225.156    TCP       78 50708 → 80 [SYN]
  258 24.063872    74.125.225.156    10.0.2.191        TCP       74 80 → 50707 [SYN,
  259 24.063984    74.125.225.156    10.0.2.191        TCP       74 80 → 50708 [SYN,
  280 24.080686    10.0.2.191        170.149.168.130   TCP       78 50709 → 80 [SYN]
  297 24.108441    170.149.168.130   10.0.2.191        TCP       58 80 → 50709 [SYN,
  323 24.142783    10.0.2.191        170.149.168.130   TCP       78 50710 → 80 [SYN]
  327 24.144690    10.0.2.191        74.125.225.60     TCP       78 50711 → 80 [SYN]
  331 24.148277    10.0.2.191        192.122.184.83    TCP       78 50712 → 80 [SYN]
  333 24.148959    10.0.2.191        192.122.184.83    TCP       78 50713 → 80 [SYN]
  334 24.148968    10.0.2.191        192.122.184.83    TCP       78 50714 → 80 [SYN]
  335 24.148971    10.0.2.191        192.122.184.83    TCP       78 50715 → 80 [SYN]
  336 24.149633    10.0.2.191        192.122.184.83    TCP       78 50716 → 80 [SYN]
  337 24.149642    10.0.2.191        192.122.184.83    TCP       78 50717 → 80 [SYN]
  338 24.149645    10.0.2.191        192.122.184.83    TCP       78 50718 → 80 [SYN]
  339 24.150074    10.0.2.191        192.122.184.91    TCP       78 50719 → 80 [SYN]
  340 24.150484    10.0.2.191        192.122.184.91    TCP       78 50720 → 80 [SYN]
  341 24.150492    10.0.2.191        192.122.184.91    TCP       78 50721 → 80 [SYN]
  342 24.150495    10.0.2.191        192.122.184.91    TCP       78 50722 → 80 [SYN]
  343 24.150498    10.0.2.191        192.122.184.91    TCP       78 50723 → 80 [SYN]
  344 24.150500    10.0.2.191        192.122.184.91    TCP       78 50724 → 80 [SYN]
  345 24.150659    192.122.184.83    10.0.2.191        TCP       74 80 → 50712 [SYN,
  347 24.151405    192.122.184.83    10.0.2.191        TCP       74 80 → 50713 [SYN,
  348 24.151467    192.122.184.83    10.0.2.191        TCP       74 80 → 50714 [SYN,
  349 24.151502    192.122.184.83    10.0.2.191        TCP       74 80 → 50715 [SYN,
  350 24.151569    74.125.225.60     10.0.2.191        TCP       74 80 → 50711 [SYN,
  352 24.151978    192.122.184.83    10.0.2.191        TCP       74 80 → 50716 [SYN,
```

```
> Frame 30: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
0000  a4 2b 8c f6 eb 81 00 1f  c6 8f 29 17 08 00 45 00   ·+······ ··)···E·
```

```
> Frame 30: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: ASUSTekC_8f:29:17 (00:1f:c6:8f:29:17), Dst: Netgear_f6:eb:81 (a4
> Internet Protocol Version 4, Src: 10.0.2.231, Dst: 63.241.108.124
> Transmission Control Protocol, Src Port: 55571, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  a4 2b 8c f6 eb 81 00 1f  c6 8f 29 17 08 00 45 00   ·+······ ··)···E·
0010  00 34 17 78 40 00 80 06  29 f8 0a 00 02 e7 3f f1   ·4·x@··· )·····?·
0020  6c 7c d9 13 00 50 79 56  05 01 00 00 00 00 80 02   l|···PyV ········
0030  20 00 3e 01 00 00 02 04  05 b4 01 03 03 08 01 01    ·>····· ········
0040  04 02                                              ··
```

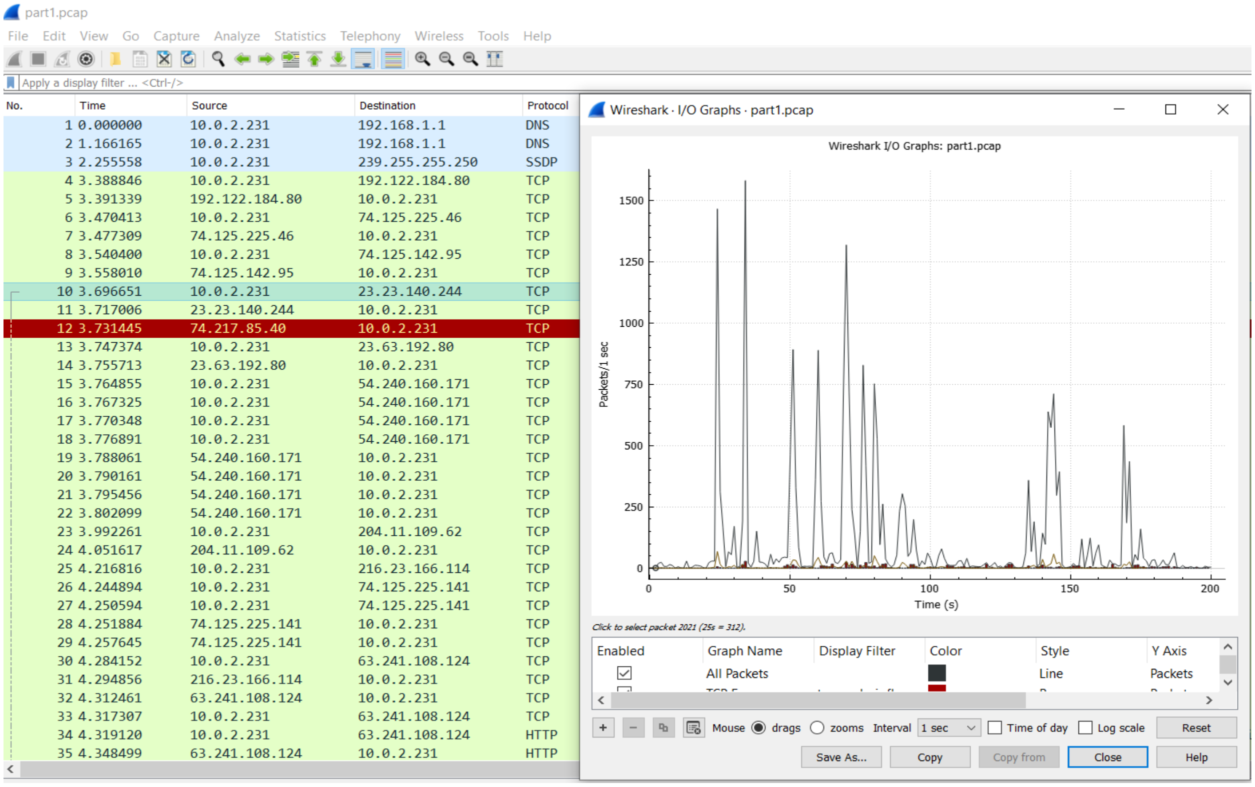

part1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source            Destination       Protocol  Leng
    1 0.000000    10.0.2.231        192.168.1.1       DNS
    2 1.166165    10.0.2.231        192.168.1.1       DNS
    3 2.255558    10.0.2.231        239.255.255.250   SSDP         1
    4 3.388846    10.0.2.231        192.122.184.80    TCP
    5 3.391339    192.122.184.80    10.0.2.231        TCP
    6 3.470413    10.0.2.231        74.125.225.46     TCP
    7 3.477309    74.125.225.46     10.0.2.231        TCP
    8 3.540400    10.0.2.231        74.125.142.95     TCP
    9 3.558010    74.125.142.95     10.0.2.231        TCP
   10 3.696651    10.0.2.231        23.23.140.244     TCP
   11 3.717006    23.23.140.244     10.0.2.231        TCP
   12 3.731445    74.217.85.40      10.0.2.231        TCP
   13 3.747374    10.0.2.231        23.63.192.80      TCP
   14 3.755713    23.63.192.80      10.0.2.231        TCP
   15 3.764855    10.0.2.231        54.240.160.171    TCP
   16 3.767325    10.0.2.231        54.240.160.171    TCP
   17 3.770348    10.0.2.231        54.240.160.171    TCP
   18 3.776891    10.0.2.231        54.240.160.171    TCP
   19 3.788061    54.240.160.171    10.0.2.231        TCP
   20 3.790161    54.240.160.171    10.0.2.231        TCP
   21 3.795456    54.240.160.171    10.0.2.231        TCP
   22 3.802099    54.240.160.171    10.0.2.231        TCP
   23 3.992261    10.0.2.231        204.11.109.62     TCP
   24 4.051617    204.11.109.62     10.0.2.231        TCP
   25 4.216816    10.0.2.231        216.23.166.114    TCP
   26 4.244894    10.0.2.231        74.125.225.141    TCP
   27 4.250594    10.0.2.231        74.125.225.141    TCP
   28 4.251884    74.125.225.141    10.0.2.231        TCP
   29 4.257645    74.125.225.141    10.0.2.231        TCP
   30 4.284152    10.0.2.231        63.241.108.124    TCP
   31 4.294856    216.23.166.114    10.0.2.231        TCP
   32 4.312461    63.241.108.124    10.0.2.231        TCP
   33 4.317307    10.0.2.231        63.241.108.124    TCP
   34 4.319120    10.0.2.231        63.241.108.124    HTTP        13
   35 4.348499    63.241.108.124    10.0.2.231        HTTP         6
```

```
> Frame 15: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)
> Ethernet II, Src: ASUSTekC_8f:29:17 (00:1f:c6:8f:29:17), Dst: Netgear_f6:eb:81 (a4
> Internet Protocol Version 4, Src: 10.0.2.231, Dst: 54.240.160.171
v Transmission Control Protocol, Src Port: 55508, Dst Port: 80, Seq: 1, Ack: 1, Len:
    Source Port: 55508
    Destination Port: 80
    [Stream index: 6]
    [TCP Segment Len: 1]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 158516739
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1495660966
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 256
    [Calculated window size: 256]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xceea [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (1 byte)
```

```
0000  a4 2b 8c f6 eb 81 00 1f  c6 8f 29 17 08 00 45 00   ·+······ ··)···E·
0010  00 29 17 70 40 00 80 06  fe dc 0a 00 02 e7 36 f0   ·)·p@··· ······6·
0020  a0 ab d8 d4 00 50 09 72  c6 03 59 25 f9 a6 50 10   ·····P·r ··Y%··P·
0030  01 00 ce ea 00 00 00                               ·······
```

The SYN flag is noted in the Info column. You can also search for packets with the SYN flag on using the filter expression “tcp.flags.syn==1”. A “SYN packet” is the start of the three-way handshake. In this case it will be sent from your computer to the remote server. The remote server should reply with a TCP segment with the SYN and ACK flags set, or a “SYN ACK packet”. On receiving this segment, your computer will ACK it, consider the connection set up, and begin sending data, which in this case will be the HTTP request.



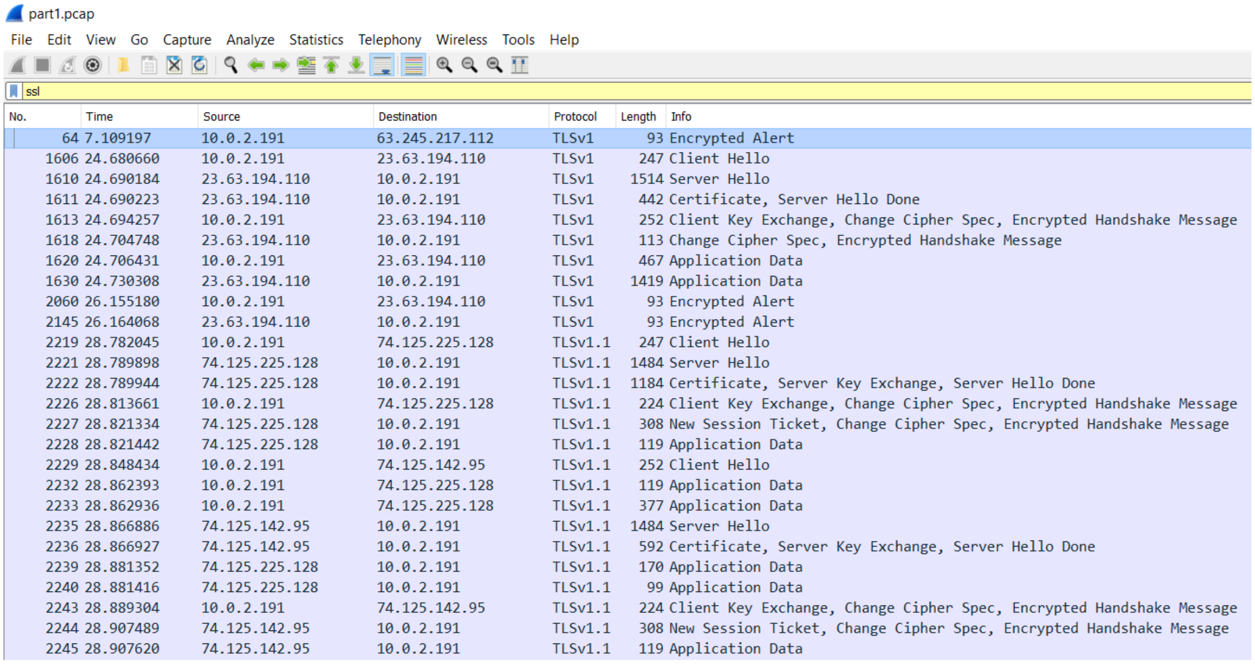
| No. | Time | Source | Destination | Protocol |
|---|---|---|---|---|
| 1 | 0.000000 | 10.0.2.231 | 192.168.1.1 | DNS |
| 2 | 1.166165 | 10.0.2.231 | 192.168.1.1 | DNS |
| 3 | 2.255558 | 10.0.2.231 | 239.255.255.250 | SSDP |
| 4 | 3.388846 | 10.0.2.231 | 192.122.184.80 | TCP |
| 5 | 3.391339 | 192.122.184.80 | 10.0.2.231 | TCP |
| 6 | 3.470413 | 10.0.2.231 | 74.125.225.46 | TCP |
| 7 | 3.477309 | 74.125.225.46 | 10.0.2.231 | TCP |
| 8 | 3.540400 | 10.0.2.231 | 74.125.142.95 | TCP |
| 9 | 3.558010 | 74.125.142.95 | 10.0.2.231 | TCP |
| 10 | 3.696651 | 10.0.2.231 | 23.23.140.244 | TCP |
| 11 | 3.717006 | 23.23.140.244 | 10.0.2.231 | TCP |
| 12 | 3.731445 | 74.217.85.40 | 10.0.2.231 | TCP |
| 13 | 3.747374 | 10.0.2.231 | 23.63.192.80 | TCP |
| 14 | 3.755713 | 23.63.192.80 | 10.0.2.231 | TCP |
| 15 | 3.764855 | 10.0.2.231 | 54.240.160.171 | TCP |
| 16 | 3.767325 | 10.0.2.231 | 54.240.160.171 | TCP |
| 17 | 3.770348 | 10.0.2.231 | 54.240.160.171 | TCP |
| 18 | 3.776891 | 10.0.2.231 | 54.240.160.171 | TCP |
| 19 | 3.788061 | 54.240.160.171 | 10.0.2.231 | TCP |
| 20 | 3.790161 | 54.240.160.171 | 10.0.2.231 | TCP |
| 21 | 3.795456 | 54.240.160.171 | 10.0.2.231 | TCP |
| 22 | 3.802099 | 54.240.160.171 | 10.0.2.231 | TCP |
| 23 | 3.992261 | 10.0.2.231 | 204.11.109.62 | TCP |
| 24 | 4.051617 | 204.11.109.62 | 10.0.2.231 | TCP |
| 25 | 4.216816 | 10.0.2.231 | 216.23.166.114 | TCP |
| 26 | 4.244894 | 10.0.2.231 | 74.125.225.141 | TCP |
| 27 | 4.250594 | 10.0.2.231 | 74.125.225.141 | TCP |
| 28 | 4.251884 | 74.125.225.141 | 10.0.2.231 | TCP |
| 29 | 4.257645 | 74.125.225.141 | 10.0.2.231 | TCP |
| 30 | 4.284152 | 10.0.2.231 | 63.241.108.124 | TCP |
| 31 | 4.294856 | 216.23.166.114 | 10.0.2.231 | TCP |
| 32 | 4.312461 | 63.241.108.124 | 10.0.2.231 | TCP |
| 33 | 4.317307 | 10.0.2.231 | 63.241.108.124 | TCP |
| 34 | 4.319120 | 10.0.2.231 | 63.241.108.124 | HTTP |
| 35 | 4.348499 | 63.241.108.124 | 10.0.2.231 | HTTP |

*Click to select packet 2021 (25s = 312).*

| Enabled | Graph Name | Display Filter | Color | Style | Y Axis |
|---|---|---|---|---|---|
| ☑ | All Packets | | ■ | Line | Packets |

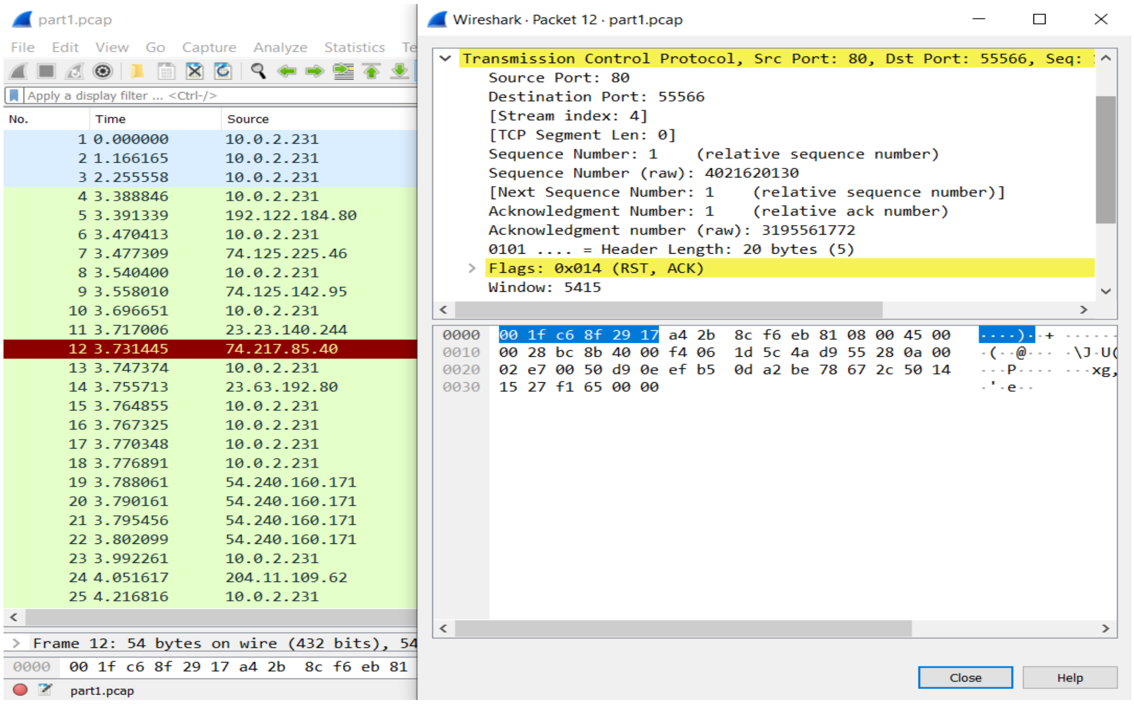
Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale

The middle portion of the TCP connection is the data transfer, or download, in our trace. This is the main event. To get an overall sense of it, we will first look at the download rate over time. Under the Statistics menu select an “IO Graph”


part1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ssl

No.    Time       Source           Destination      Protocol  Length Info
  64 7.109197     10.0.2.191       63.245.217.112   TLSv1       93 Encrypted Alert
1606 24.680660    10.0.2.191       23.63.194.110    TLSv1      247 Client Hello
1610 24.690184    23.63.194.110    10.0.2.191       TLSv1     1514 Server Hello
1611 24.690223    23.63.194.110    10.0.2.191       TLSv1      442 Certificate, Server Hello Done
1613 24.694257    10.0.2.191       23.63.194.110    TLSv1      252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1618 24.704748    23.63.194.110    10.0.2.191       TLSv1      113 Change Cipher Spec, Encrypted Handshake Message
1620 24.706431    10.0.2.191       23.63.194.110    TLSv1      467 Application Data
1630 24.730308    23.63.194.110    10.0.2.191       TLSv1     1419 Application Data
2060 26.155180    10.0.2.191       23.63.194.110    TLSv1       93 Encrypted Alert
2145 26.164068    23.63.194.110    10.0.2.191       TLSv1       93 Encrypted Alert
2219 28.782045    10.0.2.191       74.125.225.128   TLSv1.1    247 Client Hello
2221 28.789898    74.125.225.128   10.0.2.191       TLSv1.1   1484 Server Hello
2222 28.789944    74.125.225.128   10.0.2.191       TLSv1.1   1184 Certificate, Server Key Exchange, Server Hello Done
2226 28.813661    10.0.2.191       74.125.225.128   TLSv1.1    224 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2227 28.821334    74.125.225.128   10.0.2.191       TLSv1.1    308 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2228 28.821442    74.125.225.128   10.0.2.191       TLSv1.1    119 Application Data
2229 28.848434    10.0.2.191       74.125.142.95    TLSv1.1    252 Client Hello
2232 28.862393    10.0.2.191       74.125.225.128   TLSv1.1    119 Application Data
2233 28.862936    10.0.2.191       74.125.225.128   TLSv1.1    377 Application Data
2235 28.866886    74.125.142.95    10.0.2.191       TLSv1.1   1484 Server Hello
2236 28.866927    74.125.142.95    10.0.2.191       TLSv1.1    592 Certificate, Server Key Exchange, Server Hello Done
2239 28.881352    74.125.225.128   10.0.2.191       TLSv1.1    170 Application Data
2240 28.881416    74.125.225.128   10.0.2.191       TLSv1.1     99 Application Data
2243 28.889304    10.0.2.191       74.125.142.95    TLSv1.1    224 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2244 28.907489    74.125.142.95    10.0.2.191       TLSv1.1    308 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2245 28.907620    74.125.142.95    10.0.2.191       TLSv1.1    119 Application Data
```

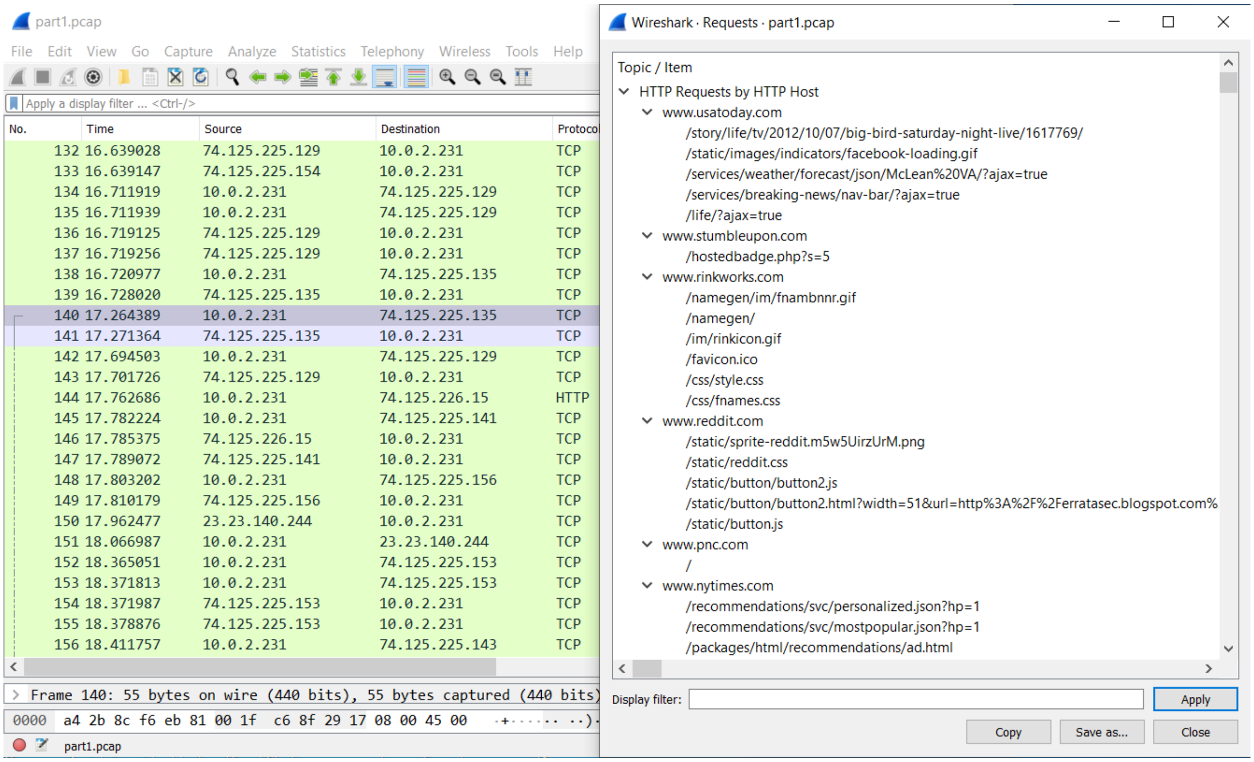
This filter will help to simplify the display by showing only SSL and TLS messages. It will exclude other TCP segments that are part of the trace, such as Acks and connection open/close.


part1.pcap
File Edit View Go Capture Analyze Statistics Te
Wireshark · Packet 12 · part1.pcap
Close
Help

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

No.  Time        Source
 1 0.000000      10.0.2.231
 2 1.166165      10.0.2.231
 3 2.255558      10.0.2.231
 4 3.388846      10.0.2.231
 5 3.391339      192.122.184.80
 6 3.470413      10.0.2.231
 7 3.477309      74.125.225.46
 8 3.540400      10.0.2.231
 9 3.558010      74.125.142.95
10 3.696651      10.0.2.231
11 3.717006      23.23.140.244
12 3.731445      74.217.85.40
13 3.747374      10.0.2.231
14 3.755713      23.63.192.80
15 3.764855      10.0.2.231
16 3.767325      10.0.2.231
17 3.770348      10.0.2.231
18 3.776891      10.0.2.231
19 3.788061      54.240.160.171
20 3.790161      54.240.160.171
21 3.795456      54.240.160.171
22 3.802099      54.240.160.171
23 3.992261      10.0.2.231
24 4.051617      204.11.109.62
25 4.216816      10.0.2.231

> Frame 12: 54 bytes on wire (432 bits), 54
0000  00 1f c6 8f 29 17 a4 2b  8c f6 eb 81
part1.pcap
```

```
v Transmission Control Protocol, Src Port: 80, Dst Port: 55566, Seq: 
      Source Port: 80
      Destination Port: 55566
      [Stream index: 4]
      [TCP Segment Len: 0]
      Sequence Number: 1    (relative sequence number)
      Sequence Number (raw): 4021620130
      [Next Sequence Number: 1    (relative sequence number)]
      Acknowledgment Number: 1    (relative ack number)
      Acknowledgment number (raw): 3195561772
      0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x014 (RST, ACK)
      Window: 5415

0000  00 1f c6 8f 29 17 a4 2b  8c f6 eb 81 08 00 45 00   ····)·+ ······
0010  00 28 bc 8b 40 00 f4 06  1d 5c 4a d9 55 28 0a 00   ·(··@··· ·\J·U(
0020  02 e7 00 50 d9 0e ef b5  0d a2 be 78 67 2c 50 14   ···P···· ···xg,
0030  15 27 f1 65 00 00                                   ·'·e··
```

The source is the system sending the data; the destination is the system receiving the data. TCP ports. TCP connects from a source port to a destination port, such as from source port 51178 to destination port 22.


part1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Requests · part1.pcap
Display filter:
Apply
Copy
Save as...
Close

```
No.        Time        Source            Destination       Protoco
     132 16.639028   74.125.225.129    10.0.2.231        TCP
     133 16.639147   74.125.225.154    10.0.2.231        TCP
     134 16.711919   10.0.2.231        74.125.225.129    TCP
     135 16.711939   10.0.2.231        74.125.225.129    TCP
     136 16.719125   74.125.225.129    10.0.2.231        TCP
     137 16.719256   74.125.225.129    10.0.2.231        TCP
     138 16.720977   10.0.2.231        74.125.225.135    TCP
     139 16.728020   74.125.225.135    10.0.2.231        TCP
     140 17.264389   10.0.2.231        74.125.225.135    TCP
     141 17.271364   74.125.225.135    10.0.2.231        TCP
     142 17.694503   10.0.2.231        74.125.225.129    TCP
     143 17.701726   74.125.225.129    10.0.2.231        TCP
     144 17.762686   10.0.2.231        74.125.226.15     HTTP
     145 17.782224   10.0.2.231        74.125.225.141    TCP
     146 17.785375   74.125.226.15     10.0.2.231        TCP
     147 17.789072   74.125.225.141    10.0.2.231        TCP
     148 17.803202   10.0.2.231        74.125.225.156    TCP
     149 17.810179   74.125.225.156    10.0.2.231        TCP
     150 17.962477   23.23.140.244     10.0.2.231        TCP
     151 18.066987   10.0.2.231        23.23.140.244     TCP
     152 18.365051   10.0.2.231        74.125.225.153    TCP
     153 18.371813   10.0.2.231        74.125.225.153    TCP
     154 18.371987   74.125.225.153    10.0.2.231        TCP
     155 18.378876   74.125.225.153    10.0.2.231        TCP
     156 18.411757   10.0.2.231        74.125.225.143    TCP

> Frame 140: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)
0000  a4 2b 8c f6 eb 81 00 1f  c6 8f 29 17 08 00 45 00   ·+······ ··)·
```

```
Topic / Item
 HTTP Requests by HTTP Host
   www.usatoday.com
     /story/life/tv/2012/10/07/big-bird-saturday-night-live/1617769/
     /static/images/indicators/facebook-loading.gif
     /services/weather/forecast/json/McLean%20VA/?ajax=true
     /services/breaking-news/nav-bar/?ajax=true
     /life/?ajax=true
   www.stumbleupon.com
     /hostedbadge.php?s=5
   www.rinkworks.com
     /namegen/im/fnambnnr.gif
     /namegen/
     /im/rinkicon.gif
     /favicon.ico
     /css/style.css
     /css/fnames.css
   www.reddit.com
     /static/sprite-reddit.m5w5UirzUrM.png
     /static/reddit.css
     /static/button/button2.js
     /static/button/button2.html?width=51&url=http%3A%2F%2Ferratasec.blogspot.com%
     /static/button.js
   www.pnc.com
     /
   www.nytimes.com
     /recommendations/svc/personalized.json?hp=1
     /recommendations/svc/mostpopular.json?hp=1
     /packages/html/recommendations/ad.html
```

You can find a list of all captured requests in the "Statistics" > "HTTP" > "Requests" menu.