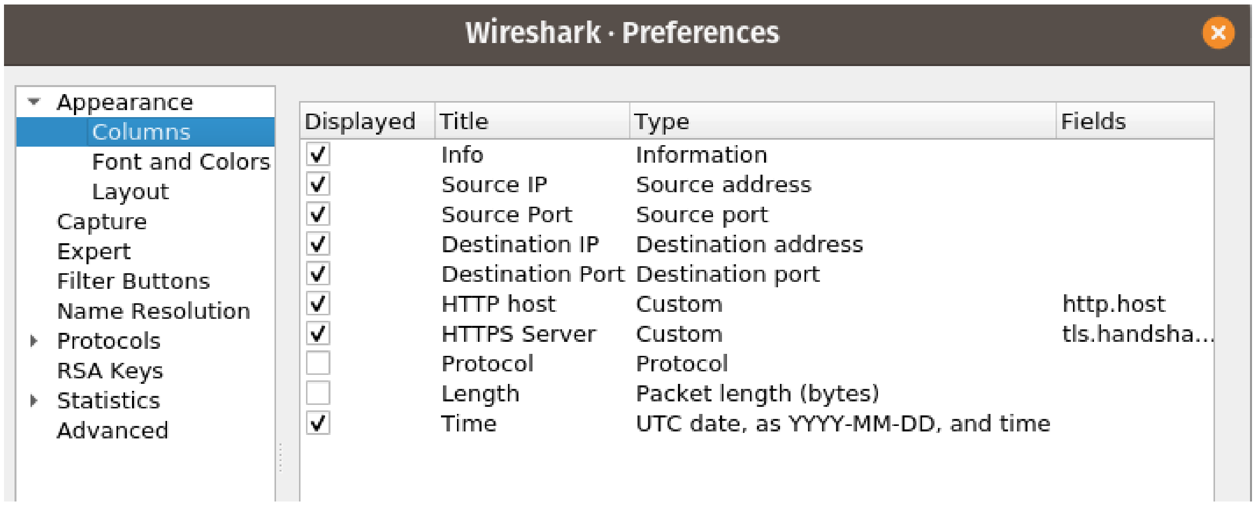
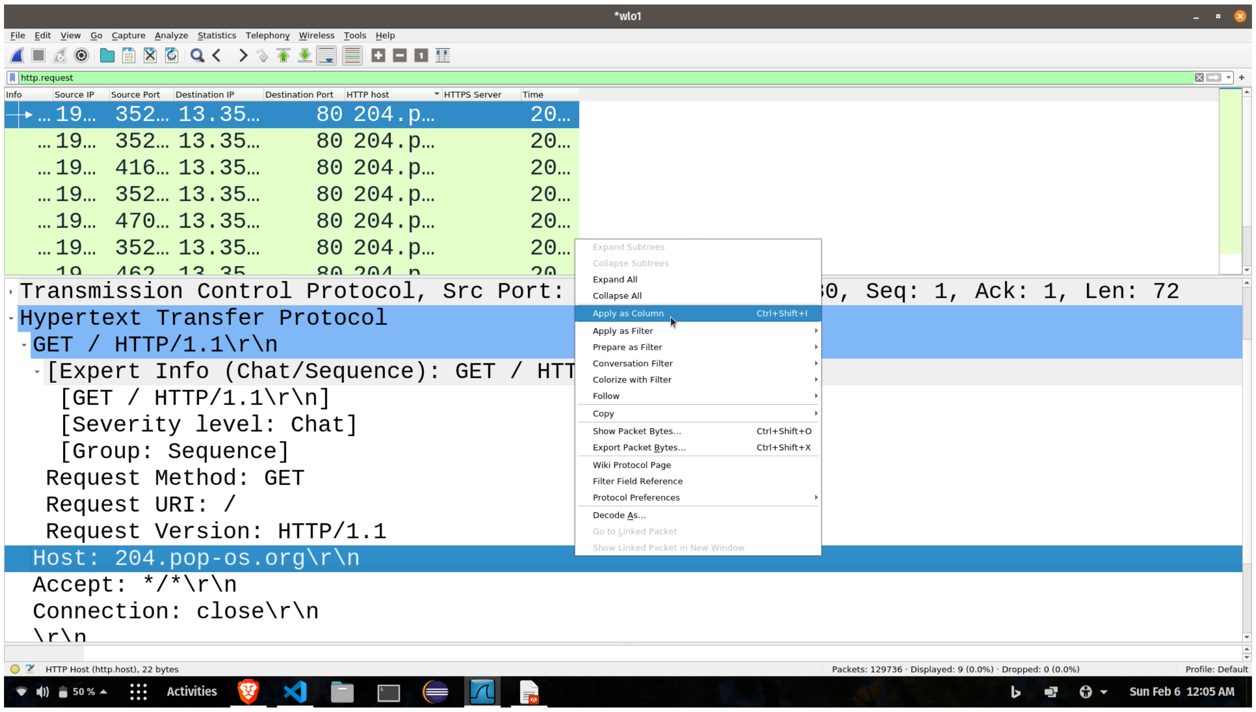
Q1



Displayed	Title	Type	Fields
✓	Info	Information	
✓	Source IP	Source address	
✓	Source Port	Source port	
✓	Destination IP	Destination address	
✓	Destination Port	Destination port	
✓	HTTP host	Custom	http.host
✓	HTTPS Server	Custom	tls.handsha…
	Protocol	Protocol	
	Length	Packet length (bytes)	
✓	Time	UTC date, as YYYY-MM-DD, and time	

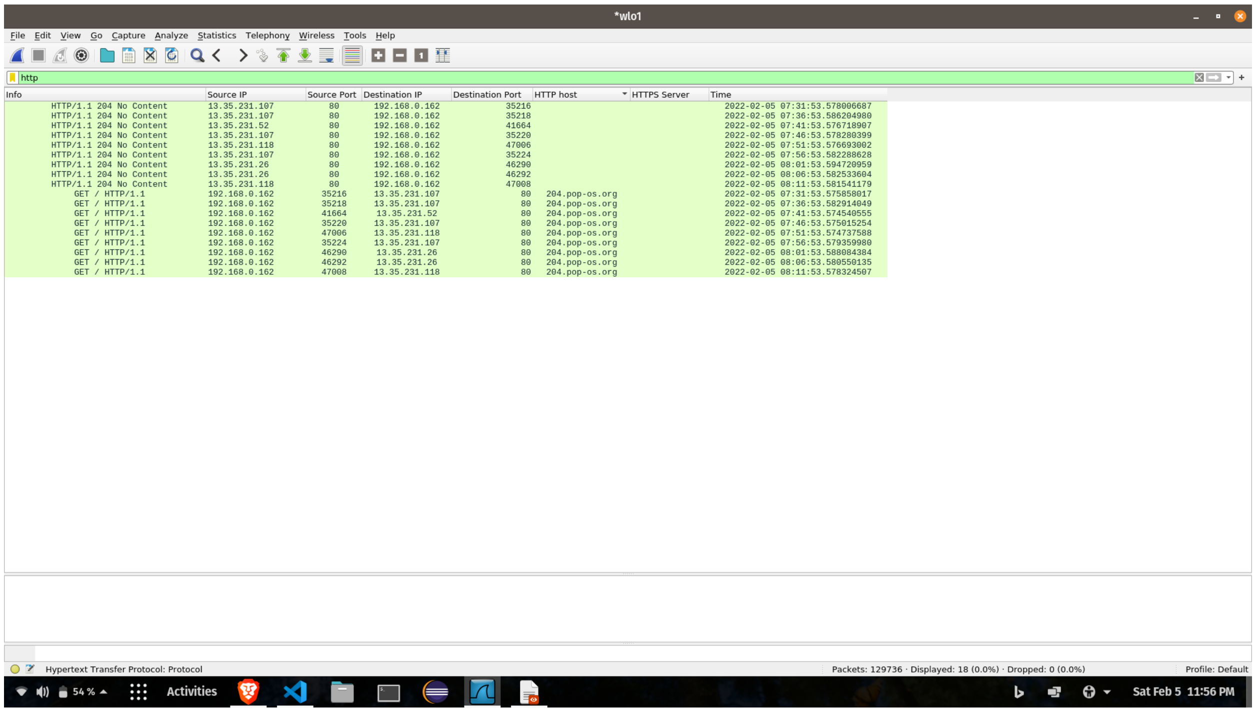
One can use preferences to add/edit/remove UTC time, Source Port, Source IP, Destination Port, Destination IP, Info.

To add an HTTP host, one can add it as a custom column by clicking Apply as a column after navigating to HTTP Host. Same Procedure for HTTP server.



```
http.request
Info  Source IP  Source Port  Destination IP  Destination Port  HTTP host  HTTPS Server  Time
…19…  352…  13.35…  80  204.p…  20…
…19…  352…  13.35…  80  204.p…  20…
…19…  416…  13.35…  80  204.p…  20…
…19…  352…  13.35…  80  204.p…  20…
…19…  470…  13.35…  80  204.p…  20…
…19…  352…  13.35…  80  204.p…  20…
 19…  462…  13.35…  80  204.p…  20…
Transmission Control Protocol, Src Port: …0, Seq: 1, Ack: 1, Len: 72
Hypertext Transfer Protocol
 GET / HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET / HTT
   [GET / HTTP/1.1\r\n]
   [Severity level: Chat]
   [Group: Sequence]
  Request Method: GET
  Request URI: /
  Request Version: HTTP/1.1
 Host: 204.pop-os.org\r\n
 Accept: */*\r\n
 Connection: close\r\n
 \r\n
HTTP Host (http.host), 22 bytes    Packets: 129736 · Displayed: 9 (0.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Final Screenshot 1



*wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Info	Source IP	Source Port	Destination IP	Destination Port	HTTP host	HTTPS Server	Time
HTTP/1.1 204 No Content	13.35.231.107	80	192.168.0.162	35216			2022-02-05 07:31:53.578006687
HTTP/1.1 204 No Content	13.35.231.107	80	192.168.0.162	35218			2022-02-05 07:36:53.586204980
HTTP/1.1 204 No Content	13.35.231.52	80	192.168.0.162	41664			2022-02-05 07:41:53.576718907
HTTP/1.1 204 No Content	13.35.231.107	80	192.168.0.162	35220			2022-02-05 07:46:53.578280399
HTTP/1.1 204 No Content	13.35.231.118	80	192.168.0.162	47006			2022-02-05 07:51:53.576693002
HTTP/1.1 204 No Content	13.35.231.107	80	192.168.0.162	35224			2022-02-05 07:56:53.582288628
HTTP/1.1 204 No Content	13.35.231.26	80	192.168.0.162	46290			2022-02-05 08:01:53.594720959
HTTP/1.1 204 No Content	13.35.231.26	80	192.168.0.162	46292			2022-02-05 08:06:53.582533604
HTTP/1.1 204 No Content	13.35.231.118	80	192.168.0.162	47008			2022-02-05 08:11:53.581541179
GET / HTTP/1.1	192.168.0.162	35216	13.35.231.107	80	204.pop-os.org		2022-02-05 07:31:53.575858017
GET / HTTP/1.1	192.168.0.162	35218	13.35.231.107	80	204.pop-os.org		2022-02-05 07:36:53.582914049
GET / HTTP/1.1	192.168.0.162	41664	13.35.231.52	80	204.pop-os.org		2022-02-05 07:41:53.574540555
GET / HTTP/1.1	192.168.0.162	35220	13.35.231.107	80	204.pop-os.org		2022-02-05 07:46:53.575015254
GET / HTTP/1.1	192.168.0.162	47006	13.35.231.118	80	204.pop-os.org		2022-02-05 07:51:53.574737588
GET / HTTP/1.1	192.168.0.162	35224	13.35.231.107	80	204.pop-os.org		2022-02-05 07:56:53.579359980
GET / HTTP/1.1	192.168.0.162	46290	13.35.231.26	80	204.pop-os.org		2022-02-05 08:01:53.588084384
GET / HTTP/1.1	192.168.0.162	46292	13.35.231.26	80	204.pop-os.org		2022-02-05 08:06:53.580550135
GET / HTTP/1.1	192.168.0.162	47008	13.35.231.118	80	204.pop-os.org		2022-02-05 08:11:53.578324507

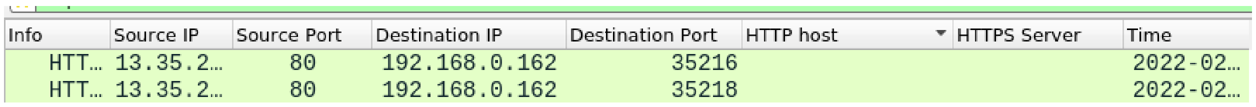
Hypertext Transfer Protocol: Protocol

Packets: 129736 · Displayed: 18 (0.0%) · Dropped: 0 (0.0%)

Profile: Default

54 % Activities Sat Feb 5 11:56 PM

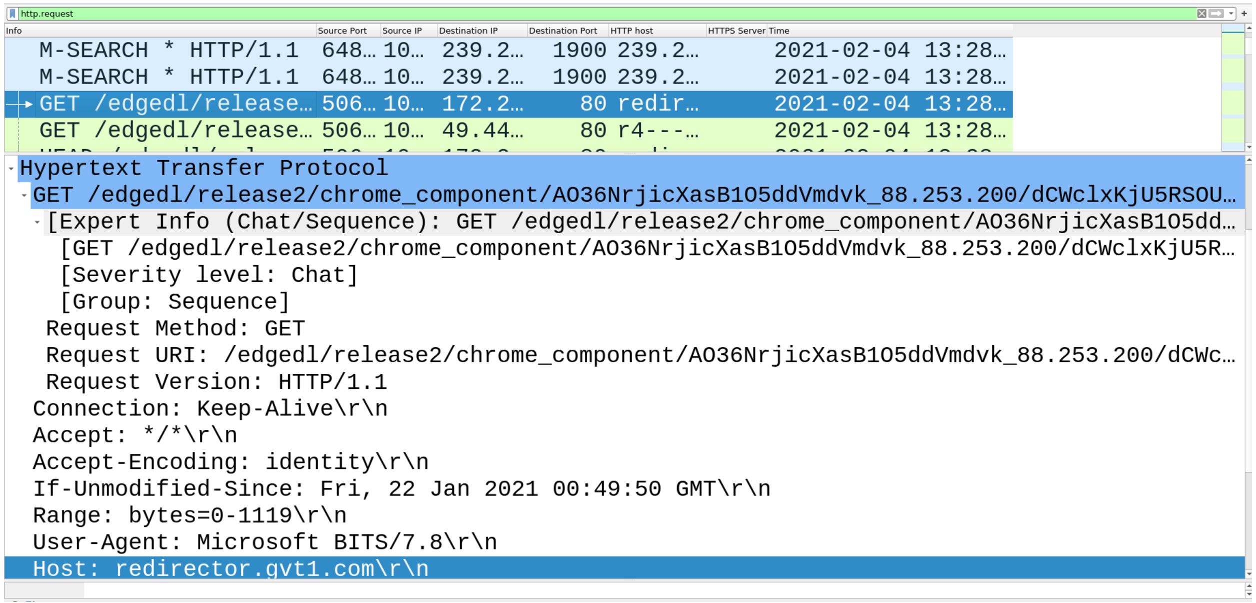
Close Up View:



Info	Source IP	Source Port	Destination IP	Destination Port	HTTP host	HTTPS Server	Time
HTT…	13.35.2…	80	192.168.0.162	35216			2022-02…
HTT…	13.35.2…	80	192.168.0.162	35218			2022-02…

Q2

HTTP request packet:

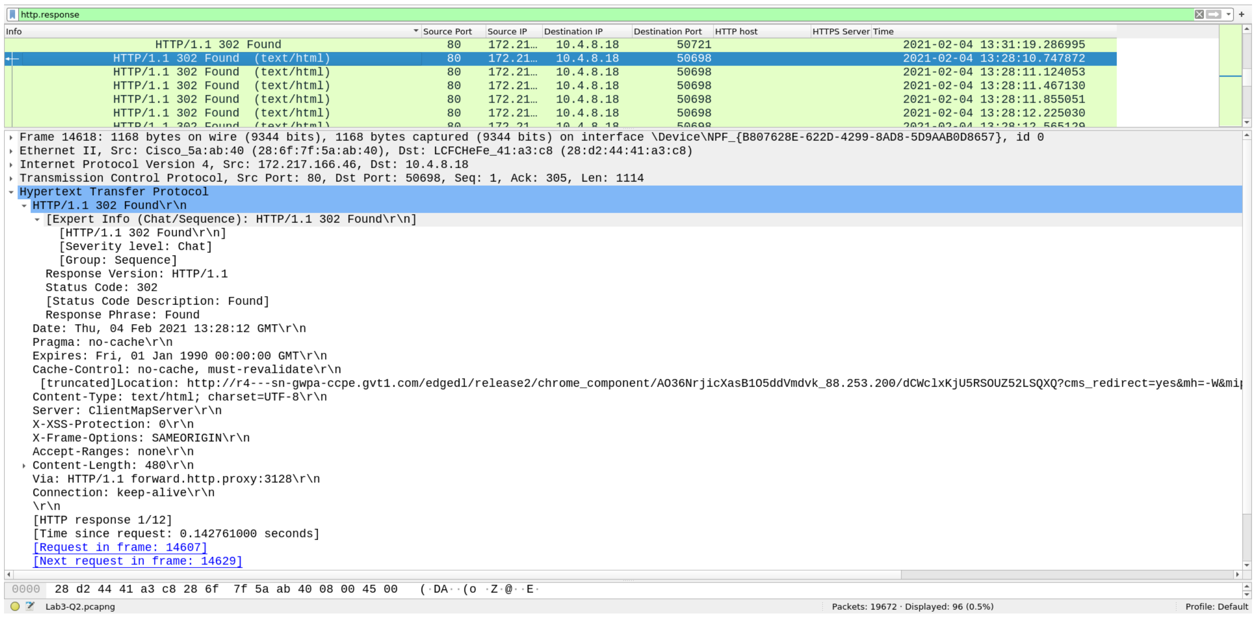


http.request

Info	Source Port	Source IP	Destination IP	Destination Port	HTTP host	HTTPS Server	Time
M-SEARCH * HTTP/1.1	648…	10…	239.2…	1900	239.2…		2021-02-04 13:28…
M-SEARCH * HTTP/1.1	648…	10…	239.2…	1900	239.2…		2021-02-04 13:28…
GET /edgedl/release…	506…	10…	172.2…	80	redir…		2021-02-04 13:28…
GET /edgedl/release…	506…	10…	49.44…	80	r4---…		2021-02-04 13:28…

```
Hypertext Transfer Protocol
 GET /edgedl/release2/chrome_component/AO36NrjicXasB1O5ddVmdvk_88.253.200/dCWclxKjU5RSOU…
  [Expert Info (Chat/Sequence): GET /edgedl/release2/chrome_component/AO36NrjicXasB1O5dd…
   [GET /edgedl/release2/chrome_component/AO36NrjicXasB1O5ddVmdvk_88.253.200/dCWclxKjU5R…
   [Severity level: Chat]
   [Group: Sequence]
  Request Method: GET
  Request URI: /edgedl/release2/chrome_component/AO36NrjicXasB1O5ddVmdvk_88.253.200/dCWc…
  Request Version: HTTP/1.1
 Connection: Keep-Alive\r\n
 Accept: */*\r\n
 Accept-Encoding: identity\r\n
 If-Unmodified-Since: Fri, 22 Jan 2021 00:49:50 GMT\r\n
 Range: bytes=0-1119\r\n
 User-Agent: Microsoft BITS/7.8\r\n
 Host: redirector.gvt1.com\r\n
```

HTTP response packet



http.response

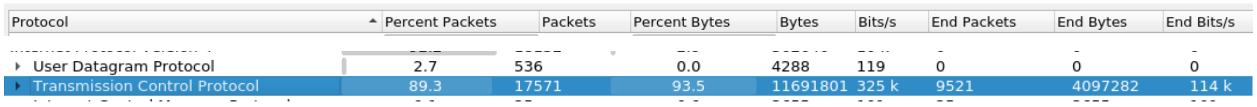
Info	Source Port	Source IP	Destination IP	Destination Port	HTTP host	HTTPS Server	Time
HTTP/1.1 302 Found	80	172.21…	10.4.8.18	50721			2021-02-04 13:31:19.286995
HTTP/1.1 302 Found (text/html)	80	172.21…	10.4.8.18	50698			2021-02-04 13:28:10.747872
HTTP/1.1 302 Found (text/html)	80	172.21…	10.4.8.18	50698			2021-02-04 13:28:11.124053
HTTP/1.1 302 Found (text/html)	80	172.21…	10.4.8.18	50698			2021-02-04 13:28:11.467130
HTTP/1.1 302 Found (text/html)	80	172.21…	10.4.8.18	50698			2021-02-04 13:28:11.855051
HTTP/1.1 302 Found (text/html)	80	172.21…	10.4.8.18	50698			2021-02-04 13:28:12.225030
HTTP/1.1 302 Found (text/html)	80	172.21…	10.4.8.18	50698			2021-02-04 13:28:12.565129

```
› Frame 14618: 1168 bytes on wire (9344 bits), 1168 bytes captured (9344 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
› Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8)
› Internet Protocol Version 4, Src: 172.217.166.46, Dst: 10.4.8.18
› Transmission Control Protocol, Src Port: 80, Dst Port: 50698, Seq: 1, Ack: 305, Len: 1114
⌄ Hypertext Transfer Protocol
  ⌄ HTTP/1.1 302 Found\r\n
    ⌄ [Expert Info (Chat/Sequence): HTTP/1.1 302 Found\r\n]
        [HTTP/1.1 302 Found\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 302
      [Status Code Description: Found]
      Response Phrase: Found
    Date: Thu, 04 Feb 2021 13:28:12 GMT\r\n
    Pragma: no-cache\r\n
    Expires: Fri, 01 Jan 1990 00:00:00 GMT\r\n
    Cache-Control: no-cache, must-revalidate\r\n
     [truncated]Location: http://r4---sn-gwpa-ccpe.gvt1.com/edgedl/release2/chrome_component/AO36NrjicXasB1O5ddVmdvk_88.253.200/dCWclxKjU5RSOUZ52LSQXQ?cms_redirect=yes&mh=-W&mi
    Content-Type: text/html; charset=UTF-8\r\n
    Server: ClientMapServer\r\n
    X-XSS-Protection: 0\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    Accept-Ranges: none\r\n
  › Content-Length: 480\r\n
    Via: HTTP/1.1 forward.http.proxy:3128\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/12]
    [Time since request: 0.142761000 seconds]
    [Request in frame: 14607]
    [Next request in frame: 14629]

0000  28 d2 44 41 a3 c8 28 6f  7f 5a ab 40 08 00 45 00   (·DA··(o ·Z·@··E·
```

Lab3-Q2.pcapng   Packets: 19672 · Displayed: 96 (0.5%)   Profile: Default

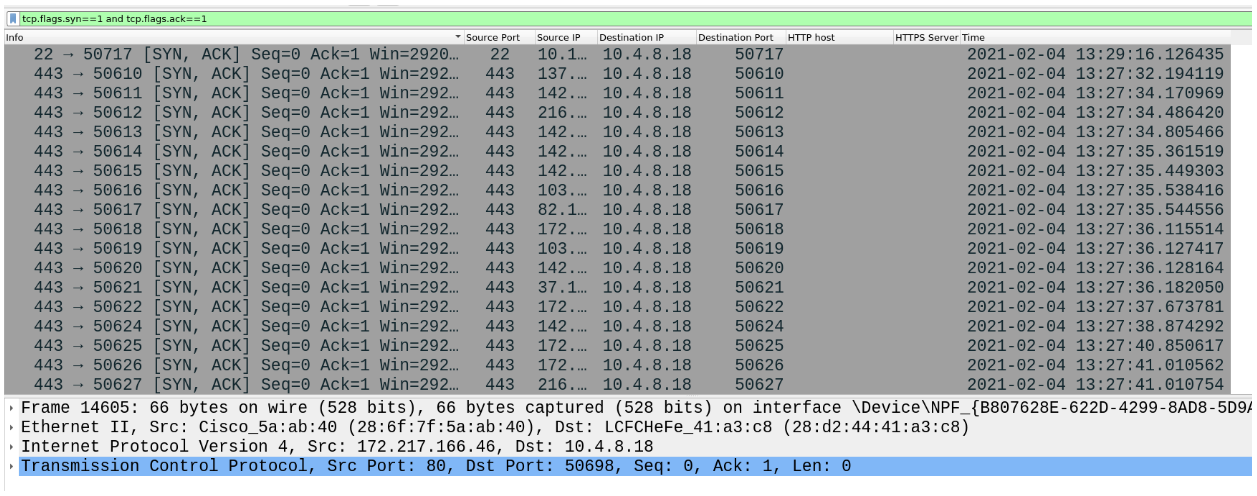
TCP and UDP Statistics



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
› User Datagram Protocol	2.7	536	0.0	4288	119	0	0	0
› Transmission Control Protocol	89.3	17571	93.5	11691801	325 k	9521	4097282	114 k

```
=================================================================================
=================================================================
IPv4 Statistics/IP Protocol Types:
Topic / Item      Count        Average       Min val       Max val       Rate (ms)      Percent        Burst
rate     Burst start
---------------------------------------------------------------------------------------------------------------
IP Protocol Types  18132                                        0.0636        100%          6.7200
14.965
 UDP            561                                        0.0020        3.09%         0.2100        24.648
 TCP            17571                                        0.0616        96.91%        6.7200
14.965
---------------------------------------------------------------------------------------------------------------
IPv6 Statistics/IP Protocol Types:
Topic / Item      Count        Average       Min val       Max val       Rate (ms)      Percent        Burst
rate     Burst start
---------------------------------------------------------------------------------------------------------------
---
IP Protocol Types  83                                        0.0003        100%          0.0600
10.162
 UDP            80                                        0.0003        96.39%        0.0600        10.162
 NONE            3                                        0.0000        3.61%         0.0100        17.228
```

TCP Packets whose SYN and ACK flags are set:

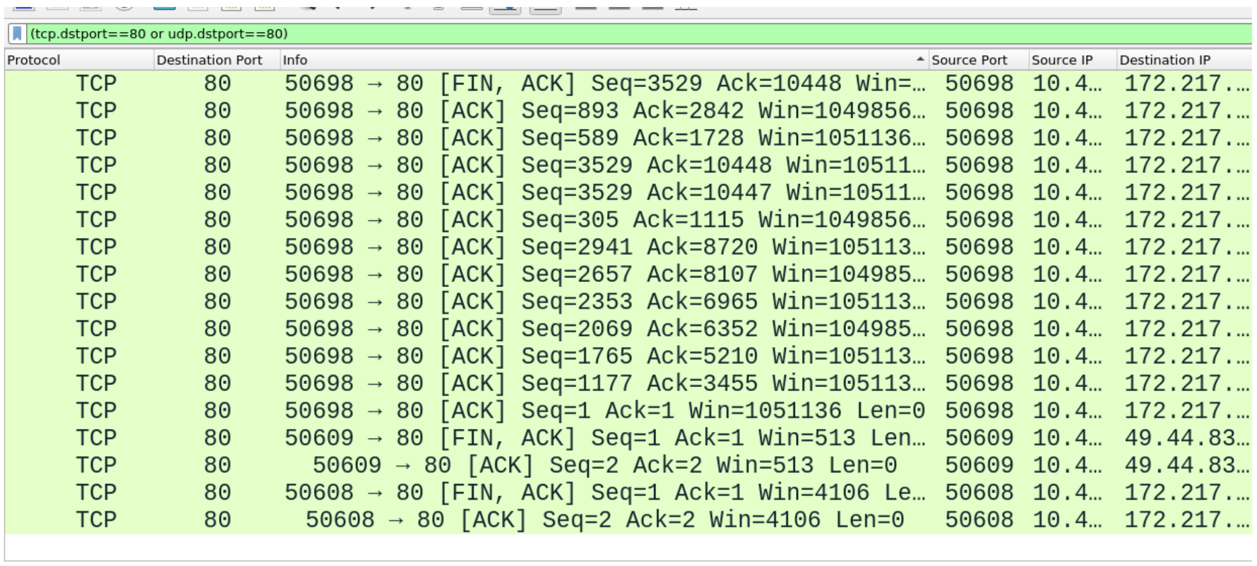


tcp.flags.syn==1 and tcp.flags.ack==1

Info	Source Port	Source IP	Destination IP	Destination Port	HTTP host	HTTPS Server	Time
22 → 50717 [SYN, ACK] Seq=0 Ack=1 Win=2920…	22	10.1…	10.4.8.18	50717			2021-02-04 13:29:16.126435
443 → 50610 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	137.…	10.4.8.18	50610			2021-02-04 13:27:32.194119
443 → 50611 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	142.…	10.4.8.18	50611			2021-02-04 13:27:34.170969
443 → 50612 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	216.…	10.4.8.18	50612			2021-02-04 13:27:34.486420
443 → 50613 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	142.…	10.4.8.18	50613			2021-02-04 13:27:34.805466
443 → 50614 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	142.…	10.4.8.18	50614			2021-02-04 13:27:35.361519
443 → 50615 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	142.…	10.4.8.18	50615			2021-02-04 13:27:35.449303
443 → 50616 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	103.…	10.4.8.18	50616			2021-02-04 13:27:35.538416
443 → 50617 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	82.1…	10.4.8.18	50617			2021-02-04 13:27:35.544556
443 → 50618 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	172.…	10.4.8.18	50618			2021-02-04 13:27:36.115514
443 → 50619 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	103.…	10.4.8.18	50619			2021-02-04 13:27:36.127417
443 → 50620 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	142.…	10.4.8.18	50620			2021-02-04 13:27:36.128164
443 → 50621 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	37.1…	10.4.8.18	50621			2021-02-04 13:27:36.182050
443 → 50622 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	172.…	10.4.8.18	50622			2021-02-04 13:27:37.673781
443 → 50624 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	142.…	10.4.8.18	50624			2021-02-04 13:27:38.874292
443 → 50625 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	172.…	10.4.8.18	50625			2021-02-04 13:27:40.850617
443 → 50626 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	172.…	10.4.8.18	50626			2021-02-04 13:27:41.010562
443 → 50627 [SYN, ACK] Seq=0 Ack=1 Win=292…	443	216.…	10.4.8.18	50627			2021-02-04 13:27:41.010754

```
Frame 14605: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9A
Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFCHeFe_41:a3:c8 (28:d2:44:41:a3:c8)
Internet Protocol Version 4, Src: 172.217.166.46, Dst: 10.4.8.18
Transmission Control Protocol, Src Port: 80, Dst Port: 50698, Seq: 0, Ack: 1, Len: 0
```

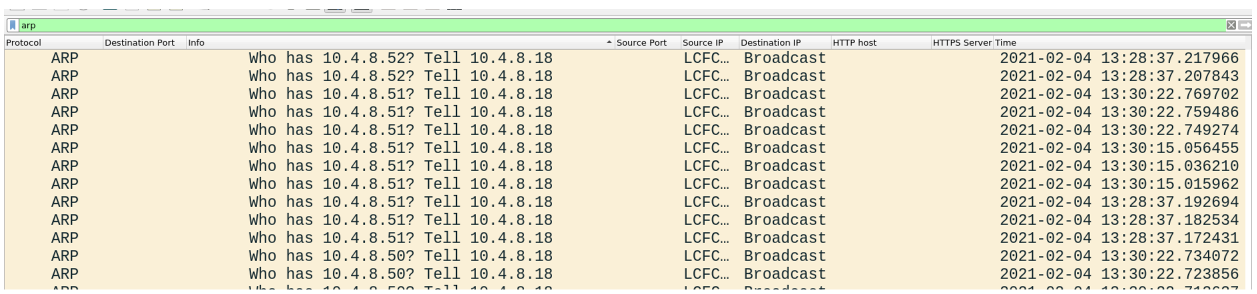
TCP and UDP packets whose dstport==80



(tcp.dstport==80 or udp.dstport==80)

Protocol	Destination Port	Info	Source Port	Source IP	Destination IP
TCP	80	50698 → 80 [FIN, ACK] Seq=3529 Ack=10448 Win=…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=893 Ack=2842 Win=1049856…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=589 Ack=1728 Win=1051136…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=3529 Ack=10448 Win=10511…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=3529 Ack=10447 Win=10511…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=305 Ack=1115 Win=1049856…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=2941 Ack=8720 Win=105113…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=2657 Ack=8107 Win=104985…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=2353 Ack=6965 Win=105113…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=2069 Ack=6352 Win=104985…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=1765 Ack=5210 Win=105113…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=1177 Ack=3455 Win=105113…	50698	10.4…	172.217.…
TCP	80	50698 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0	50698	10.4…	172.217.…
TCP	80	50609 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len…	50609	10.4…	49.44.83…
TCP	80	50609 → 80 [ACK] Seq=2 Ack=2 Win=513 Len=0	50609	10.4…	49.44.83…
TCP	80	50608 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4106 Le…	50608	10.4…	172.217.…
TCP	80	50608 → 80 [ACK] Seq=2 Ack=2 Win=4106 Len=0	50608	10.4…	172.217.…

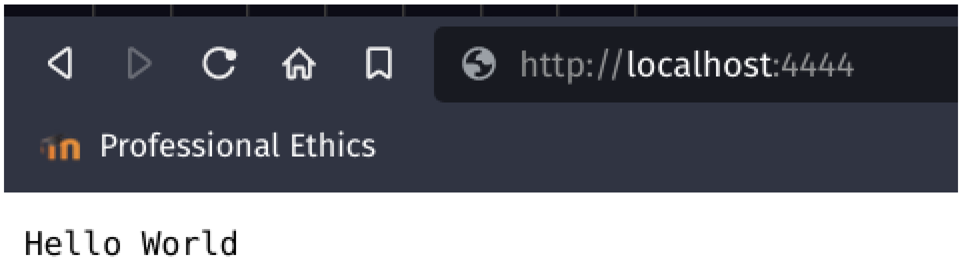
ARP Packets



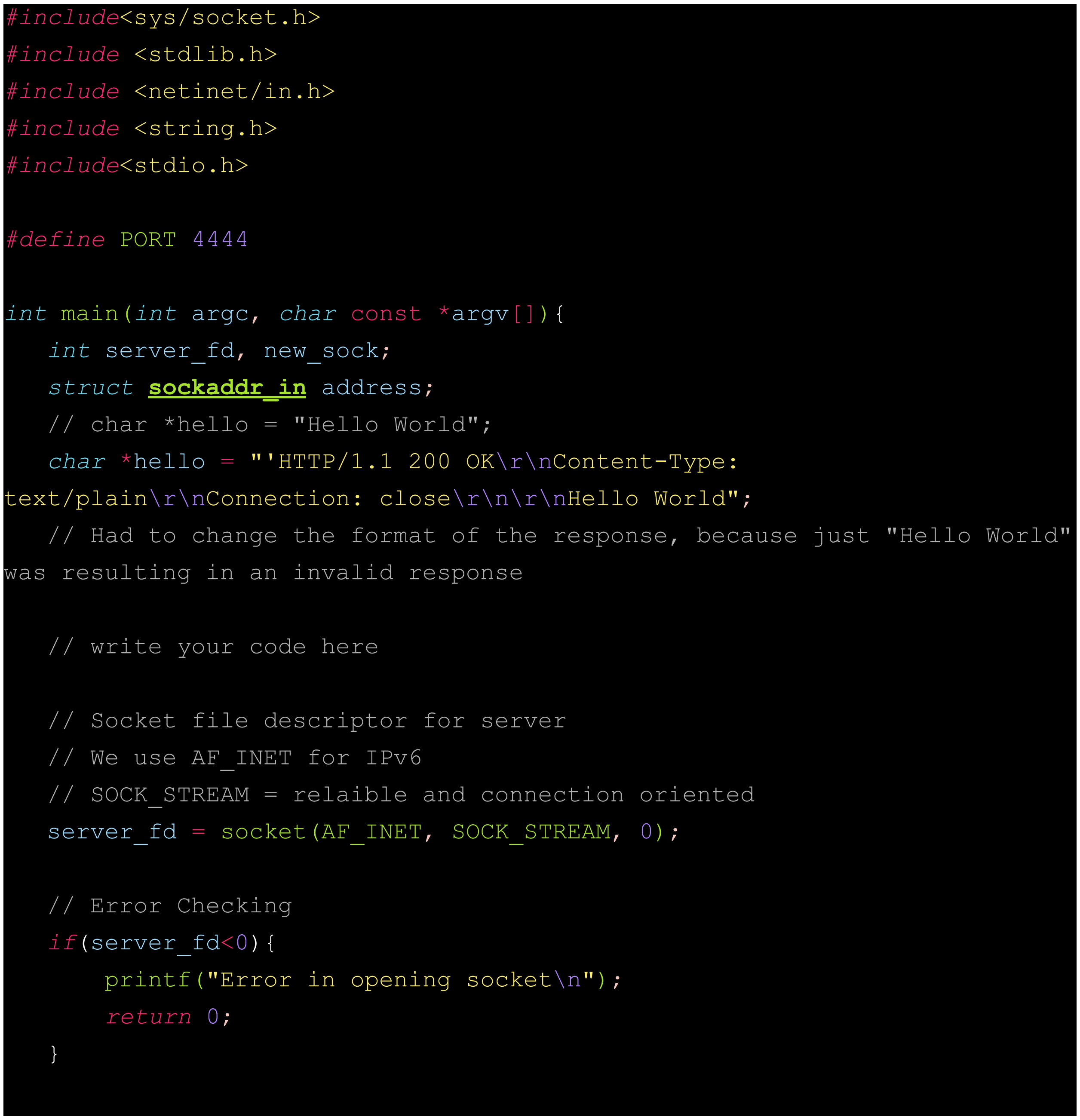
arp

Protocol	Destination Port	Info	Source Port	Source IP	Destination IP	HTTP host	HTTPS Server	Time
ARP		Who has 10.4.8.52? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:28:37.217966
ARP		Who has 10.4.8.52? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:28:37.207843
ARP		Who has 10.4.8.51? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:30:22.769702
ARP		Who has 10.4.8.51? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:30:22.759486
ARP		Who has 10.4.8.51? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:30:22.749274
ARP		Who has 10.4.8.51? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:30:15.056455
ARP		Who has 10.4.8.51? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:30:15.036210
ARP		Who has 10.4.8.51? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:30:15.015962
ARP		Who has 10.4.8.51? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:28:37.192694
ARP		Who has 10.4.8.51? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:28:37.182534
ARP		Who has 10.4.8.51? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:28:37.172431
ARP		Who has 10.4.8.50? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:30:22.734072
ARP		Who has 10.4.8.50? Tell 10.4.8.18		LCFC…	Broadcast			2021-02-04 13:30:22.723856

Q3



```
Hello World
```



```
#include<sys/socket.h>
#include <stdlib.h>
#include <netinet/in.h>
#include <string.h>
#include<stdio.h>

#define PORT 4444

int main(int argc, char const *argv[]){
   int server_fd, new_sock;
   struct sockaddr_in address;
   // char *hello = "Hello World";
   char *hello = "'HTTP/1.1 200 OK\r\nContent-Type:
text/plain\r\nConnection: close\r\n\r\nHello World";
   // Had to change the format of the response, because just "Hello World"
was resulting in an invalid response

   // write your code here

   // Socket file descriptor for server
   // We use AF_INET for IPv6
   // SOCK_STREAM = relaible and connection oriented
   server_fd = socket(AF_INET, SOCK_STREAM, 0);

   // Error Checking
   if(server_fd<0){
       printf("Error in opening socket\n");
       return 0;
   }
   // Need to specifiy address and port number so that it can bind to it
   address.sin_family = AF_INET;
   address.sin_addr.s_addr = INADDR_ANY;
   address.sin_port = htons(PORT);


   // need to bind the server_fd to an address and a port as mentioned in
struct (sockaddr_in) (4444 in this case)
   if(bind(server_fd, (struct sockaddr *) &address, sizeof(address)) ==
-1){
       printf("Cannot bind\n");
       return 0;
   }


   // this is needed so that the socket waits for client to approach. The
number 7 is the maximum queue size.
   listen(server_fd, 7);

   int addrlen = sizeof(address); // had to initialize this variable in
order to pass it as a pointer in a later function
   // it accepts the first connection request from the listening socket
queue and creates a new connected socket and returns a file descriptor
   new_sock = accept(server_fd, (struct sockaddr *) &address,
(socklen_t*)&addrlen);

   // Error Checking
   if(new_sock == -1){
       printf("Cannot accept\n");
       return 0;
   }


   send(new_sock, hello, strlen(hello), 0);
   printf("Hello message sent to browser\n");
   return 0;
}
```