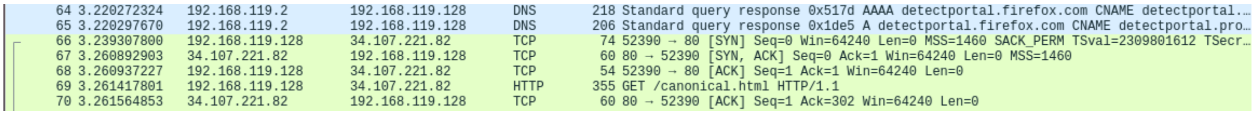
Austin Melendez
2/6/2024

CSC 138 Lab 1

Task 4

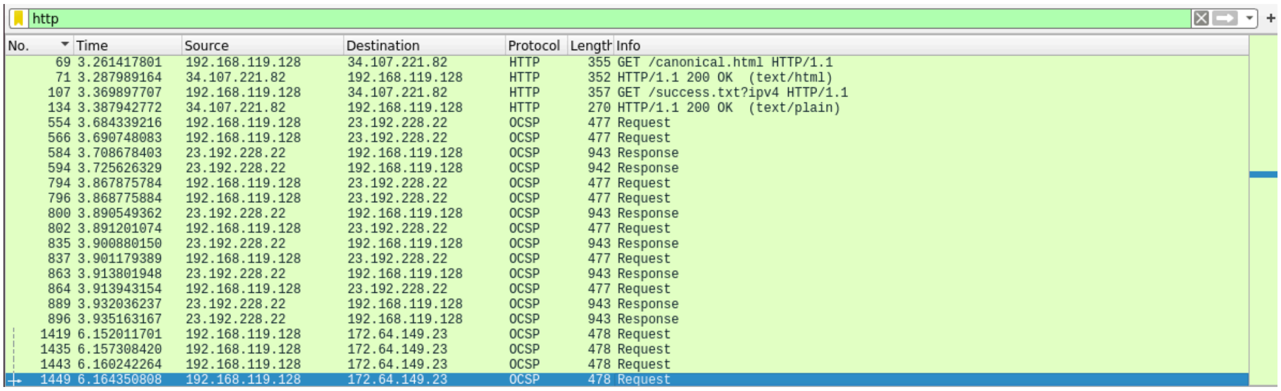
---

1) Three different protocols that appear in the protocol column in the packet-listing window are DNS, TCP and HTTP protocols. TCP protocols are communications between applications and the network, HTTP protocols are related to websites loading, and DNS protocols are redirecting traffic from the hostname to the related IP address.



```
   64 3.220272324   192.168.119.2        192.168.119.128      DNS       218 Standard query response 0x517d AAAA detectportal.firefox.com CNAME detectportal.…
   65 3.220297670   192.168.119.2        192.168.119.128      DNS       206 Standard query response 0x1de5 A detectportal.firefox.com CNAME detectportal.pro…
   66 3.239307800   192.168.119.128      34.107.221.82        TCP        74 52390 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2309801612 TSecr…
   67 3.260892903   34.107.221.82        192.168.119.128      TCP        60 80 → 52390 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   68 3.260937227   192.168.119.128      34.107.221.82        TCP        54 52390 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   69 3.261417801   192.168.119.128      34.107.221.82        HTTP      355 GET /canonical.html HTTP/1.1
   70 3.261564853   34.107.221.82        192.168.119.128      TCP        60 80 → 52390 [ACK] Seq=1 Ack=302 Win=64240 Len=0
```

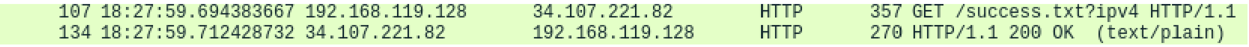
2)



http

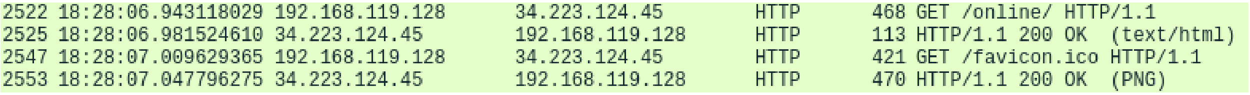
```
No.   Time          Source               Destination          Protocol Length Info
   69 3.261417801   192.168.119.128      34.107.221.82        HTTP      355 GET /canonical.html HTTP/1.1
   71 3.287989164   34.107.221.82        192.168.119.128      HTTP      352 HTTP/1.1 200 OK  (text/html)
  107 3.369897707   192.168.119.128      34.107.221.82        HTTP      357 GET /success.txt?ipv4 HTTP/1.1
  134 3.387942772   34.107.221.82        192.168.119.128      HTTP      270 HTTP/1.1 200 OK  (text/plain)
  554 3.684339216   192.168.119.128      23.192.228.22        OCSP      477 Request
  566 3.690748083   192.168.119.128      23.192.228.22        OCSP      477 Request
  584 3.708678403   23.192.228.22        192.168.119.128      OCSP      943 Response
  594 3.725626329   23.192.228.22        192.168.119.128      OCSP      942 Response
  794 3.867875784   192.168.119.128      23.192.228.22        OCSP      477 Request
  796 3.868775884   192.168.119.128      23.192.228.22        OCSP      477 Request
  800 3.890549362   23.192.228.22        192.168.119.128      OCSP      943 Response
  802 3.891201074   192.168.119.128      23.192.228.22        OCSP      477 Request
  835 3.900880150   23.192.228.22        192.168.119.128      OCSP      943 Response
  837 3.901179389   192.168.119.128      23.192.228.22        OCSP      477 Request
  863 3.913801948   23.192.228.22        192.168.119.128      OCSP      943 Response
  864 3.913943154   192.168.119.128      23.192.228.22        OCSP      477 Request
  889 3.932036237   23.192.228.22        192.168.119.128      OCSP      943 Response
  896 3.935163167   23.192.228.22        192.168.119.128      OCSP      943 Response
 1419 6.152011701   192.168.119.128      172.64.149.23        OCSP      478 Request
 1435 6.157308420   192.168.119.128      172.64.149.23        OCSP      478 Request
 1443 6.160242264   192.168.119.128      172.64.149.23        OCSP      478 Request
 1449 6.164350808   192.168.119.128      172.64.149.23        OCSP      478 Request
```

3) It took about 0.018045 seconds between the HTTP GET and OK response.

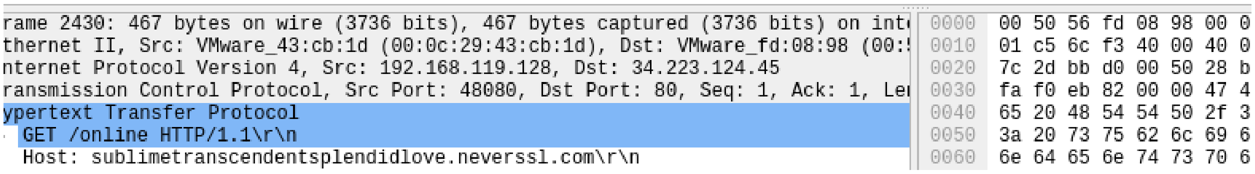


```
  107 18:27:59.694383667 192.168.119.128      34.107.221.82        HTTP      357 GET /success.txt?ipv4 HTTP/1.1
  134 18:27:59.712428732 34.107.221.82        192.168.119.128      HTTP      270 HTTP/1.1 200 OK  (text/plain)
```

4) The internet address of neverssl is 34.223.124.25 and the internet address of my computer is 192.168.119.128



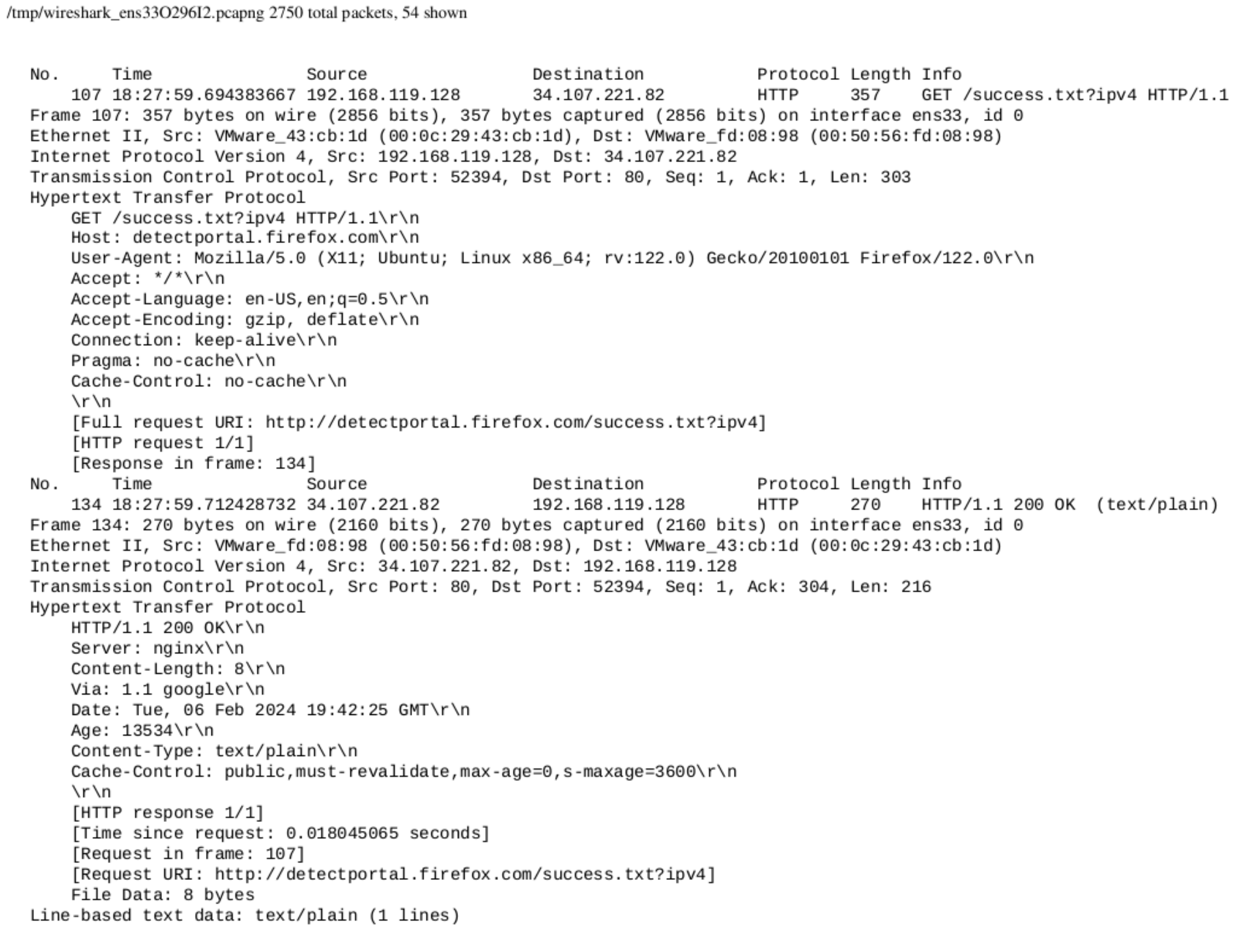
```
2522 18:28:06.943118029 192.168.119.128      34.223.124.45        HTTP      468 GET /online/ HTTP/1.1
2525 18:28:06.981524610 34.223.124.45        192.168.119.128      HTTP      113 HTTP/1.1 200 OK  (text/html)
2547 18:28:07.009629365 192.168.119.128      34.223.124.45        HTTP      421 GET /favicon.ico HTTP/1.1
2553 18:28:07.047796275 34.223.124.45        192.168.119.128      HTTP      470 HTTP/1.1 200 OK  (PNG)
```



```
rame 2430: 467 bytes on wire (3736 bits), 467 bytes captured (3736 bits) on int   0000  00 50 56 fd 08 98 00 0
thernet II, Src: VMware_43:cb:1d (00:0c:29:43:cb:1d), Dst: VMware_fd:08:98 (00:!  0010  01 c5 6c f3 40 00 40 0
nternet Protocol Version 4, Src: 192.168.119.128, Dst: 34.223.124.45                0020  7c 2d bb d0 00 50 28 b
ransmission Control Protocol, Src Port: 48080, Dst Port: 80, Seq: 1, Ack: 1, Le   0030  fa f0 eb 82 00 00 47 4
ypertext Transfer Protocol                                                          0040  65 20 48 54 54 50 2f 3
  GET /online HTTP/1.1\r\n                                                          0050  3a 20 73 75 62 6c 69 6
  Host: sublimetranscendentsplendidlove.neverssl.com\r\n                            0060  6e 64 65 6e 74 73 70 6
```

5) Some HTTP status codes I see in the Info section of Wireshark are GET, OK, Request and Response. The purpose of status codes are to communicate the details of action easily. These codes are used when retrieving a site (GET), when the site has been loaded (OK), when a site or application requests data (Request) and when the network responds/provides the data (Response).

6)

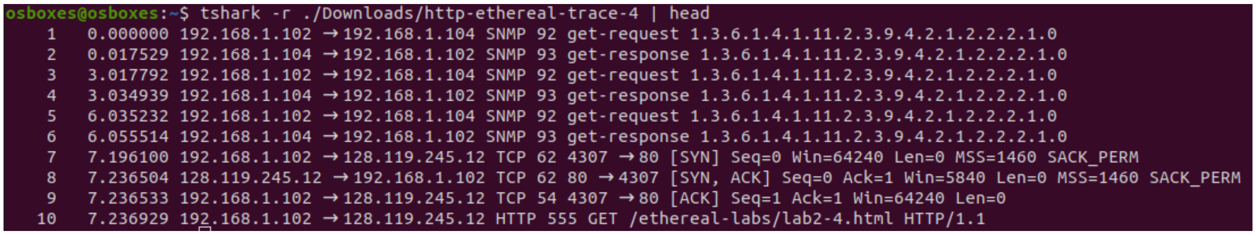


/tmp/wireshark_ens33O296I2.pcapng 2750 total packets, 54 shown

```
No.     Time               Source                Destination           Protocol Length Info
    107 18:27:59.694383667 192.168.119.128       34.107.221.82         HTTP     357    GET /success.txt?ipv4 HTTP/1.1
Frame 107: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface ens33, id 0
Ethernet II, Src: VMware_43:cb:1d (00:0c:29:43:cb:1d), Dst: VMware_fd:08:98 (00:50:56:fd:08:98)
Internet Protocol Version 4, Src: 192.168.119.128, Dst: 34.107.221.82
Transmission Control Protocol, Src Port: 52394, Dst Port: 80, Seq: 1, Ack: 1, Len: 303
Hypertext Transfer Protocol
    GET /success.txt?ipv4 HTTP/1.1\r\n
    Host: detectportal.firefox.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:122.0) Gecko/20100101 Firefox/122.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://detectportal.firefox.com/success.txt?ipv4]
    [HTTP request 1/1]
    [Response in frame: 134]
No.     Time               Source                Destination           Protocol Length Info
    134 18:27:59.712428732 34.107.221.82         192.168.119.128       HTTP     270    HTTP/1.1 200 OK  (text/plain)
Frame 134: 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits) on interface ens33, id 0
Ethernet II, Src: VMware_fd:08:98 (00:50:56:fd:08:98), Dst: VMware_43:cb:1d (00:0c:29:43:cb:1d)
Internet Protocol Version 4, Src: 34.107.221.82, Dst: 192.168.119.128
Transmission Control Protocol, Src Port: 80, Dst Port: 52394, Seq: 1, Ack: 304, Len: 216
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Server: nginx\r\n
    Content-Length: 8\r\n
    Via: 1.1 google\r\n
    Date: Tue, 06 Feb 2024 19:42:25 GMT\r\n
    Age: 13534\r\n
    Content-Type: text/plain\r\n
    Cache-Control: public,must-revalidate,max-age=0,s-maxage=3600\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.018045065 seconds]
    [Request in frame: 107]
    [Request URI: http://detectportal.firefox.com/success.txt?ipv4]
    File Data: 8 bytes
Line-based text data: text/plain (1 lines)
```

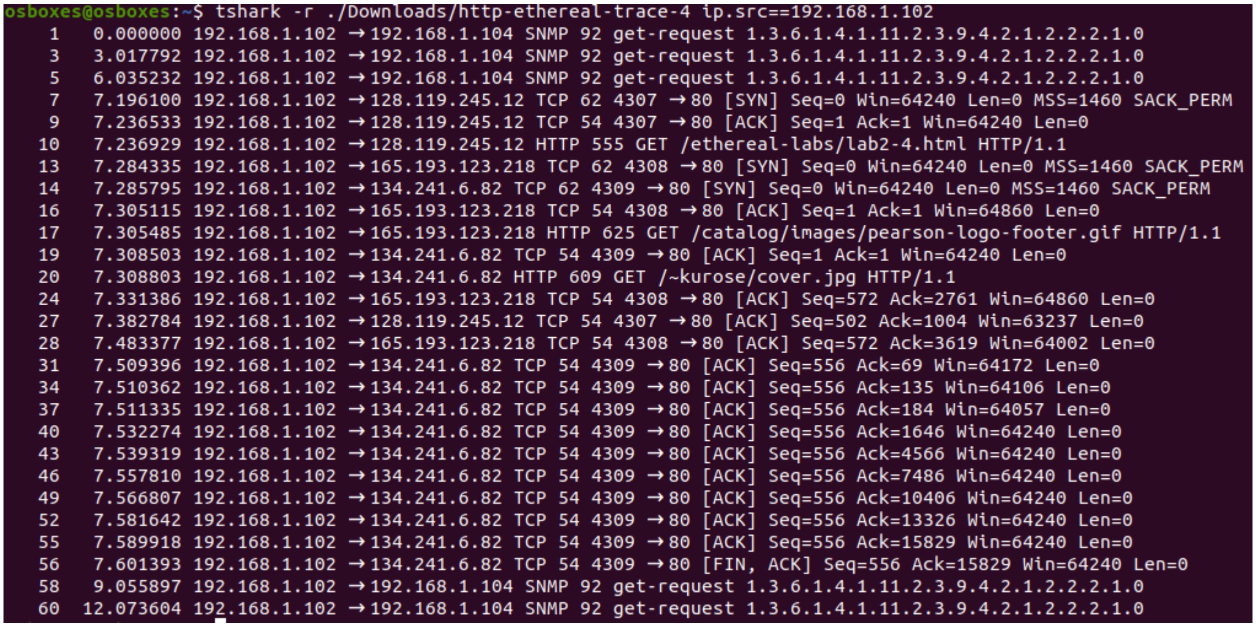
Task 6

1) Ten packets are shown when you run the command from option c, this is because you are piping the command into head, which only shows the first 10 responses. I can see SNMP, TCP, and HTTP protocols in the displayed window.



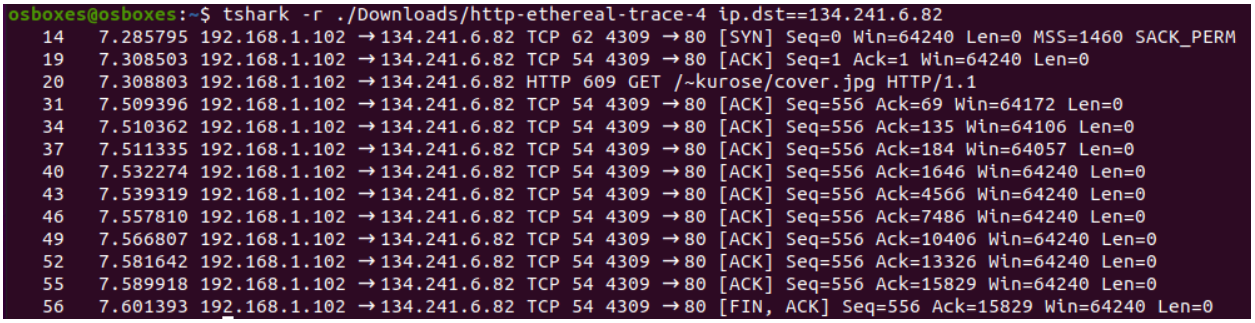
```
osboxes@osboxes:~$ tshark -r ./Downloads/http-ethereal-trace-4 | head
    1   0.000000 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    2   0.017529 192.168.1.104 → 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    3   3.017792 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    4   3.034939 192.168.1.104 → 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    5   6.035232 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    6   6.055514 192.168.1.104 → 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    7   7.196100 192.168.1.102 → 128.119.245.12 TCP 62 4307 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
    8   7.236504 128.119.245.12 → 192.168.1.102 TCP 62 80 → 4307 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
    9   7.236533 192.168.1.102 → 128.119.245.12 TCP 54 4307 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   10   7.236929 192.168.1.102 → 128.119.245.12 HTTP 555 GET /ethereal-labs/lab2-4.html HTTP/1.1
```

2) 27 packets are sourced from the host 192.168.1.102



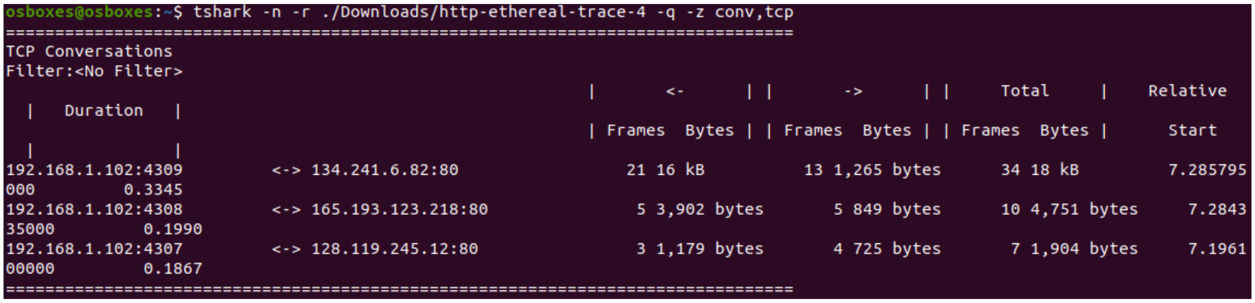
```
osboxes@osboxes:~$ tshark -r ./Downloads/http-ethereal-trace-4 ip.src==192.168.1.102
    1   0.000000 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    3   3.017792 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    5   6.035232 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    7   7.196100 192.168.1.102 → 128.119.245.12 TCP 62 4307 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
    9   7.236533 192.168.1.102 → 128.119.245.12 TCP 54 4307 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   10   7.236929 192.168.1.102 → 128.119.245.12 HTTP 555 GET /ethereal-labs/lab2-4.html HTTP/1.1
   13   7.284335 192.168.1.102 → 165.193.123.218 TCP 62 4308 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   14   7.285795 192.168.1.102 → 134.241.6.82 TCP 62 4309 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   16   7.305115 192.168.1.102 → 165.193.123.218 TCP 54 4308 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
   17   7.305485 192.168.1.102 → 165.193.123.218 HTTP 625 GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
   19   7.308503 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   20   7.308803 192.168.1.102 → 134.241.6.82 HTTP 609 GET /~kurose/cover.jpg HTTP/1.1
   24   7.331386 192.168.1.102 → 165.193.123.218 TCP 54 4308 → 80 [ACK] Seq=572 Ack=2761 Win=64860 Len=0
   27   7.382784 192.168.1.102 → 128.119.245.12 TCP 54 4307 → 80 [ACK] Seq=502 Ack=1004 Win=63237 Len=0
   28   7.483377 192.168.1.102 → 165.193.123.218 TCP 54 4308 → 80 [ACK] Seq=572 Ack=3619 Win=64002 Len=0
   31   7.509396 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=69 Win=64172 Len=0
   34   7.510362 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=135 Win=64106 Len=0
   37   7.511335 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=184 Win=64057 Len=0
   40   7.532274 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=1646 Win=64240 Len=0
   43   7.539319 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=4566 Win=64240 Len=0
   46   7.557810 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=7486 Win=64240 Len=0
   49   7.566807 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=10406 Win=64240 Len=0
   52   7.581642 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=13326 Win=64240 Len=0
   55   7.589918 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=15829 Win=64240 Len=0
   56   7.601393 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [FIN, ACK] Seq=556 Ack=15829 Win=64240 Len=0
   58   9.055897 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   60  12.073604 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
```

3) 13 packets are destined for the host 134.241.6.82



```
osboxes@osboxes:~$ tshark -r ./Downloads/http-ethereal-trace-4 ip.dst==134.241.6.82
   14   7.285795 192.168.1.102 → 134.241.6.82 TCP 62 4309 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   19   7.308503 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   20   7.308803 192.168.1.102 → 134.241.6.82 HTTP 609 GET /~kurose/cover.jpg HTTP/1.1
   31   7.509396 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=69 Win=64172 Len=0
   34   7.510362 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=135 Win=64106 Len=0
   37   7.511335 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=184 Win=64057 Len=0
   40   7.532274 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=1646 Win=64240 Len=0
   43   7.539319 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=4566 Win=64240 Len=0
   46   7.557810 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=7486 Win=64240 Len=0
   49   7.566807 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=10406 Win=64240 Len=0
   52   7.581642 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=13326 Win=64240 Len=0
   55   7.589918 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=15829 Win=64240 Len=0
   56   7.601393 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [FIN, ACK] Seq=556 Ack=15829 Win=64240 Len=0
```

4)



```
osboxes@osboxes:~$ tshark -n -r ./Downloads/http-ethereal-trace-4 -q -z conv,tcp
================================================================================
TCP Conversations
Filter:<No Filter>
                                                           |       <-      | |       ->      | |     Total     |    Relative
  |   Duration   |
                                                           | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |      Start
  |              |
192.168.1.102:4309         <-> 134.241.6.82:80                 21 16 kB          13 1,265 bytes      34 18 kB          7.285795
000          0.3345
192.168.1.102:4308         <-> 165.193.123.218:80               5 3,902 bytes       5 849 bytes       10 4,751 bytes     7.2843
35000          0.1990
192.168.1.102:4307         <-> 128.119.245.12:80                3 1,179 bytes       4 725 bytes        7 1,904 bytes     7.1961
00000          0.1867
================================================================================
```