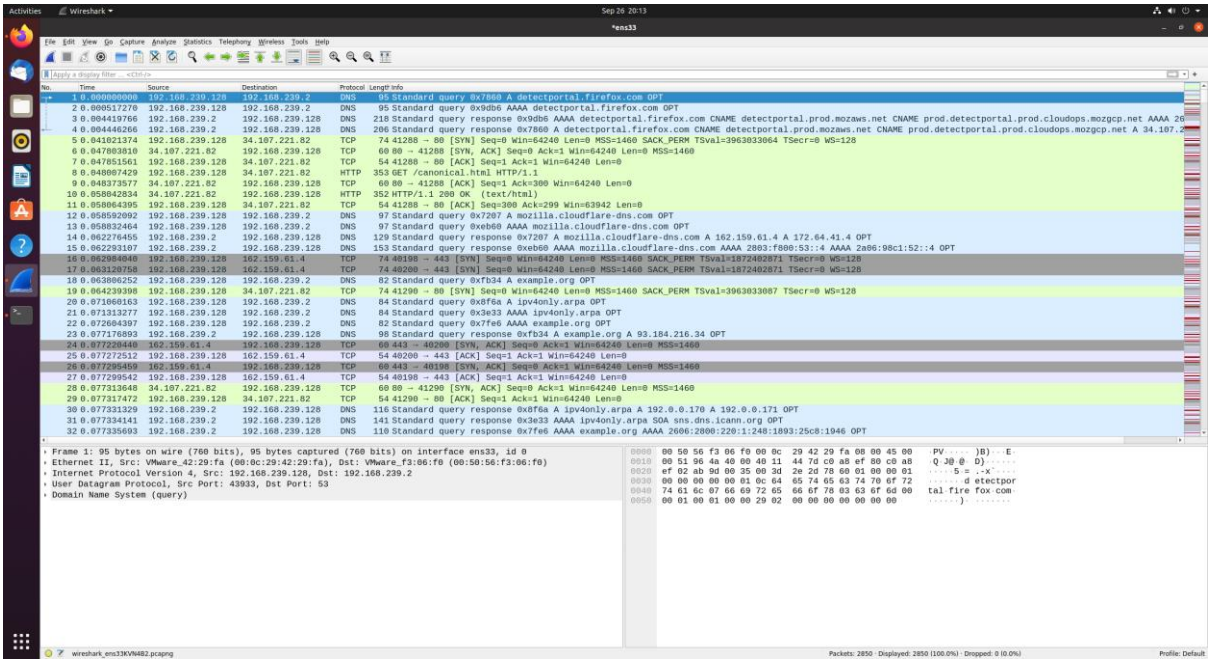
CSC138-01 Lab1

303833894 Yunjeong Lee

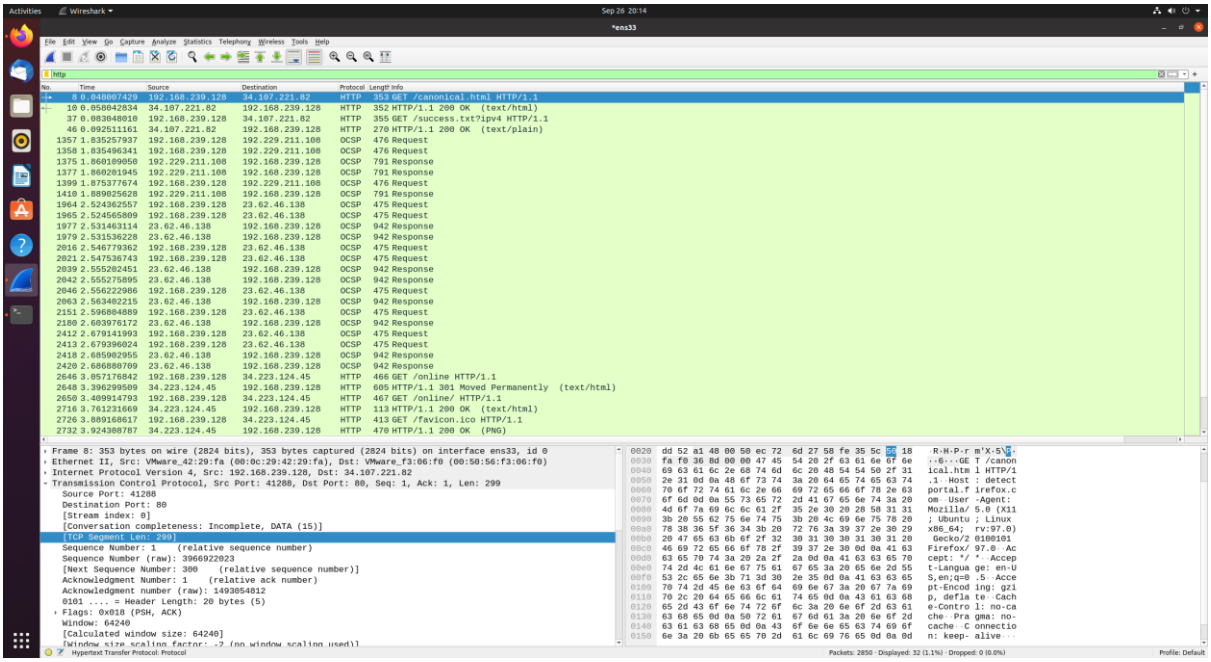
Task 4: Record your observation and answer the following questions.

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window? Attach screen shots of your observation. What are these protocols used for?

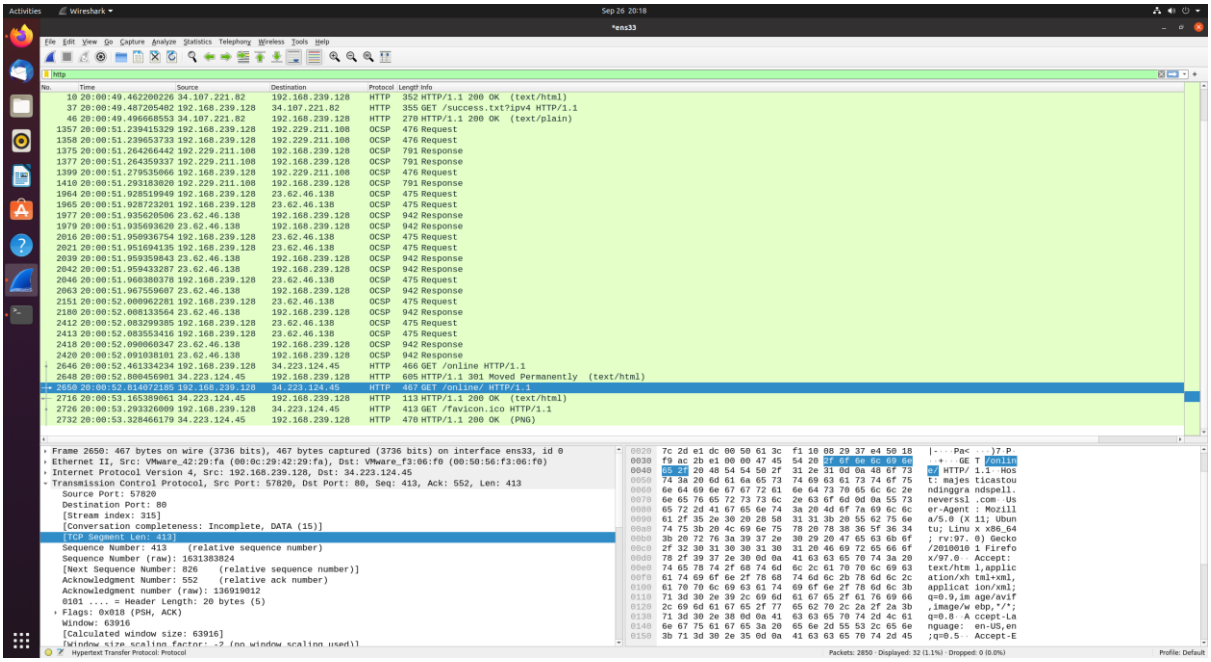


There are DNS, TCP, and HTTP. First, DNS is used for translating human-readable domain names into IP addresses that are used by computers to communicate over a network. TCP is a core protocol of the Internet Protocol (IP). It provides reliable, ordered, and error-checked delivery of packets, making it suitable for applications. HTTP is the protocol used for transmitting web pages, images, videos, and other resources over the World Wide Web. It defines how messages are formatted and transmitted, as well as how web servers and browsers should respond to various commands.

2. On the display filter specification bar, type http and press enter. Attach screenshot of your result?



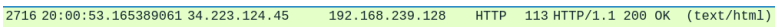
3. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.) You may see several get request and Ok messages, you can pick any and record your finding. Attach a screenshot. Answer: some milliseconds.



It took about 351.316876 milliseconds, from 20:00:52.814072185 to 20:00:53.165389061.

4. What is the Internet address of the www.neverssl.com? What is the Internet address of your computer? Attach a screenshot for each of the answers.

The Internet address of my computer is 192.168.239.128, which is the source of GET request.



The Internet address of the www.neversll.com is 34.223.124.45, which is the source of 200 OK response.

5. What HTTP status codes do you see in the "info" column? What is the purpose of status codes?

   We can see 200 OK, 301 Moved Permanently in the "info" column. The purpose of status codes is to provide a concise way for the server to communicate the outcome of the client's request. This helps the client understand what happened with the request, enabling appropriate actions to be taken, such as displaying a webpage, redirecting to a new location, or displaying an error message. It helps in debugging, troubleshooting, and understanding the current state of the communication between the client and the server.

6. Print the two HTTP messages (GET and OK) referred to in question 3 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK. Attach screenshots of the printed packets.

/tmp/wireshark_ens33KVN4B2.pcapng 2850 total packets, 32 shown

```
No.     Time              Source                Destination           Protocol Length Info
   2650 20:00:52.814072185 192.168.239.128       34.223.124.45         HTTP     467    GET /online/ HTTP/1.1
Frame 2650: 467 bytes on wire (3736 bits), 467 bytes captured (3736 bits) on interface ens33, id 0
Ethernet II, Src: VMware_42:29:fa (00:0c:29:42:29:fa), Dst: VMware_f3:06:f0 (00:50:56:f3:06:f0)
Internet Protocol Version 4, Src: 192.168.239.128, Dst: 34.223.124.45
Transmission Control Protocol, Src Port: 57820, Dst Port: 80, Seq: 413, Ack: 552, Len: 413
    Source Port: 57820
    Destination Port: 80
    [Stream index: 315]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 413]
    Sequence Number: 413    (relative sequence number)
    Sequence Number (raw): 1631383824
    [Next Sequence Number: 826    (relative sequence number)]
    Acknowledgment Number: 552    (relative ack number)
    Acknowledgment number (raw): 136919012
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 63916
    [Calculated window size: 63916]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x2be1 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (413 bytes)
Hypertext Transfer Protocol
    GET /online/ HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /online/ HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /online/
        Request Version: HTTP/1.1
    Host: majesticastoundinggrandspell.neverssl.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://www.neverssl.com/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://majesticastoundinggrandspell.neverssl.com/online/]
    [HTTP request 2/3]
    [Prev request in frame: 2646]
    [Response in frame: 2716]
    [Next request in frame: 2726]
```

/tmp/wireshark_ens33KVN4B2.pcapng 2850 total packets, 32 shown

```
No.     Time              Source                Destination           Protocol Length Info
   2716 20:00:53.165389061 34.223.124.45         192.168.239.128       HTTP     113    HTTP/1.1 200 OK  (text/html)
Frame 2716: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface ens33, id 0
Ethernet II, Src: VMware_f3:06:f0 (00:50:56:f3:06:f0), Dst: VMware_42:29:fa (00:0c:29:42:29:fa)
Internet Protocol Version 4, Src: 34.223.124.45, Dst: 192.168.239.128
Transmission Control Protocol, Src Port: 80, Dst Port: 57820, Seq: 2012, Ack: 826, Len: 59
    Source Port: 80
    Destination Port: 57820
    [Stream index: 315]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 59]
    Sequence Number: 2012    (relative sequence number)
    Sequence Number (raw): 136920472
    [Next Sequence Number: 2071    (relative sequence number)]
    Acknowledgment Number: 826    (relative ack number)
    Acknowledgment number (raw): 1631384237
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x44e0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (59 bytes)
    TCP segment data (59 bytes)
[2 Reassembled TCP Segments (1519 bytes): #2714(1460), #2716(59)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Wed, 27 Sep 2023 00:00:53 GMT\r\n
    Server: Apache/2.4.57 ()\r\n
    Last-Modified: Wed, 29 Jun 2022 00:23:22 GMT\r\n
    ETag: "8be-5e28b29291e10-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
    Content-Length: 1173\r\n
    Keep-Alive: timeout=5, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 2/3]
    [Time since request: 0.351316876 seconds]
    [Prev request in frame: 2646]
    [Prev response in frame: 2648]
    [Request in frame: 2650]
    [Next request in frame: 2726]
    [Next response in frame: 2732]
    [Request URI: http://majesticastoundinggrandspell.neverssl.com/online/]
    Content-encoded entity body (gzip): 1173 bytes -> 2238 bytes
    File Data: 2238 bytes
Line-based text data: text/html (79 lines)
```

Task 6: Answer questions on Tshark Task 5

1. How many packets can you see when you run the command mentioned in option 'c'. What protocols did you observe in the displayed window? Attach a screenshot.

```
osboxes@osboxes:~/Desktop$ tshark -r 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
```

There are 10 packets.

There are SNMP, TCT, HTTP protocols.

2. How many packets are sourced from host 192.168.1.102? (You can get your answer when you run command shown in point 'd')

```
osboxes@osboxes:~/Desktop$ tshark -r 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
```

There are 27 packets.

3. How many packets are destined to the host 134.241.6.82?

```
osboxes@osboxes:~/Desktop$ tshark -r 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
```

There are 13 packets.

4. Attach screenshot of output from task 5.f.

```
osboxes@osboxes:~/Desktop$ tshark -n -r 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      7.285795000         0.3345
192.168.1.102:4308      <-> 165.193.123.218:80        5 3,902 bytes       5 849 bytes       10 4,751 bytes     7.284335000         0.1990
192.168.1.102:4307      <-> 128.119.245.12:80         3 1,179 bytes       4 725 bytes        7 1,904 bytes     7.196100000         0.1867
================================================================================
```