CSC/CPE 138 Computer Networking Fundamentals SPRING2024

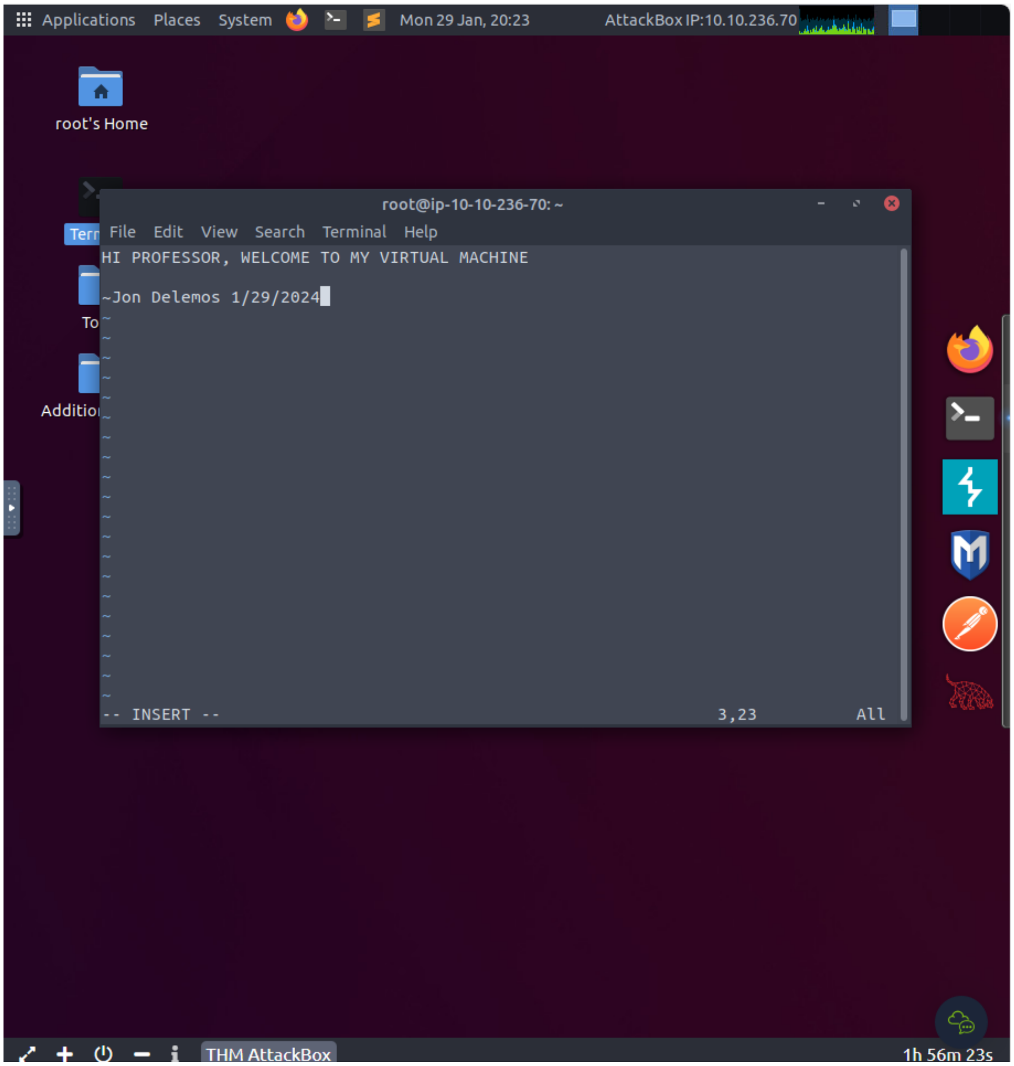
Lab 1 : Introduction to Wireshark and Packet Capture

Submission Deadline: 9th February, 2024

Lab adapted from Computer Networking: A Top-Down Approach, Kurose Ross, 8th edition.

Student name: _*Jonathon Delemos*_____ Section :_______4_______ Student ID: 213441385___________

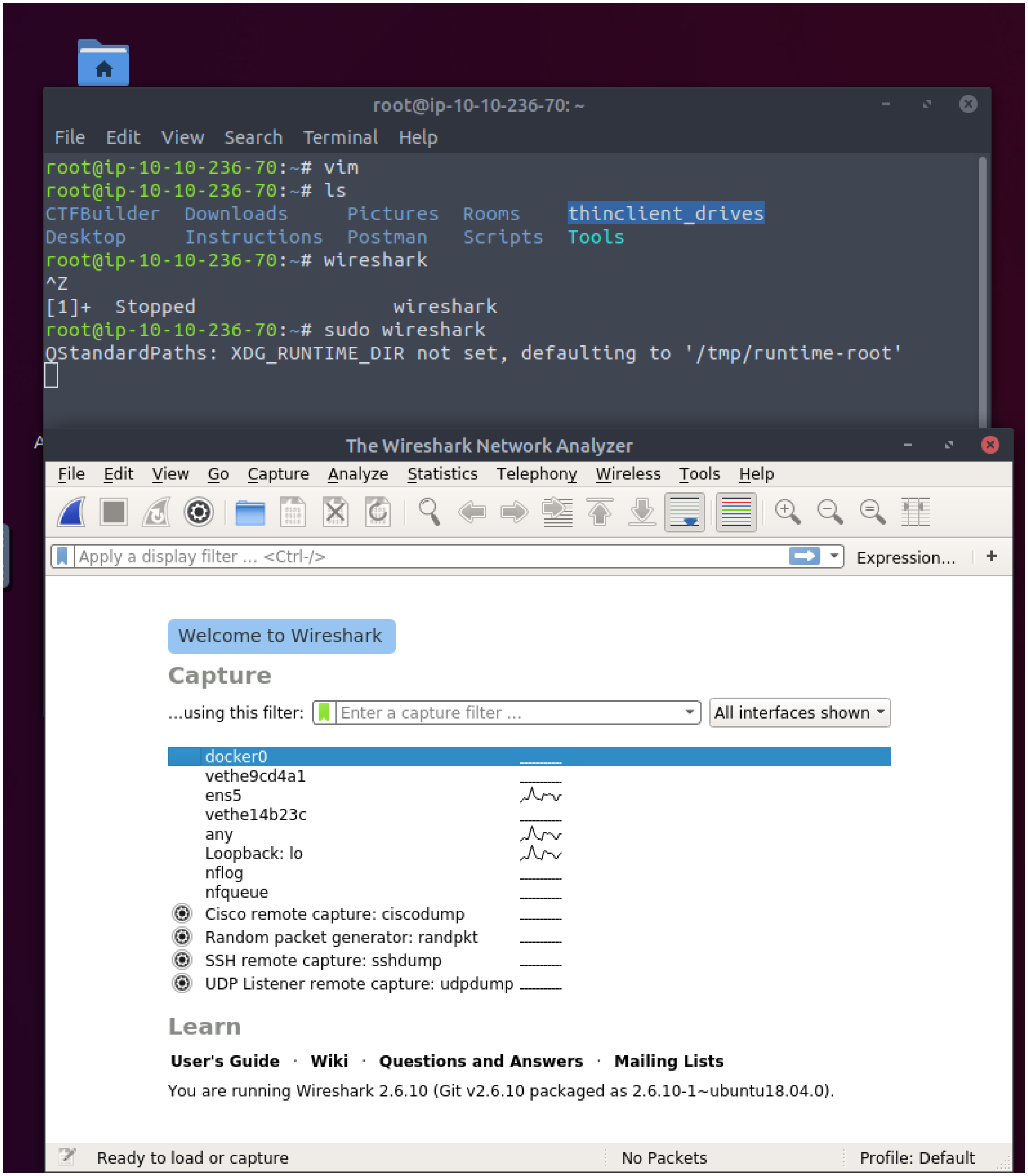
1. TASK – INTSALL VM – COMPLETE



```
HI PROFESSOR, WELCOME TO MY VIRTUAL MACHINE

~Jon Delemos 1/29/2024
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                          3,23          All
```

2. TASK – INSTALL WIRESHARK – COMPLETE



root@ip-10-10-236-70: ~
File Edit View Search Terminal Help

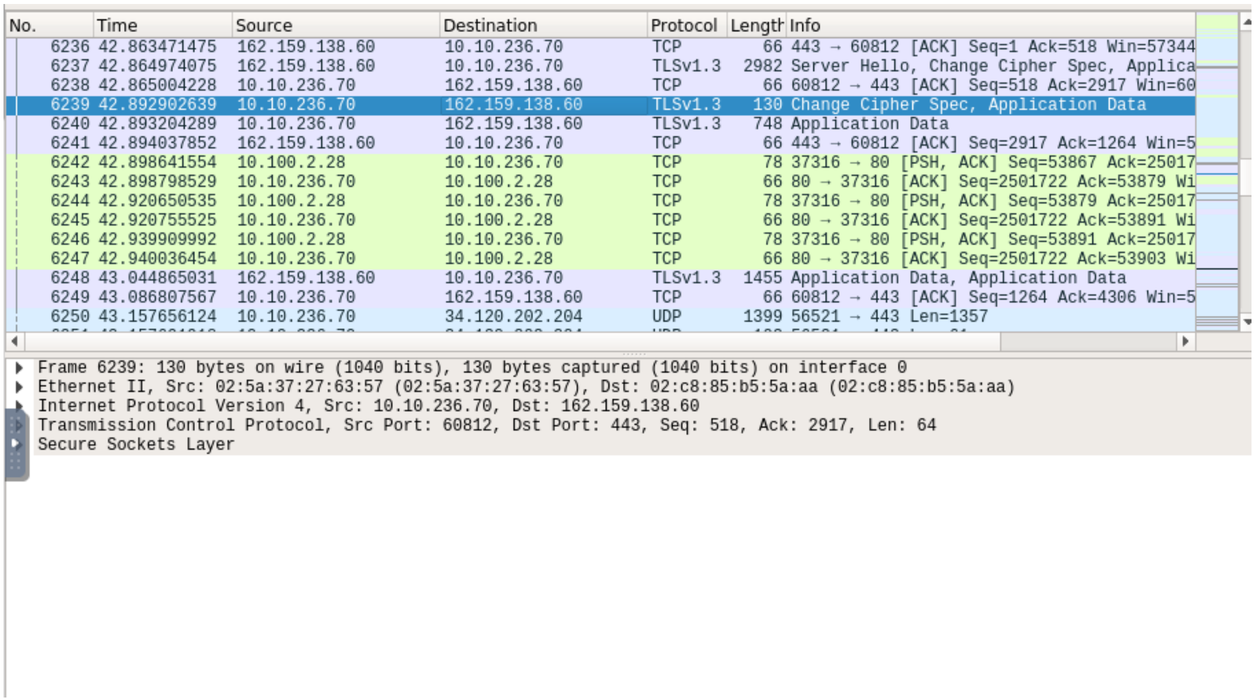
```
root@ip-10-10-236-70:~# vim
root@ip-10-10-236-70:~# ls
CTFBuilder  Downloads     Pictures  Rooms    thinclient_drives
Desktop     Instructions  Postman   Scripts  Tools
root@ip-10-10-236-70:~# wireshark
^Z
[1]+  Stopped                 wireshark
root@ip-10-10-236-70:~# sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
docker0
vethe9cd4a1
ens5
vethe14b23c
any
Loopback: lo
nflog
nfqueue
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

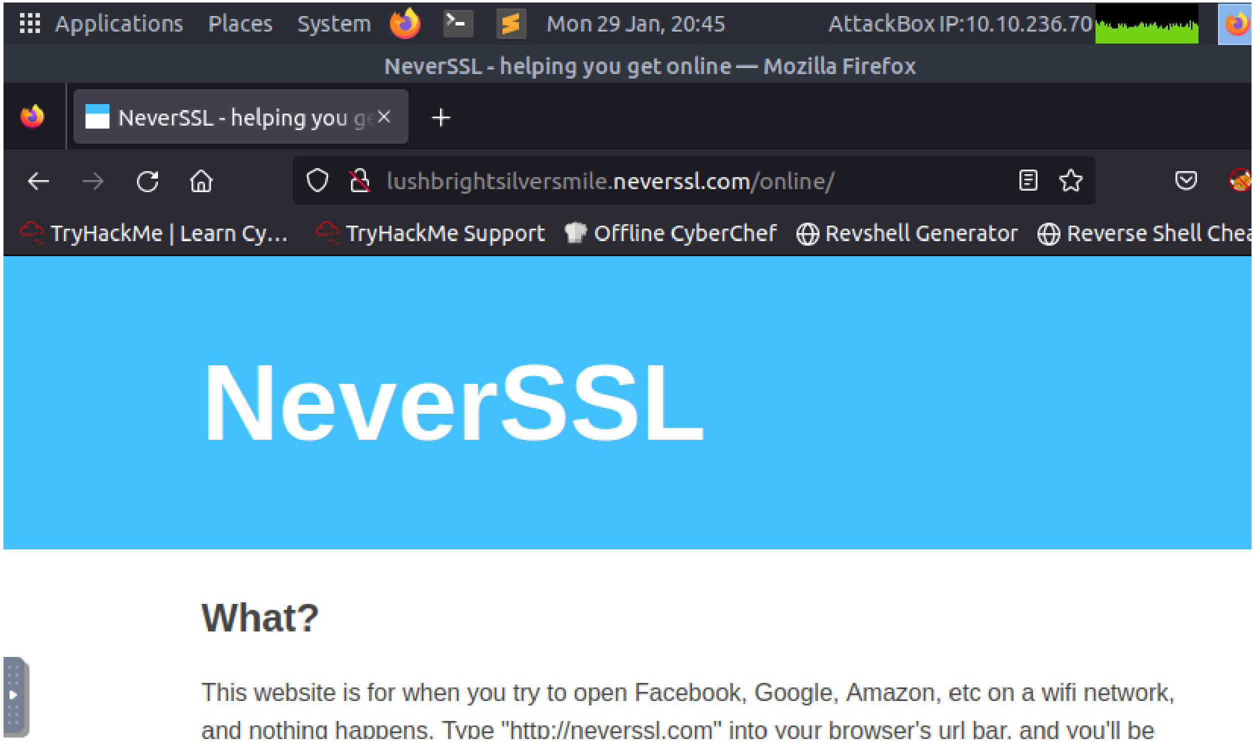
Ready to load or capture   No Packets   Profile: Default

3. TASK – TEST WIRESHARK – COMPLETE



```
No.     Time         Source           Destination      Protocol Length Info
   6236 42.863471475 162.159.138.60   10.10.236.70     TCP        66 443 → 60812 [ACK] Seq=1 Ack=518 Win=57344
   6237 42.864974075 162.159.138.60   10.10.236.70     TLSv1.3  2982 Server Hello, Change Cipher Spec, Applica
   6238 42.865004228 10.10.236.70     162.159.138.60   TCP        66 60812 → 443 [ACK] Seq=518 Ack=2917 Win=60
   6239 42.892902639 10.10.236.70     162.159.138.60   TLSv1.3   130 Change Cipher Spec, Application Data
   6240 42.893204289 10.10.236.70     162.159.138.60   TLSv1.3   748 Application Data
   6241 42.894037852 162.159.138.60   10.10.236.70     TCP        66 443 → 60812 [ACK] Seq=2917 Ack=1264 Win=5
   6242 42.898641554 10.100.2.28      10.10.236.70     TCP        78 37316 → 80 [PSH, ACK] Seq=53867 Ack=25017
   6243 42.898798529 10.10.236.70     10.100.2.28      TCP        66 80 → 37316 [ACK] Seq=2501722 Ack=53879 Wi
   6244 42.920650535 10.100.2.28      10.10.236.70     TCP        78 37316 → 80 [PSH, ACK] Seq=53879 Ack=25017
   6245 42.920755525 10.10.236.70     10.100.2.28      TCP        66 80 → 37316 [ACK] Seq=2501722 Ack=53891 Wi
   6246 42.939909992 10.100.2.28      10.10.236.70     TCP        78 37316 → 80 [PSH, ACK] Seq=53891 Ack=25017
   6247 42.940036454 10.10.236.70     10.100.2.28      TCP        66 80 → 37316 [ACK] Seq=2501722 Ack=53903 Wi
   6248 43.044865031 162.159.138.60   10.10.236.70     TLSv1.3  1455 Application Data, Application Data
   6249 43.086807567 10.10.236.70     162.159.138.60   TCP        66 60812 → 443 [ACK] Seq=1264 Ack=4306 Win=5
   6250 43.157656124 10.10.236.70     34.120.202.204   UDP      1399 56521 → 443 Len=1357

▸ Frame 6239: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
▸ Ethernet II, Src: 02:5a:37:27:63:57 (02:5a:37:27:63:57), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
▸ Internet Protocol Version 4, Src: 10.10.236.70, Dst: 162.159.138.60
▸ Transmission Control Protocol, Src Port: 60812, Dst Port: 443, Seq: 518, Ack: 2917, Len: 64
▸ Secure Sockets Layer
```



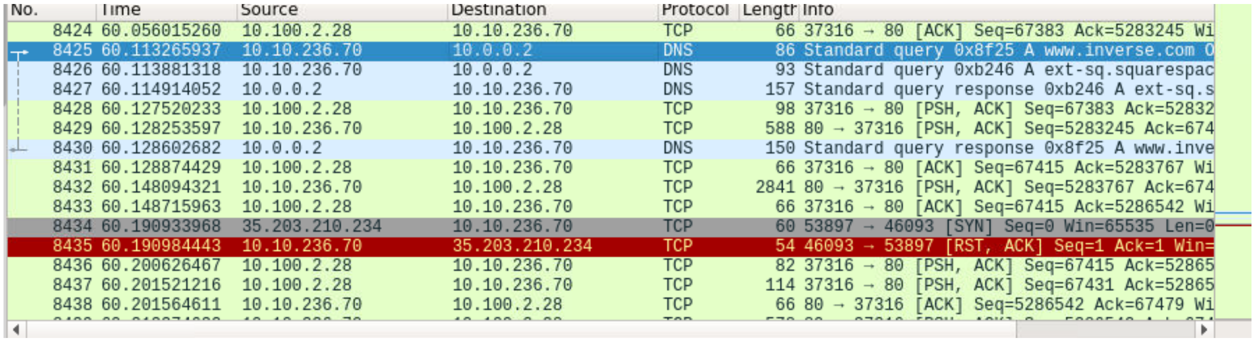
NeverSSL

What?

This website is for when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's url bar, and you'll be

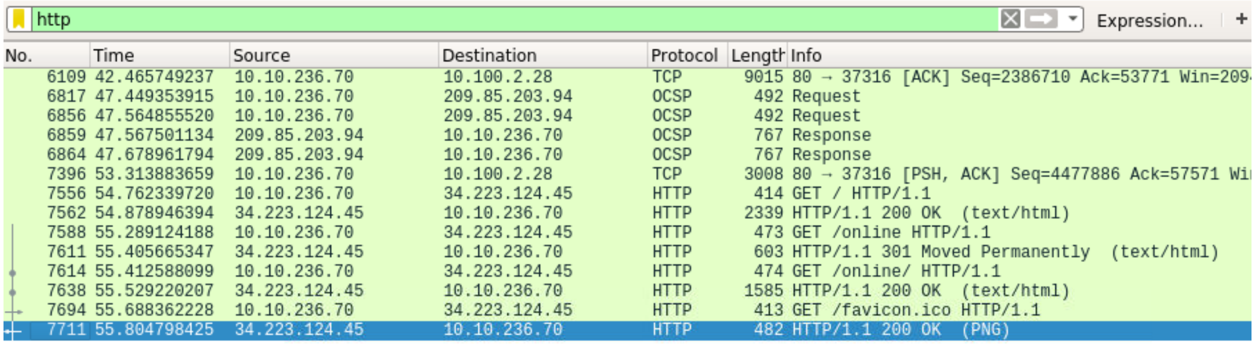
4. TASK – DOCUMENTATION – COMPLETE

   a. DOMAIN NAME SYSTEM, TRANSFER CONTROL PROTOCOL, TRANSFER CONTROL PROTOCOL



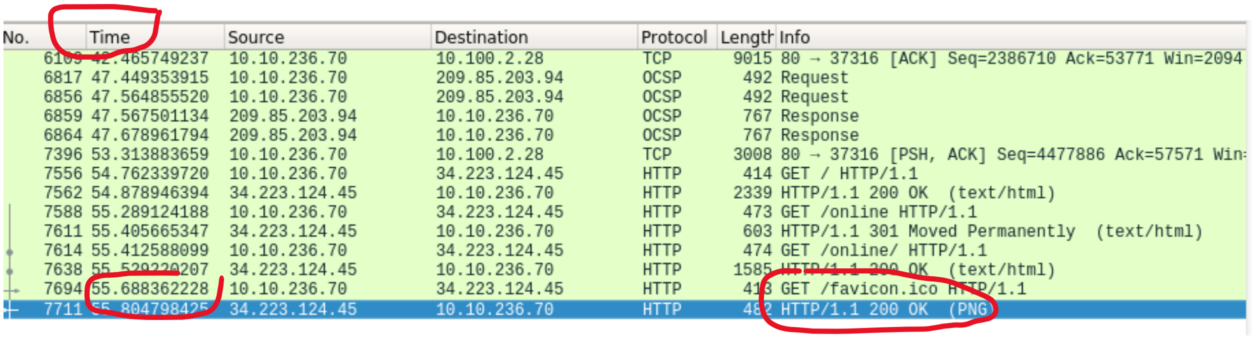
```
No.   Time         Source          Destination     Protocol Length Info
 8424 60.056015260 10.100.2.28     10.10.236.70    TCP        66 37316 → 80 [ACK] Seq=67383 Ack=5283245 Wi
 8425 60.113265937 10.10.236.70    10.0.0.2        DNS        86 Standard query 0x8f25 A www.inverse.com O
 8426 60.113881318 10.10.236.70    10.0.0.2        DNS        93 Standard query 0xb246 A ext-sq.squarespac
 8427 60.114914052 10.0.0.2        10.10.236.70    DNS       157 Standard query response 0xb246 A ext-sq.s
 8428 60.127520233 10.100.2.28     10.10.236.70    TCP        98 37316 → 80 [PSH, ACK] Seq=67383 Ack=52832
 8429 60.128253597 10.10.236.70    10.100.2.28     TCP       588 80 → 37316 [PSH, ACK] Seq=5283245 Ack=674
 8430 60.128602682 10.0.0.2        10.10.236.70    DNS       150 Standard query response 0x8f25 A www.inve
 8431 60.128874429 10.100.2.28     10.10.236.70    TCP        66 37316 → 80 [ACK] Seq=67415 Ack=5283767 Wi
 8432 60.148094321 10.10.236.70    10.100.2.28     TCP      2841 80 → 37316 [PSH, ACK] Seq=5283767 Ack=674
 8433 60.148715963 10.100.2.28     10.10.236.70    TCP        66 37316 → 80 [ACK] Seq=67415 Ack=5286542 Wi
 8434 60.190933968 35.203.210.234  10.10.236.70    TCP        60 53897 → 46093 [SYN] Seq=0 Win=65535 Len=0
 8435 60.190984443 10.10.236.70    35.203.210.234  TCP        54 46093 → 53897 [RST, ACK] Seq=1 Ack=1 Win=
 8436 60.200626467 10.100.2.28     10.10.236.70    TCP        82 37316 → 80 [PSH, ACK] Seq=67415 Ack=52865
 8437 60.201521216 10.100.2.28     10.10.236.70    TCP       114 37316 → 80 [PSH, ACK] Seq=67431 Ack=52865
 8438 60.201564611 10.10.236.70    10.100.2.28     TCP        66 80 → 37316 [ACK] Seq=5286542 Ack=67479 Wi
```

   b. DISPLAY – HTTP



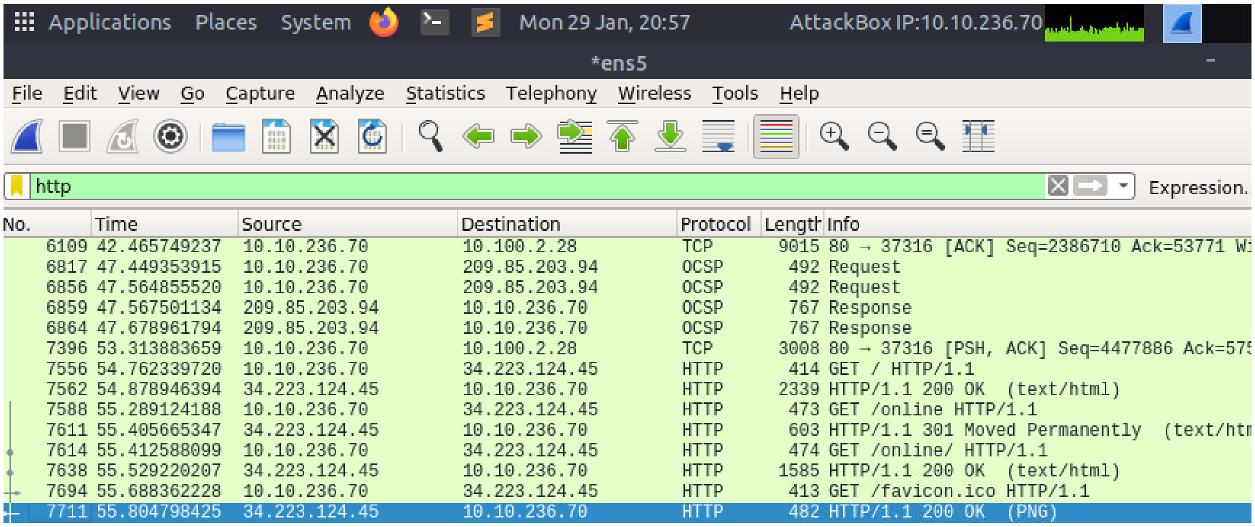
```
No.   Time         Source          Destination     Protocol Length Info
 6109 42.465749237 10.10.236.70    10.100.2.28     TCP      9015 80 → 37316 [ACK] Seq=2386710 Ack=53771 Win=209
 6817 47.449353915 10.10.236.70    209.85.203.94   OCSP      492 Request
 6856 47.564855520 10.10.236.70    209.85.203.94   OCSP      492 Request
 6859 47.567501134 209.85.203.94   10.10.236.70    OCSP      767 Response
 6864 47.678961794 209.85.203.94   10.10.236.70    OCSP      767 Response
 7396 53.313883659 10.10.236.70    10.100.2.28     TCP      3008 80 → 37316 [PSH, ACK] Seq=4477886 Ack=57571 Wi
 7556 54.762339720 10.10.236.70    34.223.124.45   HTTP      414 GET / HTTP/1.1
 7562 54.878946394 34.223.124.45   10.10.236.70    HTTP     2339 HTTP/1.1 200 OK  (text/html)
 7588 55.289124188 10.10.236.70    34.223.124.45   HTTP      473 GET /online HTTP/1.1
 7611 55.405665347 34.223.124.45   10.10.236.70    HTTP      603 HTTP/1.1 301 Moved Permanently  (text/html)
 7614 55.412588099 10.10.236.70    34.223.124.45   HTTP      474 GET /online/ HTTP/1.1
 7638 55.529220207 34.223.124.45   10.10.236.70    HTTP     1585 HTTP/1.1 200 OK  (text/html)
 7694 55.688362228 10.10.236.70    34.223.124.45   HTTP      413 GET /favicon.ico HTTP/1.1
 7711 55.804798425 34.223.124.45   10.10.236.70    HTTP      482 HTTP/1.1 200 OK  (PNG)
```

   c. CALCULATE TIME – APPROXIMATELY .11 seconds



```
No.   Time         Source          Destination     Protocol Length Info
 6109 42.465749237 10.10.236.70    10.100.2.28     TCP      9015 80 → 37316 [ACK] Seq=2386710 Ack=53771 Win=2094
 6817 47.449353915 10.10.236.70    209.85.203.94   OCSP      492 Request
 6856 47.564855520 10.10.236.70    209.85.203.94   OCSP      492 Request
 6859 47.567501134 209.85.203.94   10.10.236.70    OCSP      767 Response
 6864 47.678961794 209.85.203.94   10.10.236.70    OCSP      767 Response
 7396 53.313883659 10.10.236.70    10.100.2.28     TCP      3008 80 → 37316 [PSH, ACK] Seq=4477886 Ack=57571 Win=
 7556 54.762339720 10.10.236.70    34.223.124.45   HTTP      414 GET / HTTP/1.1
 7562 54.878946394 34.223.124.45   10.10.236.70    HTTP     2339 HTTP/1.1 200 OK  (text/html)
 7588 55.289124188 10.10.236.70    34.223.124.45   HTTP      473 GET /online HTTP/1.1
 7611 55.405665347 34.223.124.45   10.10.236.70    HTTP      603 HTTP/1.1 301 Moved Permanently  (text/html)
 7614 55.412588099 10.10.236.70    34.223.124.45   HTTP      474 GET /online/ HTTP/1.1
 7638 55.529220207 34.223.124.45   10.10.236.70    HTTP     1585 HTTP/1.1 200 OK  (text/html)
 7694 55.688362228 10.10.236.70    34.223.124.45   HTTP      413 GET /favicon.ico HTTP/1.1
 7711 55.804798425 34.223.124.45   10.10.236.70    HTTP      482 HTTP/1.1 200 OK  (PNG)
```

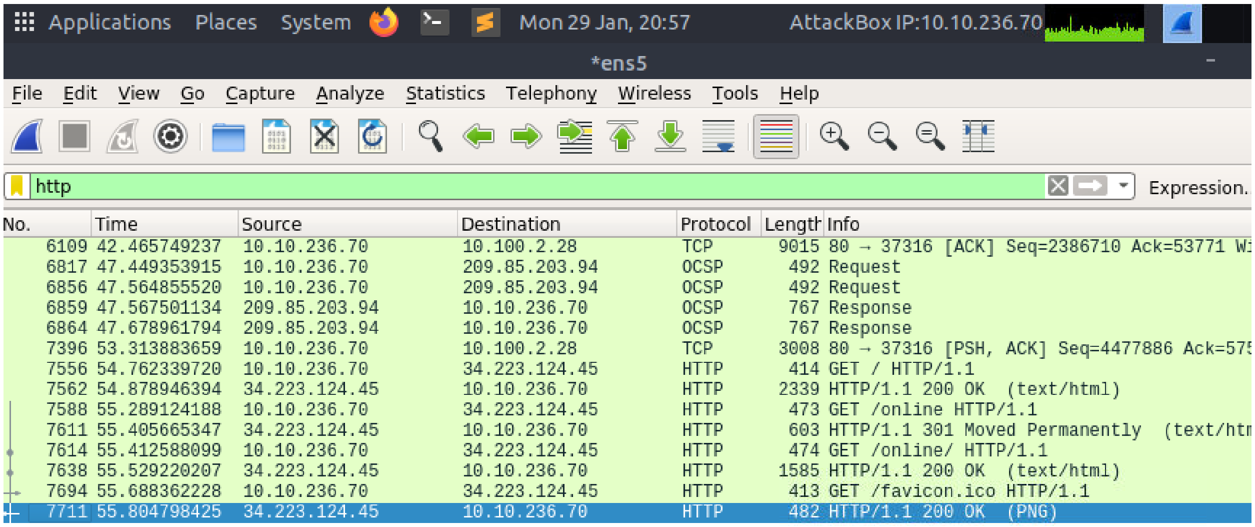
d. FIND YOUR IP/TARGET IP – TARGET 34. – YOUR IP 10.



http

```
No.     Time         Source          Destination     Protocol Length Info
  6109 42.465749237 10.10.236.70    10.100.2.28     TCP      9015 80 → 37316 [ACK] Seq=2386710 Ack=53771 Wi
  6817 47.449353915 10.10.236.70    209.85.203.94   OCSP      492 Request
  6856 47.564855520 10.10.236.70    209.85.203.94   OCSP      492 Request
  6859 47.567501134 209.85.203.94   10.10.236.70    OCSP      767 Response
  6864 47.678961794 209.85.203.94   10.10.236.70    OCSP      767 Response
  7396 53.313883659 10.10.236.70    10.100.2.28     TCP      3008 80 → 37316 [PSH, ACK] Seq=4477886 Ack=575
  7556 54.762339720 10.10.236.70    34.223.124.45   HTTP      414 GET / HTTP/1.1
  7562 54.878946394 34.223.124.45   10.10.236.70    HTTP     2339 HTTP/1.1 200 OK  (text/html)
  7588 55.289124188 10.10.236.70    34.223.124.45   HTTP      473 GET /online HTTP/1.1
  7611 55.405665347 34.223.124.45   10.10.236.70    HTTP      603 HTTP/1.1 301 Moved Permanently  (text/htm
  7614 55.412588099 10.10.236.70    34.223.124.45   HTTP      474 GET /online/ HTTP/1.1
  7638 55.529220207 34.223.124.45   10.10.236.70    HTTP     1585 HTTP/1.1 200 OK  (text/html)
  7694 55.688362228 10.10.236.70    34.223.124.45   HTTP      413 GET /favicon.ico HTTP/1.1
  7711 55.804798425 34.223.124.45   10.10.236.70    HTTP      482 HTTP/1.1 200 OK  (PNG)
```

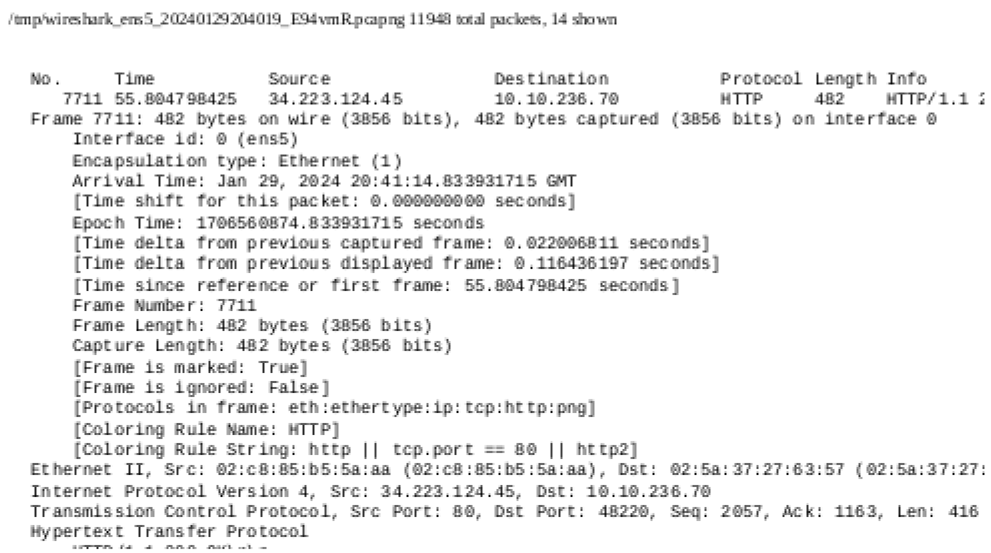
e. LOCATE STATUS CODE – 200-299 REPRESENTS SUCCESS



http

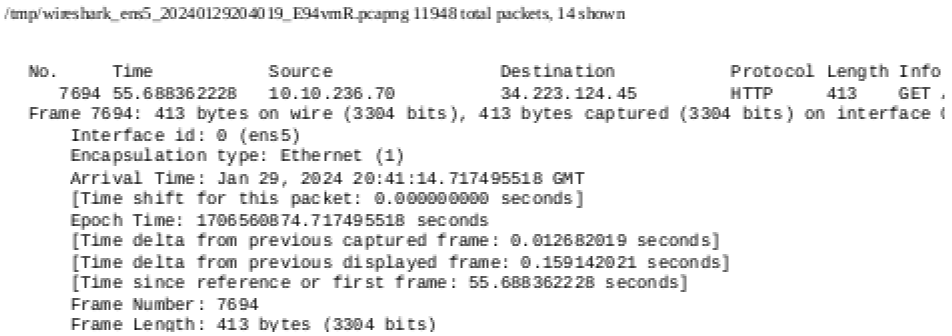
```
No.     Time         Source          Destination     Protocol Length Info
  6109 42.465749237 10.10.236.70    10.100.2.28     TCP      9015 80 → 37316 [ACK] Seq=2386710 Ack=53771 Wi
  6817 47.449353915 10.10.236.70    209.85.203.94   OCSP      492 Request
  6856 47.564855520 10.10.236.70    209.85.203.94   OCSP      492 Request
  6859 47.567501134 209.85.203.94   10.10.236.70    OCSP      767 Response
  6864 47.678961794 209.85.203.94   10.10.236.70    OCSP      767 Response
  7396 53.313883659 10.10.236.70    10.100.2.28     TCP      3008 80 → 37316 [PSH, ACK] Seq=4477886 Ack=575
  7556 54.762339720 10.10.236.70    34.223.124.45   HTTP      414 GET / HTTP/1.1
  7562 54.878946394 34.223.124.45   10.10.236.70    HTTP     2339 HTTP/1.1 200 OK  (text/html)
  7588 55.289124188 10.10.236.70    34.223.124.45   HTTP      473 GET /online HTTP/1.1
  7611 55.405665347 34.223.124.45   10.10.236.70    HTTP      603 HTTP/1.1 301 Moved Permanently  (text/htm
  7614 55.412588099 10.10.236.70    34.223.124.45   HTTP      474 GET /online/ HTTP/1.1
  7638 55.529220207 34.223.124.45   10.10.236.70    HTTP     1585 HTTP/1.1 200 OK  (text/html)
  7694 55.688362228 10.10.236.70    34.223.124.45   HTTP      413 GET /favicon.ico HTTP/1.1
  7711 55.804798425 34.223.124.45   10.10.236.70    HTTP      482 HTTP/1.1 200 OK  (PNG)
```

f. PRINT THE DATA



/tmp/wireshark_ens5_20240129204019_E94vmR.pcapng 11948 total packets, 14 shown

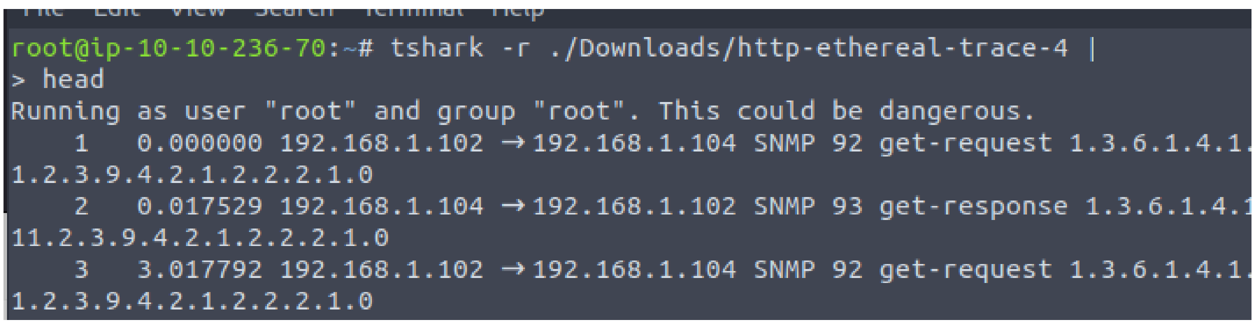
```
No.     Time           Source                Destination           Protocol Length Info
   7711 55.804798425   34.223.124.45         10.10.236.70          HTTP     482    HTTP/1.1 2
Frame 7711: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface 0
    Interface id: 0 (ens5)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 29, 2024 20:41:14.833931715 GMT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1706560874.833931715 seconds
    [Time delta from previous captured frame: 0.022006811 seconds]
    [Time delta from previous displayed frame: 0.116436197 seconds]
    [Time since reference or first frame: 55.804798425 seconds]
    Frame Number: 7711
    Frame Length: 482 bytes (3856 bits)
    Capture Length: 482 bytes (3856 bits)
    [Frame is marked: True]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:png]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa), Dst: 02:5a:37:27:63:57 (02:5a:37:27:
Internet Protocol Version 4, Src: 34.223.124.45, Dst: 10.10.236.70
Transmission Control Protocol, Src Port: 80, Dst Port: 48220, Seq: 2057, Ack: 1163, Len: 416
Hypertext Transfer Protocol
```



/tmp/wireshark_ens5_20240129204019_E94vmR.pcapng 11948 total packets, 14 shown

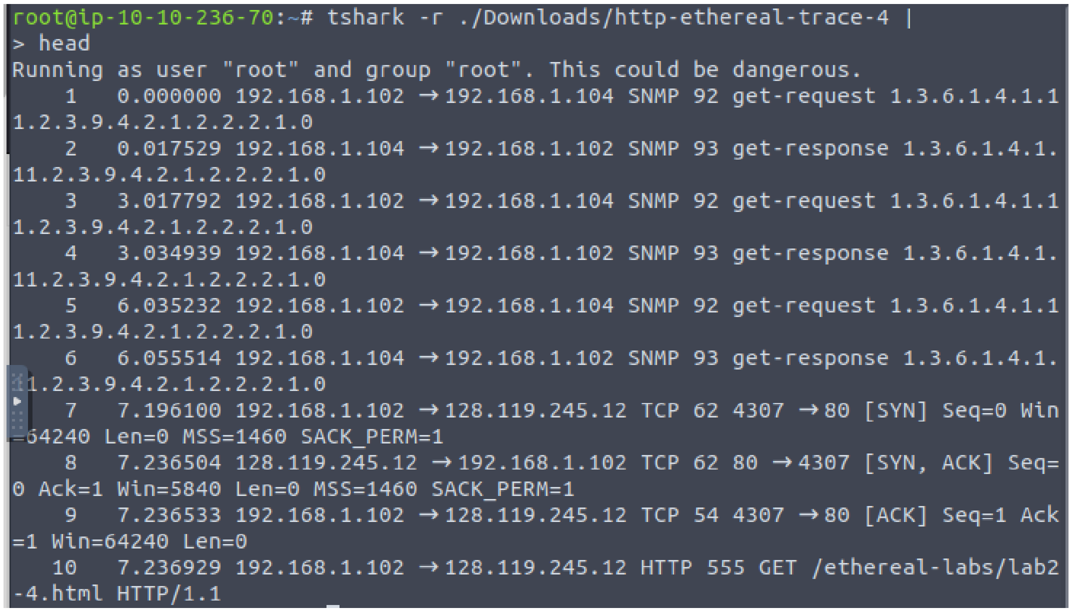
```
No.     Time           Source                Destination           Protocol Length Info
   7694 55.688362228   10.10.236.70          34.223.124.45         HTTP     413    GET .
Frame 7694: 413 bytes on wire (3304 bits), 413 bytes captured (3304 bits) on interface (
    Interface id: 0 (ens5)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 29, 2024 20:41:14.717495518 GMT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1706560874.717495518 seconds
    [Time delta from previous captured frame: 0.012682019 seconds]
    [Time delta from previous displayed frame: 0.159142021 seconds]
    [Time since reference or first frame: 55.688362228 seconds]
    Frame Number: 7694
    Frame Length: 413 bytes (3304 bits)
```

5. – INSTALL TShark



```
root@ip-10-10-236-70:~# tshark -r ./Downloads/http-ethereal-trace-4 |
> head
Running as user "root" and group "root". This could be dangerous.
    1   0.000000 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.
1.2.3.9.4.2.1.2.2.2.1.0
    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.
1.2.3.9.4.2.1.2.2.2.1.0
```

6. – TSHARK a. INSTALL

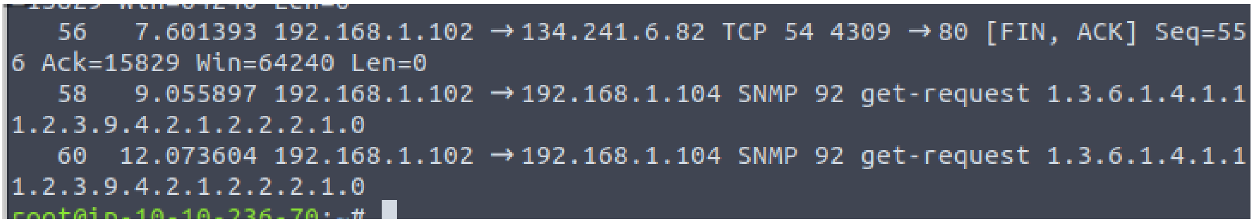


```
root@ip-10-10-236-70:~# tshark -r ./Downloads/http-ethereal-trace-4 |
> head
Running as user "root" and group "root". This could be dangerous.
    1   0.000000 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.1
1.2.3.9.4.2.1.2.2.2.1.0
    2   0.017529 192.168.1.104 → 192.168.1.102 SNMP 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 1.3.6.1.4.1.1
1.2.3.9.4.2.1.2.2.2.1.0
    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 1.3.6.1.4.1.1
1.2.3.9.4.2.1.2.2.2.1.0
    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=1
    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=1
    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
```

b. PACKET DOWNLOAD COMPLETE (DISPLAY ABOVE)

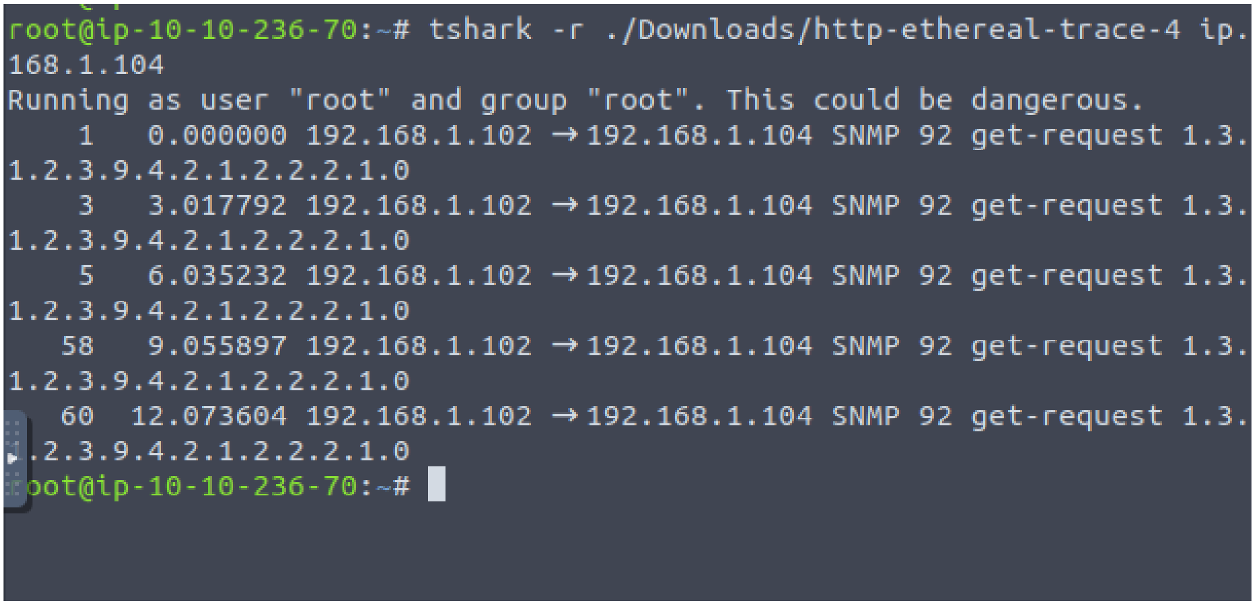
c. HEAD FUNCTION RETURNS TOP 10

d. LISTED SOURCE OF ALL 192. PACKETS



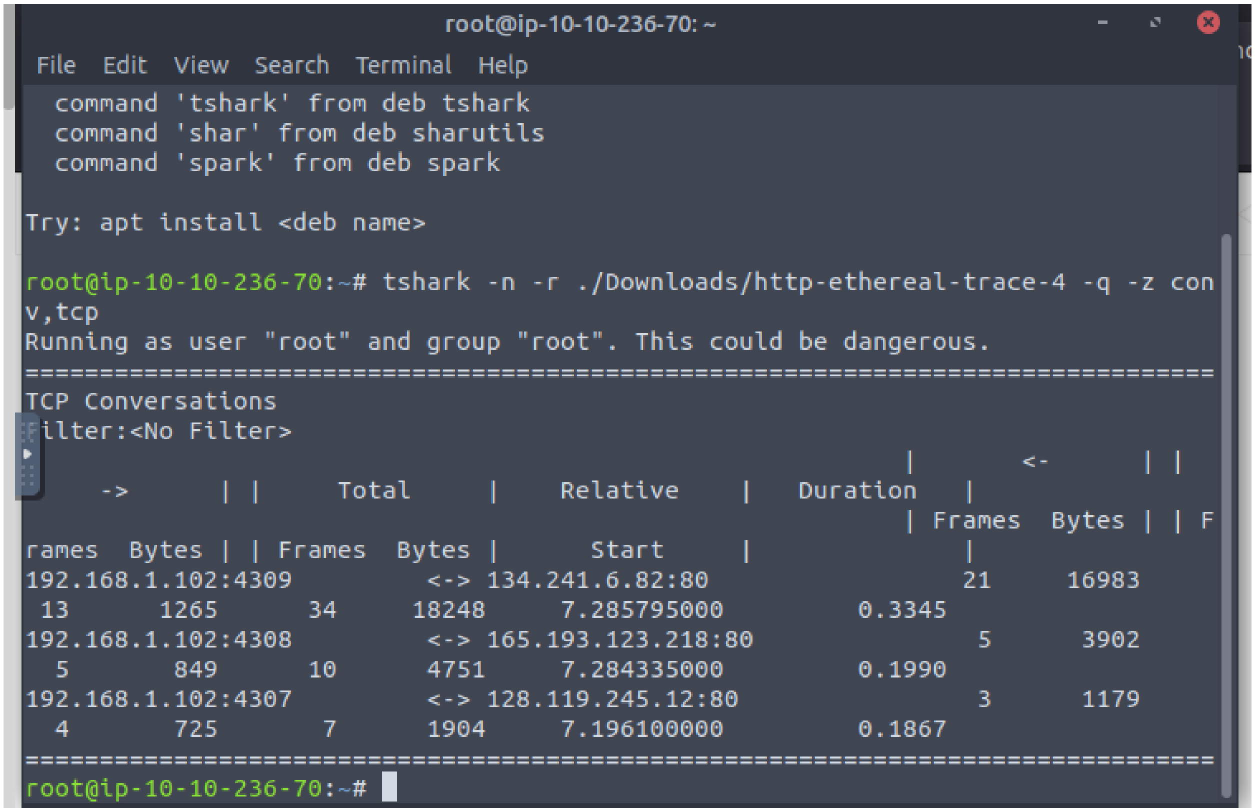
```
   56   7.601393 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [FIN, ACK] Seq=55
6 Ack=15829 Win=64240 Len=0
   58   9.055897 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.1
1.2.3.9.4.2.1.2.2.2.1.0
   60  12.073604 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.1
1.2.3.9.4.2.1.2.2.2.1.0
root@ip-10-10-236-70:~#
```

e. DESTINATION PACKETS



```
root@ip-10-10-236-70:~# tshark -r ./Downloads/http-ethereal-trace-4 ip.
168.1.104
Running as user "root" and group "root". This could be dangerous.
    1   0.000000 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.
1.2.3.9.4.2.1.2.2.2.1.0
    3   3.017792 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.
1.2.3.9.4.2.1.2.2.2.1.0
    5   6.035232 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.
1.2.3.9.4.2.1.2.2.2.1.0
   58   9.055897 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.
1.2.3.9.4.2.1.2.2.2.1.0
   60  12.073604 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.
.2.3.9.4.2.1.2.2.2.1.0
oot@ip-10-10-236-70:~#
```

f. ATTACH SCREENSHOT OF FINAL COMMAND



```
  command 'tshark' from deb tshark
  command 'shar' from deb sharutils
  command 'spark' from deb spark

Try: apt install <deb name>

root@ip-10-10-236-70:~# tshark -n -r ./Downloads/http-ethereal-trace-4 -q -z con
v,tcp
Running as user "root" and group "root". This could be dangerous.
================================================================================
TCP Conversations
ilter:<No Filter>
                                                           |       <-      | |
    ->      | |      Total      |    Relative     |   Duration    |
                                                           | Frames  Bytes | | F
rames  Bytes | | Frames  Bytes |      Start      |               |
192.168.1.102:4309         <-> 134.241.6.82:80                 21     16983
 13      1265      34      18248      7.285795000        0.3345
192.168.1.102:4308         <-> 165.193.123.218:80               5      3902
  5       849      10       4751      7.284335000        0.1990
192.168.1.102:4307         <-> 128.119.245.12:80                3      1179
  4       725       7       1904      7.196100000        0.1867
================================================================================
root@ip-10-10-236-70:~#
```