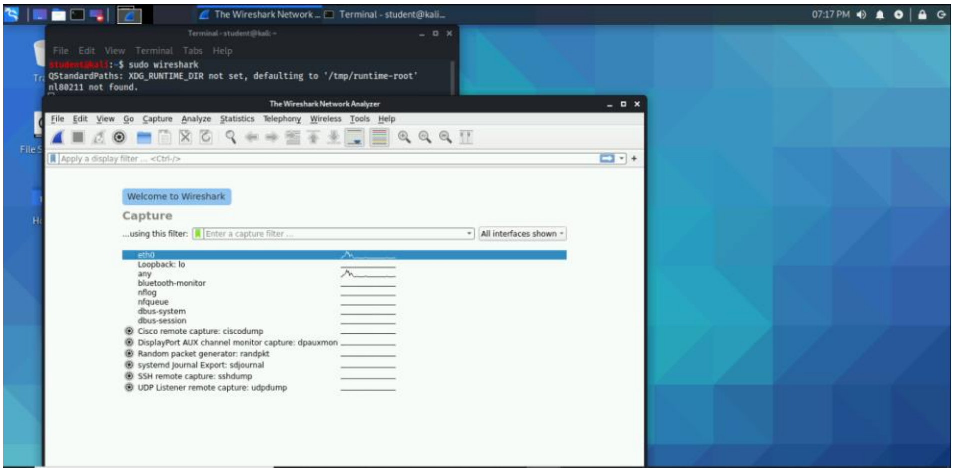
Task Description:

The main objective of this task is to capture and analyze network traffic and log.

Execution and Screenshots

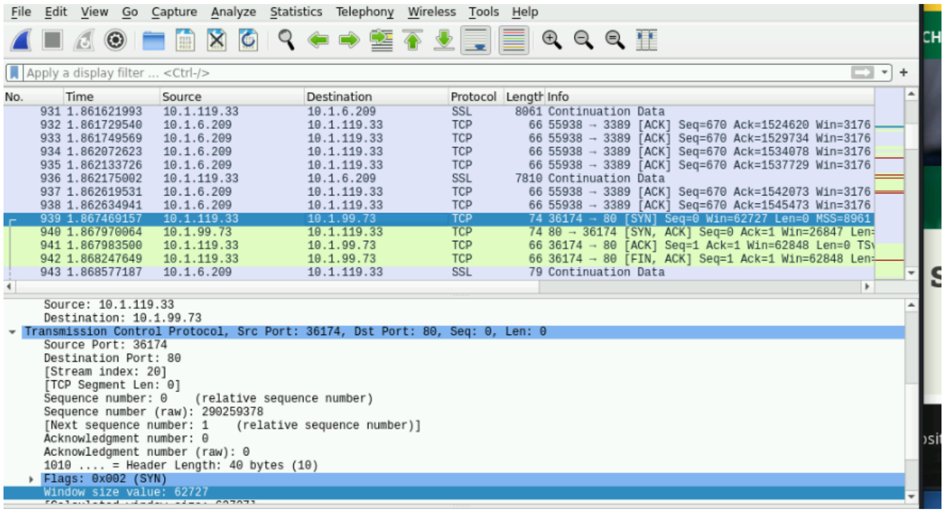
This lab will require the VACR Kali Linux machine which is equipped with Wireshark. The initial setup of this lab is just turning on the given virtual machine. The machine was already logged in with student user. Then when VM is up and running, we will start Wireshark as follows.



```
student@kali:~$ sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
nl80211 not found.
```

The Wireshark Network ...
Terminal - student@kali...
07:17 PM
Terminal - student@kali: ~
File Edit View Terminal Tabs Help
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

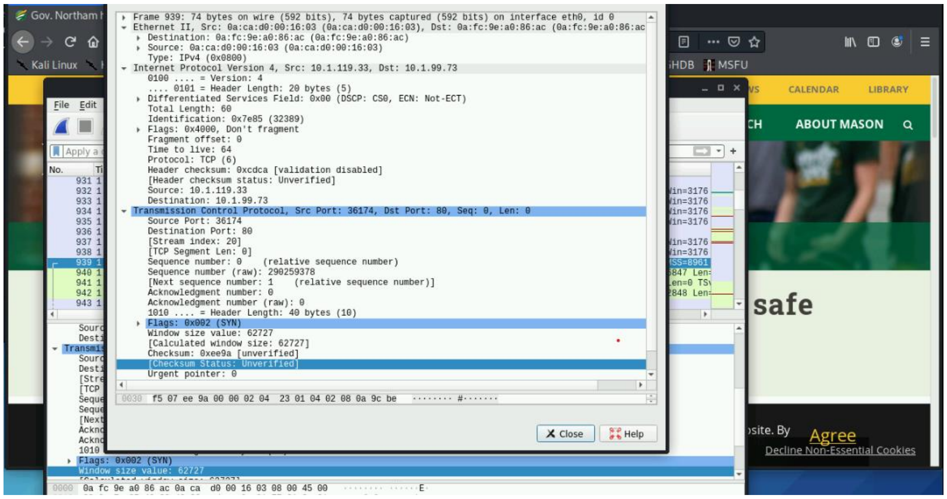
I browsed www2.gmu.edu and clicked on one of the packets which is shown below



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

```
No.   Time        Source        Destination   Protocol Length Info
  931 1.861621993 10.1.119.33   10.1.6.209    SSL     8061 Continuation Data
  932 1.861729540 10.1.6.209    10.1.119.33   TCP       66 55938 → 3389 [ACK] Seq=670 Ack=1524620 Win=3176
  933 1.861749569 10.1.6.209    10.1.119.33   TCP       66 55938 → 3389 [ACK] Seq=670 Ack=1529734 Win=3176
  934 1.862072623 10.1.6.209    10.1.119.33   TCP       66 55938 → 3389 [ACK] Seq=670 Ack=1534078 Win=3176
  935 1.862133726 10.1.6.209    10.1.119.33   TCP       66 55938 → 3389 [ACK] Seq=670 Ack=1537729 Win=3176
  936 1.862175002 10.1.119.33   10.1.6.209    SSL     7810 Continuation Data
  937 1.862619531 10.1.6.209    10.1.119.33   TCP       66 55938 → 3389 [ACK] Seq=670 Ack=1542073 Win=3176
  938 1.862634941 10.1.6.209    10.1.119.33   TCP       66 55938 → 3389 [ACK] Seq=670 Ack=1545473 Win=3176
  939 1.867469157 10.1.119.33   10.1.99.73    TCP       74 36174 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961
  940 1.867970064 10.1.99.73    10.1.119.33   TCP       74 80 → 36174 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=
  941 1.867983500 10.1.119.33   10.1.99.73    TCP       66 36174 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSv
  942 1.868247649 10.1.119.33   10.1.99.73    TCP       66 36174 → 80 [FIN, ACK] Seq=1 Ack=1 Win=62848 Len=
  943 1.868577187 10.1.6.209    10.1.119.33   SSL       79 Continuation Data
```

```
    Source: 10.1.119.33
    Destination: 10.1.99.73
▾ Transmission Control Protocol, Src Port: 36174, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 36174
    Destination Port: 80
    [Stream index: 20]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 290259378
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x002 (SYN)
    Window size value: 62727
```



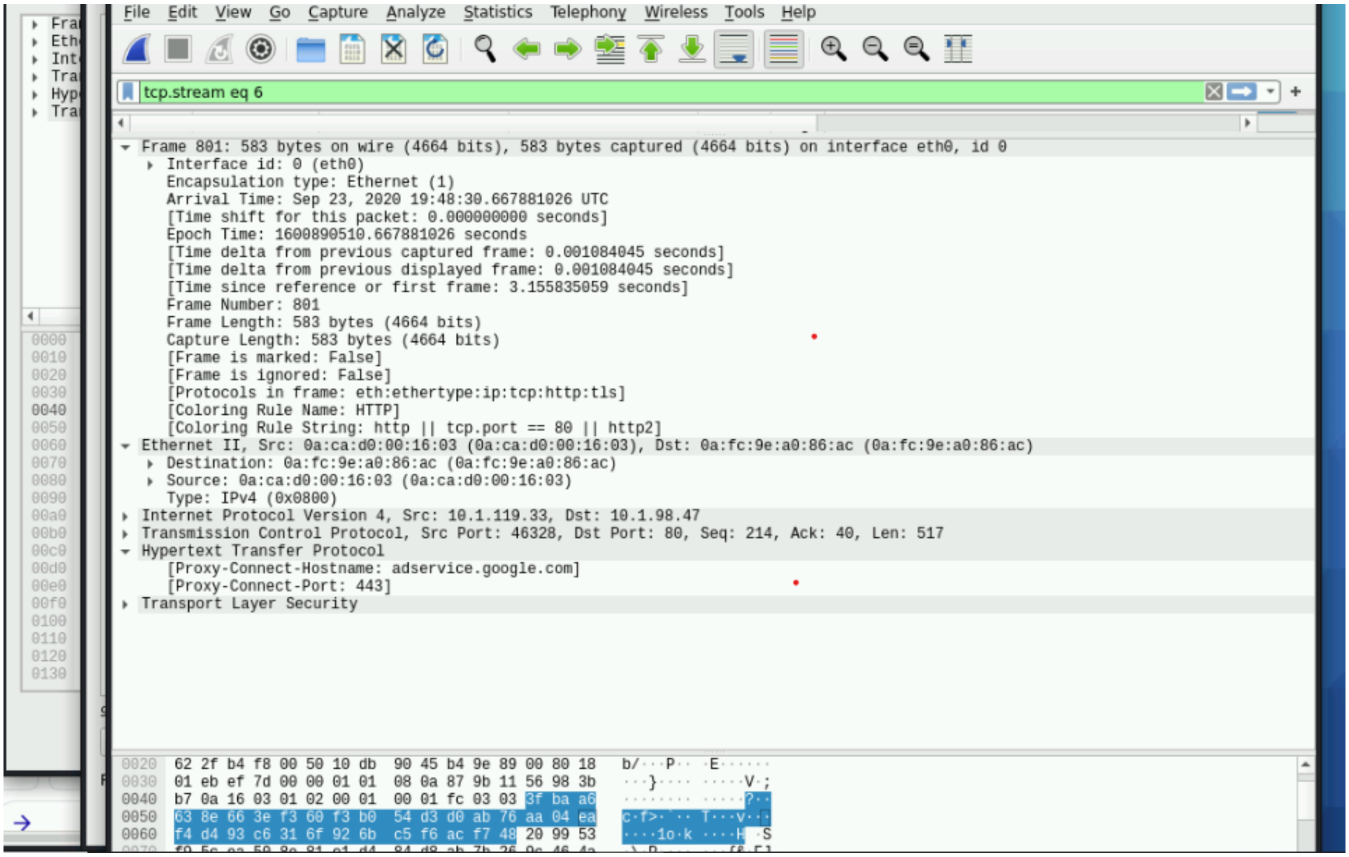
```
Frame 939: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: 0a:ca:d0:00:16:03 (0a:ca:d0:00:16:03), Dst: 0a:fc:9e:a0:86:ac (0a:fc:9e:a0:86:ac
    Destination: 0a:fc:9e:a0:86:ac (0a:fc:9e:a0:86:ac)
    Source: 0a:ca:d0:00:16:03 (0a:ca:d0:00:16:03)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.1.119.33, Dst: 10.1.99.73
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x7e85 (32389)
    Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xcdca [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.1.119.33
    Destination: 10.1.99.73
Transmission Control Protocol, Src Port: 36174, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 36174
    Destination Port: 80
    [Stream index: 20]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 290259378
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
    Flags: 0x002 (SYN)
    Window size value: 62727
    [Calculated window size: 62727]
    Checksum: 0xee9a [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0

0030  f5 07 ee 9a 00 00 02 04  23 01 04 02 08 0a 9c be   ········ #·······
```

Length of packet: 74 bytes

Source IP:10.1.119.33

Destination IP: 10.1.99.73

Again, I went to google.com and the outcome was as follows:



```
tcp.stream eq 6
```

```
▾ Frame 801: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface eth0, id 0
  ▸ Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 23, 2020 19:48:30.667881026 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600890510.667881026 seconds
    [Time delta from previous captured frame: 0.001084045 seconds]
    [Time delta from previous displayed frame: 0.001084045 seconds]
    [Time since reference or first frame: 3.155835059 seconds]
    Frame Number: 801
    Frame Length: 583 bytes (4664 bits)
    Capture Length: 583 bytes (4664 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:tls]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▾ Ethernet II, Src: 0a:ca:d0:00:16:03 (0a:ca:d0:00:16:03), Dst: 0a:fc:9e:a0:86:ac (0a:fc:9e:a0:86:ac)
  ▸ Destination: 0a:fc:9e:a0:86:ac (0a:fc:9e:a0:86:ac)
  ▸ Source: 0a:ca:d0:00:16:03 (0a:ca:d0:00:16:03)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.1.119.33, Dst: 10.1.98.47
▸ Transmission Control Protocol, Src Port: 46328, Dst Port: 80, Seq: 214, Ack: 40, Len: 517
▾ Hypertext Transfer Protocol
    [Proxy-Connect-Hostname: adservice.google.com]
    [Proxy-Connect-Port: 443]
▸ Transport Layer Security
```

```
0020  62 2f b4 f8 00 50 10 db  90 45 b4 9e 89 00 80 18   b/···P·· ·E······
0030  01 eb ef 7d 00 00 01 01  08 0a 87 9b 11 56 98 3b   ···}···· ·····V·;
0040  b7 0a 16 03 01 02 00 01  00 01 fc 03 03 3f ba a6   ········ ·····?··
0050  63 8e 66 3e f3 60 f3 b0  54 d3 d0 ab 76 aa 04 ea   c·f>·`·· T···v···
0060  f4 d4 93 c6 31 6f 92 6b  c5 f6 ac f7 48 20 99 53   ····1o·k ····H ·S
```

Observations

Whenever entered any web address in the web browser the packets started coming in until I stopped capturing the packets.

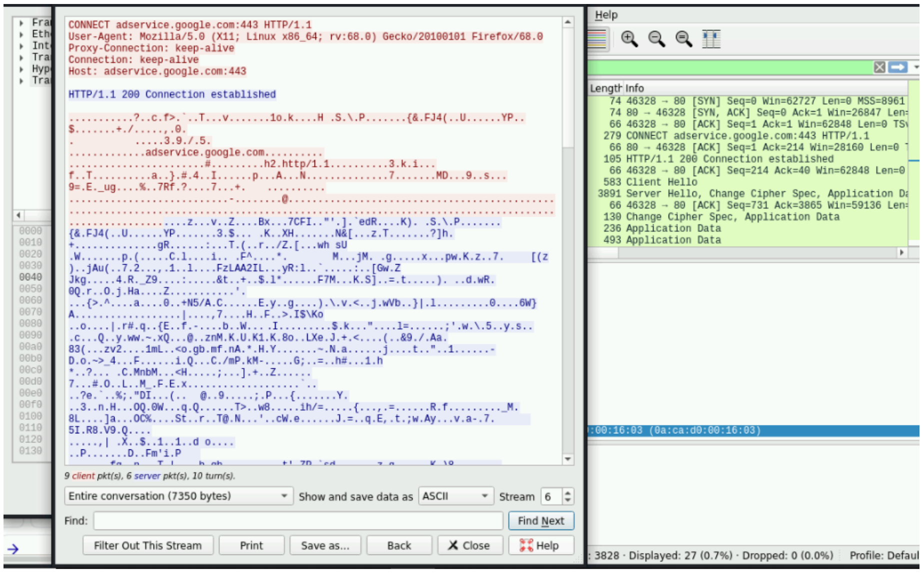
From the above packet capture

- Length of the packet: 583 bytes
- Sender's and receiver's IP addresses: Src: 10.1.119.33, Dst: 10.1.98.47
- Protocol used: TCP
- Source’s MAC Address: 0a:ca:d0:00:16:03 (0a:ca:d0:00:16:03)
- Destination’s MAC Address: 0a:fc:9e:a0:86:ac (0a:fc:9e:a0:86:ac)

Answers to Questions

The shown Destination IP is found to be Destination: 10.1.98.47.

I think its incorrect because it is hashed and converted to different IP because the ip for google.com ranges from 172.217.0.0-172.217.255.255.



```
CONNECT adservice.google.com:443 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Proxy-Connection: keep-alive
Connection: keep-alive
Host: adservice.google.com:443

HTTP/1.1 200 Connection established

...........?..c.f>.`..T...v.......1o.k....H .S.\.P.......{&.FJ4(..U......YP..
$.......+./.....,.0.
.          .....3.9./.5.
.............adservice.google.com..........
........................#.........h2.http/1.1..........3.k.i...
f..T..........a..}.#.4..I......p...A...N..............7.......MD...9..s...
9=.E._ug....%..7Rf.?....7...+.    ..........
..........................-........@..........................................
..............................................................................
................z...v..Z....Bx...7CFI.."'.].`edR....K). .S.\.P.......
{&.FJ4(..U......YP.......3.$... .K..XH.......N&[...z.T.......?]h.
+..............gR......:...T.(..r../Z.[...wh sU
.W.......p.(.....C.l....i.. .F^....*.        M...jM. .g.....x...pw.K.z..7.    [(z
)..jAu(..7.2...,.1..l....FzLAA2IL...yR:l..`.....:..[Gw.Z
Jkg.....4.R._Z9....:.....&t..+..$.l*......F7M...K.S]..=.t.....). ..d.wR.
0Q.r..O.j.Ha....Z...........'.
...{>.^....a....0..+N5/A.C......E.y..g....).\.v.<..j.wVb..}|.l.........0....6W}
A..................|....,7....H..F..>.I$\Ko
..o....|.r#.q..{E..f.-....b..W... .I.........$.k..."....l=......;'.w.\.5..y.s..
.c...Q..y.ww.~.xQ...@..znM.K.U.K1.K.8o..LXe.J.+.<....(..&9./.Aa.
83(...zv2....1mL..<o.gb.mf.nA.*.H.Y.......~.N.a......j....t.."..1......-
D.o.~>_4...F......i.Q...C./mP.kM-.....G;..=..h#...1.h
*..?... .C.MnbM...<H.....;...].+..Z......
7...#.O..L..M_.F.E.x....................`..
..?e.`..%;."DI...(..  @..9.....;.P...{.......Y.
..3..n.H...OQ.0W...q.Q......T>..w8.....ih/=.....{...,.=......R.f.........._M.
8L....]a...OC%....St..r..T@.N...'..cW.e......J.=..q.E,.t.;w.Ay...v.a-.7.
5I.R8.V9.Q....
.....,| .X..$..1..1..d o....
..P.......D..Fm'i.P
```

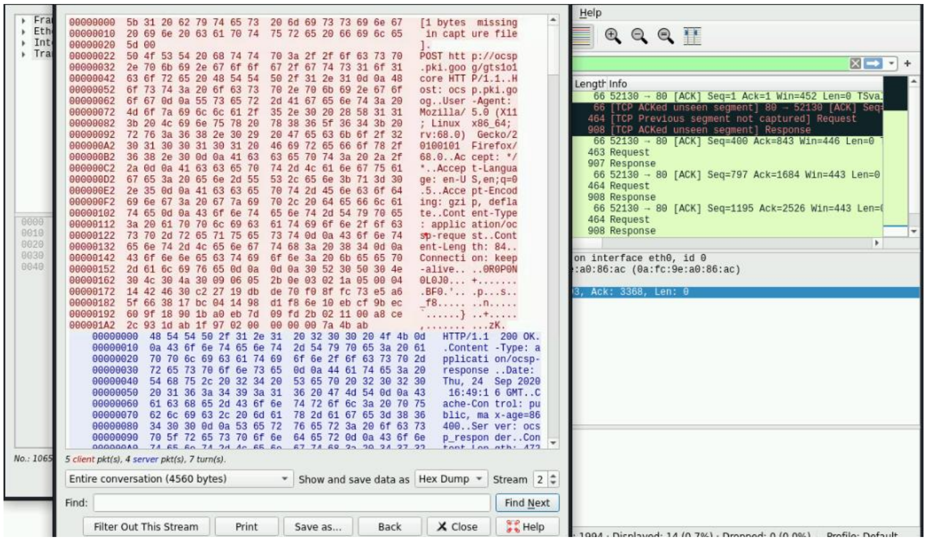
9 client pkt(s), 6 server pkt(s), 10 turn(s).

Entire conversation (7350 bytes)   Show and save data as ASCII   Stream 6

```
Length Info
    74 46328 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961
    74 80 → 46328 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=
    66 46328 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSv
   279 CONNECT adservice.google.com:443 HTTP/1.1
    66 80 → 46328 [ACK] Seq=1 Ack=214 Win=28160 Len=0
   105 HTTP/1.1 200 Connection established
    66 46328 → 80 [ACK] Seq=214 Ack=40 Win=62848 Len=0
   583 Client Hello
  3891 Server Hello, Change Cipher Spec, Application Da
    66 46328 → 80 [ACK] Seq=731 Ack=3865 Win=59136 Len=
   130 Change Cipher Spec, Application Data
   236 Application Data
   493 Application Data
```

```
:00:16:03 (0a:ca:d0:00:16:03)
```

: 3828 · Displayed: 27 (0.7%) · Dropped: 0 (0.0%)   Profile: Defaul



```
00000000  5b 31 20 62 79 74 65 73  20 6d 69 73 73 69 6e 67   [1 bytes  missing
00000010  20 69 6e 20 63 61 70 74  75 72 65 20 66 69 6c 65    in capt ure file
00000020  5d 00                                              ].
00000022  50 4f 53 54 20 68 74 74  70 3a 2f 2f 6f 63 73 70   POST htt p://ocsp
00000032  2e 70 6b 69 2e 67 6f 6f  67 2f 67 74 73 31 6f 31   .pki.goo g/gts1o1
00000042  63 6f 72 65 20 48 54 54  50 2f 31 2e 31 0d 0a 48   core HTT P/1.1..H
00000052  6f 73 74 3a 20 6f 63 73  70 2e 70 6b 69 2e 67 6f   ost: ocs p.pki.go
00000062  6f 67 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   og..User -Agent: 
00000072  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 58 31 31   Mozilla/ 5.0 (X11
00000082  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux  x86_64; 
00000092  72 76 3a 36 38 2e 30 29  20 47 65 63 6b 6f 2f 32   rv:68.0)  Gecko/2
000000A2  30 31 30 30 31 30 31 20  46 69 72 65 66 6f 78 2f   0100101  Firefox/
000000B2  36 38 2e 30 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   68.0..Ac cept: */
000000C2  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   *..Accep t-Langua
000000D2  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
000000E2  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5..Acce pt-Encod
000000F2  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
00000102  74 65 0d 0a 43 6f 6e 74  65 6e 74 2d 54 79 70 65   te..Cont ent-Type
00000112  3a 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 6f 63   : applic ation/oc
00000122  73 70 2d 72 65 71 75 65  73 74 0d 0a 43 6f 6e 74   sp-reque st..Cont
00000132  65 6e 74 2d 4c 65 6e 67  74 68 3a 20 38 34 0d 0a   ent-Leng th: 84..
00000142  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 6b 65 65 70   Connecti on: keep
00000152  2d 61 6c 69 76 65 0d 0a  0d 0a 30 52 30 50 30 4e   -alive.. ..0R0P0N
00000162  30 4c 30 4a 30 09 06 05  2b 0e 03 02 1a 05 00 04   0L0J0... +.......
00000172  14 42 46 30 c2 27 19 db  de 70 f0 8f fc 73 e5 a6   .BF0.'.. .p...s..
00000182  5f 66 38 17 bc 04 14 98  d1 f8 6e 10 eb cf 9b ec   _f8..... ..n.....
00000192  60 9f 18 90 1b a0 eb 7d  09 fd 2b 02 11 00 a8 ce   `......} ..+.....
000001A2  2c 93 1d ab 1f 97 02 00  00 00 00 7a 4b ab         ,....... ...zK.
    00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
    00000010  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 61   .Content -Type: a
    00000020  70 70 6c 69 63 61 74 69  6f 6e 2f 6f 63 73 70 2d   pplicati on/ocsp-
    00000030  72 65 73 70 6f 6e 73 65  0d 0a 44 61 74 65 3a 20   response ..Date: 
    00000040  54 68 75 2c 20 32 34 20  53 65 70 20 32 30 32 30   Thu, 24  Sep 2020
    00000050  20 31 36 3a 34 39 3a 31  36 20 47 4d 54 0d 0a 43    16:49:1 6 GMT..C
    00000060  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 70 75   ache-Con trol: pu
    00000070  62 6c 69 63 2c 20 6d 61  78 2d 61 67 65 3d 38 36   blic, ma x-age=86
    00000080  34 30 30 0d 0a 53 65 72  76 65 72 3a 20 6f 63 73   400..Ser ver: ocs
    00000090  70 5f 72 65 73 70 6f 6e  64 65 72 0d 0a 43 6f 6e   p_respon der..Con
```

5 client pkt(s), 4 server pkt(s), 7 turn(s).

Entire conversation (4560 bytes)   Show and save data as Hex Dump   Stream 2

```
Length Info
    66 52130 → 80 [ACK] Seq=1 Ack=1 Win=452 Len=0 TSva
    66 [TCP ACKed unseen segment] 80 → 52130 [ACK] Seq=
   464 [TCP Previous segment not captured] Request
   908 [TCP ACKed unseen segment] Response
    66 52130 → 80 [ACK] Seq=400 Ack=843 Win=446 Len=0
   463 Request
   907 Response
    66 52130 → 80 [ACK] Seq=797 Ack=1684 Win=443 Len=0
   464 Request
   908 Response
    66 52130 → 80 [ACK] Seq=1195 Ack=2526 Win=443 Len=
   464 Request
   908 Response
```

```
on interface eth0, id 0
:a0:86:ac (0a:fc:9e:a0:86:ac)
3, Ack: 3368, Len: 0
```

Looking at the TCP stream, it is showing what is communicating between webserver and browser. It is the data from a TCP as is seen by the application layer. The exchange is like all the website we visit. The traffic from source to destination and destination to source is denoted by red and blue colors, respectively. The non-printable characters are replaced by dots in this report. I changed it to hex dump and it looked human readable.

Conclusion

To conclude, Wireshark is a very powerful tool which can be used to monitor the traffic, keep logs of the traffic, and analyze the traffic in a network. As we saw in the lab activity, we can easily see each packet and find the nature of each packets separately. It helped me to understand TCP handshake and packet handling in a network. Thus, Wireshark is a great tool in studying behavior of packets in a network.