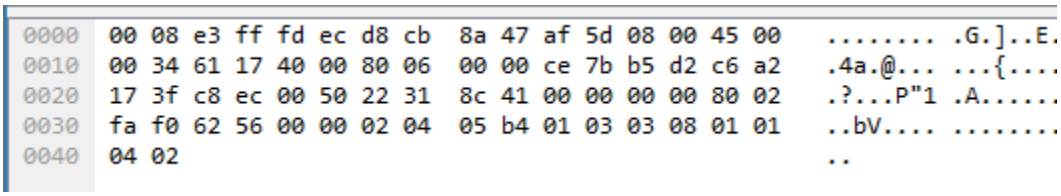
Lab 3 – T00533766



```
0000  00 08 e3 ff fd ec d8 cb  8a 47 af 5d 08 00 45 00   ........ .G.]..E.
0010  00 34 61 17 40 00 80 06  00 00 ce 7b b5 d2 c6 a2   .4a.@... ...{....
0020  17 3f c8 ec 00 50 22 31  8c 41 00 00 00 00 80 02   .?...P"1 .A......
0030  fa f0 62 56 00 00 02 04  05 b4 01 03 03 08 01 01   ..bV.... ........
0040  04 02                                             ..
```

00 08 e3 ff fd ec d8 cb 8a 47 af 5d 08 00 45 00

00 34 61 17 40 00 80 06 00 00 ce 7b b5 d2 c6 a2

17 3f C8 ec 00 50 22 31 8c 41 00 00 00 00 80 02

fa f0 62 56 00 00 02 04 05 b4 01 03 03 08 01 01

04 02

Ethernet Header: DATALINK MAC LAYER

00 08 e3 ff fd ec d8 cb 8a 47 af 5d 08 00

Ethernet Destination: 00 08 e3 ff fd ec

Ethernet Source: d8 cb 8a 47 af 5d

Payload Type: 08 00 => IPv4

Destination Address:0008e3fffdec	Source Address:d8cb8a47af5d	Type: IPv4	Data	CRC

IP header: TRANSPORT LAYER

45 00 00 34 61 17 40 00 80 06 00 00 ce 7b b5 d2 c6 a2 17 3f

45: 4=> IPv4

45: 5=> Header Length = 5*4 = 20 bytes

00: Contains the Precedence value for packet, TOS value

Below is 00 from the IP header in binary:

0 0 0 0 0 0 0 0: Precedence Value => Routine for this packet

0 0 0 0 0 0 0 0: TOS bits

0 0 0: Normal delay

0 0 0: Normal throughput

0 0 0: Normal Reliability

0 0 0 0 0 0 0 0: Must be zero

00 34: These describe the length of the IP datagram => 34(hex=> 0X0034) converted to decimal = 52 bytes. The IP datagram is 52 bytes long.

61 17: The identification of the datagram for fragmentation. 6117(hex=> 0x6117) in decimal is 24855.

40 00: in binary = (0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0)

1 Don't fragment flag set

0 More Fragments flag set

0: Fragment Offset

80: Time for datagram to live = 128 i.e. (0x0080) in decimal

06: The protocol used is TCP (6)

00 00: Check sum of the datagram

ce 7b b5 d2: Source IP address: 206.123.181.210

c6 a2 17 3f: Destination IP address: 198.162.23.63

Version: 4	IP Header Length: 20	Type Of Service: 00	Total Length: 52
Identification: 24855	Flags: 40 00		Fragment Offset: 0
Time to live: 128	Protocol: TCP(6)		Header Checksum: 00 00
Source IP address: 206.123.181.210			
Destination IP address: 198.162.23.63			
Options			Padding: Just to fill size of TCP header

TCP Header: NETWORK LAYER

C8 ec 00 50 22 31 8c 41 00 00 00 00 80 02

fa f0 62 56 00 00 02 04 05 b4 01 03 03 08 01 01

04 02

c8 ec: Source port: 51436

00 50: Destination Port: 80

22 31 8c 41: Sequence Number: 573672513

00 00 00 00: Acknowledgment Number: 0

80: TCP Header/offset length = 8*4 = 32 bytes

02 = Flags = 0 0 0 0 0 0 1 0

NONCE: 0

Congestion Window reduced: 0

ECHO: 0

Urgent: 0

Acknowledgment: 0

Push: 0

Reset: 0

Syn: 1 =>The SYN[chronize] flag is the **TCP** packet flag that is used to initiate a TCP connection. A packet containing solely a SYN flag is the first part of the "**three-way handshake**" of TCP connection initiation. It is responded to with a **SYN-ACK** packet.

Fin: 0

Fa f0: Window size: 64240

62 56: check sum: 25174

00 00: Urgent pointer

02 04 05 b4 01 03 03 08 01 01 04 02: Optional

02 04 05 b4: TCP max segment size

01: NOP No-Operation flag

03 03 08: Window scale: Kind = 03, Length = 03, Shift = 08

01: No operation

01: No operation

04 02: TCP SACK permitted, length 2

<table>
<tr><td colspan="4">Source Port: 51436</td><td colspan="4">Destination Port: 80</td></tr>
<tr><td colspan="8">Sequence Number:573672513</td></tr>
<tr><td colspan="8">Acknowledgment Number: 0</td></tr>
<tr><td colspan="2">Data Offset: 32</td><td colspan="2">Reserved
0 0 0</td><td>U
R
G
0</td><td>A
C
K
0</td><td>P
S
H
0</td><td>R
S
T
0</td><td>S
Y
N
1</td><td>F
I
N
0</td><td>Window-Size:
64240</td></tr>
<tr><td colspan="4">Checksum: 25174</td><td colspan="4">Urgent Pointer: 0</td></tr>
<tr><td colspan="6">Options: 12 bytes</td><td colspan="2">Padding: Just to fill size of TCP header</td></tr>
<tr><td colspan="8">Data</td></tr>
</table>