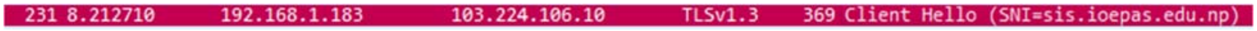
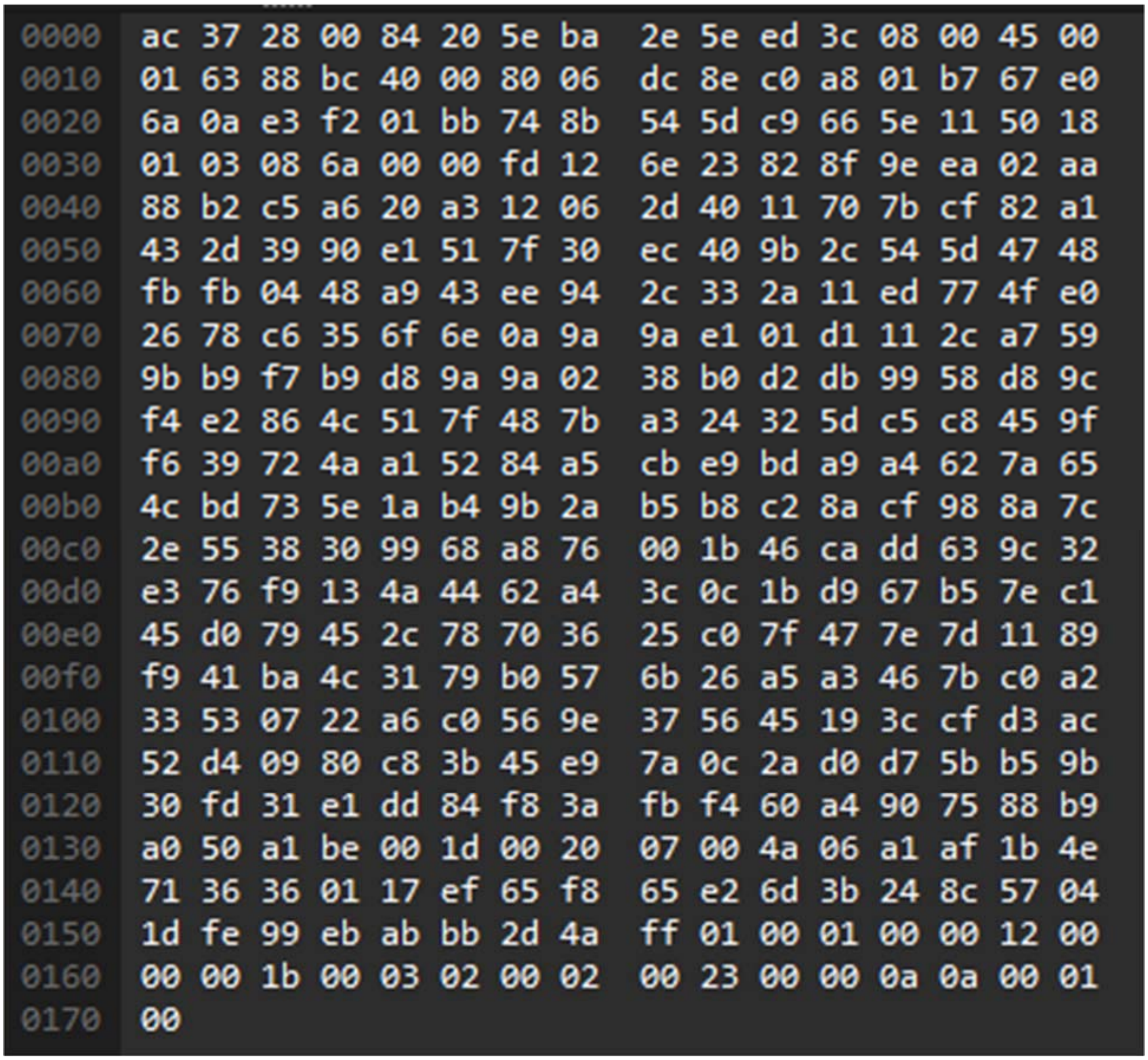
Analysis of Packet Captured After Logging into a Website

Packet Captured



```
231 8.212710    192.168.1.183    103.224.106.10    TLSv1.3    369 Client Hello (SNI=sis.ioepas.edu.np)
```

Frame



```
0000  ac 37 28 00 84 20 5e ba  2e 5e ed 3c 08 00 45 00
0010  01 63 88 bc 40 00 80 06  dc 8e c0 a8 01 b7 67 e0
0020  6a 0a e3 f2 01 bb 74 8b  54 5d c9 66 5e 11 50 18
0030  01 03 08 6a 00 00 fd 12  6e 23 82 8f 9e ea 02 aa
0040  88 b2 c5 a6 20 a3 12 06  2d 40 11 70 7b cf 82 a1
0050  43 2d 39 90 e1 51 7f 30  ec 40 9b 2c 54 5d 47 48
0060  fb fb 04 48 a9 43 ee 94  2c 33 2a 11 ed 77 4f e0
0070  26 78 c6 35 6f 6e 0a 9a  9a e1 01 d1 11 2c a7 59
0080  9b b9 f7 b9 d8 9a 9a 02  38 b0 d2 db 99 58 d8 9c
0090  f4 e2 86 4c 51 7f 48 7b  a3 24 32 5d c5 c8 45 9f
00a0  f6 39 72 4a a1 52 84 a5  cb e9 bd a9 a4 62 7a 65
00b0  4c bd 73 5e 1a b4 9b 2a  b5 b8 c2 8a cf 98 8a 7c
00c0  2e 55 38 30 99 68 a8 76  00 1b 46 ca dd 63 9c 32
00d0  e3 76 f9 13 4a 44 62 a4  3c 0c 1b d9 67 b5 7e c1
00e0  45 d0 79 45 2c 78 70 36  25 c0 7f 47 7e 7d 11 89
00f0  f9 41 ba 4c 31 79 b0 57  6b 26 a5 a3 46 7b c0 a2
0100  33 53 07 22 a6 c0 56 9e  37 56 45 19 3c cf d3 ac
0110  52 d4 09 80 c8 3b 45 e9  7a 0c 2a d0 d7 5b b5 9b
0120  30 fd 31 e1 dd 84 f8 3a  fb f4 60 a4 90 75 88 b9
0130  a0 50 a1 be 00 1d 00 20  07 00 4a 06 a1 af 1b 4e
0140  71 36 36 01 17 ef 65 f8  65 e2 6d 3b 24 8c 57 04
0150  1d fe 99 eb ab bb 2d 4a  ff 01 00 01 00 00 12 00
0160  00 00 1b 00 03 02 00 02  00 23 00 00 0a 0a 00 01
0170  00
```

Description of Each Fields

Frame

Field	Value
Frame No:	231
Frame Length:	369 bytes (2952 bits)
Interface Id:	0
Capture Length:	369 bytes (2952 bits)
Protocols in frame:	eth:ethertype:ip:tcp:tls

Ethernet II

Field	Value
Destination:	TaicangT&WEl_00:84:20 (ac:37:28:00:84:20)
Source:	5e:ba:2e:5e:ed:3c
Type:	IPv4 (0x0800)

IPV4

Field	Value
Version	4
Header Length	20 bytes
Differentiated Services Field:	0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length	355

Identification:	0x88bc (35004)
Flags	0x2
Fragment Offset	0
Time to Leave	128
Protocol	TCP (6)
Header Checksum	0xdc8e
Header checksum status:	Unverified
Source Address:	192.168.1.183
Destination Address:	103.224.106.10

TCP

Field	**Value**
Source Port:	58354
Destination Port:	443
Sequence:	1413
Length:	315
Header Length:	20 bytes (5)
Flags:	0x018 (PSH, ACK)
Window Size:	66304
Urgent Pointer:	0

TLS

TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Field	Value
Content type:	Handshake (22)
Version:	TLS 1.0 (0x0301)
Length:	1722

Handshake Protocol: client Hello

Handshake Type:	client Hello (1)
Length:	1718
Version:	TLS 1.0 (0x0303)

Conclusion

This packet analysis reveals a standard TLS handshake initiation over IPV4 to a Student Information System of Paschimanchal Campus. By doing this I am able to capture packets related to logging on a website.