COMPUTER NETWORKS AND SECURITY LABORATORY

Group C

Assignment No. 15

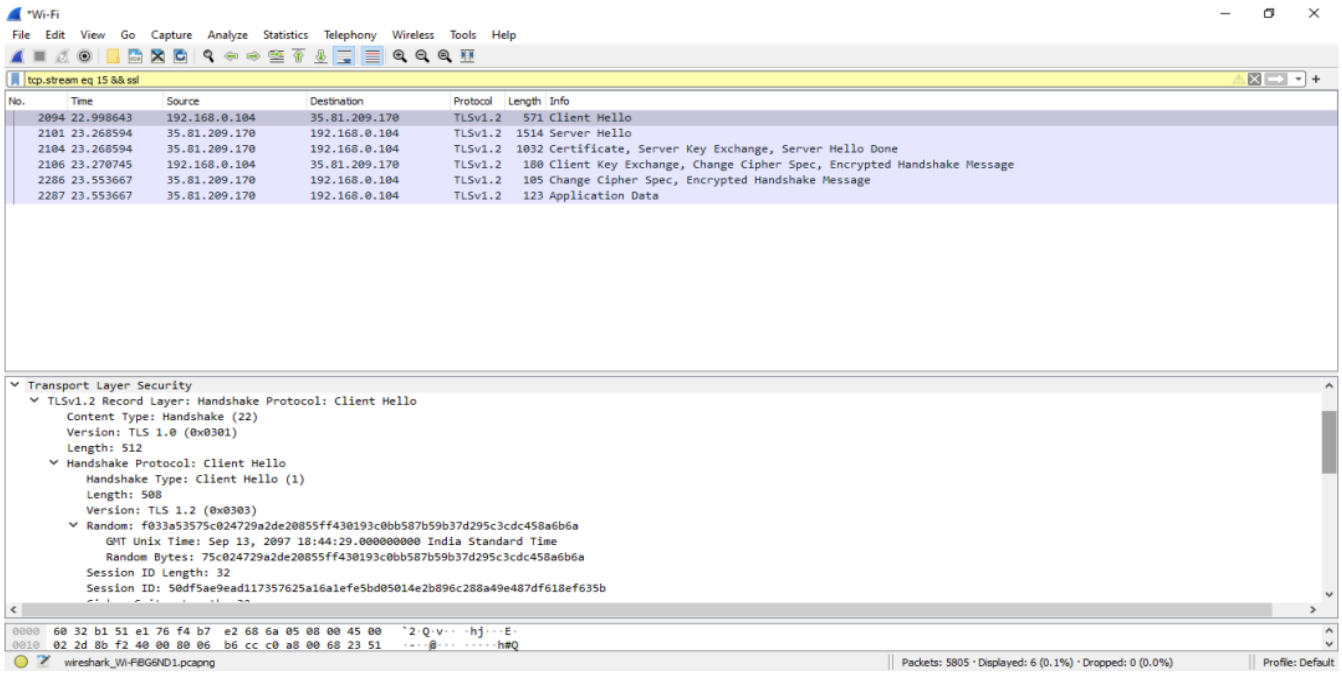
NAME :- OJUS P. JAISWAL

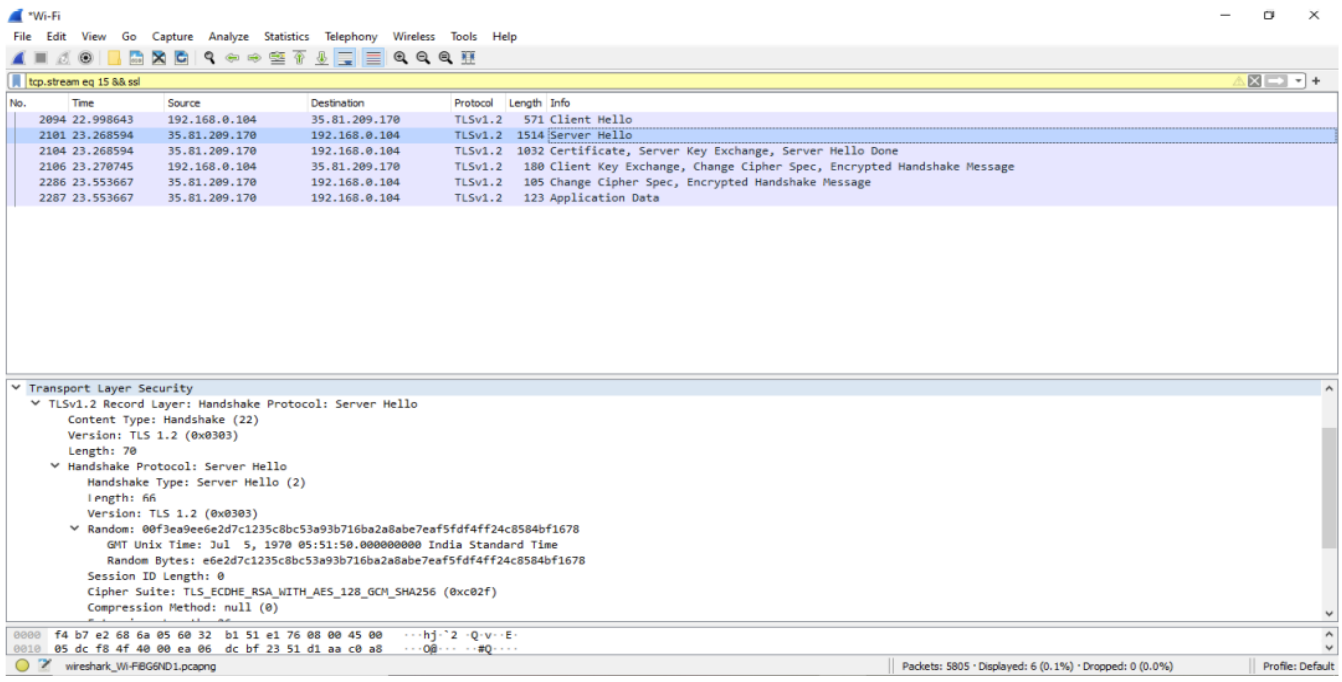
ROLL NO. :- TACO19108

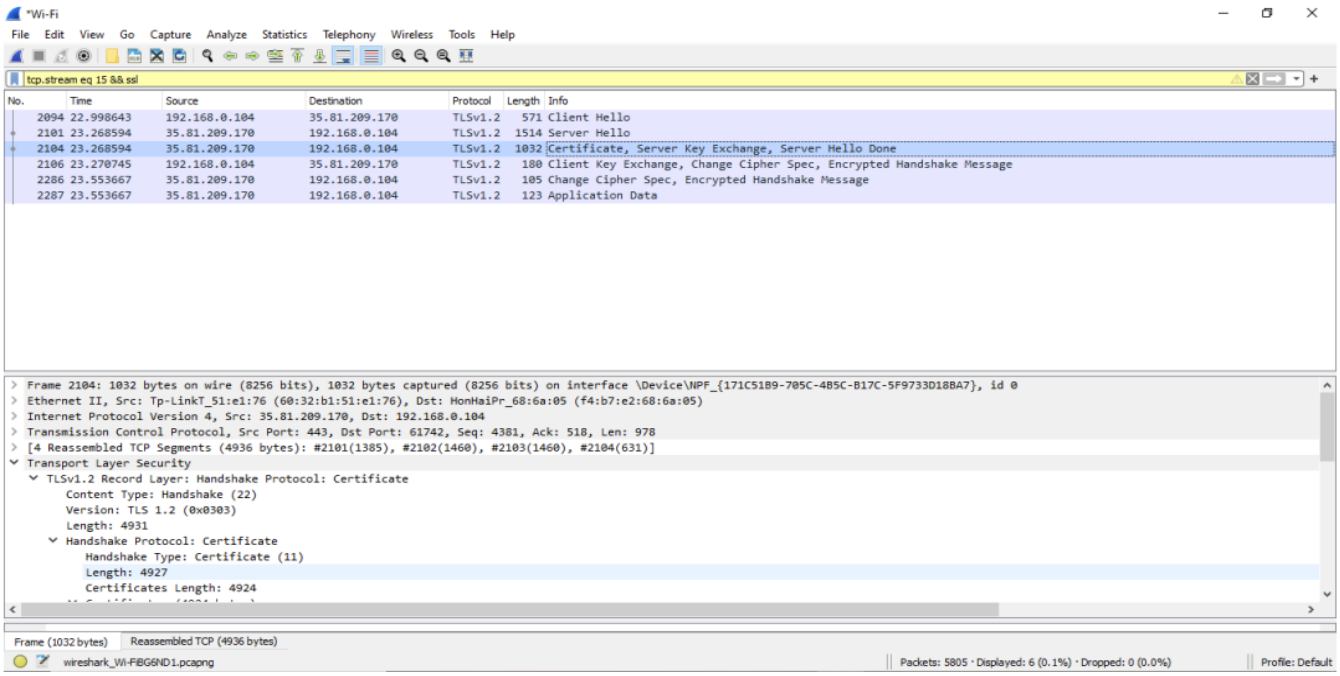
YEAR AND DIV :- TE A

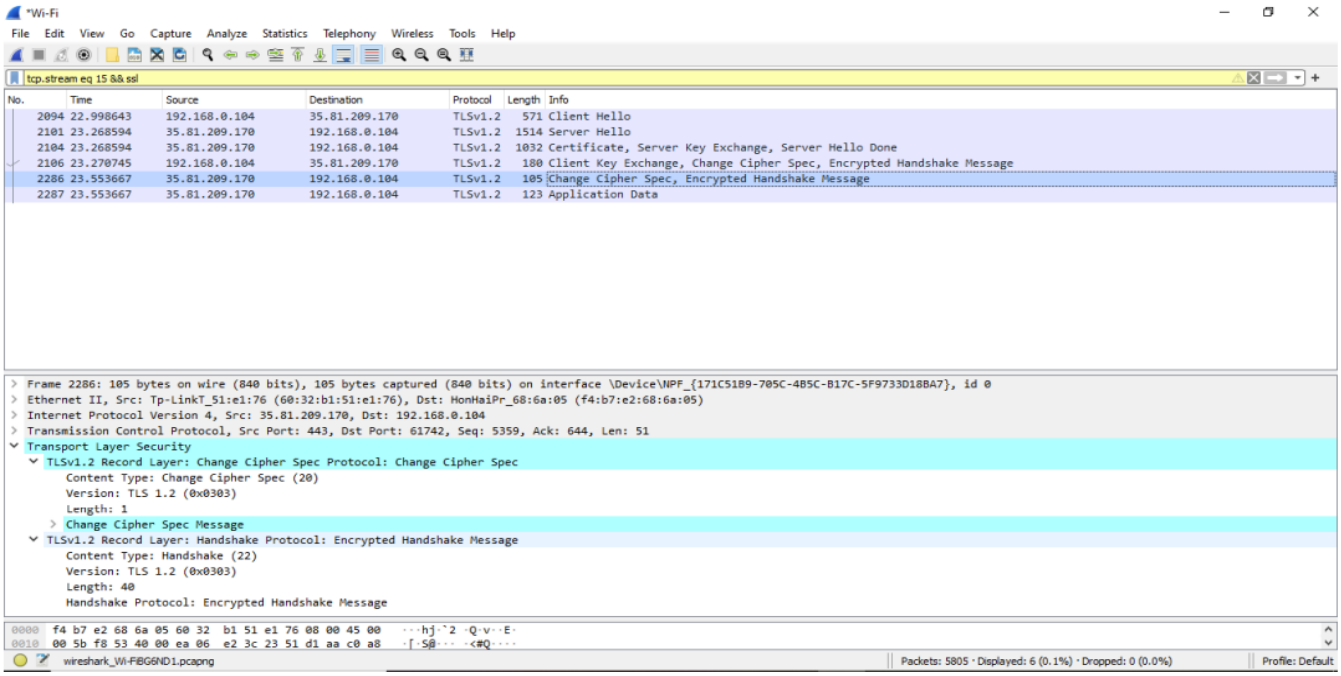
Ques :- To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).

Solution :-






*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 15 && ssl
No. Time Source Destination Protocol Length Info
2094 22.998643 192.168.0.104 35.81.209.170 TLSv1.2 571 Client Hello
2101 23.268594 35.81.209.170 192.168.0.104 TLSv1.2 1514 Server Hello
2104 23.268594 35.81.209.170 192.168.0.104 TLSv1.2 1032 Certificate, Server Key Exchange, Server Hello Done
2106 23.270745 192.168.0.104 35.81.209.170 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2286 23.553667 35.81.209.170 192.168.0.104 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
2287 23.553667 35.81.209.170 192.168.0.104 TLSv1.2 123 Application Data
Frame 2104: 1032 bytes on wire (8256 bits), 1032 bytes captured (8256 bits) on interface \Device\NPF_{171C51B9-705C-4B5C-B17C-5F9733D18BA7}, id 0
Ethernet II, Src: Tp-LinkT_51:e1:76 (60:32:b1:51:e1:76), Dst: HonHaiPr_68:6a:05 (f4:b7:e2:68:6a:05)
Internet Protocol Version 4, Src: 35.81.209.170, Dst: 192.168.0.104
Transmission Control Protocol, Src Port: 443, Dst Port: 61742, Seq: 4381, Ack: 518, Len: 978
[4 Reassembled TCP Segments (4936 bytes): #2101(1385), #2102(1460), #2103(1460), #2104(631)]
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4931
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 4927
Certificates Length: 4924
Frame (1032 bytes)
Reassembled TCP (4936 bytes)
wireshark_Wi-FiBG6ND1.pcapng
Packets: 5805 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%)
Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 15 && ssl
No. Time Source Destination Protocol Length Info
2094 22.998643 192.168.0.104 35.81.209.170 TLSv1.2 571 Client Hello
2101 23.268594 35.81.209.170 192.168.0.104 TLSv1.2 1514 Server Hello
2104 23.268594 35.81.209.170 192.168.0.104 TLSv1.2 1032 Certificate, Server Key Exchange, Server Hello Done
2106 23.270745 192.168.0.104 35.81.209.170 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2286 23.553667 35.81.209.170 192.168.0.104 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
2287 23.553667 35.81.209.170 192.168.0.104 TLSv1.2 123 Application Data
Frame 2286: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \Device\NPF_{171C51B9-705C-4B5C-B17C-5F9733D18BA7}, id 0
Ethernet II, Src: Tp-LinkT_51:e1:76 (60:32:b1:51:e1:76), Dst: HonHaiPr_68:6a:05 (f4:b7:e2:68:6a:05)
Internet Protocol Version 4, Src: 35.81.209.170, Dst: 192.168.0.104
Transmission Control Protocol, Src Port: 443, Dst Port: 61742, Seq: 5359, Ack: 644, Len: 51
Transport Layer Security
TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.2 (0x0303)
Length: 1
Change Cipher Spec Message
TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 40
Handshake Protocol: Encrypted Handshake Message
0000 f4 b7 e2 68 6a 05 60 32 b1 51 e1 76 08 00 45 00
0010 00 5b f8 53 40 00 ea 06 e2 3c 23 51 d1 aa c0 a8
wireshark_Wi-FiBG6ND1.pcapng
Packets: 5805 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%)
Profile: Default