

CNS Lab

Assignment 11

Prn : 21510111

Name Siddharth Shrinivas Salunkhe

Batch : B5

1. Filrer trace using ssl

ssl					
No.	Time	Source	Destination	Protocol	Length Info
4	0.021328	192.168.1.102	173.194.79.106	TLSv1	186 Client Hello (SNI=www.google.com)
6	0.041634	173.194.79.106	192.168.1.102	TLSv1	1484 Server Hello
7	0.041697	173.194.79.106	192.168.1.102	TLSv1	377 Certificate, Server Hello Done
9	0.088543	192.168.1.102	173.194.79.106	TLSv1	252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.105145	173.194.79.106	192.168.1.102	TLSv1	113 Change Cipher Spec, Encrypted Handshake Message
12	0.105436	192.168.1.102	173.194.79.106	TLSv1	239 Application Data
13	0.136468	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
15	0.137993	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
17	0.138469	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Application Data, Application Data
19	0.138632	173.194.79.106	192.168.1.102	TLSv1	316 Application Data, Application Data
21	0.140271	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Application Data
23	0.144028	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
25	0.144465	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
27	0.150300	173.194.79.106	192.168.1.102	TLSv1	270 Application Data, Application Data
29	0.150959	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Application Data
31	0.155107	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
33	0.155529	173.194.79.106	192.168.1.102	TLSv1	1484 Application Data
34	0.163139	173.194.79.106	192.168.1.102	TLSv1	1484 Application Data, Application Data, Application Data
36	0.164031	173.194.79.106	192.168.1.102	TLSv1	1484 Application Data, Application Data
37	0.169767	173.194.79.106	192.168.1.102	TLSv1	1484 Application Data
39	0.170028	173.194.79.106	192.168.1.102	TLSv1	1484 Application Data, Application Data, Application Data
40	0.176414	173.194.79.106	192.168.1.102	TLSv1	130 Application Data, Application Data
42	0.177209	192.168.1.102	173.194.79.106	TLSv1	93 Encrypted Alert

2. Client-side hello

```
▶ Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: CiscoLinksys_e3:e9:8d (00:16:b6:e3:e9:8d)
▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106
▶ Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 1, Ack: 1, Len: 120
▼ Transport Layer Security
  ▼ TLSv1 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 115
    ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 111
      Version: TLS 1.0 (0x0301)
      ▶ Random: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f
      Session ID Length: 0
      Cipher Suites Length: 46
      ▶ Cipher Suites (23 suites)
      Compression Methods Length: 2
      ▶ Compression Methods (2 methods)
      Extensions Length: 23
      ▶ Extension: server_name (len=19) name=www.google.com
        [JA4: t10d230100_6a57a6f57151_e3b0c44298fc]
        [JA4_r: t10d230100_0003,0004,0005,0006,0008,0009,000a,0011,0012,0013,0014,0015,0016,002f,0032,0033,0035,0038,0039,0096,00]
        [JA3 Fullstring: 769,57-56-53-22-19-10-51-50-47-154-153-150-5-4-21-18-9-20-17-8-6-3-255,0,,]
        [JA3: 06a92bf69b367389d2feb0d70501ddfe]
```

3. Server-side hello

```
▶ Frame 6: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interface en0, id 0
▶ Ethernet II, Src: CiscoLinksys_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_a2:05:1d (70:56:81:a2:05:1d)
▶ Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1, Ack: 121, Len: 1418
▼ Transport Layer Security
  ▼ TLSv1 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 85
    ▼ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 81
      Version: TLS 1.0 (0x0301)
      ▶ Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
      Session ID Length: 32
      Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0cebfcccf4
      Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
      Compression Method: null (0)
      Extensions Length: 9
      ▶ Extension: server_name (len=0)
      ▶ Extension: renegotiation_info (len=1)
        [JA3S Fullstring: 769,5,0-65281]
        [JA3S: d2e6f7ef558ea8036c7e21b163b2d1af]
      TLS segment data (1328 bytes)
```

4. Client key exchange

```
▶ Frame 9: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: CiscoLinksys_e3:e9:8d (00:16:b6:e3:e9:8d)
▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106
▶ Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 121, Ack: 1730, Len: 186
▼ Transport Layer Security
  ▼ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 134
    ▼ Handshake Protocol: Client Key Exchange
      Handshake Type: Client Key Exchange (16)
      Length: 130
      ▶ RSA Encrypted PreMaster Secret
  ▼ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.0 (0x0301)
    Length: 1
    Change Cipher Spec Message
  ▼ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 36
    Handshake Protocol: Encrypted Handshake Message
```

5. Encrypted data :

```
▶ Frame 12: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: CiscoLinksys_e3:e9:8d (00:16:b6:e3:e9:8d)
▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106
▶ Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 307, Ack: 1777, Len: 173
▼ Transport Layer Security
  ▼ TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Content Type: Application Data (23)
    Version: TLS 1.0 (0x0301)
    Length: 168
    Encrypted Application Data [truncated]: 52e78fc0f73eec8a76cc499ad794fd69ee412be8ba893114f5d8906232bdd0924f0dc7d99fd7c277755
    [Application Data Protocol: Hypertext Transfer Protocol]
```