Encryption Report

Prepared by: Isabelle Jaber

Date: August 5th, 2024

Table of Contents:

INTRODUCTION

The objective of this report is to show a trusted and encrypted connection between the client and “https://google.com”. Identification of a ClientHello Message, ServerHello Message, and KeyExchange Message, as well as confirmation of encrypted application data are crucial steps in this process.

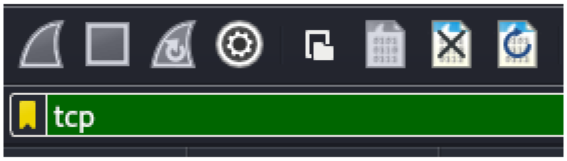
METHODOLOGY

Tools Used

- Wireshark
- Firefox

Procedure Followed

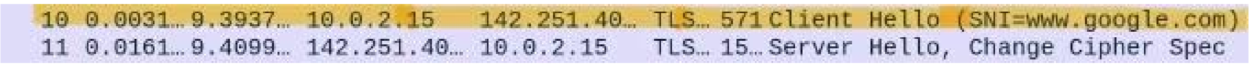
- Opened Firefox
- Opened Wireshare and started an eth0 network capture.
- Typed “https://google.com” into the search bar in Firefox.
- Stopped and saved the network capture in Wireshark.
- Entered the following filter to find the necessary logs:



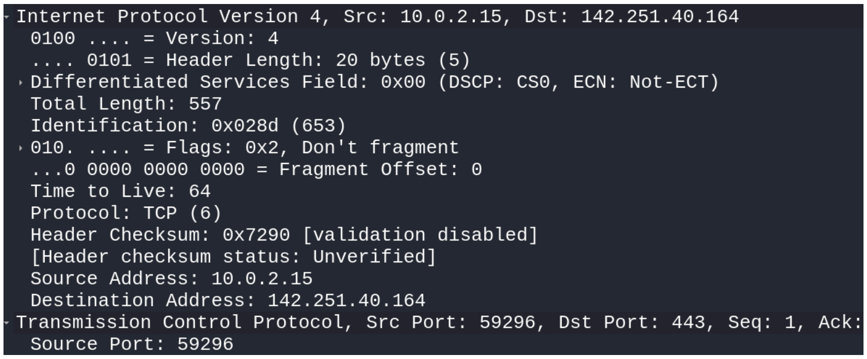
```
tcp
```

TLS Handshake Analysis

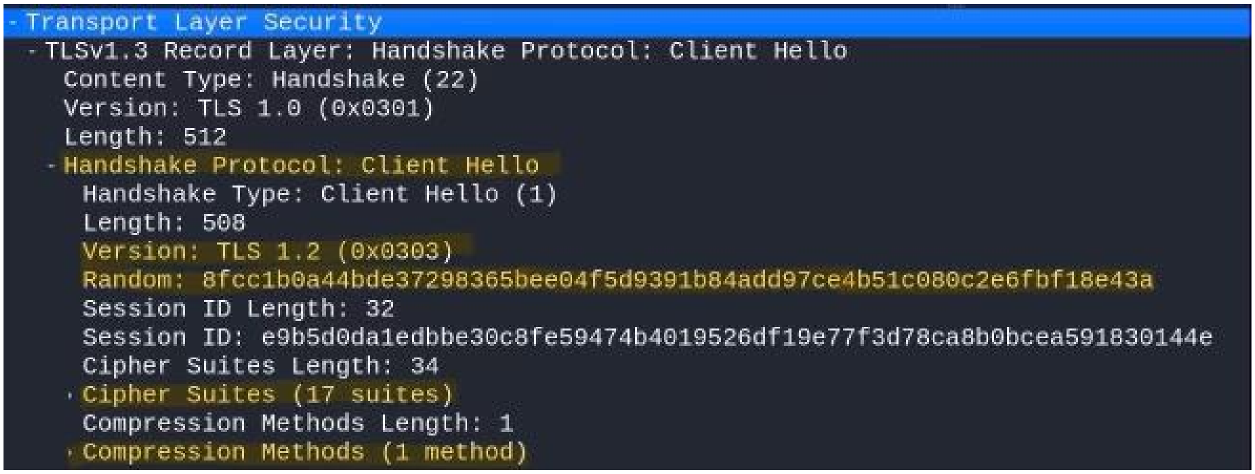
- ClientHello Message



```
10 0.0031… 9.3937… 10.0.2.15    142.251.40… TLS… 571 Client Hello (SNI=www.google.com)
11 0.0161… 9.4099… 142.251.40… 10.0.2.15    TLS… 15… Server Hello, Change Cipher Spec
```

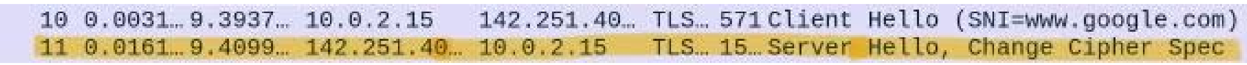


```
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.40.164
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 557
  Identification: 0x028d (653)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x7290 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.2.15
  Destination Address: 142.251.40.164
Transmission Control Protocol, Src Port: 59296, Dst Port: 443, Seq: 1, Ack:
  Source Port: 59296
```

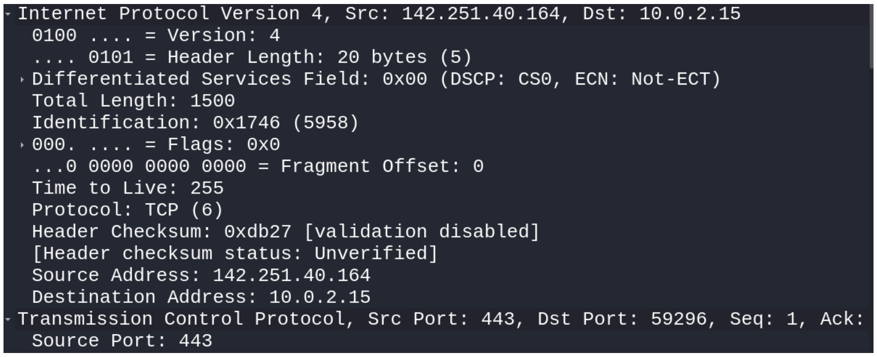


```
- Transport Layer Security
 - TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  - Handshake Protocol: Client Hello
     Handshake Type: Client Hello (1)
     Length: 508
     Version: TLS 1.2 (0x0303)
     Random: 8fcc1b0a44bde37298365bee04f5d9391b84add97ce4b51c080c2e6fbf18e43a
     Session ID Length: 32
     Session ID: e9b5d0da1edbbe30c8fe59474b4019526df19e77f3d78ca8b0bcea591830144e
     Cipher Suites Length: 34
   › Cipher Suites (17 suites)
     Compression Methods Length: 1
   › Compression Methods (1 method)
```

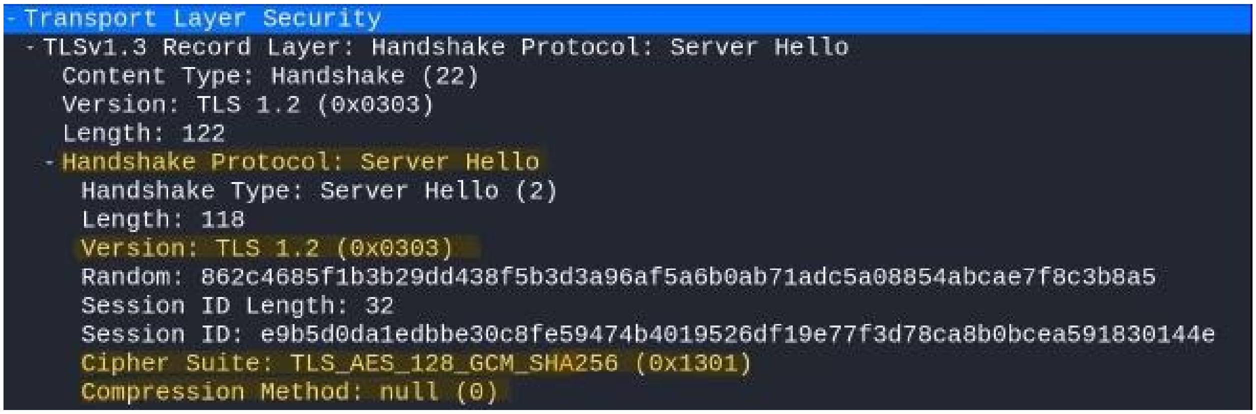
- ○ Purpose and Significance
  - ■ The purpose of the ClientHello message in the TLS handshake process is to send the server a list of the client’s cryptographic information. This includes the TLS version and the CipherSuites supported by the client (in order of preference). The message also contains a random byte string that is used in subsequent computations. It may also include the data compression methods supported by the client.
- ServerHello Message



```
10 0.0031… 9.3937…  10.0.2.15     142.251.40…  TLS… 571 Client Hello (SNI=www.google.com)
11 0.0161… 9.4099…  142.251.40…  10.0.2.15     TLS… 15… Server Hello, Change Cipher Spec
```



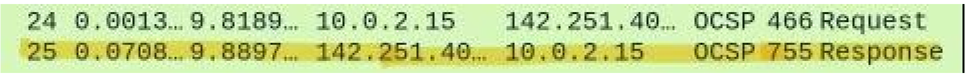
```
- Internet Protocol Version 4, Src: 142.251.40.164, Dst: 10.0.2.15
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 1500
   Identification: 0x1746 (5958)
 › 000. .... = Flags: 0x0
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 255
   Protocol: TCP (6)
   Header Checksum: 0xdb27 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 142.251.40.164
   Destination Address: 10.0.2.15
- Transmission Control Protocol, Src Port: 443, Dst Port: 59296, Seq: 1, Ack:
   Source Port: 443
```



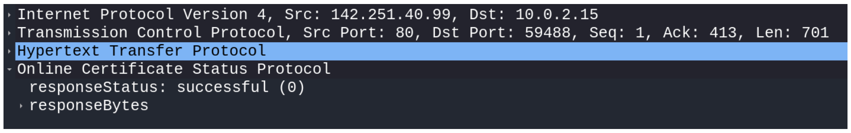
```
- Transport Layer Security
 - TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 122
  - Handshake Protocol: Server Hello
     Handshake Type: Server Hello (2)
     Length: 118
     Version: TLS 1.2 (0x0303)
     Random: 862c4685f1b3b29dd438f5b3d3a96af5a6b0ab71adc5a08854abcae7f8c3b8a5
     Session ID Length: 32
     Session ID: e9b5d0da1edbbe30c8fe59474b4019526df19e77f3d78ca8b0bcea591830144e
     Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
     Compression Method: null (0)
```

- Purpose and Significance
    - The ServerHello message contains the CipherSuite chosen by the server from the list provided by the client in the ClientHello message, the session ID, another random byte string, and potentially a compression method. The server also sends its digital certificate.

- Key Exchange Message



```
24 0.0013… 9.8189… 10.0.2.15     142.251.40…  OCSP 466 Request
25 0.0708… 9.8897… 142.251.40…  10.0.2.15     OCSP 755 Response
```



```
› Internet Protocol Version 4, Src: 142.251.40.99, Dst: 10.0.2.15
› Transmission Control Protocol, Src Port: 80, Dst Port: 59488, Seq: 1, Ack: 413, Len: 701
› Hypertext Transfer Protocol
- Online Certificate Status Protocol
   responseStatus: successful (0)
  › responseBytes
```

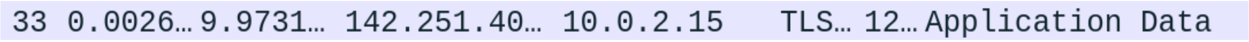
- Purpose and Significance
    - The purpose of the Key Exchange Message is to provide a trusted secure connection between the client and the server by providing verified digital certificates. In this case, OCSP (Online Certificate Status Protocol) is used to verify these certificates. OCSP is a protocol that certificate authorities (CAs) use to determine the status of secure TLS certificates.

PACKET DETAILS

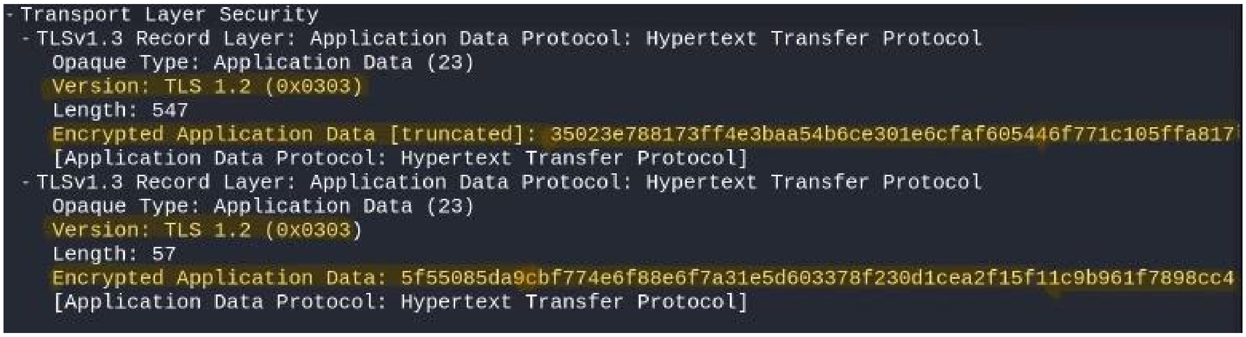
Source and Destination Information

1. ClientHello Packet
    - Source IP: 10.0.2.15
    - Source Port: 59296
    - Destination IP: 142.251.40.164
    - Destination Port: 443
2. ServerHello Packet
    - Source IP: 142.251.40.164
    - Source Port: 443
    - Destination IP: 10.0.2.15
    - Destination Port: 59296
3. Key Exchange Packet
    - Source IP: 142.25140.99
    - Source Port: 80
    - Destination IP: 10.0.2.15
    - Destination Port: 59488

Encryption Verification



```
33 0.0026… 9.9731…  142.251.40…  10.0.2.15   TLS… 12… Application Data
```



```
- Transport Layer Security
  - TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 547
      Encrypted Application Data [truncated]: 35023e788173ff4e3baa54b6ce301e6cfaf605446f771c105ffa817
      [Application Data Protocol: Hypertext Transfer Protocol]
  - TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 57
      Encrypted Application Data: 5f55085da9cbf774e6f88e6f7a31e5d603378f230d1cea2f15f11c9b961f7898cc4
      [Application Data Protocol: Hypertext Transfer Protocol]
```