

# Encryption Report

## Introduction

The objective of this report is to analyze the TLS handshake for an HTTPS connection to <https://www.google.com> using Wireshark on a Kali Linux virtual machine. The report will provide detailed information on the ClientHello, ServerHello, and Key Exchange messages exchanged during the TLS handshake, including timestamps, IP addresses, port numbers, and the verification of encrypted packets post-handshake.

## Methodology

### A. Tools Used

- Wireshark

### B. Procedure followed

#### 1. Setting Up the Environment

Ensure you have a Kali Linux VM and Wireshark installed.

1. Install Wireshark
2. Run Wireshark with root privileges:

```
sudo wireshark
```

#### 2. Configuring Wireshark to Capture Traffic

##### Select the Network Interface:

- Open Wireshark.
- Choose the network interface that your VM uses to connect to the internet. This is typically eth0.

##### Start the Capture:

- Click on the selected interface.
- Click the **Start** button.

### 3. Initiate HTTPS Connection

#### Open a Web Browser:

- Open a web browser on your Kali VM.

#### Visit <https://www.google.com>:

- Type the URL in the address bar and press Enter.

### 4. Capturing the TLS Handshake

#### Stop the Capture:

- Once the page loads, return to Wireshark and click the **Stop** button

#### Filter the Traffic:

- In the Wireshark filter bar, type `tls` and press Enter. This filters the captured packets to show only TLS traffic.

### 5. Analyzing the TLS Handshake

#### Identify the TLS Handshake Packets:

- Look for packets labeled as ClientHello, ServerHello, and other handshake-related messages.

#### Examine ClientHello Packet:

- Click on the ClientHello packet.
- Expand the sections in the packet details pane:
  - **TLSv1.3 Record Layer.**
  - **Handshake Protocol: Client Hello.**

#### Examine ServerHello Packet:

- Click on the ServerHello packet.
- Expand the sections in the packet details pane:
  - **TLSv1.3 Record Layer.**
  - **Handshake Protocol: Server Hello.**

#### Select an Application Data Packet:

- Scroll through the filtered list to find a packet labeled as Application Data.

#### Expand Packet Details:

- Click on the Application Data packet to select it.
- In the packet details pane, expand the sections:
  - **Frame**
  - **Ethernet II**
  - **Internet Protocol Version 4 (or IPv6)**
  - **Transmission Control Protocol (TCP)**
  - **Transport Layer Security (TLS)**

## Highlight Encrypted Data:

- Highlight the section showing Application Data.
- This section confirms that the data is encrypted.

## Examine Finished Packets:

- These packets mark the end of the handshake and the beginning of encrypted application data.

# TLS Handshake Analysis

- ClientHello Message

```
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 650
Version: TLS 1.2 (0x0303)
Random: 569dd7172b2af0645d171e6b9e2ac0f868749ddf4e094d77fd8fdd306cb8bbd0
Session ID Length: 32
Session ID: b04d243b669080e4415876e17fa96961c93ddab907105dd4d1603d6dd9914c1c
Cipher Suites Length: 34
  Cipher Suites (17 suites)
Compression Methods Length: 1
  Compression Methods (1 method)
Extensions Length: 543
  Extension: server_name (len=19) name=www.google.com
    Type: server_name (0)
    Length: 19
  Server Name Indication extension
  Extension: extended_master_secret (len=0)
    Type: extended_master_secret (23)
    Length: 0
  Extension: renegotiation_info (len=1)
    Type: renegotiation_info (65281)
    Length: 1
  Renegotiation Info extension
  Extension: supported_groups (len=14)
    Type: supported_groups (10)
    Length: 14
    Supported Groups List Length: 12
    Supported Groups (6 groups)
  Extension: ec_point_formats (len=2)
    Type: ec_point_formats (11)
    Length: 2
    EC point formats Length: 1
    Elliptic curves point formats (1)
  Extension: application_layer_protocol_negotiation (len=14)
    Type: application_layer_protocol_negotiation (16)
```

```
0000 52 54 00 12 35 00 08 00 27 1e 27 d8 08 00 45 00 RT...5...E
0010 02 bb 31 88 40 00 40 06 42 87 0a 00 02 0f 8e fb ..1.@.B.....
0020 29 24 e0 66 01 bb 08 33 56 f1 00 00 69 bc 50 18 )$.f...3V...i.P
0030 7d 78 c6 db 00 00 16 03 01 02 8e 01 00 02 8a 03 }x.....
```

- Timestamp: 2024/216 17:38:35 .292770846
- Purpose and Significance
  - The ClientHello message is the initial step in the TLS handshake, where the client proposes security parameters (such as supported cipher suites and TLS versions) to the server.
- ServerHello Message

```

- TLSv1.3 Record Layer: Handshake Protocol: Server Hello
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 128
- Handshake Protocol: Server Hello
  Handshake Type: Server Hello (2)
  Length: 124
  Version: TLS 1.2 (0x0303)
  Random: 97697779fe62e47e0c4b34bf817eebbd95ab5dd91b747d4496e9130347dc67de
  Session ID Length: 32
  Session ID: b04d243b669080e4415876e17fa96961c93ddab907105dd4d1603d6dd9914c1c
  Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
  Compression Method: null (0)
  Extensions Length: 52
- Extension: pre_shared_key (len=2)
  Type: pre_shared_key (41)
  Length: 2
  - Pre-Shared Key extension
- Extension: key_share (len=36) x25519
  Type: key_share (51)
  Length: 36
  - Key Share extension
- Extension: supported_versions (len=2) TLS 1.3
  Type: supported_versions (43)
  Length: 2
  Supported Version: TLS 1.3 (0x0304)
  [JA3S Fullstring: 771,4865,41-51-43]
  [JA3S: 2b0648ab686ee45e0e7c35fcfb0eea7e]
- TLSv1.3 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
- TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
  Opaque Type: Application Data (23)
  Version: TLS 1.2 (0x0303)
  Length: 72
  Encrypted Application Data: 7d4b1e85de98944d0451181c96247dd4af055bbcaa4cbf41755f32726a36d6f82ff97543842e78cc7f955ef0e591bc875f45

```

- Timestamp: 2024/216 17:38:35.367331023
- Purpose and Significance
  - The ClientHello message is the initial step in the TLS handshake, where the client proposes security parameters (such as supported cipher suites and TLS versions) to the server.
- Key Exchange Message

```

Extensions Length: 52
- Extension: pre_shared_key (len=2)
  Type: pre_shared_key (41)
  Length: 2
  - Pre-Shared Key extension
- Extension: key_share (len=36) x25519
  Type: key_share (51)
  Length: 36
  - Key Share extension
- Extension: supported_versions (len=2) TLS 1.3
  Type: supported_versions (43)
  Length: 2
  Supported Version: TLS 1.3 (0x0304)
  [JA3S Fullstring: 771,4865,41-51-43]
  [JA3S: 2b0648ab686ee45e0e7c35fcfb0eea7e]

```

- Purpose and Significance
  - The Key Exchange message establishes the shared secret key used for encrypting the session. This message completes the key exchange process necessary for secure communication.

# Packet Details

## A. Source and Destination Information

1. ClientHello Packet
  - Source IP: 10.0.2.15
  - Source Port: 49640
  - Destination IP: 142.251.41.36
  - Destination Port: 443
2. ServerHello Packet
  - Source IP: 142.251.41.36
  - Source Port: 443
  - Destination IP: 10.0.2.15
  - Destination Port: 49640
3. Key Exchange Packet
  - In TLSv1.3 the key exchange information is given via the ServerHello packet under extensions.

## B. Encryption Verification

[Screenshot to confirm that packets are encrypted after the handshake.]

```

  TLSv1.3 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
  TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 72
    Encrypted Application Data: 7d4b1e85de98944d0451181c69247dd4af055bbcaa4cbf41755f32726a36d6f82ff97543842e78cc7f955ef0e591bc875f45
    [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: 547
    Encrypted Application Data [truncated]: 6331059c22185bd1c149617325f7e11228fa799f3e2334b44be2027e071a1b35d324877ba39d521131cf563e
    [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: 9f24a29f4c84f19b9f503b8c3b13d64e42aacdb7a833feea4c68160224d347462ae371aa9850a8495d4df598859c01516450
    [Application Data Protocol: Hypertext Transfer Protocol]
  TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Opaque Type: Application Data (23)
    Encrypted Application Data [truncated]: 15 d1 2e 24 67 e0 ce 4f 5f 10 69 6f a2 65 17 03 03 02 23 03 31 05 9c 22 18 5b d1 c1 49 61 73 25 f7 e1 12 28 fa 79 9f 3e 23 34 b4 4b e2 02 7e 07 1a 1b 35 d3 24 87 7b a3 9d 52 11 31 cf 56 3e 49 62 f0 0a 83 ae 7d a8 77 9a 4d 98 fa 0e d1 46 0e 7d ab 51 79 be f1 18 e2 59 e3 d0 e5 09 27 7a e0 f6 00 53 19 d4 6e f2 3c 77 e6 eb 8d ca 08 5c bc d4 cf 34 e7 c5 9a cb 01 9c 2f e6 a0 c5 21 6a 08 c4 1b d2 05 d2 67 1d ef b1 41 ca 24 b9 fa 45 56 15 8b 33 98 43 48 30 c3 7c af 00 48 ee 5e a8 99 3e ad e2 15 df 2b 9b 0a 2d 5a ae 8e c6 7a fe e7 8a d3 dd af 0d bc 43 87 9d 9c ff d0 1a e2 ea f3
    ..$.g..0...io.e..
    ..#c1... "[..Ias%
    ...(.y.> #4.K.~.
    ..$.$.{. .R.1.V>I
    b...].w .M....F.
    }.Qy.... Y....'z.
    ..S..n.< w.....\
    ..4..... /...!j.
    ....g... .A.$..EV
    ..3.CH0. |..H.^..
    >.....+... -Z...Z..
    .....C. ....

```

Bytes 275-821: Encrypted Application Data (tls.app\_data)