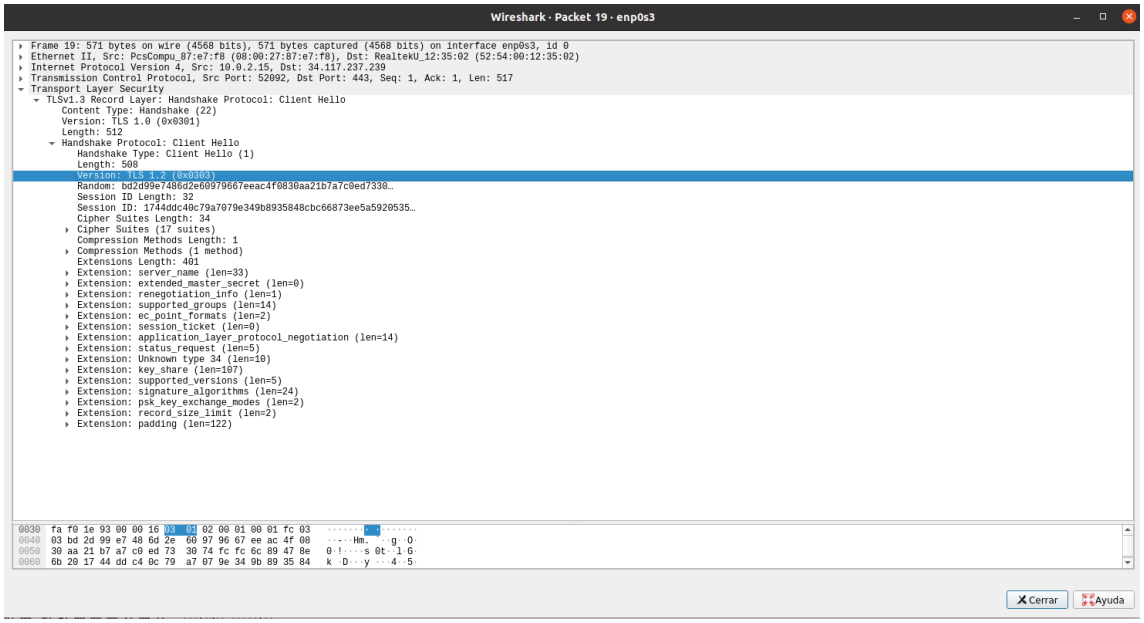
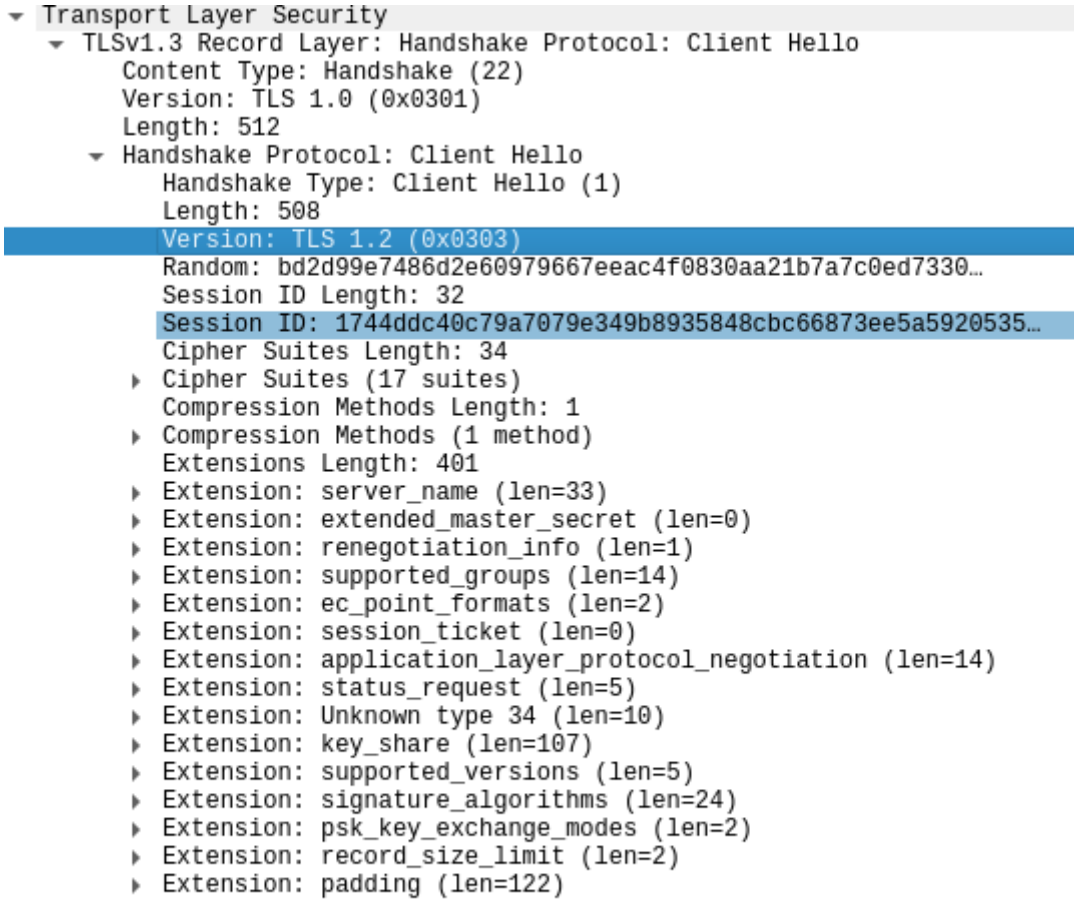
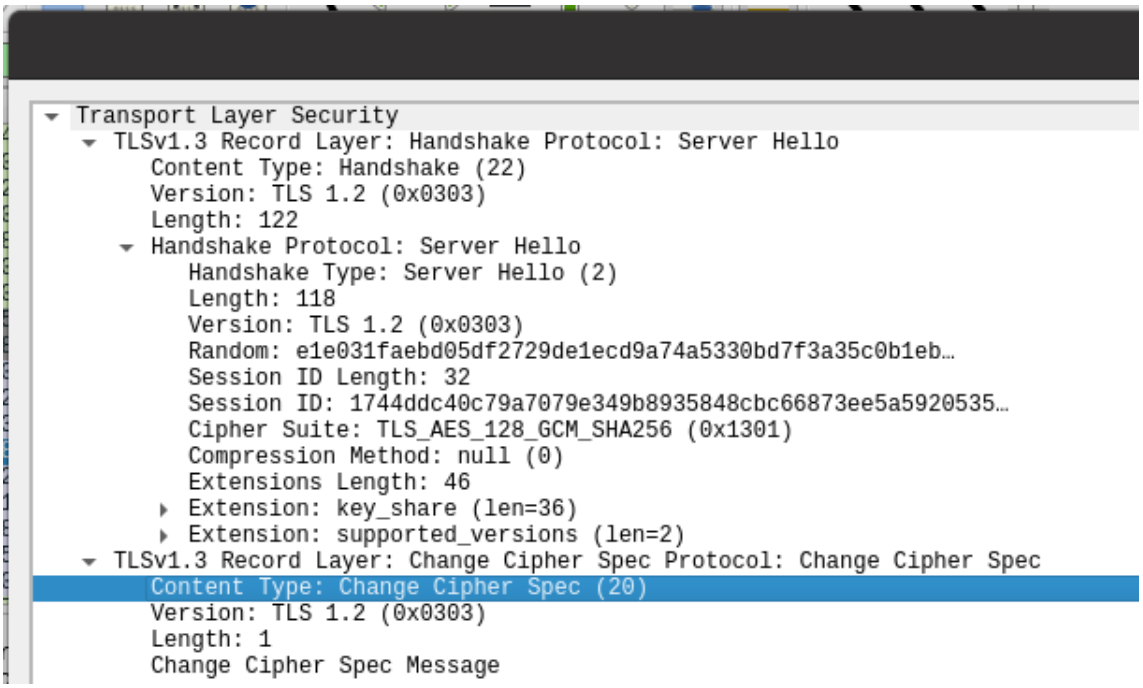
Primero El cliente le envia al server un paquete con un las distintas claves de encriptawcion para que el servidor escoja cual de todas decide usar la captura del paquete de las claves es el es siguiente:

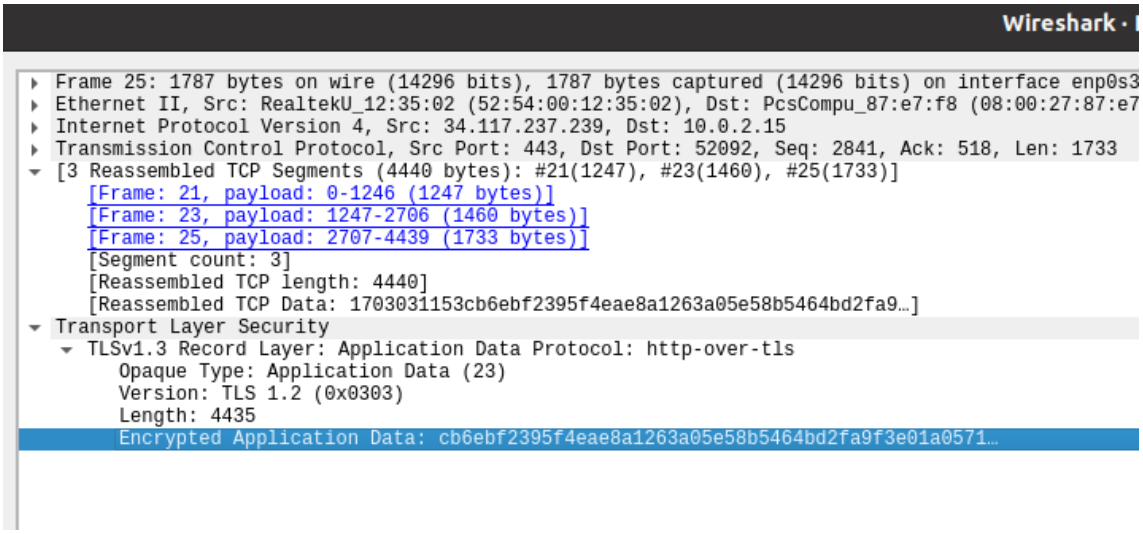




Ahora el server nos responde con La clave que ha elegido, ya que el que decide que cod de cifrado usar es el servidor TLS.



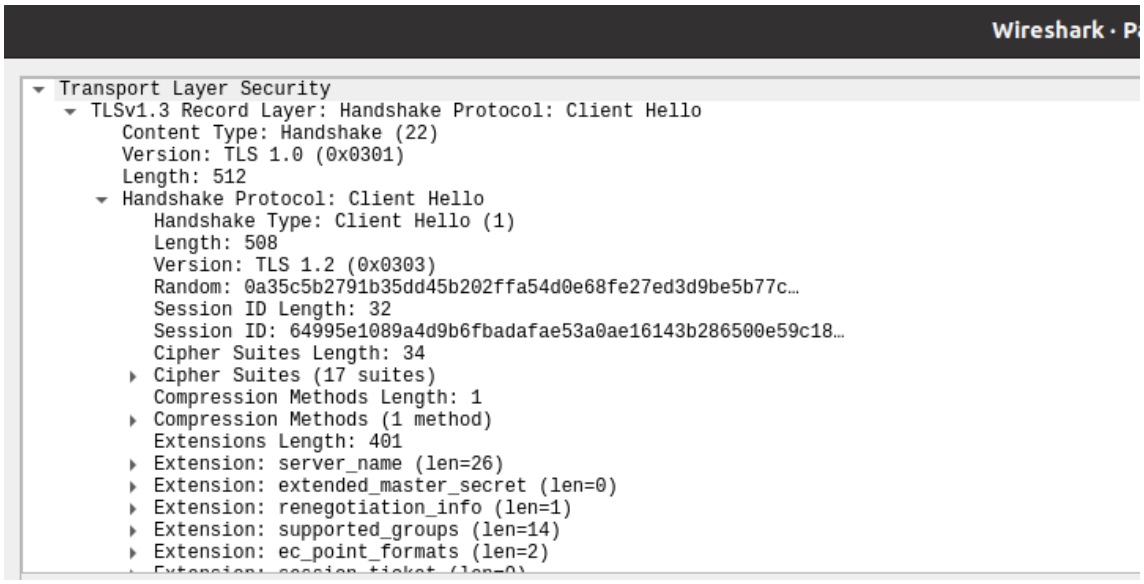
Aquí tienes el cifrado de un paquete con TLS, es ilegible a nos ser que conozcas las claves de cifrado.



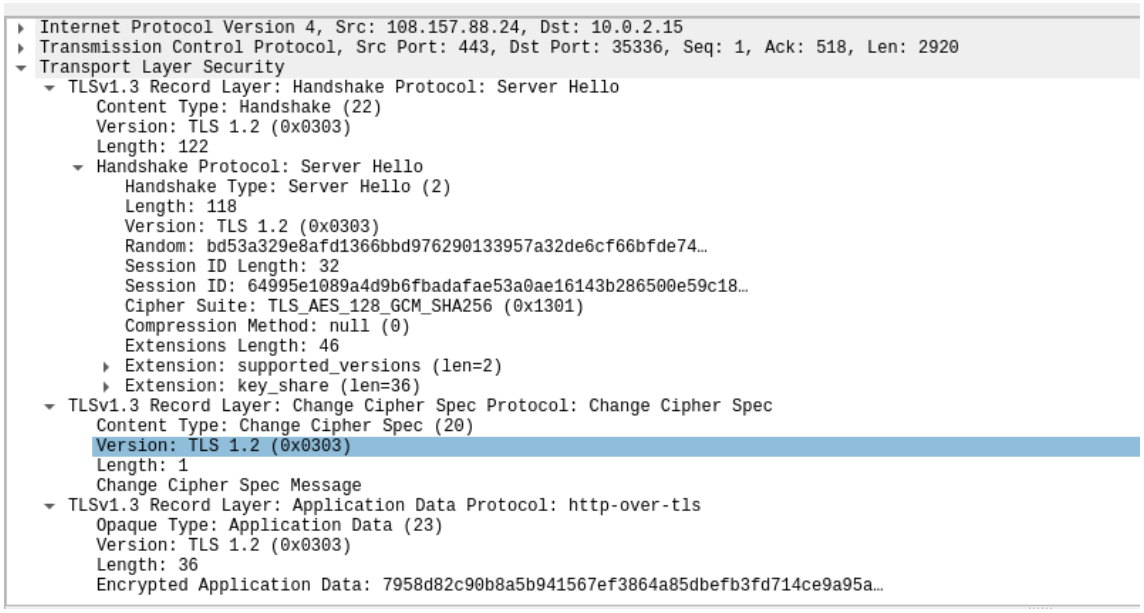
2.Ejercicio que nos has enviado

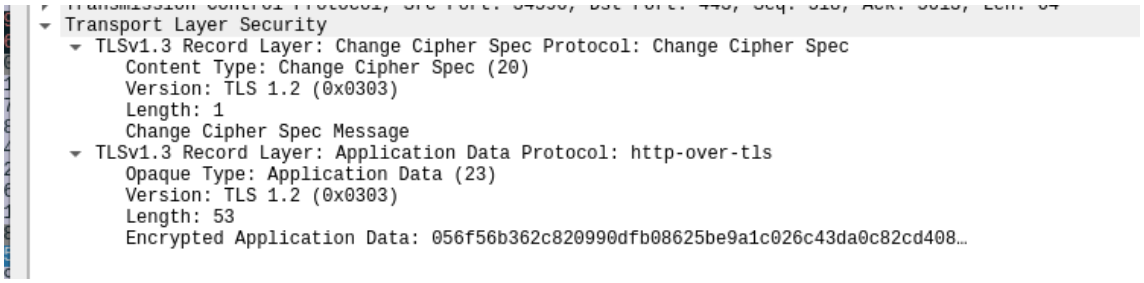
1. EL mundo con firefox

Aquí podemos ver que nosotros le enviamos un paquete por TCP ya que el TLS o el SSL se montan sobre el protocolo orientado a conexión TCP, Aquí vemos el Client Hello el primer paquete que enviamos al server esperando la contestación del mismos con un Server Hello, que es el mensaje en el que el servidor escoje cual va ha ser nuestra clave de cifrado entre todas las claves que hemos mandado como opciones al server.

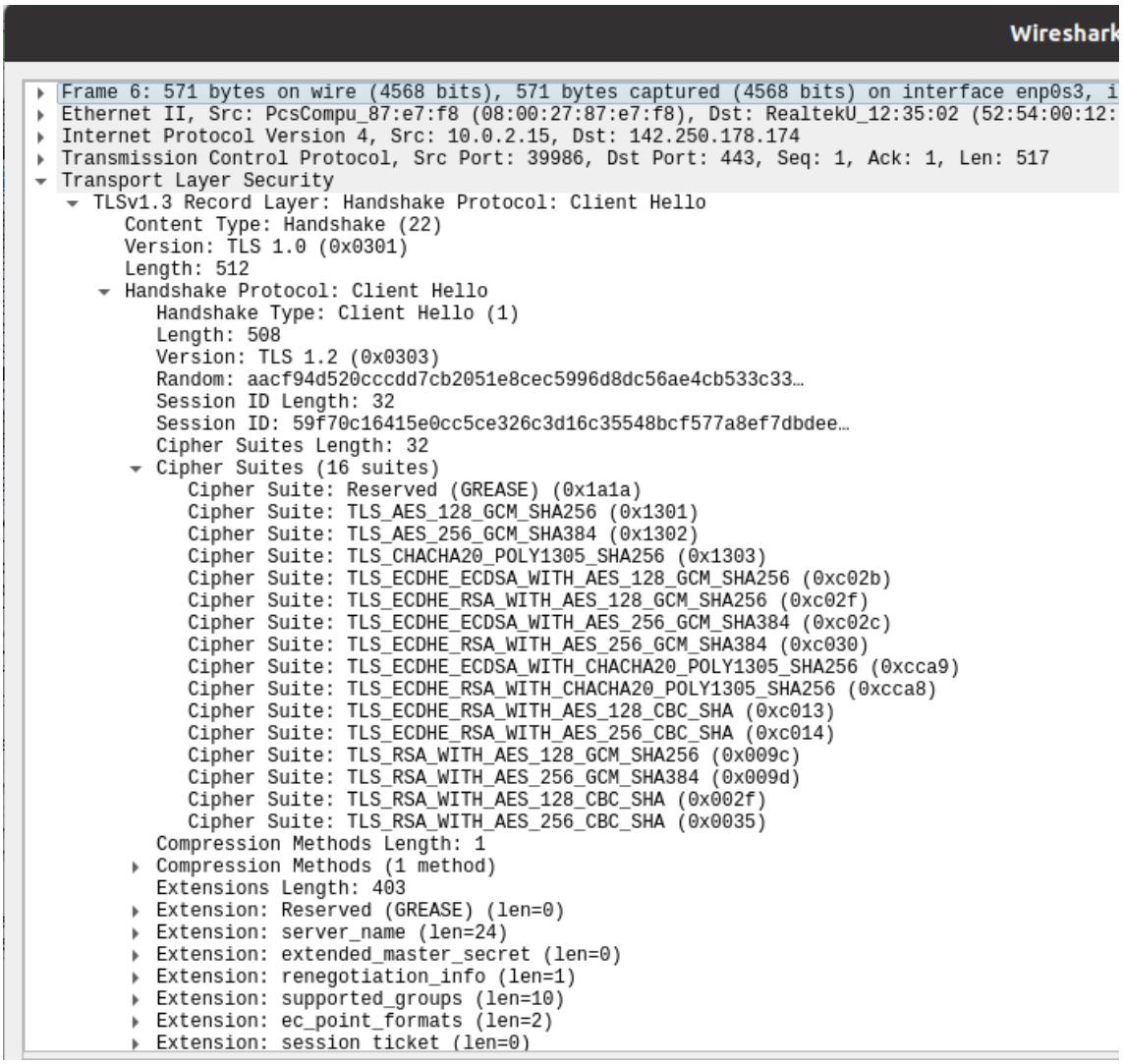


Aquí tenemos el Server Hello, en este paquete el servidor correspondiente nos responde con el método de cifrado escogido.asi convirtiéndose en una clave simétrica para el cifrado publico.

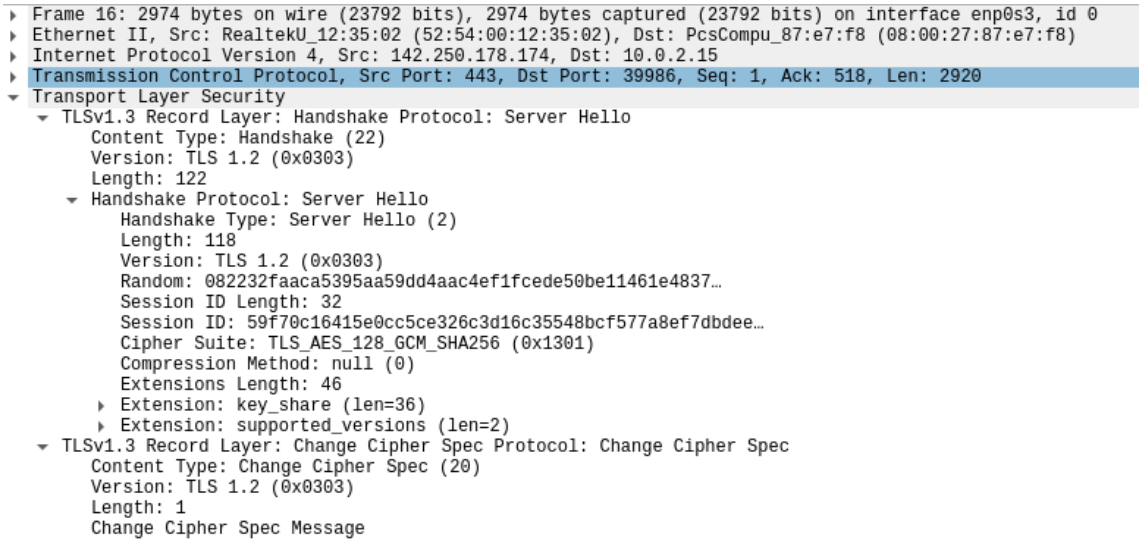




1.2 El mundo con Chrome.

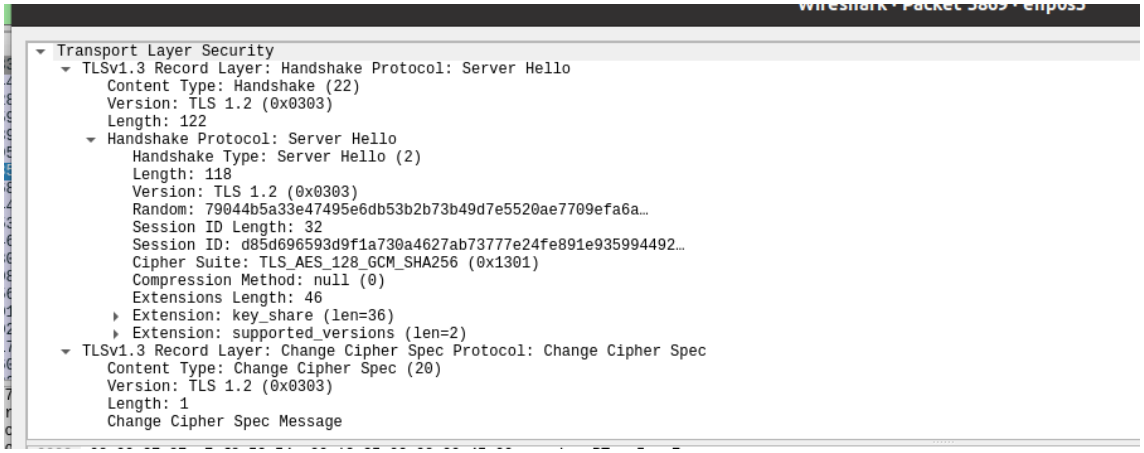


El cipher switch



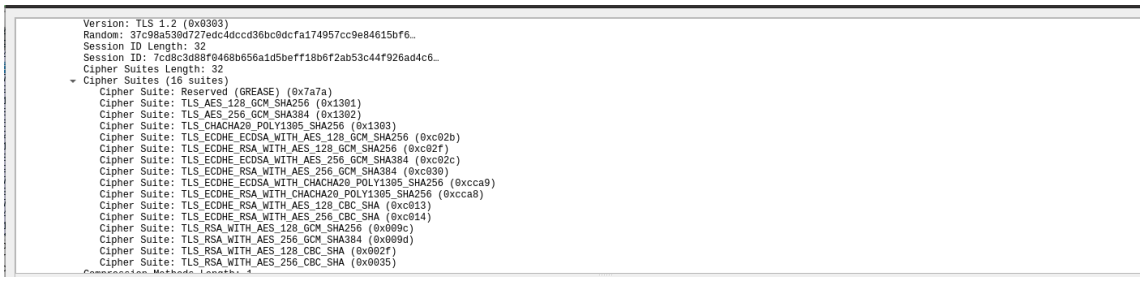
1.3 firefox con Youtube

```
▸ Frame 16: 2974 bytes on wire (23792 bits), 2974 bytes captured (23792 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_87:e7:f8 (08:00:27:87:e7:f8)
▸ Internet Protocol Version 4, Src: 142.250.178.174, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 39986, Seq: 1, Ack: 518, Len: 2920
▾ 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: 082232faaca5395aa59dd4aac4ef1fcede50be11461e4837…
        Session ID Length: 32
        Session ID: 59f70c16415e0cc5ce326c3d16c35548bcf577a8ef7dbdee…
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Compression Method: null (0)
        Extensions Length: 46
      ▸ Extension: key_share (len=36)
      ▸ Extension: supported_versions (len=2)
  ▾ 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
```



```
▾ 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: 79044b5a33e47495e6db53b2b73b49d7e5520ae7709efa6a…
        Session ID Length: 32
        Session ID: d85d696593d9f1a730a4627ab73777e24fe891e935994492…
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Compression Method: null (0)
        Extensions Length: 46
      ▸ Extension: key_share (len=36)
      ▸ Extension: supported_versions (len=2)
  ▾ 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
```

Youtube en Google



```
      Version: TLS 1.2 (0x0303)
      Random: 37c98a530d727edc4dccd36bc0dcfa174957cc9e84615bf6…
      Session ID Length: 32
      Session ID: 7cd8c3d88f0468b656a1d5beff18b6f2ab53c44f926ad4c6…
      Cipher Suites Length: 32
    ▾ Cipher Suites (16 suites)
        Cipher Suite: Reserved (GREASE) (0x7a7a)
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
        Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
        Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
```

```
Wireshark · Packet 19 · en
▸ Frame 19: 2974 bytes on wire (23792 bits), 2974 bytes captured (23792 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_87:e7:f8 (08:00:27:87:e7:f8)
▸ Internet Protocol Version 4, Src: 142.250.200.78, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 33948, Seq: 1, Ack: 518, Len: 2920
▾ 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: fe0810b26328660e765ead09415ce2ee9a7f276e7dd52a57…
        Session ID Length: 32
        Session ID: 7cd8c3d88f0468b656a1d5beff18b6f2ab53c44f926ad4c6…
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Compression Method: null (0)
        Extensions Length: 46
      ▸ Extension: key_share (len=36)
      ▸ Extension: supported_versions (len=2)
  ▾ 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
```

3.Apuntes.

TLS (Trasfer Layer Security) es un protocolo de la capa de aplicación utizado para el envio de paquetes de de forma “Segura ” a través de la red, lo utilizan la mayoría de navegador es el sucesor de SSL o Secure Sockets Layer, se monta en el protocolo TCP de transporte ya que esta orientado a conexión ya que envían varios paquetes previos al envio del primer paquete de datos, los datos suelen ir encriptados con un protocolo ASIMETRICO , usualmente es el RSA, pero no es el único, también podemos encontrar otros tales como ElGAMAL.

TLS/SSL, con protocolos usados para la certificación de identidad entre un servidor y un cliente, asegurando así una comunicación “segura entre ambos ordenadores”.

TLS usa un Cipher Switch que consiste en el envio desde el cliente al servidor con los diferentes cipher switch, dejando el trabajo de elegir el formato al servidor que recibe la información.