

Solucion.pdf



Juandf03



Seguridad de la Información



3º Grado en Ingeniería Informática



Escuela Técnica Superior de Ingeniería Informática
Universidad de Málaga



MÁSTER EN

Inteligencia Artificial & Data Management

MADRID

Formamos
talento para un futuro
Sostenible

saber más





**YA TIENES UN TÍTULO,
AHORA DA EL SALTO AL
MUNDO LABORAL.**

**POTENCIA TU PERFIL
CON LAS TECNOLOGÍAS
MÁS DEMANDADAS.**



Servicio de carreras
para que encuentres
curro en 180 días.

Índice

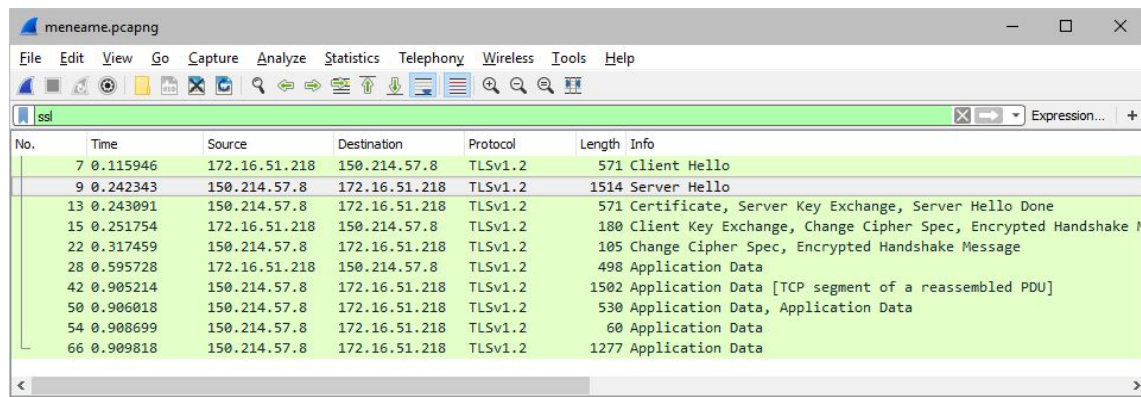
1. Negociación en el protocolo TLS	2
Traza meneame.pcapng.	2
¿Cuándo se procede con el handshake y la fase de conexión?	2
¿Qué versión de TLS se utiliza?	2
En la parte del cliente, ¿en qué trama se puede ver las suites de cifrado que soporta el cliente?	3
¿Qué suite de cifrado acepta finalmente para el proceso de conexión?	4
¿En qué trama se envía el certificado digital del servidor?	5
¿El servidor autentica al cliente? ¿Y el cliente al servidor?	6
Traza tlsv13_test.pcapng.	6
¿Cuándo se procede con el handshake y la fase de conexión?	7
¿Qué versión de TLS se utiliza?	7
En la parte del cliente, ¿en qué trama se puede ver las suites de cifrado que soporta el cliente?	8
¿Qué suite de cifrado acepta finalmente para el proceso de conexión?	9
¿En qué trama se envía el certificado digital del servidor?	10
¿El servidor autentica al cliente? ¿Y el cliente al servidor?	10
2. TLSv1.3 (RFC 8446)	10
Explica con tus palabras cuál es la principal diferencia entre TLS v1.2 ...	10
¿En qué momento aproximado se envía el certificado digital del servidor?	10

1. Negociación en el protocolo TLS

WUOLAH

Traza meneame.pcapng.

A. ¿Cuándo se procede con el handshake y la fase de conexión?

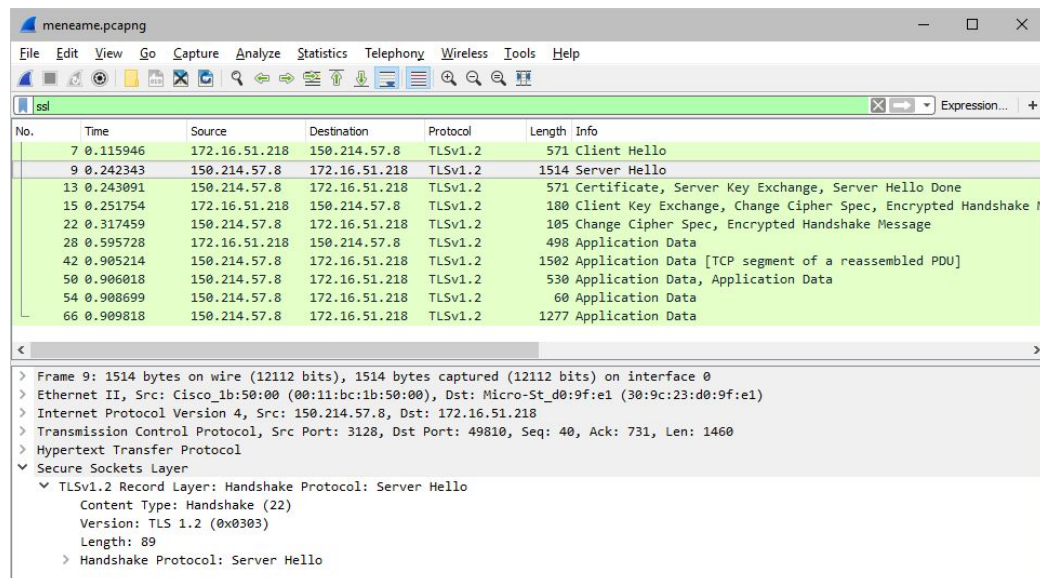


The screenshot shows a Wireshark capture of a TLS session. The packet list on the left shows packets 7 through 66. The packet details pane on the right shows the selected packet (7) as a TLSv1.2 Client Hello. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
7	0.115946	172.16.51.218	150.214.57.8	TLSv1.2	571	Client Hello
9	0.242343	150.214.57.8	172.16.51.218	TLSv1.2	1514	Server Hello
13	0.243091	150.214.57.8	172.16.51.218	TLSv1.2	571	Certificate, Server Key Exchange, Server Hello Done
15	0.251754	172.16.51.218	150.214.57.8	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
22	0.317459	150.214.57.8	172.16.51.218	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
28	0.595728	172.16.51.218	150.214.57.8	TLSv1.2	498	Application Data
42	0.905214	150.214.57.8	172.16.51.218	TLSv1.2	1502	Application Data [TCP segment of a reassembled PDU]
50	0.906018	150.214.57.8	172.16.51.218	TLSv1.2	530	Application Data, Application Data
54	0.908699	150.214.57.8	172.16.51.218	TLSv1.2	60	Application Data
66	0.909818	150.214.57.8	172.16.51.218	TLSv1.2	1277	Application Data

El handshake tiene lugar entre las tramas 7 y 22, mientras que la fase de conexión corresponde a las demás: intercambio de datos (Application Data).

B. ¿Qué versión de TLS se utiliza?



The screenshot shows a Wireshark capture of a TLS session. The packet list on the left shows packets 7 through 66. The packet details pane on the right shows the selected packet (7) as a TLSv1.2 Client Hello. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
7	0.115946	172.16.51.218	150.214.57.8	TLSv1.2	571	Client Hello
9	0.242343	150.214.57.8	172.16.51.218	TLSv1.2	1514	Server Hello
13	0.243091	150.214.57.8	172.16.51.218	TLSv1.2	571	Certificate, Server Key Exchange, Server Hello Done
15	0.251754	172.16.51.218	150.214.57.8	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
22	0.317459	150.214.57.8	172.16.51.218	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
28	0.595728	172.16.51.218	150.214.57.8	TLSv1.2	498	Application Data
42	0.905214	150.214.57.8	172.16.51.218	TLSv1.2	1502	Application Data [TCP segment of a reassembled PDU]
50	0.906018	150.214.57.8	172.16.51.218	TLSv1.2	530	Application Data, Application Data
54	0.908699	150.214.57.8	172.16.51.218	TLSv1.2	60	Application Data
66	0.909818	150.214.57.8	172.16.51.218	TLSv1.2	1277	Application Data

**BEST
LIFE**
EXPERIENCE

Duerme bajo las estrellas

Del Sahara



Marruecos, Aventura en el Sahara

en 5 días

- ♥ Transporte privado en autobús
- ♥ Pasajes de **barco** ida y vuelta
- ♥ Visita a **medina de Fez, Chefchaoun y Assilah**
- ♥ **Guía Marroquí** durante todo el viaje
- ♥ Excursión **en camellos** por las dunas del sahara
- ♥ Atardecer y amanecer en **el desierto**
- ♥ Alojamiento 4 noches, media pensión (**Hotel + Jaima**)
- ♥ **Fotos** del viaje



Seguridad de la Información



Comparte estos flyers en tu clase y consigue más dinero y recompensas



Banco de apuntes de la

WUOLAH

1 Imprime esta hoja

2 Recorta por la mitad

3 Coloca en un lugar visible para que tus compis puedan escanar y acceder a apuntes

4 Llévate dinero por cada descarga de los documentos descargados a través de tu QR



La conexión se inicializa con la versión 1.0, pero en la respuesta del servidor (trama 9) se indica que puede utilizarse la versión 1.2; por tanto, esta última versión es la que se utiliza (a partir de la trama 10).

C. En la parte del cliente, ¿en qué trama se puede ver las suites de cifrado que soporta el cliente?

The screenshot shows the Wireshark interface with the following details:

- Packet List:** Frame 7 (0.115946) is a TLSv1.2 Client Hello from 172.16.51.218 to 150.214.57.8. The length is 571 bytes.
- Packet Details:** The 'Secure Sockets Layer' section is expanded, showing the 'Handshake Protocol: Client Hello' (Length: 508). The 'Cipher Suites' field is highlighted, listing 18 supported cipher suites.
- Packet Bytes:** The raw data of the packet is shown in hexadecimal and ASCII.

The supported cipher suites listed in the 'Cipher Suites' field are:

- TLS_AES_128_GCM_SHA256 (0x1301)
- TLS_CHACHA20_POLY1305_SHA256 (0x1303)
- TLS_AES_256_GCM_SHA384 (0x1302)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc030)
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc032)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc033)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc034)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc035)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc036)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc037)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc038)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc039)
- TLS_RSA_WITH_AES_128_CBC_SHA (0xc03a)
- TLS_RSA_WITH_AES_256_CBC_SHA (0xc03b)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xc03c)

Al abrir la trama 7 (primera trama del cliente), en el campo Secure Sockets Layer.

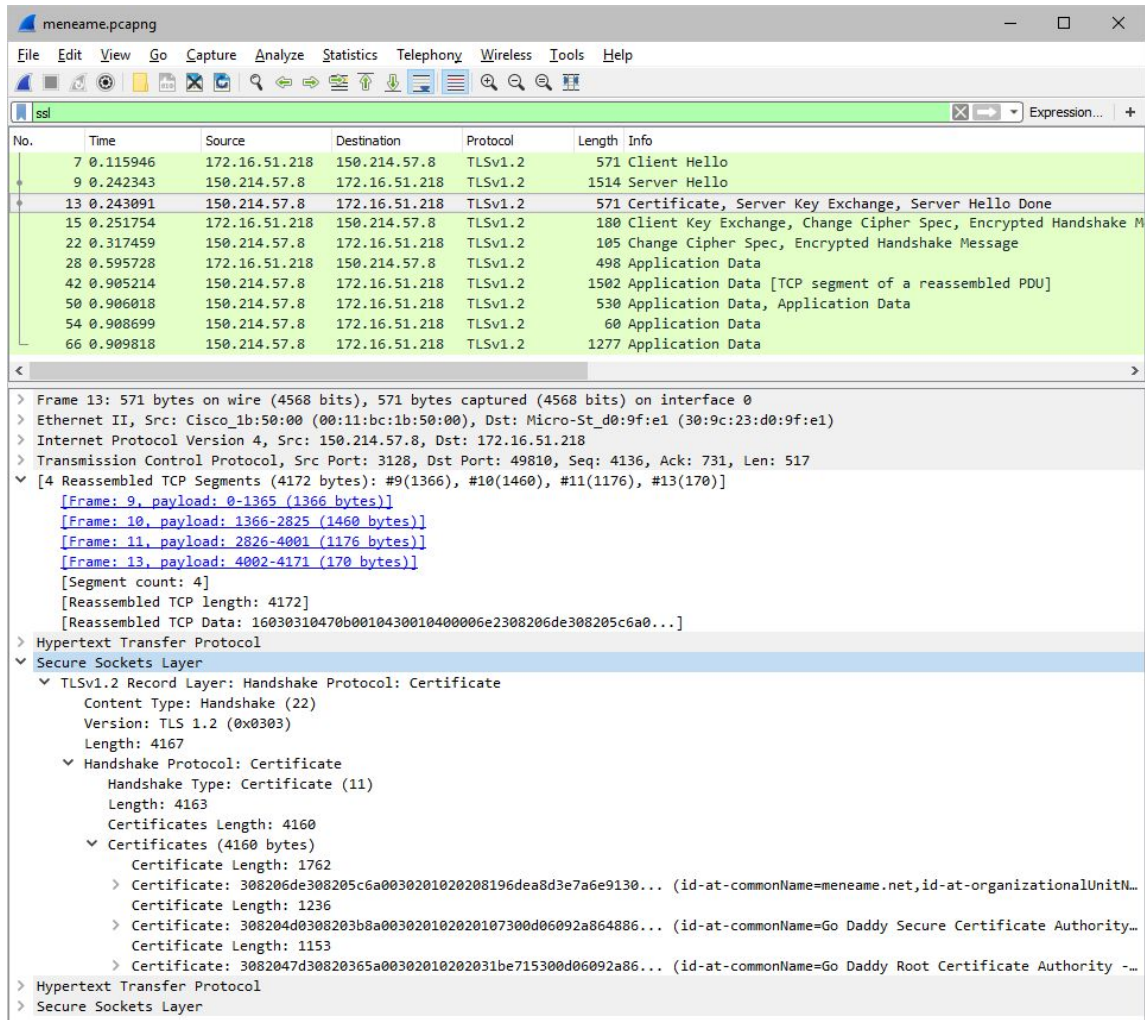
D. ¿Qué suite de cifrado acepta finalmente para el proceso de conexión?

No.	Time	Source	Destination	Protocol	Length	Info
7	0.115946	172.16.51.218	150.214.57.8	TLSv1.2	571	Client Hello
9	0.242343	150.214.57.8	172.16.51.218	TLSv1.2	1514	Server Hello
13	0.243091	150.214.57.8	172.16.51.218	TLSv1.2	571	Certificate, Server Key Exchange, Server Hello Done
15	0.251754	172.16.51.218	150.214.57.8	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake M
22	0.317459	150.214.57.8	172.16.51.218	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
28	0.595728	172.16.51.218	150.214.57.8	TLSv1.2	498	Application Data
42	0.905214	150.214.57.8	172.16.51.218	TLSv1.2	1502	Application Data [TCP segment of a reassembled PDU]
50	0.906018	150.214.57.8	172.16.51.218	TLSv1.2	530	Application Data, Application Data
54	0.908699	150.214.57.8	172.16.51.218	TLSv1.2	60	Application Data
66	0.909818	150.214.57.8	172.16.51.218	TLSv1.2	1277	Application Data

> Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Cisco_1b:50:00 (00:11:bc:1b:50:00), Dst: Micro-St_d0:9f:e1 (30:9c:23:d0:9f:e1)
> Internet Protocol Version 4, Src: 150.214.57.8, Dst: 172.16.51.218
> Transmission Control Protocol, Src Port: 3128, Dst Port: 49810, Seq: 40, Ack: 731, Len: 1460
> Hypertext Transfer Protocol
> Secure Sockets Layer
> TLSv1.2 Record Layer: Handshake Protocol: Server Hello
> Content Type: Handshake (22)
> Version: TLS 1.2 (0x0303)
> Length: 89
> Handshake Protocol: Server Hello
> Handshake Type: Server Hello (2)
> Length: 85
> Version: TLS 1.2 (0x0303)
> Random: 1166f352f5d7eb61cd26d527150e58fbf99332c10ee749ad...
> Session ID Length: 32
> Session ID: e5435c7e52cf43f90684d3d0bc1e34d7453f02b5023c0b41...
> Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
> Compression Method: null (0)
> Extensions Length: 13
> Extension: renegotiation_info (len=1)
> Extension: ec_point_formats (len=4)

La suite final se encuentra especificada en la respuesta del servidor a la trama del apartado anterior, es decir, la trama 9. La respuesta del servidor establece la suite de cifrado TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f).

E. ¿En qué trama se envía el certificado digital del servidor?



No.	Time	Source	Destination	Protocol	Length	Info
7	0.115946	172.16.51.218	150.214.57.8	TLSv1.2	571	Client Hello
9	0.242343	150.214.57.8	172.16.51.218	TLSv1.2	1514	Server Hello
13	0.243091	150.214.57.8	172.16.51.218	TLSv1.2	571	Certificate, Server Key Exchange, Server Hello Done
15	0.251754	172.16.51.218	150.214.57.8	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
22	0.317459	150.214.57.8	172.16.51.218	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
28	0.595728	172.16.51.218	150.214.57.8	TLSv1.2	498	Application Data
42	0.905214	150.214.57.8	172.16.51.218	TLSv1.2	1502	Application Data [TCP segment of a reassembled PDU]
50	0.906018	150.214.57.8	172.16.51.218	TLSv1.2	530	Application Data, Application Data
54	0.908699	150.214.57.8	172.16.51.218	TLSv1.2	60	Application Data
66	0.909818	150.214.57.8	172.16.51.218	TLSv1.2	1277	Application Data

Frame 13: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0
> Ethernet II, Src: Cisco_1b:50:00 (00:11:bc:1b:50:00), Dst: Micro-St_d0:9f:e1 (30:9c:23:d0:9f:e1)
> Internet Protocol Version 4, Src: 150.214.57.8, Dst: 172.16.51.218
> Transmission Control Protocol, Src Port: 3128, Dst Port: 49810, Seq: 4136, Ack: 731, Len: 517
✖ [4 Reassembled TCP Segments (4172 bytes): #9(1366), #10(1460), #11(1176), #13(170)]
[Frame: 9, payload: 0-1365 (1366 bytes)]
[Frame: 10, payload: 1366-2825 (1460 bytes)]
[Frame: 11, payload: 2826-4001 (1176 bytes)]
[Frame: 13, payload: 4002-4171 (170 bytes)]
[Segment count: 4]
[Reassembled TCP length: 4172]
[Reassembled TCP Data: 16030310470b0010430010400006e2308206de308205c6a0...]
> Hypertext Transfer Protocol
✖ Secure Sockets Layer
✖ TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4167
✖ Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 4163
Certificates Length: 4160
✖ Certificates (4160 bytes)
Certificate Length: 1762
> Certificate: 308206de308205c6a0030201020208196dea8d3e7a6e9130... (id-at-commonName=meneame.net,id-at-organizationalUnitN...
Certificate Length: 1236
> Certificate: 308204d0308203b8a003020102020107300d06092a864886... (id-at-commonName=Go Daddy Secure Certificate Authority...
Certificate Length: 1153
> Certificate: 3082047d30820365a00302010202031be715300d06092a86... (id-at-commonName=Go Daddy Root Certificate Authority -...
> Hypertext Transfer Protocol
> Secure Sockets Layer

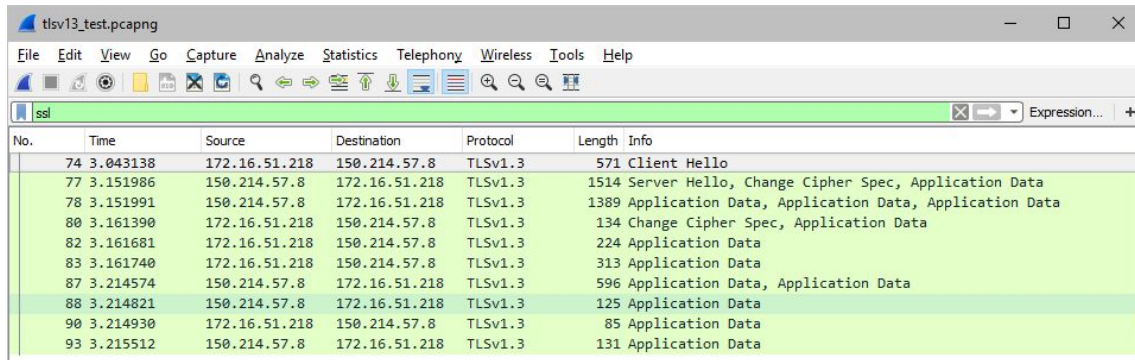
Se envía en la trama 13, una vez este envía su saludo (trama 9).

F. ¿El servidor autentica al cliente? ¿Y el cliente al servidor?

Solo se autentica el servidor, en la trama 13 (apartado anterior).

Traza **tlsv13_test.pcapng**.

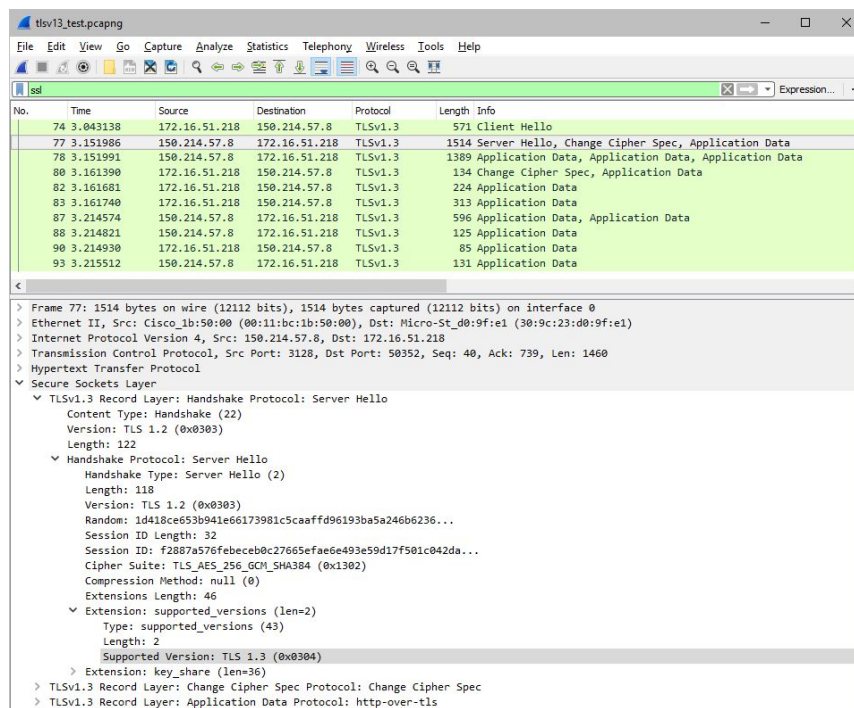
A. ¿Cuándo se procede con el handshake y la fase de conexión?



No.	Time	Source	Destination	Protocol	Length	Info
74	3.043138	172.16.51.218	150.214.57.8	TLSv1.3	571	Client Hello
77	3.151986	150.214.57.8	172.16.51.218	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
78	3.151991	150.214.57.8	172.16.51.218	TLSv1.3	1389	Application Data, Application Data, Application Data
80	3.161390	172.16.51.218	150.214.57.8	TLSv1.3	134	Change Cipher Spec, Application Data
82	3.161681	172.16.51.218	150.214.57.8	TLSv1.3	224	Application Data
83	3.161740	172.16.51.218	150.214.57.8	TLSv1.3	313	Application Data
87	3.214574	150.214.57.8	172.16.51.218	TLSv1.3	596	Application Data, Application Data
88	3.214821	150.214.57.8	172.16.51.218	TLSv1.3	125	Application Data
90	3.214930	172.16.51.218	150.214.57.8	TLSv1.3	85	Application Data
93	3.215512	150.214.57.8	172.16.51.218	TLSv1.3	131	Application Data

El handshake tiene lugar entre las tramas 74 y 80, mientras que la fase de conexión se realiza en las demás: intercambio de datos (Application Data).

B. ¿Qué versión de TLS se utiliza?



Frame 77: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Cisco_Ib:50:00 (00:11:bc:1b:50:00), Dst: Micro-St_d0:9f:e1 (30:9c:23:d0:9f:e1)
> Internet Protocol Version 4, Src: 150.214.57.8, Dst: 172.16.51.218
> Transmission Control Protocol, Src Port: 3128, Dst Port: 50352, Seq: 40, Ack: 739, Len: 1460
> Hypertext Transfer Protocol
> Secure Sockets Layer
 > 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: 1d418ce653b941e66173981c5caaffd96193ba5a246b6236...
 Session ID Length: 32
 Session ID: f2887a57f6becebc27665efae6e493e59d17f501c042da...
 Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
 Compression Method: null (0)
 Extensions Length: 46
 > Extension: supported_versions (len=2)
 Type: supported_versions (43)
 Length: 2
 Supported Version: TLS 1.3 (0x0304)
 > Extension: key_share (len=36)
 > TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 > TLSv1.3 Record Layer: Application Data Protocol: http-over-tls



En la trama 74 (primera trama del cliente), en el campo Secure Sockets Layer.

D. ¿Qué suite de cifrado acepta finalmente para el proceso de conexión?

The image shows a Wireshark capture of a TLS handshake. The top pane displays a list of packets, with packet 77 selected. The bottom pane shows the details of packet 77, specifically the TLSv1.3 Record Layer: Handshake Protocol: Server Hello. The 'Cipher Suite' field is highlighted, showing 'TLS_AES_256_GCM_SHA384 (0x1302)'. The bottom status bar indicates 'Cipher Suite (ssl.handshake.ciphersuite), 2 bytes'.

No.	Time	Source	Destination	Protocol	Length	Info
74	3.043138	172.16.51.218	150.214.57.8	TLSv1.3	571	Client Hello
77	3.151986	150.214.57.8	172.16.51.218	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
78	3.151991	150.214.57.8	172.16.51.218	TLSv1.3	1389	Application Data, Application Data, Application Data
80	3.161390	172.16.51.218	150.214.57.8	TLSv1.3	134	Change Cipher Spec, Application Data
82	3.161681	172.16.51.218	150.214.57.8	TLSv1.3	224	Application Data
83	3.161740	172.16.51.218	150.214.57.8	TLSv1.3	313	Application Data
87	3.214574	150.214.57.8	172.16.51.218	TLSv1.3	596	Application Data, Application Data
88	3.214821	150.214.57.8	172.16.51.218	TLSv1.3	125	Application Data
90	3.214930	172.16.51.218	150.214.57.8	TLSv1.3	85	Application Data
93	3.215512	150.214.57.8	172.16.51.218	TLSv1.3	131	Application Data

Frame 77: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Cisco_1b:50:00 (00:11:bc:1b:50:00), Dst: Micro-St_d0:9f:e1 (30:9c:23:d0:9f:e1)
> Internet Protocol Version 4, Src: 150.214.57.8, Dst: 172.16.51.218
> Transmission Control Protocol, Src Port: 3128, Dst Port: 50352, Seq: 40, Ack: 739, Len: 1460
> Hypertext Transfer Protocol
▼ Secure Sockets Layer
 ▼ 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: 1d418ce653b941e66173981c5caaffd96193ba5a246b6236...
 Session ID Length: 32
 Session ID: f2887a576febeceb0c27665efae6e493e59d17f501c042da...
 Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
 Compression Method: null (0)
 Extensions Length: 46
 > Extension: supported_versions (len=2)
 > Extension: key_share (len=36)
 ▼ 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: http-over-tls
 Opaque Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 32
 Encrypted Application Data: 936a9a0172e3c98e7f66b5e174bcca8e3201258cd44522f6...

0000 2d e4 13 02 00 00 2e 00 2b 00 02 03 04 00 33 00 - - - - - + - - - - - 3
0009 24 00 1d 00 20 32 f7 a4 a8 80 39 05 44 2e db bc \$ - - - 2 - - - 9 D - -
00a0 41 f7 02 1d a7 d8 e3 c7 28 18 1f 79 47 57 24 31 A - - - - - (- - y G W \$ 1
00b0 d7 d9 7a 1f 34 14 03 03 00 01 01 17 03 03 00 20 - - z - 4 - - - - -
00c0 93 6a 9a 01 72 e3 c9 8e 7f 66 b5 e1 74 bc ca 8e j - - - - - f - - t - -
00d0 32 01 25 8c d4 45 22 f6 1e 3a 4e d8 a7 2f 30 23 2 - - % - - E - - - 4 N - - / 0 #

Cipher Suite (ssl.handshake.ciphersuite), 2 bytes | Packets: 182 · Displayed: 10 (5.5%) | Profile: Default

La suite final se encuentra especificada en la respuesta del servidor a la trama del apartado anterior, es decir, la trama 74. La respuesta del servidor establece la suite de cifrado TLS_AES_256_GCM_SHA384 (0x1302).

E. ~~¿En qué trama se envía el certificado digital del servidor?~~

F. ¿El servidor autentica al cliente? ¿Y el cliente al servidor?

Solo se autentica el servidor en la trama 78 (tercera trama).

2. TLSv1.3 (RFC 8446)

Explica con tus palabras cuál es la principal diferencia entre TLS v1.2 y TLS v1.3 desde el punto de vista del handshake inicial.

La principal diferencia es que en la versión 1.3 los campos Server Encrypted Extensions, Server Certificate y Server Handshake Verify son cifrados y enviados en la tercera trama (trama 78) del protocolo como «Application Data, Application Data, Application Data», cosa que no ocurre con la versión 1.2.

¿En qué momento aproximado se envía el certificado digital del servidor?

Se envía en la tercera trama (trama 78).

EL SUBIDÓN

DE SIERRA NEVADA

¡BIENVENIDA COMUNIDAD
UNIVERSITARIA!



**EXPERT
2 DÍAS
CONSECUTIVOS**

84 €

**LONG EXPERT
5 DÍAS
DE LIBRE USO**

180 €

Válido para toda la temporada 2024/25. Producto no reembolsable

