Autor: Sergio Camacho Marín

Fecha: 20/01/2020

Asignatura: Seguridad de la información

Práctica 6

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

  -Meneame:

tls

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

  -Tlsv13_test:

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

- ¿Qué versión de TLS se utiliza?

  -Meneame:

Wireshark · Packet 9 · meneame.pcapng

```
> 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
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 89
```

  -Tlsv13_test:

Wireshark · Packet 77 · tlsv13_test.pcapng

```
    [Proxy-Connect-Port: 443]
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 122
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 118
        Version: TLS 1.2 (0x0303)
        Random: 1d418ce653b941e66173981c5caaffd96193ba5a246b6236…
```

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

  -Meneame: En la trama 7

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

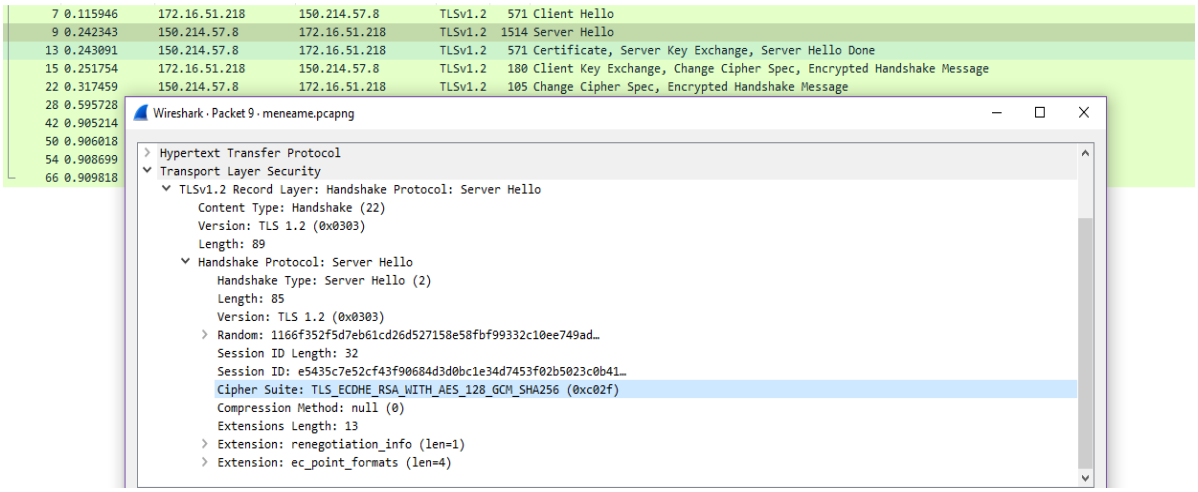
```
    Session ID: a172bb065fad2ff04678e75788109ce5c5d348d9fc62cb70…
    Cipher Suites Length: 36
  ⌄ Cipher Suites (18 suites)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Cipher 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_CHACHA20_POLY1305_SHA256 (0xcca9)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
      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_AES_256_CBC_SHA (0xc00a)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
```

-Tlsv13_test: En la trama 74

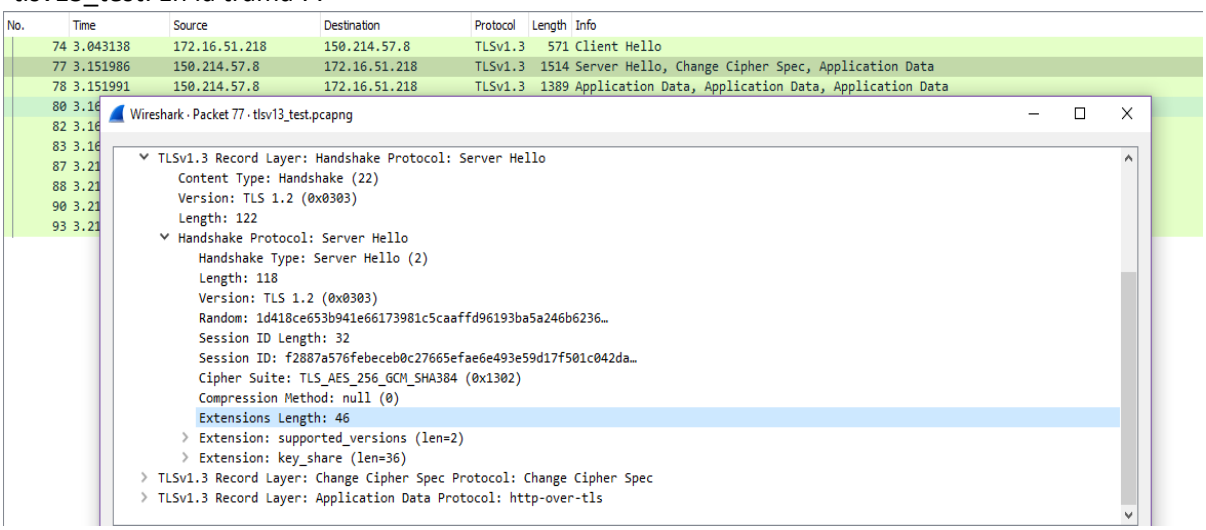
74	3.043138	172.16.51.218	150.214.57.8	TLSv1.3	571	Client Hello
77	3.151986	150.214.57.8	172.16.51.218	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
78	3.151991	150.214.57.8	172.16.51.218	TLSv1.3	1389	Application Data, Application Data, Application Data
80	3.161390	172.16.51.218	150.214.57.8	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

```
    Session ID: f2887a576febeceb0c27665efae6e493e59d17f501c042da…
    Cipher Suites Length: 36
  ⌄ Cipher Suites (18 suites)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      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_CHACHA20_POLY1305_SHA256 (0xcca9)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
      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_AES_256_CBC_SHA (0xc00a)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
```

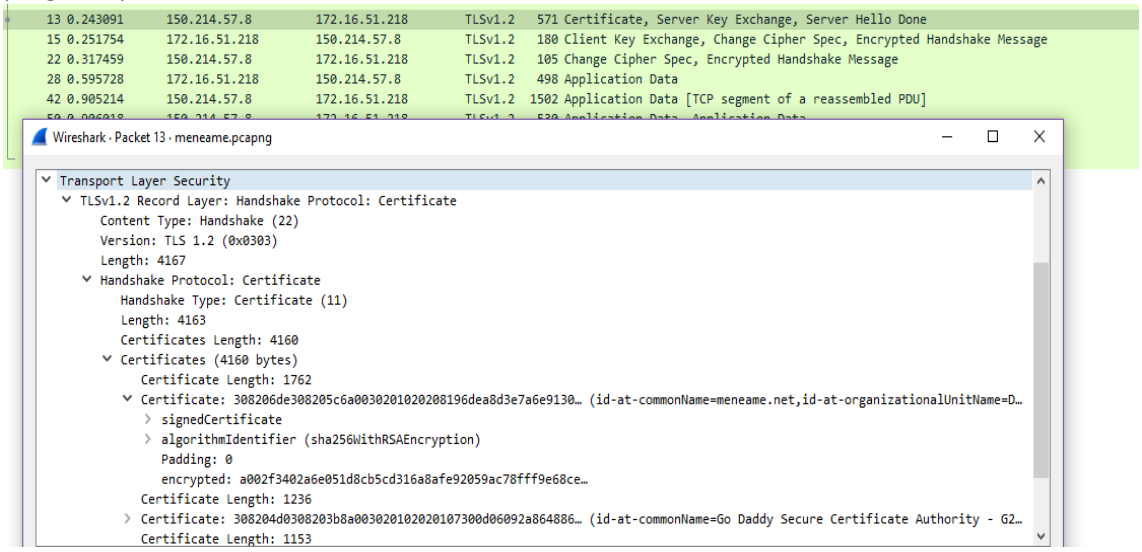
- ¿Qué suite de cifrado se acepta finalmente para el proceso de conexión?
  -Meneame: En la trama 9



-tlsv13_test: En la trama 77



- ¿En qué trama se envía el certificado digital del servidor? NOTA: No responder esta pregunta para la web (b): En la trama 13



- ¿El servidor se autentica al cliente? ¿Y el cliente al servidor?

  -Meneame:

  El servidor se autentica mediante un certificado, cosa que no hace el cliente debido a que no es necesario dentro del protocolo TLS que el cliente se autentique.

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

- Explica con tus palabras cual es la principal diferencia entre TLS v1.2 y TLS v1.3 desde el punto de vista del handshake inicial.
  En TLS v1.3, el único protocolo para el intercambio de claves es Diffie-Hellmann. Y al nivel de cifrado simétrico solo acepta AES-GCM.

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

```
Length: 118
Version: TLS 1.2 (0x0303)
Random: 1d418ce653b941e66173981c5caaffd96193ba5a246b6236…
Session ID Length: 32
Session ID: f2887a576febeceb0c27665efae6e493e59d17f501c042da…
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
```

- ¿En qué momento aproximado se envía el certificado digital del servidor?
  A partir de la trama 78, se envía el certificado cifrado junto con extensiones cifradas, la verificación del cifrado y la finalización del handshake

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