PRÁCTICA 7: TLS

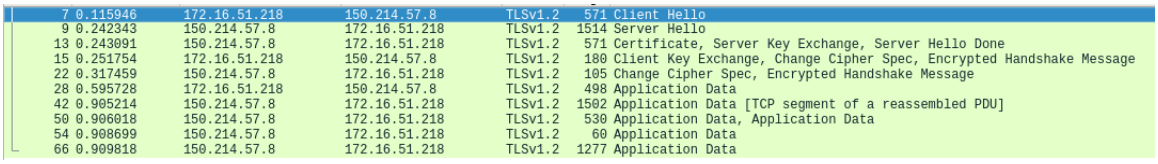
Cristina Díaz García

Enero 2019

Índice

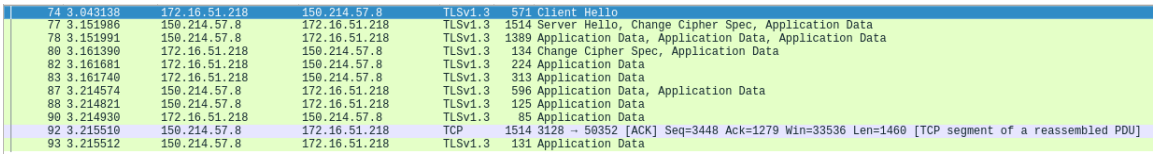
1. Ejercicio 1

https://www.meneame.net



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

https://tls13.pinterjann.is/



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
92	3.215510	150.214.57.8	172.16.51.218	TCP	1514 3128 → 50352 [ACK] Seq=3448 Ack=1279 Win=33536 Len=1460 [TCP segment of a reassembled PDU]
93	3.215512	150.214.57.8	172.16.51.218	TLSv1.3	131 Application Data

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

  En ambos casos se inicia con el Client Hello que se envía al abrir la página.

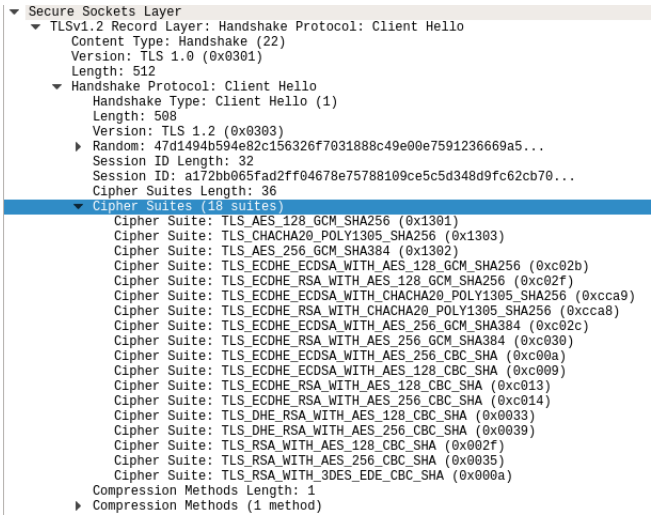
  En el caso de *https://www.meneame.net*, esto ocurre en el séptimo paquete. Con *https://tls13.pinterjann.is/*, es en el número 74.

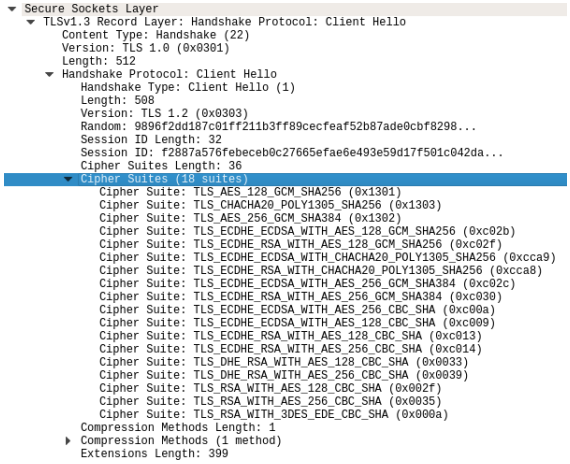
- ¿Qué versión de TLS se utiliza?

  En el caso de *https://www.meneame.net*, se usa la versión 1.2 de TLS. Por otra parte, *https://tls13.pinterjann.is/* usa la 1.3.

- En la parte del cliente, ¿en qué trama se puede ver la suite de cifrado? ¿Cómo se interpreta la suite de cifrado?

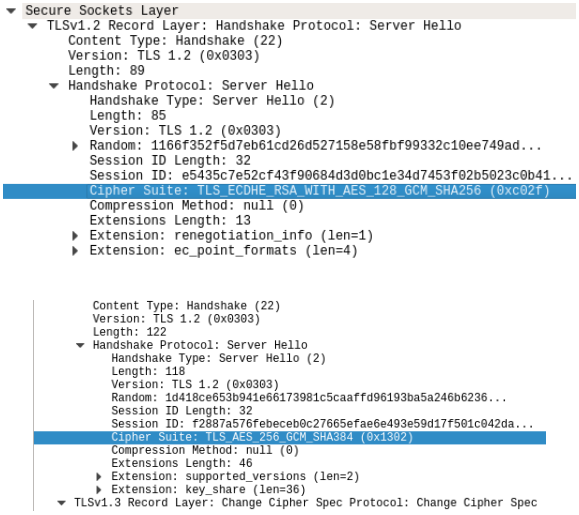
  En la capa de Secure Sockets Layer (SSL).





Se interpreta como los protocolos y algoritmos que se usan para proteger la información: se usa TLS, opcionalmente un algoritmo de intercambio de clave (RSA, Diffie-Hellman efímero, curvas elípticas...), el algoritmo de cifrado y los modos en los que trabaja (AES128, 3DES_CBC, CHACHA20...) y finalmente la función que usa para el Hash (SHA256, SHA384...)

- ¿Qué suite de cifrado se acepta finalmente para el proceso de conexión?



En el caso de *https://www.meneame.net*, finalmente se usa TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. Por otra parte, *https://tls13.pinterjann.is/* usa TLS_AES_256_GCM_SHA384.

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

  En la número 13.

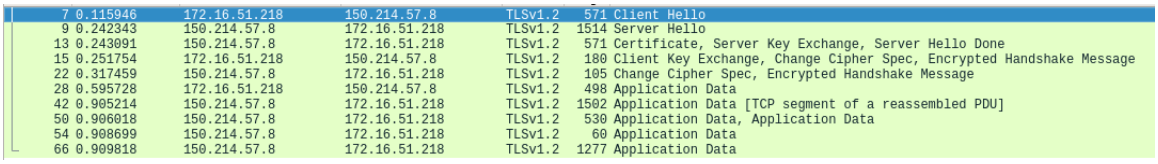
- ¿El servidor se autentica al cliente? ¿Y el cliente al servidor?

  El servidor se autentica mediante el paso del certificado digital (apartado anterior). El cliente en ningún momento se autentica.

2. Ejercicio 2

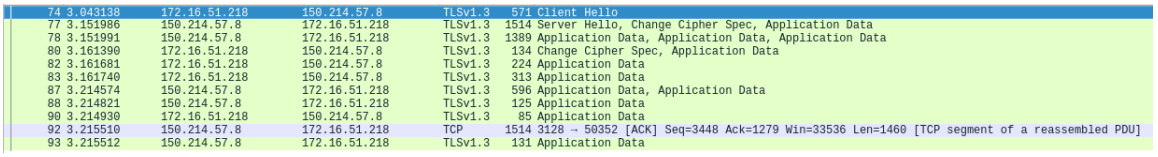
- Explica con tus palabras cual es la principal diferencia entre TLS v1.2 y TLS v1.3 desde el punto de vista del handshake inicial.

  TLS v1.2



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

  TLS v1.3



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
92	3.215510	150.214.57.8	172.16.51.218	TCP	1514 3128 → 50352 [ACK] Seq=3448 Ack=1279 Win=33536 Len=1460 [TCP segment of a reassembled PDU]
93	3.215512	150.214.57.8	172.16.51.218	TLSv1.3	131 Application Data

  Como se puede ver, en el primer mensaje del servidor, *Server Hello*, se envía también la activación de la suite (*Change Cipher Spec*), por lo que el inicio de las comuncaciones se hace más rápidamente.

  También se intercambian las claves al inicio de la sesión, lo que permite empezar a cifrar desde el principio, que lleva también a una mayor rapidez y seguridad de la comunicaicón.

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

  En el mismo momento en el que se pasa el *Server Hello*. Va cifrado porque las claves ya se habían intercambiado previamente.