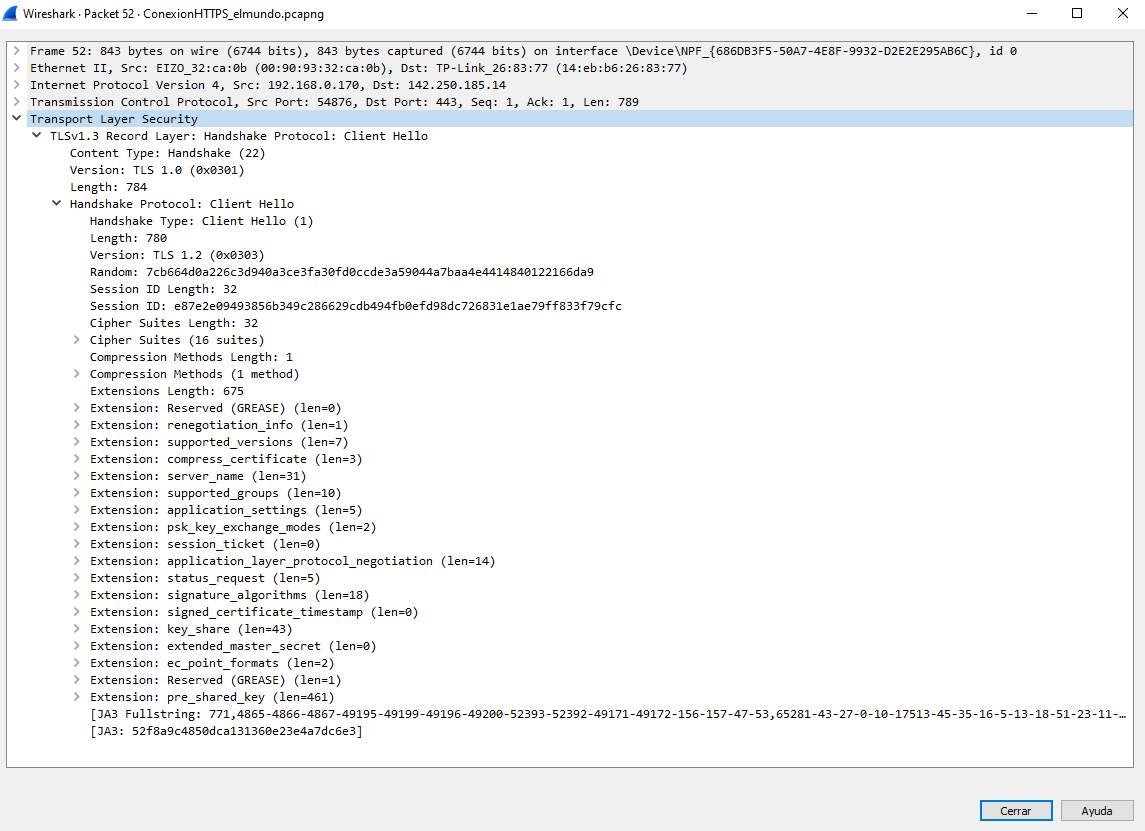
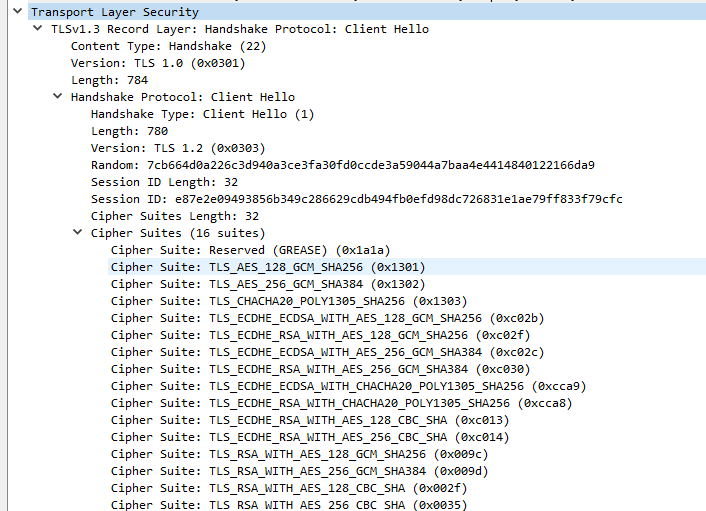
**NOMBRE:** **TURNO 1**

**1-Con la traza de “**[ConexionHTTPS\_elmundo.pcapng”](https://aulavirtual33.educa.madrid.org/ies.laarboleda.alcorcon/pluginfile.php/29598/question/questiontext/10054/2/61434/ConexionHTTPS_elmundo.pcapng)

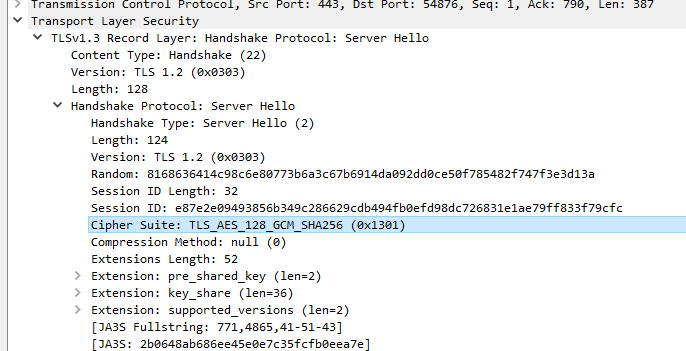
1.1-Localiza los "cipher suites" que el cliente le ofrece, mostrando un pantallazo (1 punto).

En el paquete de client hello tenemos los cypher suit que ofrece el cliente al servidor.



1.2-Localiza la "cipher suit" que usa elmundo.es para realizar los cifrados, mostrando un pantallazo (1 punto).

Para saber el cypher suit que van ha utilizar tenemos que mirar el Server Hello , en el podemos ver la cypher suit que van ha utilizar para la conexión entre ellos



1-Nombra y explica los pasos de [DHCP](https://aulavirtual33.educa.madrid.org/ies.laarboleda.alcorcon/mod/assign/view.php?id=27051) (1 punto)

1. Discover, en este el equipo que necesita de una IP de DHCP hace un discover, buscando al servidor DHCP para asi que este le conteste con la información relevante a la configuración de red.

2.DHCP OFFER, en este el servidor envia una configuración IP al cliente, ofreciendole la misma, en ella podemos encontrar tanto la IP, el DNS, la puerta de enlace, etc.

3.Request, el equipo que recibe la oferta del servidor con la ocnfiguracion contesta con un Request aceptando asi la configuracion enviada por el DHCP.

4. Por ultimo el DHCP envía un ACK comunicandole al cliente que ya ha recibido la informacion de que se queda con la IP y le configuracion que le ha enviado anteriormente.

2-Explica el protocolo OSPF. (1 punto)

OSPF es un ptotocolo orientado a conexión, en el que calcula la distancia que hay entre las redes escojiendo la ruta mas corta para el paquete que enviemos.

3-Explica BPSK, QAM-16 y QAM-64 (1 punto)

QAM-16 y QAM-64 So modulaciones digitales que permiten mas frecuencias y amplitudes, siendo menos tolerantes al ruido ya que cunado hay un poco de ruido el dispositivo receptor puede no tener suficientes medios para que le llegue la conexión, ademas QAM-16 tiene 4 puntos por cuadrante y QAM-64 tiene 16 ppuntos

4-Nombra las frecuencias utilizadas en 4G (1 punto)

En el 4G se urliza la frecuencia 2.4, esta tiene un rango de 2,414-2,489, esta tiene la caracteristica que atraviesa objetos, es tolerante al ruido por lo que es mas lenta.

5-¿Qué es Diffie-Hellman? (1 punto)

Dififie-Hellman es un cifrado de clave privada o simetrica, el cual es utilizado en diversos protocolos para la creacion de una clave simetrica a traves de dos claves publicas provenientes de dos equipos que no se han comunicado nunca a traves de la red y para ello ultiliza diversos calculos.

6-¿Qué es SHA-256? (1 punto)

El Sha 256 es la evolución del hash y es una de las vesiones mas utilizadas de SHA, fue desarrolado por la NSA, para hacer de logitud fija el HASH, es ultizado en las conexiones seguras a traves de internet.

7-¿Qué es RSA? (1 punto)

Es un cifrado de clave publica o asimetrica en el cual se conforma por diversos numeros y letras provenientes de diversos calculos, en el se ultiliza los certificados digitales permitiendo al certificacion de tu identidad a traves de esas claves, utilizando tu clave pública pueden ver que eres tu, y no otro. Es utilizado en las conexiondes seguras a internet

8-Con la red 192.168.1.128/24 hacemos 3 subredes. ¿Cuál es la primera IP válida de la última subred? (1 punto)

192.168.1.128/24

255.255.255.00000000

2^2=4

La mascara entonces pasa a ser:

255.255.255.11000000

por lo tanto tenemos 2^6-2 hosts por subred

2^6-2=62 hosts disponibles por subred

|  |  |  |  |
| --- | --- | --- | --- |
| Direccion de Red | Primera IP valida | Ultima IP valida | Broadcast |
| 192.168.1.128 | 192.168.1.129 | 192.168.1.190 | 192.168.1.191 |
| 192.168.1.192 | 192.168.1.193 | 192.168.1.254 | 192.168.1.255 |
| 192.168.1. | 192.168.1. | 192.168.1. | 192.168.1. |

255,255,255,11100000

|  |  |  |  |
| --- | --- | --- | --- |
| Direccion de Red | Primera IP valida | Ultima IP valida | Broadcast |
| 192.168.1.128 | 192.168.1.129 | 192.168.1.158 | 192.168.1.159 |
| 192.168.1.160 | 192.168.1.161 | 192.168.1.190 | 192.168.1.191 |
| 192.168.1.192 | 192.168.1.193 | 192.168.1.221 | 192.168.1.222 |