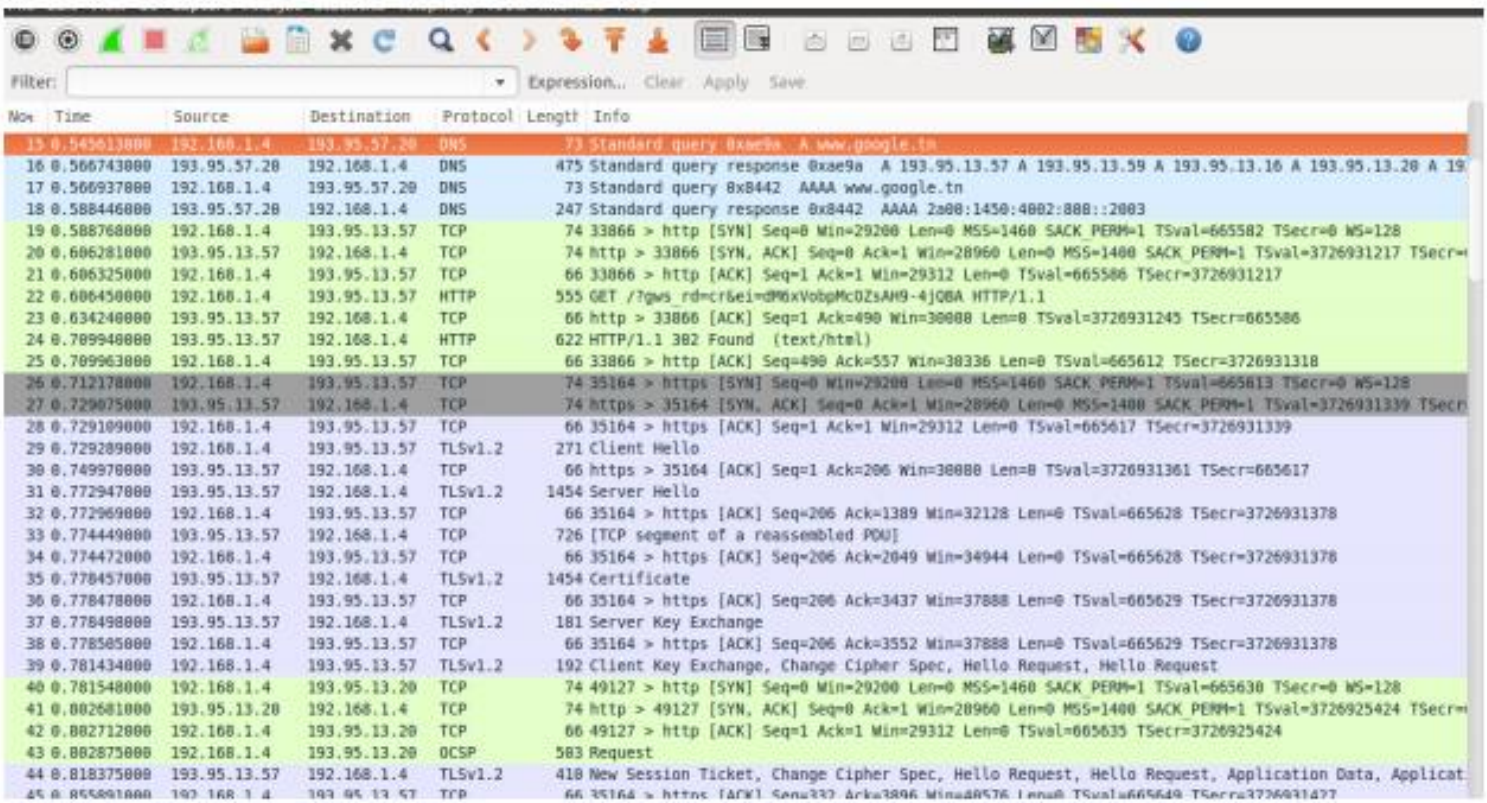
Exercice : SSL/TLS

HTTPS (HTTP sur SSL/TLS) permet sécuriser les communications entre un serveur Web et un navigateur. La figure ci-dessous présente des paquets capturés chez un client web (navigateur) qui accède au site www.google.tn (la première colonne donne les numéros des paquets capturés).

Le navigateur calcule une clé secrète K (master key) et l'envoi au serveur dans un canal sécurisé.



No.	Time	Source	Destination	Protocol	Length	Info
15	0.545613000	192.168.1.4	193.95.57.20	DNS	73	Standard query 0xae9a A www.google.tn
16	0.566743000	193.95.57.20	192.168.1.4	DNS	475	Standard query response 0xae9a A 193.95.13.57 A 193.95.13.59 A 193.95.13.16 A 193.95.13.20 A 19
17	0.566937000	192.168.1.4	193.95.57.20	DNS	73	Standard query 0x8442 AAAA www.google.tn
18	0.588446000	193.95.57.20	192.168.1.4	DNS	247	Standard query response 0x8442 AAAA 2a00:1450:4002:808::2003
19	0.588768000	192.168.1.4	193.95.13.57	TCP	74	33866 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=665582 TSecr=0 WS=128
20	0.606281000	193.95.13.57	192.168.1.4	TCP	74	http > 33866 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1400 SACK_PERM=1 TSval=3726931217 TSecr=
21	0.606325000	192.168.1.4	193.95.13.57	TCP	66	33866 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=665586 TSecr=3726931217
22	0.606450000	192.168.1.4	193.95.13.57	HTTP	555	GET /?gws_rd=cr&ei=dM6xVobpMcOZsAH9-4jQBA HTTP/1.1
23	0.634240000	193.95.13.57	192.168.1.4	TCP	66	http > 33866 [ACK] Seq=1 Ack=490 Win=30080 Len=0 TSval=3726931245 TSecr=665586
24	0.709940000	193.95.13.57	192.168.1.4	HTTP	622	HTTP/1.1 302 Found (text/html)
25	0.709963000	192.168.1.4	193.95.13.57	TCP	66	33866 > http [ACK] Seq=490 Ack=557 Win=30336 Len=0 TSval=665612 TSecr=3726931318
26	0.712178000	192.168.1.4	193.95.13.57	TCP	74	35164 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=665613 TSecr=0 WS=128
27	0.729075000	193.95.13.57	192.168.1.4	TCP	74	https > 35164 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1400 SACK_PERM=1 TSval=3726931339 TSecr
28	0.729109000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=665617 TSecr=3726931339
29	0.729289000	192.168.1.4	193.95.13.57	TLSv1.2	271	Client Hello
30	0.749970000	193.95.13.57	192.168.1.4	TCP	66	https > 35164 [ACK] Seq=1 Ack=206 Win=30080 Len=0 TSval=3726931361 TSecr=665617
31	0.772947000	193.95.13.57	192.168.1.4	TLSv1.2	1454	Server Hello
32	0.772969000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=206 Ack=1389 Win=32128 Len=0 TSval=665628 TSecr=3726931378
33	0.774449000	193.95.13.57	192.168.1.4	TCP	726	[TCP segment of a reassembled PDU]
34	0.774472000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=206 Ack=2049 Win=34944 Len=0 TSval=665628 TSecr=3726931378
35	0.778457000	193.95.13.57	192.168.1.4	TLSv1.2	1454	Certificate
36	0.778478000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=206 Ack=3437 Win=37888 Len=0 TSval=665629 TSecr=3726931378
37	0.778498000	193.95.13.57	192.168.1.4	TLSv1.2	181	Server Key Exchange
38	0.778585000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=206 Ack=3552 Win=37888 Len=0 TSval=665629 TSecr=3726931378
39	0.781434000	192.168.1.4	193.95.13.57	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
40	0.781548000	192.168.1.4	193.95.13.20	TCP	74	49127 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=665630 TSecr=0 WS=128
41	0.802681000	193.95.13.20	192.168.1.4	TCP	74	http > 49127 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1400 SACK_PERM=1 TSval=3726925424 TSecr=
42	0.802712000	192.168.1.4	193.95.13.20	TCP	66	49127 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=665635 TSecr=3726925424
43	0.802875000	192.168.1.4	193.95.13.20	OCSP	583	Request
44	0.818375000	193.95.13.57	192.168.1.4	TLSv1.2	410	New Session Ticket, Change Cipher Spec, Hello Request, Hello Request, Application Data, Applicat

1. Que représentent les paquets 15, 16, 17 et 18 ?

2. Que représentent les paquets 19, 20 et 21 ?

3. Que représentent les paquets 26, 27 et 28 ?

4. Sur son navigateur, l'utilisateur a tapé l'adresse http://www.google.tn ou https://www.google.tn ? Expliquer.

5. Préciser, à l'aide d'un schéma, les différents messages échangés pour établir une connexion sécurisée entre le client et www.google.tn

6. Pourquoi on n'utilise pas directement le chiffrement asymétrique pour sécuriser les communications HTTPS ? Donner deux raisons.

7. La clé K (Premaster key) est-elle envoyée au serveur dans un canal sécurisé et authentifié ? expliquer ?

8. Pourquoi certains anciens navigateurs web ne peuvent pas utiliser HTTPS ?

9. À votre avis, la clé privée du serveur web est stockée en clair ou protégé par mot de passe ? Expliquer.

10. Il est possible d'utiliser un certificat client stocké sur le navigateur pour l'échange HTTPS. Donnez un avantage et un inconvénient de procéder ainsi.