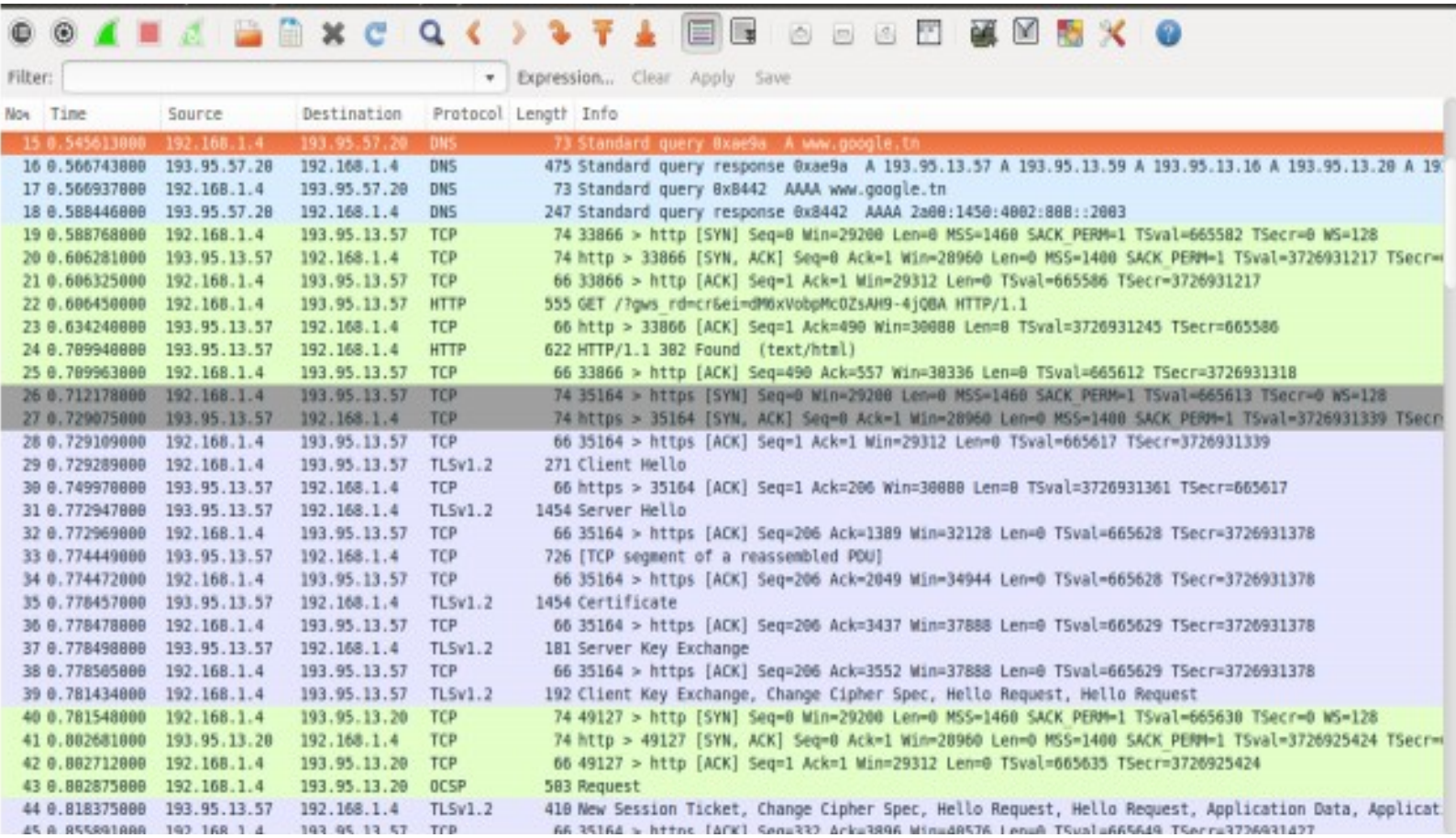
Exercice: SSL/TLS

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.



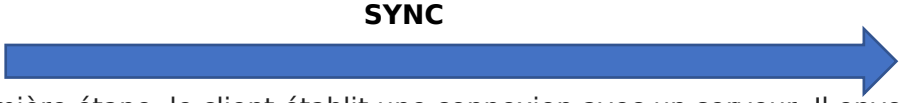
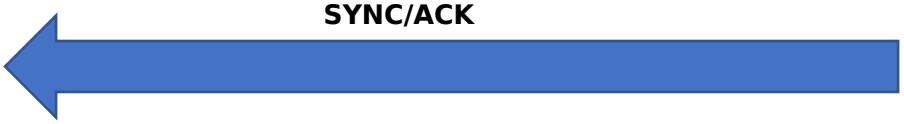
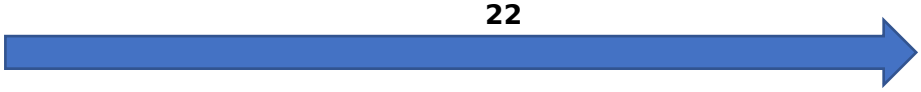
1. **Que représentent les paquets 15, 16, 17 et 18 ?**
   La requête et réponse auprès du serveur DNS. Demande d'établissement de connexion du client auprès du serveur DNS qui transmet cette requête au serveur du site www.google.tn

2. **Que représentent les paquets 19, 20 et 21 ?**
   Établissement de la poignée de main en 3 étapes (3 way handshake), établissement de la connexion TCP

3. **Que représentent les paquets 26, 27 et 28 ?**
   Établissement de connexion sécurisée

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

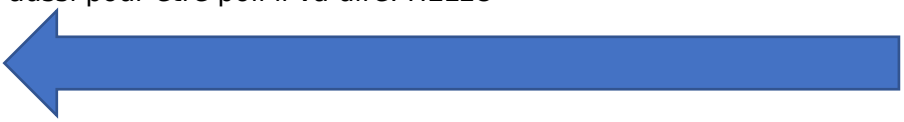
5. Préciser, à l'aide d'un schéma, les différents messages échangés pour établir une connexion sécurisée entre le client et www.google.tn !

CLIENT 192.168.1.4		SERVEUR 193.95.13.57
15-16-17-18 **Requête DNS** **Recherche de la destination à travers le serveur DNS**		
19-20-21 **Établissement de la connexion TCP** **3 étapes**		
SYNC  Dans la première étape, le client établit une connexion avec un serveur. Il envoie un segment avec SYN et informe le serveur qu'il veut commencer une communication, et quel doit être son numéro de séquence.		
SYNC/ACK  Dans cette étape, le serveur répond à la demande du client avec le signal SYN-ACK défini. ACK vous aide à signifier la réponse du segment qui est reçu et SYN signifie quel numéro de séquence il doit pouvoir commencer avec les segments.		
ACK  Dans cette dernière étape, le client accuse réception de la réponse du serveur et ils créent tous les deux une connexion stable pour commencer le processus de transfert de données.		
ESTABLISHED, **On peut maintenant commencer l'initialisation d'une connexion SSL**		
INITIALISATION DE LA CONNEXION SSL		
22  **Le client (192.168.1.4): envoie un paquet qui comporte:** le protocole SSL qu'il supporte (Version). Un session ID Liste des modes de chiffrage (RSA-MD5) qu'il va supporter. Et étant poli il ne va oublier de dire HELLO		

23 -24

Le serveur (193.93.15.57): analyse les informations que le client à envoyé

Il vérifie la version SSL
Génère un session ID
Sélectionne le mode de chiffrage.
Il envoie le certificat (la clé publique).
Et lui aussi pour être poli il va dire: HELLO



25

Le client (192.168.1.4): reçoit le certificat et le valide, après vérification de la validité et l'authenticité auprès de l'autorité certifiante (vérifier la signature présente à la fin du certificat). Il a une liste de certificats pré-utilisés de différentes autorités.

Sur Google chrome: paramètres avancées , Security, gérer les certificats, autorités de certifications intermédiaires) =

D'où l'importance d'avoir un navigateur à jour !

A savoir: à chaque fois qu'on reçoit le message qui nous demande d'accepter un certificat = le certificat sera ajouté à cette liste.

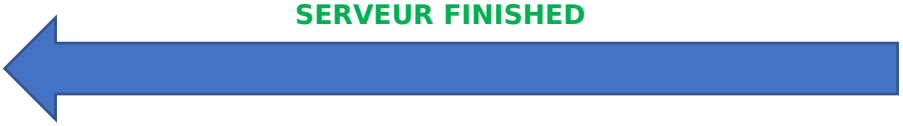
Va créer un numéro (clé) aléatoire (Premaster Security) et l'envoyer au serveur en le chiffrant avec la clé publique du serveur (et que le serveur est capable de le déchiffrer)

26 -27

Client et serveur font un calcul de clé et une communication symétrique (A clé unique) est faite entre eux, car la communication asymétrique est impossible: (seul le serveur possède un certificat et le client n'a pas de pair de clés).

CLIENT FINISHID

SERVEUR FINISHED



28

ÉCHANGES DE MESSAGES CHIFFRÉS

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

A cause de la lenteur d'exécution, et des algorithmes de chiffrement et de déchiffrement qui sont assez complexes

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

Oui. Elle chiffrée asymétriquement par le client et le serveur

Pourquoi certains anciens navigateurs web ne peuvent pas utiliser HTTPS ?

Manque d'une BD, et possibilité de chiffrage pas assez importante

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

Protégée par un mot de passe. Elle est confidentielle (parce qu'elle est faite pour déchiffrer et signer les messages)

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.

Avantage: Identifier le client, permet l'authentification auprès du serveur

Inconvénient: si faille dans le navigateur, l'attaquant a accès à toutes vos communications