1.3 Partie 3 — Anatomie d'une requête HTTP *(exercice indépendant)*

1.3.1 Exercice 5 — Lire une requête HTTP

Voici une requête HTTP telle qu'elle est envoyée par le navigateur d'Alice lorsqu'elle se connecte à son espace client :

```
GET /mon-compte/messages?page=2 HTTP/1.1
Host: www.boutique-exemple.fr
User-Agent: Mozilla/5.0 (Windows NT 10.0) Firefox/120.0
Accept-Language: fr-FR,fr;q=0.9
Cookie: session_id=a3f9c21d; panier=42
Referer: https://www.boutique-exemple.fr/catalogue
Connection: keep-alive
```

5.1 Identifier dans cette requête : - la **méthode HTTP** utilisée - la **ressource demandée** (chemin + paramètre éventuel) - le **nom de domaine** du serveur contacté - la **version du protocole** HTTP utilisée

5.2 À quelle couche du modèle TCP/IP cette requête appartient-elle ? À quel moment de l'encapsulation est-elle construite ?

5.3 L'en-tête `Host` contient le nom de domaine du serveur. Expliquer pourquoi cet en-tête est indispensable, alors que le navigateur connaît déjà l'adresse IP du serveur.
(Indice : un même serveur peut héberger plusieurs sites web sur la même adresse IP — c'est ce qu'on appelle l'hébergement mutualisé.)

5.4 L'en-tête `Cookie` contient un identifiant de session. À quoi sert-il ? Que se passerait-il si quelqu'un interceptait cet en-tête sur un réseau Wi-Fi public non chiffré (HTTP simple) ?

5.5 Compléter le tableau suivant en indiquant qui peut lire chacun de ces en-têtes selon le protocole utilisé :

En-tête	Lisible par le FAI en HTTP ?	Lisible par le FAI en HTTPS ?	Lisible par le serveur ?
`Host`			
`Cookie`			
`User-Agent`			
`Referer`			

5.6 *(Question ouverte)* La méthode `GET` place les paramètres directement dans l'URL (ex. `?page=2`). La méthode `POST`, elle, les place dans le **corps** de la requête, qui n'est pas visible dans l'URL. En HTTP simple (non chiffré), cette différence protège-t-elle les données envoyées en `POST` d'une interception ? Justifier.

1.4 Partie 4 — HTTPS et confidentialité *(exercice indépendant)*

1.4.1 Exercice 6 — Ce que voit (ou ne voit pas) votre FAI

Léa navigue sur internet depuis chez elle. Elle se connecte à son espace personnel sur le site `https://www.banque-exemple.fr/mon-compte/virements`.

Pour chaque information, indiquer si le FAI de Léa peut la connaître, en justifiant :

Information	Visible par le FAI ?	Justification
L'adresse IP du serveur de la banque		
Le nom de domaine `www.banque-exemple.fr`		
Le chemin `/mon-compte/virements`		
Le contenu du virement (montant, bénéficiaire)		
Le fait que Léa utilise le protocole HTTPS		

6.2 À quel niveau du modèle TCP/IP le chiffrement TLS (utilisé par HTTPS) intervient-il ?

6.3 Un ami dit à Léa : *« Le cadenas dans la barre d'adresse prouve que personne ne peut savoir ce que tu fais sur internet. »* Cette affirmation est-elle entièrement vraie ? Corriger-la si nécessaire.

1.5 Partie 5 — VPN *(exercice indépendant, niveau un peu plus difficile)*

1.5.1 Exercice 7 — Comprendre le VPN

Léa installe un logiciel VPN sur son ordinateur et l'active avant de naviguer.

7.1 Rappeler ce qu'est un tunnel VPN et à quelle couche du modèle TCP/IP il intervient principalement.

7.2 Compléter le tableau comparatif suivant :

Situation	Le FAI voit le nom de domaine visité	Le FAI voit le contenu des échanges	Le FAI voit l'IP du serveur final
HTTP simple			
HTTPS (sans VPN)			
HTTPS + VPN			

7.3 Léa pense qu'avec un VPN elle est totalement invisible sur internet. Citer **deux limites** à cette affirmation.

7.4 *(Question ouverte)* Le lycée de Léa bloque l'accès à certains sites via un proxy filtrant. Léa active son VPN. Le filtrage du lycée est-il encore efficace ? Expliquer pourquoi en précisant à quelle couche agit chacun des deux systèmes.
