

APR-TP 1:

-c) les Protocols : TCP , OSCP , ARP , DNS , ICMPv6 , MDNS , NTP , QUIC , TCP , TLSv1.3 , UDP , HTTP

-d) Non, toutes les couches du modèle OSI ne sont pas représentées dans la fenêtre du milieu de Wireshark. La couche physique, qui concerne le support de transmission et qui est la couche 1 du modèle OSI, n'est pas visible dans les captures de Wireshark. Wireshark démarre généralement à la couche liaison de données (couche 2) et remonte à partir de là.

-e)Exemples de trames capturé :

1. Segment TCP (Couche 4) :

- Protocole : TCP
- taille : 1200 octets

2.Trame ARP (Couche 2) :

- Protocole : ARP
- taille : 64 octets

3.Paquet DNS (Couche 3) :

- Protocole : DNS
- taille : 256 octets

4.Paquet ICMPv6 (Couche 3) :

- Protocole : ICMPv6
- taille : 88 octets

-f) Pour une trame dans laquelle le protocole HTTP :

Convert Hexdecimal a octect

1. Ethernet :

- '0cb6d248957ef8633fbebcb160800' => 14 octets

2. IPv4 :

- '4500019a1171400040063043c0a801275db8d822' => 20 octets

3. TCP :

- 'd0f00050fcb7d6115059dd57801801f634ab00000101080a9730f1cbc0eb5281' => 32 octets

4. HTTP :

- '474554202f20485454502f312e310d0a486f73743a206578616d706c652e636f6d0d0a557365722d4167656e743a204d6f7a696c6c612f352e3020285831313b204c696e7578207838365f36343b2072763a3130392e3029204765636b6f2f32303130303130312046697265666f782f3131312e300d0a4163636570743a20746578742f68746d6c2c6170706c69636174696f6e2f7868746d6c2b786d6c2c6170706c69636174696f6e2f786d6c3b713d302e392c696d6167652f617669662c696d6167652f776562702c2a2f2a3b713d302e380d0a4163636570742d4c616e67756167653a20656e2d55532c656e3b713d302e350d0a4163636570742d456e636f64696e673a20677a69702c206465666c6174650d0a444e543a20310d0a436f6e6e656374696f6e3a206b6565702d616c6976650d0a557067726164652d496e7365637572652d52657175657374733a20310d0a536176652d446174613a206f6e0d0a0d0a' => 358 octets

Taille Total = 14 + 20 + 32 + 358 = 424 octect

```
▶ Frame 30100: 424 bytes on wire (3392 bits), 424 bytes captured  
▶ Ethernet II, Src: IntelCor_be:bc:16 (f8:63:3f:be:bc:16), Dst: D  
▶ Internet Protocol Version 4, Src: 192.168.1.39, Dst: 93.184.216  
▶ Transmission Control Protocol, Src Port: 53488, Dst Port: 80, S  
▶ Hypertext Transfer Protocol
```

g)-Dans une trame de capture HTTP, les octets sont capturés dans l'ordre des couches réseau, de la plus basse à la plus haute :

1. En-tête de trame Ethernet.
2. En-tête IPv4.
3. En-tête TCP.
4. Données HTTP.

L'en-tête Ethernet contient les adresses MAC, l'en-tête IPv4 gère les adresses IP, l'en-tête TCP assure la fiabilité, et les données HTTP incluent le contenu de la page web. Cette encapsulation permet la transmission efficace des données HTTP sur le réseau.