Travaux Dirigés
Etude d'échanges entre machines, protocoles, couches et encapsulation

Observez la capture de trafic ci-dessous faite avec Wireshark (en amphi Ensimag, par une connexion Wifi).

Longueur d'en-tête Ethernet (couche 2) : 14 octets. Le type associé à IP est 0x0800

0 5	6 11	12 13
Adresse MAC Dest	Adresse MAC Src	Type Prot encapsulé

Longueur d'en-tête IP(v4) : 20 octets (sans options) ; se termine par Adresse IP Source (4 octets) puis Adresse IP Destination (4 octets).

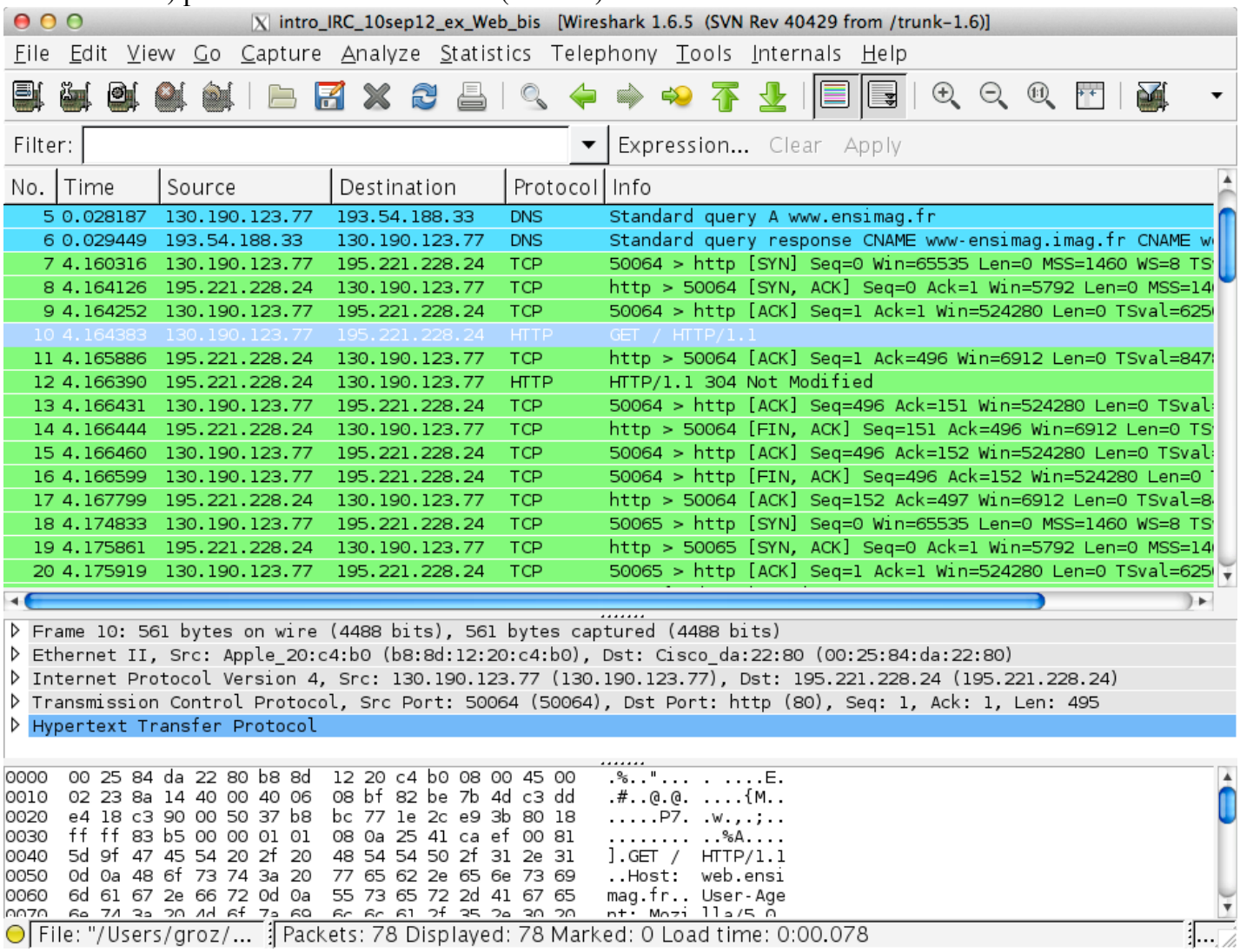


Diagramme de couches (statique)

Question 1. *Repérez les machines (hôtes) qui interviennent dans les échanges capturés. Pour chaque machine impliquée, identifiez les protocoles qu'elle a utilisés dans cet échange. Puis dessinez l'empilement des couches avec les protocoles présents (et utilisés par la machine dans l'échange) dans chaque couche.*

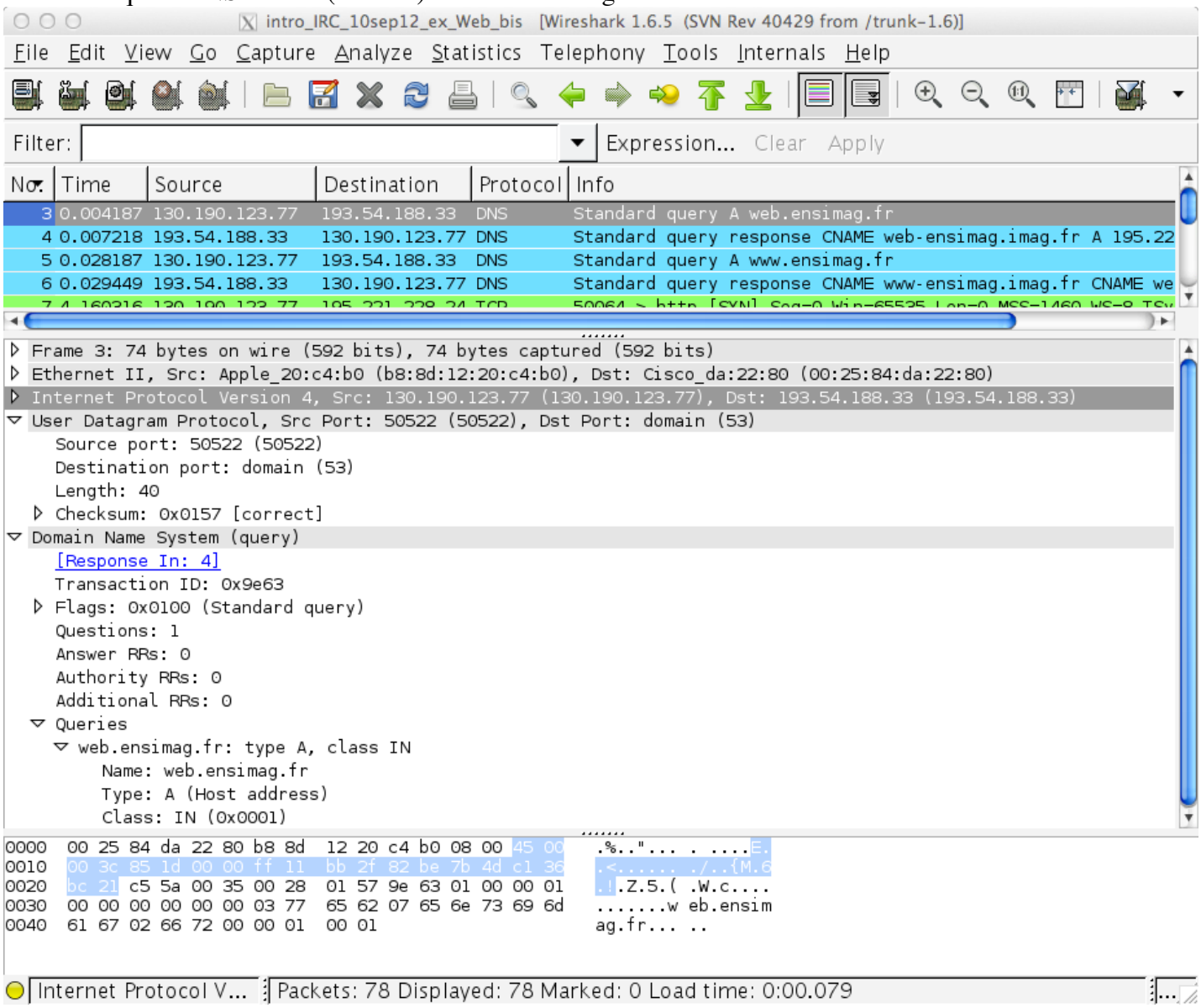
Diagramme temporel (dynamique)

Question 2. *Tracez autant de lignes de vie parallèles que nécessaire et représentez les échanges ci-dessus sur un diagramme temporel.*

Question 3. *Expliquez en français les phases du dialogue telles que vous pouvez les observer sur cette succession de 16 messages.*

Analyse d'en-tête UDP

On s'intéresse maintenant au contenu de l'en-tête du PDU UDP dans lequel est encapsulée la requête DNS initiale (trame 3). Les octets surlignés sont ceux de l'en-tête IP.



Question 4. *Quelle est la longueur de l'en-tête UDP ?*

Question 5. *Où apparaît dans la trame le port source (50522) ? Convertissez 53 et 50522 en hexadécimal (aucun calcul n'est nécessaire).*

Question 6. *Wireshark a décodé dans cet en-tête une longueur de 40 (en décimal). Où apparaît cette longueur dans la trame ? Que mesure-t-elle ?*

Question 7. *Comment Wireshark sait il où finit l'en-tête UDP et où commence la requête DNS ?*