Travaux Dirigés
Architecture en couches, DNS et TCP

Exercice 1
Multiplexage et architecture en couches

Un utilisateur sur telesun.imag.fr (adresse IP 195.221.228.9) exécute un navigateur WWW pour accéder aux documents sur web.ensimag.fr (adresse IP 195.221.228.24). Au même instant, un autre utilisateur travaillant sur la même machine telesun utilise ssh pour travailler sur web.ensimag.fr.

Question 1. *Faites un schéma qui présente l'architecture en couches des protocoles utilisés, les points de connexion avec les ports et adresses, et les chemins empruntés par les données échangées au niveau de ces applications.*

Exercice 2

Analyse de réponse DNS

Nous poursuivons l'étude de la capture de trafic étudiée lors du TD 1.
On s'intéresse à la réponse DNS qui se trouve dans la trame 4 (nous avions vu la requête DNS en trame 3), détaillée dans la figure 1. La réponse DNS rappelle la question, puis fournit 12 éléments de réponse, appelés RR, répartis en trois catégories.

Question 2. *Rappelez ce que signifie RR dans le DNS, l'origine de la terminologie, et les informations qu'ils peuvent contenir.*

Question 3. *Pourquoi y a-t-il 2 « Answers » et non pas une seule ?*

Question 4. *A quoi servent les 4 éléments de réponses classés « Authoritative nameservers » ? Dans quels cas seraient-ils utilisés ?*

Question 5. *Pourquoi y a-t-il des « Additional RR » ? Pourquoi ne pouvait-on fournir et trouver les informations correspondantes dans la catégorie au-dessus ?*

Question 6. *En revenant à la suite des échanges (trames 7 et suivantes) quel(s) élément(s) de réponse ont été réellement utilisés ?*

En-tête TCP (1er aperçu)

On regarde maintenant l'en-tête TCP de la trame 8, en figure 2. Octets surlignés : en-tête IP.

Question 7. *Repérez d'abord les octets correspondant aux différents champs (ports source et destination, numérotation des octets, longueur etc.). Indiquez ce que vaut chacun en hexadécimal.*

Question 8. *Pourquoi Wireshark écrit-il TCP dans la colonne Protocol de la trame 8 et HTTP pour la trame 10 ? Et que représente le http en minuscule qui apparaît au début de la colonne Info : « http > 50064 » ?*

Question 9. *Où se trouvent les drapeaux ? Comment y décode-t-on que les deux drapeaux SYN et ACK sont levés (et pas les autres) ?*

Question 10. *Quel sera le numéro (absolu) du premier octet de la couche application (requête HTTP) qui sera envoyé par la machine 130.190.123.77 ?*

Question 11. *Que recouvre la longueur de 40 octets ?*

Réponse HTTP

Question 12. *Comment le client DNS savait-il que la réponse contenue dans la trame 4 était bien une réponse à sa question posée en trame 3 (dans le dialogue complet, on voit que le client pose successivement deux questions, une pour web.ensimag.fr, l'autre pour www.ensimag.fr) ? Et comment le navigateur de la machine 130.190.123.77 sait-il que la réponse du serveur « Not modified » en trame 12 correspond bien à sa requête en trame 10 ? Comparez ces deux mécanismes (entre la solution pour le DNS et celle pour HTTP).*

Question 13. *Vous pourrez étudier si vous le souhaitez les en-têtes TCP et HTTP de la trame 12 (figure 3).*

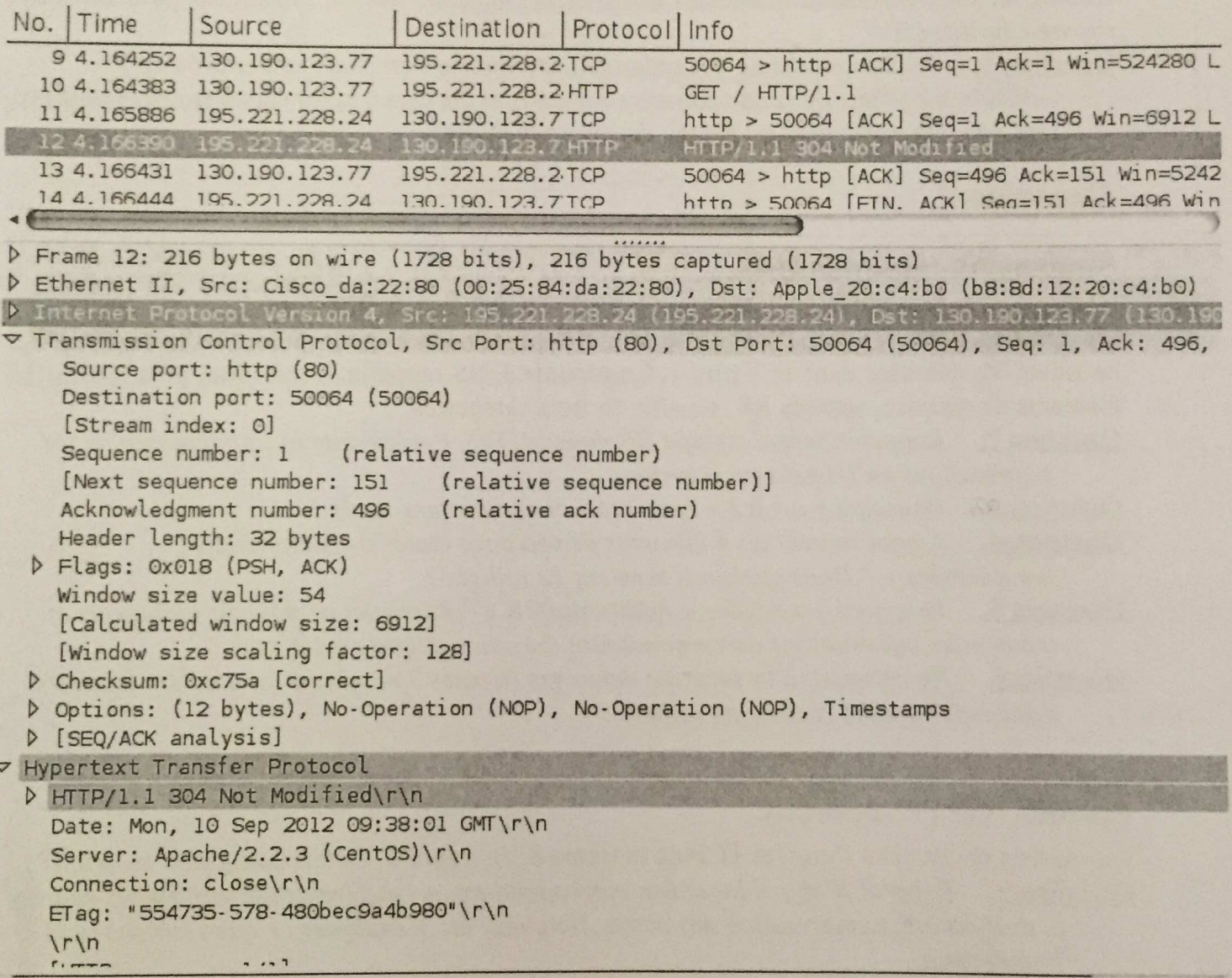


Figure 3. Détail trame 12 : réponse HTTP

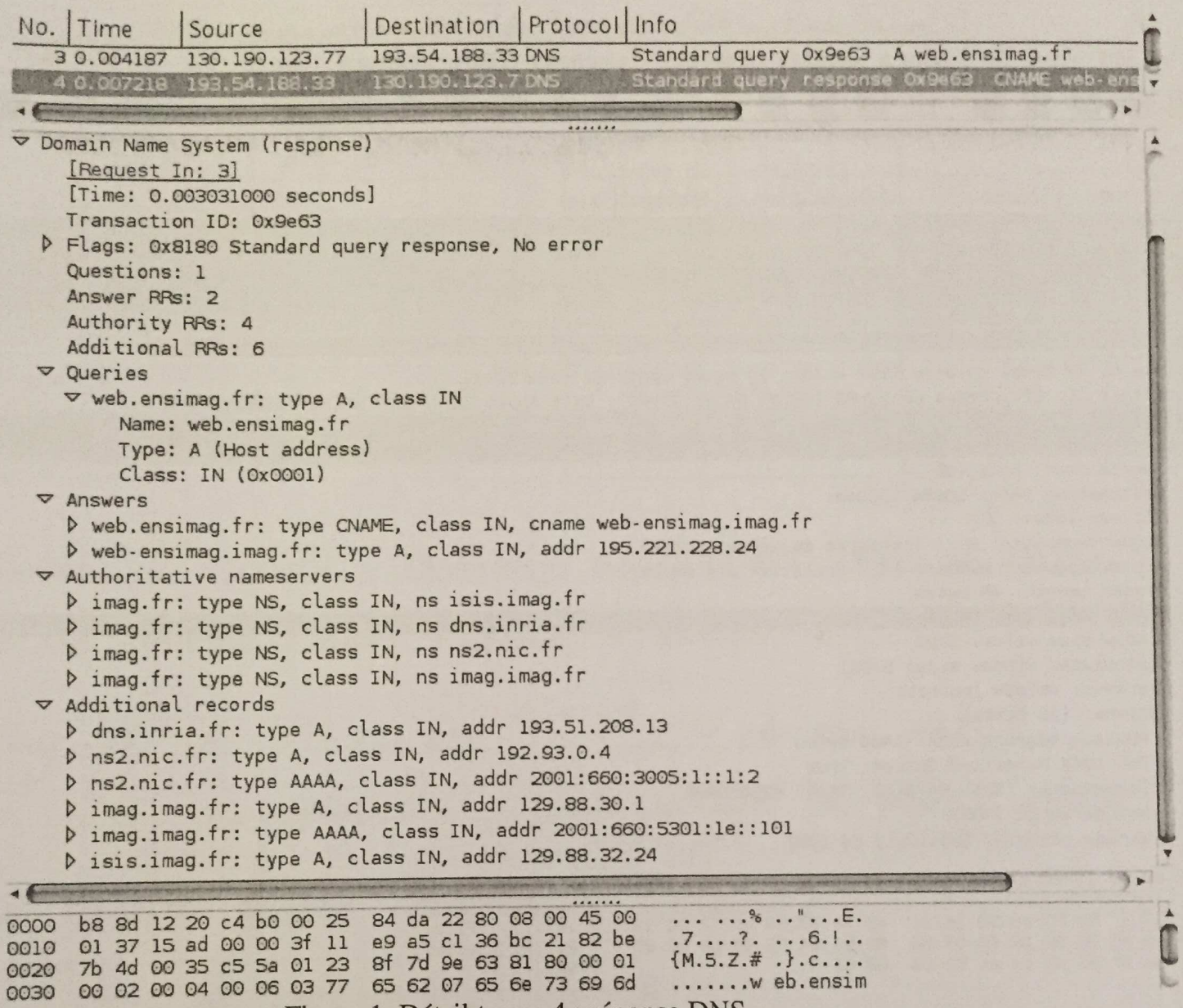


Figure 1. Détail trame 4 : réponse DNS

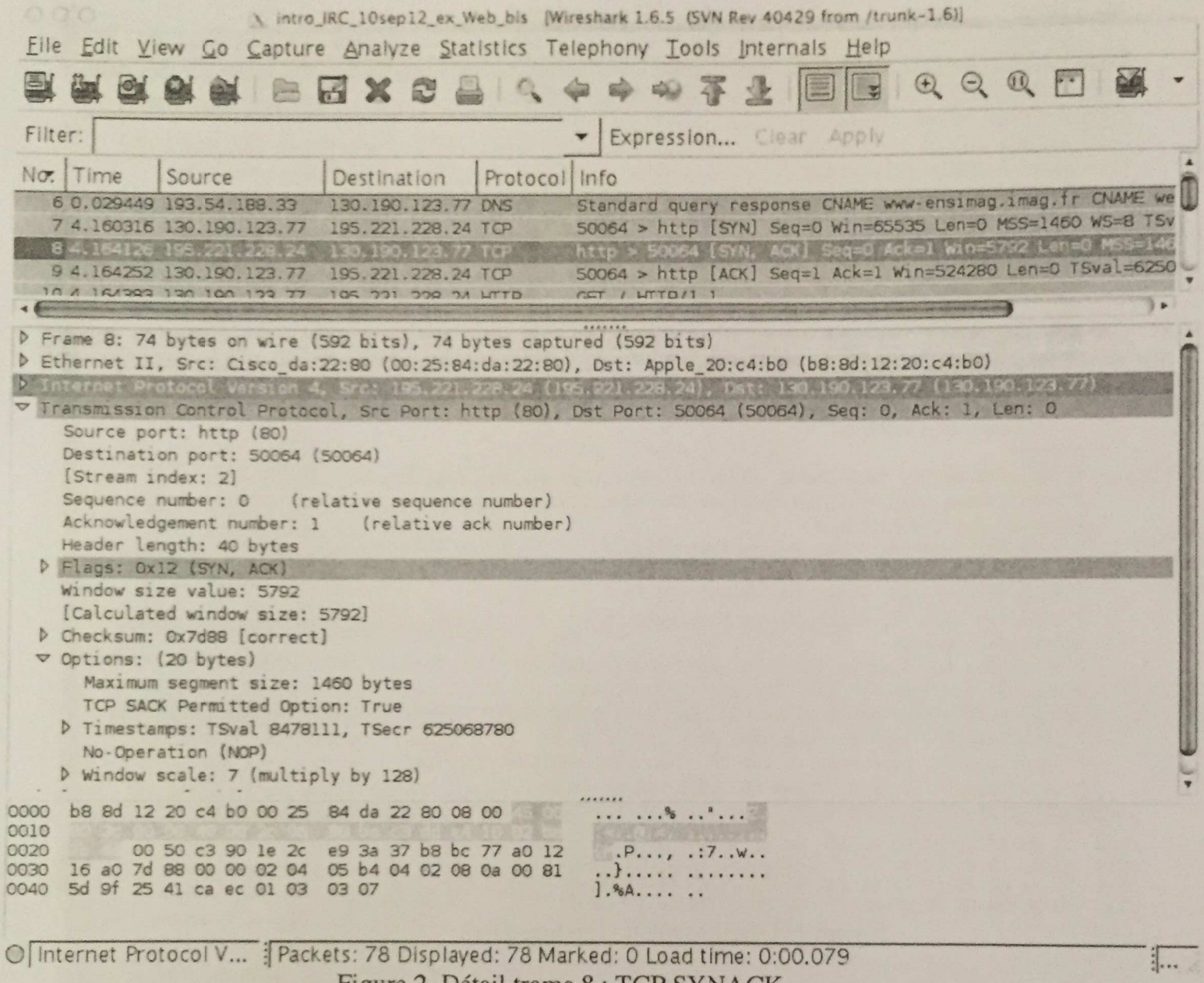
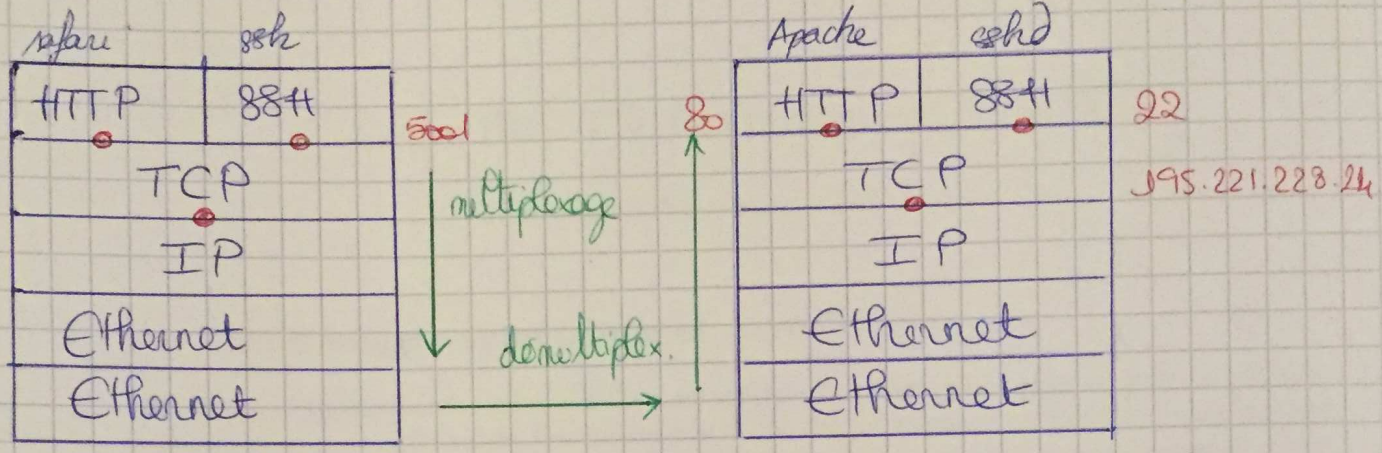


Figure 2. Détail trame 8 : TCP SYNACK.

Exo 1 1) Port http : 80 Port ssh : 22

telesun.imag.fr web.ensimag.fr



2) RR : ressource record : Données enregistrées dans le DNS
sous la forme NOM + option + valeur

telesun.imag.fr A 195.221.228.9 (IP du nom DNS)
imag.fr NS ns.imag.fr (nom serveur ⇒ plusieurs serveurs regroupés pour fiabilité)
ensimag.fr CNAME telesun.imag.fr (Alias)

3) On pose la question sur un alias

Rép 1 → nous donne le nom canonique
Rép 2 → nous donne l'adresse IP

4) Les 4 éléments réponses sont les noms serveurs
Ils seraient utilisés pour avoir une réponse d'autorité et non du cache

5) Ce sont des enregistrements supplémentaires (cache)
↳ On a directement l'IP au lieu de refaire une recherche de nom

6) —