

## 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 avons 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 (1<sup>er</sup> 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).

No.	Time	Source	Destination	Protocol	Info
9	4.164252	130.190.123.77	195.221.228.2	TCP	50064 > http [ACK] Seq=1 Ack=1 Win=524280 L
10	4.164383	130.190.123.77	195.221.228.2	HTTP	GET / HTTP/1.1
11	4.165886	195.221.228.24	130.190.123.7	TCP	http > 50064 [ACK] Seq=1 Ack=496 Win=6912 L
12	4.166390	195.221.228.24	130.190.123.7	HTTP	HTTP/1.1 304 Not Modified
13	4.166431	130.190.123.77	195.221.228.2	TCP	50064 > http [ACK] Seq=496 Ack=151 Win=5242
14	4.166444	195.221.228.24	130.190.123.7	TCP	http > 50064 [FIN, ACK] Seq=151 Ack=496 Win

.....

▷ Frame 12: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits)

▷ Ethernet II, Src: Cisco\_da:22:80 (00:25:84:da:22:80), Dst: Apple\_20:c4:b0 (b8:8d:12:20:c4:b0)

▷ Internet Protocol Version 4, Src: 195.221.228.24 (195.221.228.24), Dst: 130.190.123.77 (130.190.123.77)

▽ Transmission Control Protocol, Src Port: http (80), Dst Port: 50064 (50064), Seq: 1, Ack: 496, Source port: http (80)  
Destination port: 50064 (50064)  
[Stream index: 0]  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 151 (relative sequence number)]  
Acknowledgment number: 496 (relative ack number)  
Header length: 32 bytes

▷ Flags: 0x018 (PSH, ACK)  
Window size value: 54  
[Calculated window size: 6912]  
[Window size scaling factor: 128]

▷ Checksum: 0xc75a [correct]  
▷ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
▷ [SEQ/ACK analysis]

▽ Hypertext Transfer Protocol

▷ HTTP/1.1 304 Not Modified\r\n  
Date: Mon, 10 Sep 2012 09:38:01 GMT\r\n  
Server: Apache/2.2.3 (CentOS)\r\n  
Connection: close\r\n  
ETag: "554735-578-480bec9a4b980"\r\n  
\r\n

Figure 3. Détail trame 12 : réponse HTTP



No.	Time	Source	Destination	Protocol	Info
3	0.004187	130.190.123.77	193.54.188.33	DNS	Standard query 0x9e63 A web.ensimag.fr
4	0.007218	193.54.188.33	130.190.123.7	DNS	Standard query response 0x9e63 CNAME web.ens

Domain Name System (response)

[Request In: 3]

[Time: 0.003031000 seconds]

Transaction ID: 0x9e63

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 4

Additional RRs: 6

Queries

web.ensimag.fr: type A, class IN

Name: web.ensimag.fr

Type: A (Host address)

Class: IN (0x0001)

Answers

web.ensimag.fr: type CNAME, class IN, cname web-ensimag.imag.fr

web-ensimag.imag.fr: type A, class IN, addr 195.221.228.24

Authoritative nameservers

imag.fr: type NS, class IN, ns isis.imag.fr

imag.fr: type NS, class IN, ns dns.inria.fr

imag.fr: type NS, class IN, ns ns2.nic.fr

imag.fr: type NS, class IN, ns imag.imag.fr

Additional records

dns.inria.fr: type A, class IN, addr 193.51.208.13

ns2.nic.fr: type A, class IN, addr 192.93.0.4

ns2.nic.fr: type AAAA, class IN, addr 2001:660:3005:1::1:2

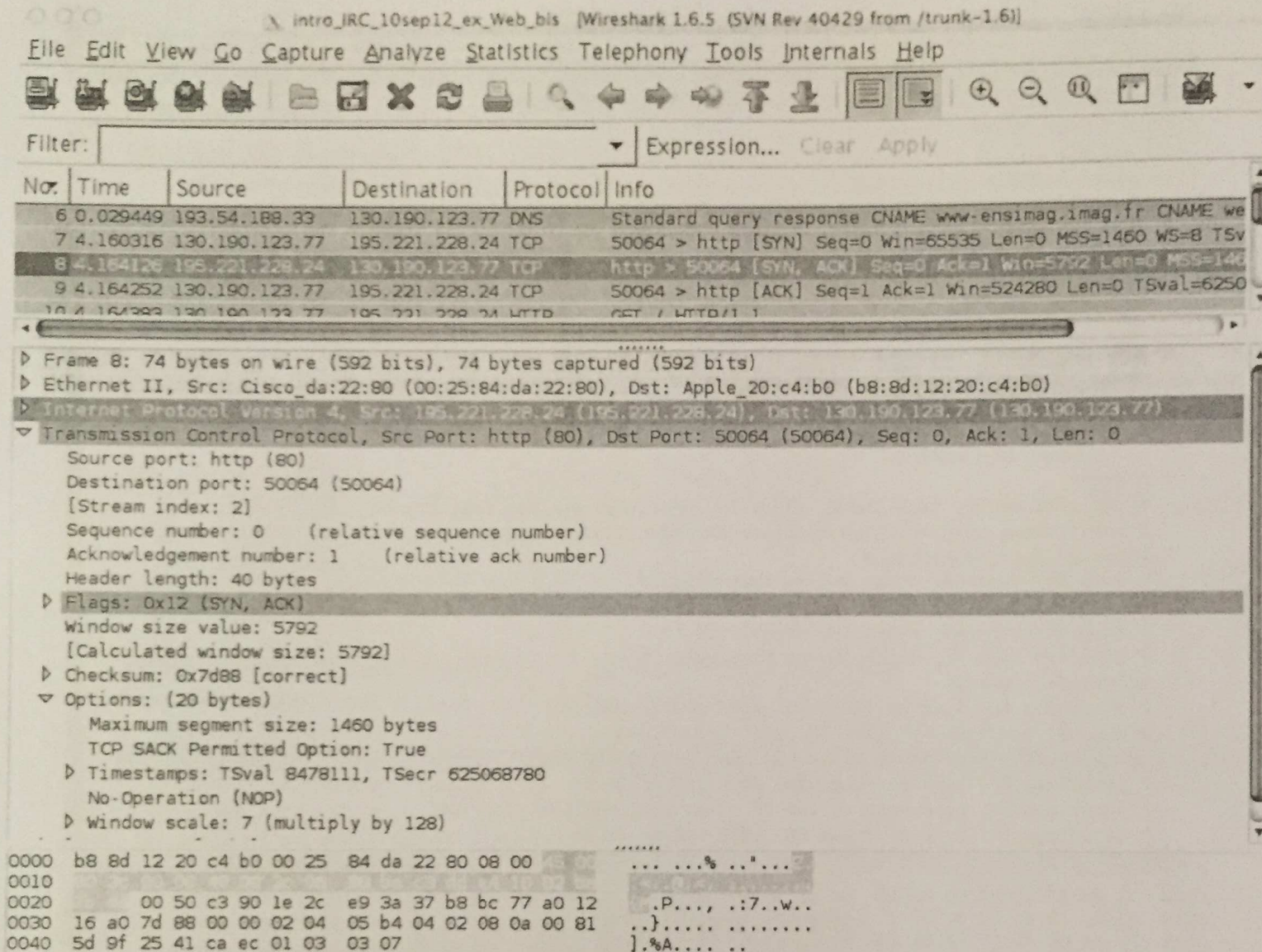
imag.imag.fr: type A, class IN, addr 129.88.30.1

imag.imag.fr: type AAAA, class IN, addr 2001:660:5301:1e::101

isis.imag.fr: type A, class IN, addr 129.88.32.24

Figure 1. Détail trame 4 : réponse DNS





Internet Protocol V... Packets: 78 Displayed: 78 Marked: 0 Load time: 0:00.079

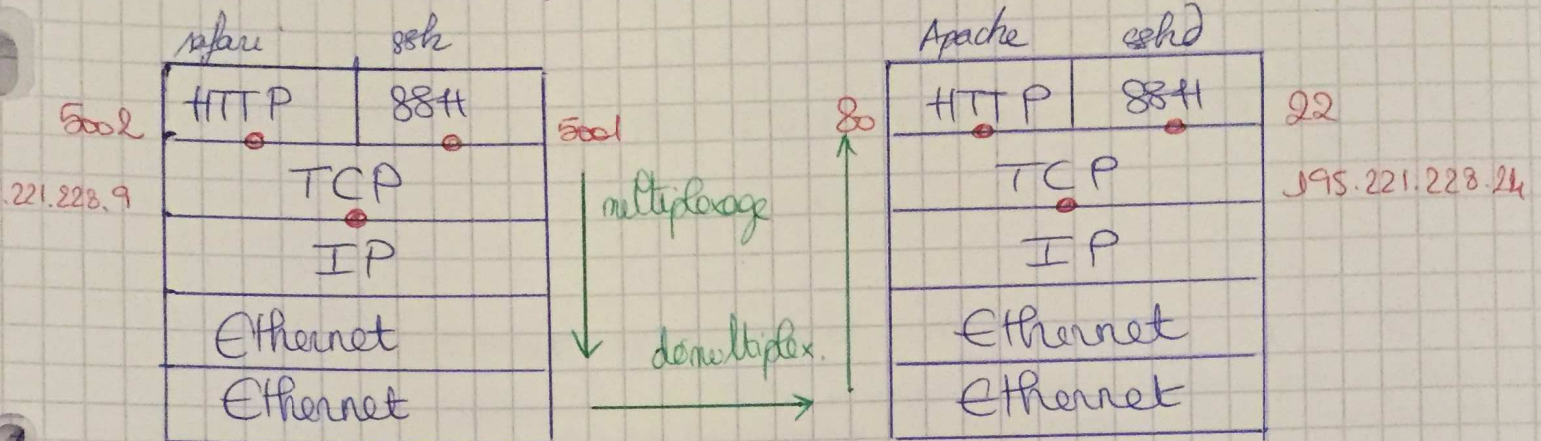
Figure 2. Détail trame 8 : TCP SYNACK.



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

telesun.imag.fr

web.msiimag.fr



2) RR : resource 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 (name server  $\Rightarrow$  plusieurs serveurs regroupés pour fiabilité)

msimag.fr CNAME telesun.imag.fr (alias)

3) On pose la question sur un alias

Rép 1  $\rightarrow$  nous donne le nom canonique

Rép 2  $\rightarrow$  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)  
 $\rightarrow$  On a directement l'IP au lieu  
de refaire une recherche de nom

6) /