# ED• Découverte de l'analyse de trames avec Wireshark

Cette séance d'exercices dirigés est un mélange d'exercices et de TP à faire en autonomie. En particulier, la partie Wireshark est une ouverture à des expérimentations qu'on peut mener seul chez soi afin de découvrir l'intensité des échanges de données qui vous entoure sur vos réseaux domestiques. Wireshark est installable sur machine linux ou windows (macOS probablement aussi) gratuitement.

Le but de la 2ème partie de cette séance, après l'exercice 0, a pour but d'introduire les différentes couches protocolaires et leur rôle. Mais surtout faire découvrir le mécanisme d'encapsulation qui est fondamental et dont on se servira pendant toutes les séances ou presque. Les couches et l'encapsulation sont indissociables.

## Exercice 1 : Un exemple de Structure : la Trame Ethernet

Le format de l'information qui passe sur le médium de communication est le suivant, ce qui est en gras matérialise la trame Ethernet :

| **Adresse destination** | **Adresse source** | **Type** | **Informations** | **FCS** |
|---|---|---|---|---|
| 6 octets | 6 octets | 2 octets | 46 à 1500 octets | 4 octets |

L'entête Ethernet est une forme d'étiquetage de la trame. Le champ type en particulier indique ce qu'elle contient. Pour mieux comprendre la trame, on peut essayer de la comparer à un wagon, le wagon tombereau est une bonne métaphore pour commencer.



**Caractéristiques du wagon:**
**-"87 SNCF" circule sur le pur RFN**
**- Charge autorisée 20,5t sur une ligne catégorie A, et 24,5t sur une ligne catégorie B ou C.**
**- Vitesse max : 90km/h**
**- Surface Plancher 24m²**

**Type de contenu**


source : http://tgveurofrance.com.pagesperso-orange.fr/wagons4.htm (13/05/2021)

RFN = Réseau Ferré National

Ligne cat A : permet des wagons avec 16t par essieu, et 5t/m

Ligne cat B : 18t/essieu et 5t/m

Ligne cat C : 20t/essieu et 6,4t/m

(http://docplayer.fr/106969222-Reconnaissance-de-l-aptitude-au-transport.html, 13/05/2021)

D'après le format de la trame Ethernet quelle est la longueur minimum de données transportables ?

D'après le format de la trame, quelle est la longueur minimum d'une trame Ethernet ?

Quelle est la longueur maximum de données transportables ? Quelle est la longueur maximum d'une trame Ethernet ?

Voici la trace hexadécimale d'une communication point à point prélevée par un espion de ligne ou analyseur de protocole (SNOOP, mais on peut refaire l'exercice avec un logiciel plus récent Wireshark):

```
00: 0800 2018 ba40 aa00 0400 1fc8 0800 4500    .. ..@.....................E.
16: 0028 e903 4000 3f06 6a5c a3ad 2041 a3ad    .(..@.?.j\.. A..
32: 80d4 0558 0017 088d dee0 ba77 8925 5010    ...X.....................w.%P.
48: 7d78 1972 0000 0000 0000 0000 0000 0000    }x.r............
```

Retrouver les champs de la trame Ethernet dans la trace hexadécimale précédente.

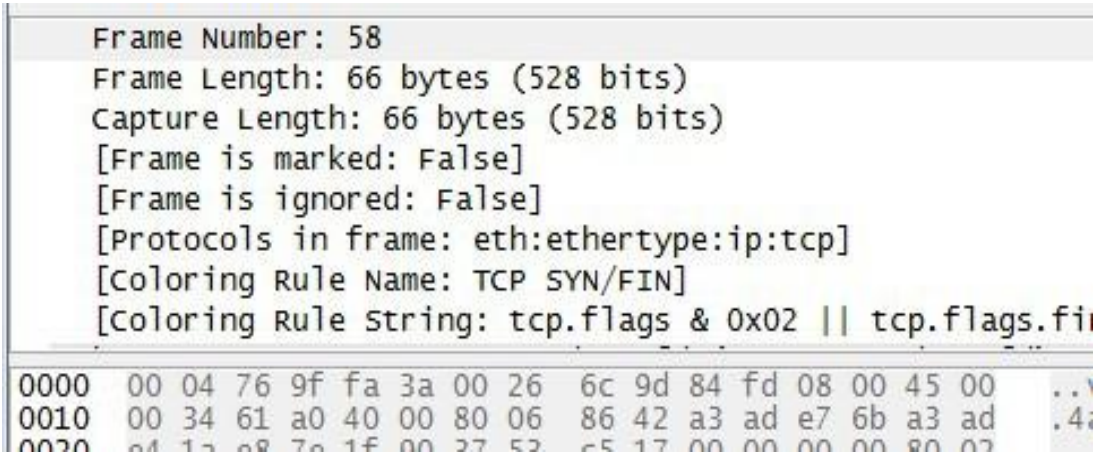
Pourquoi la partie correspondant au FCS[1] est à zéro ?

Pourquoi les 8 octets à la fin de la partie information de la trame sont à zéro ?

## Exercice 2 : Analyseur de protocole et adresses dans une trame Ethernet (à faire soi-même en autonomie)

Soit la trace d'une trame Ethernet capturée par un analyseur de protocole, Wireshark pour être plus précis, sur le réseau :

[1] On utilise CRC, Cyclic Redundancy Code, comme synonyme de FCS, Frame Check Sequence.On trouve les 2 termes dans la littérature.




Ci-dessous la structure d'une trame Ethernet comme dans l'exercice précédent :

| **Adresse destination** | **Adresse source** | **Type** | **Informations** | **FCS** |
|---|---|---|---|---|
| 6 octets | 6 octets | 2 octets | 46 à 1500 octets | 4 octets |

Quelle est l'adresse MAC de destination de la trame ? Quelle est l'adresse MAC de la source de la trame ?

a) 4C:ED:DE:E5:A5:6B
b) 00:04:76:9F:FA:3A
c) 00:26:6C:9D:84:FD
d) AA:ED:DF:E5:A5:6B

## Exercice 3 : Analyse de trame contenant un message de couche 7, DNS, transporté en UDP[2] avec l'outil Wireshark

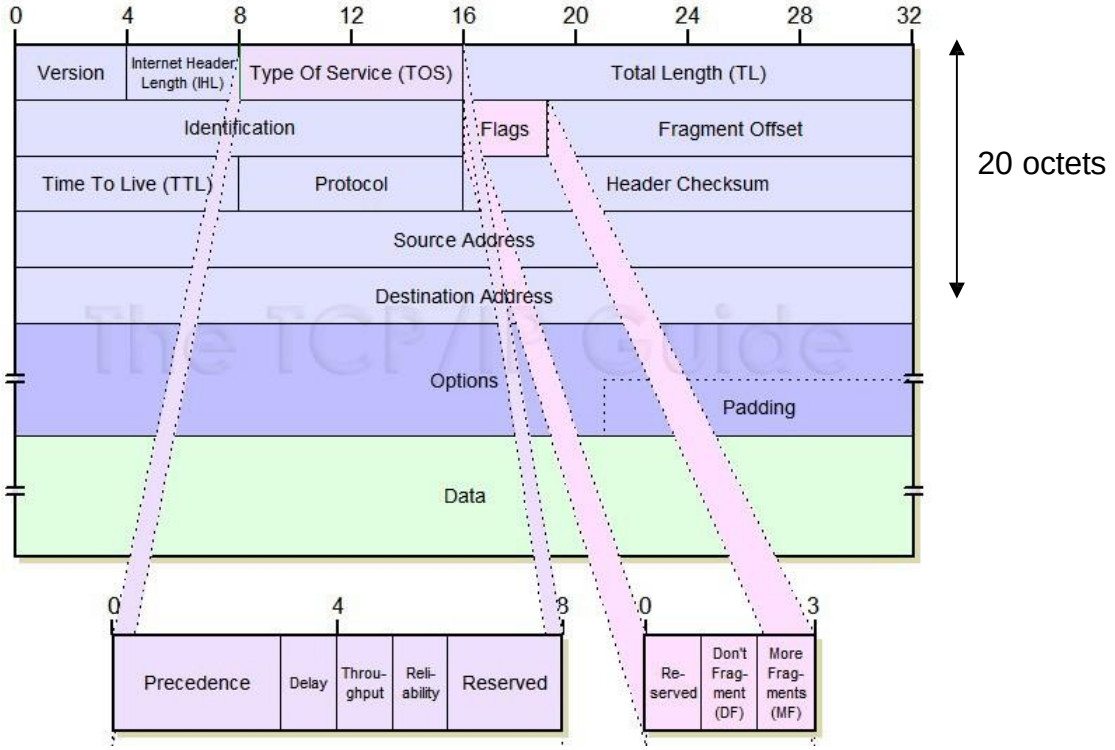
On s'intéresse à un échange client/serveur de type DNS (Domain Name System), qui est le système de gestion des correspondances entre nom de machine et ses adresses IP. Enfin, pas seulement, il fait beaucoup plus de choses, mais cela sera exploré dans une séance faite par S. Bortzmeyer. L'échange capturé avec Wireshark est un échange avec le transport UDP, User Datagram Protocol.

[2] DNS = Domain Name System, UDP = User Datagram Protocol

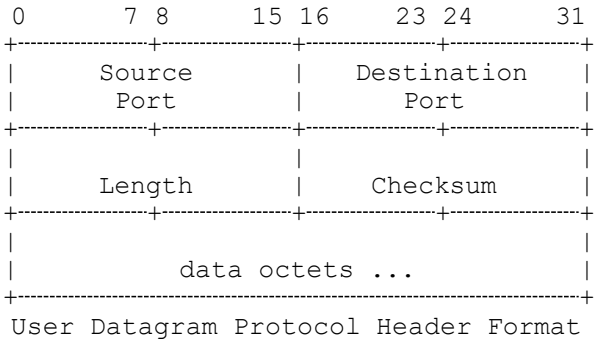
On donne la structure d'une trame Ethernet :

| **Adresse destination** | **Adresse source** | **Type** | **Informations** | **FCS** |
|---|---|---|---|---|
| 6 octets | 6 octets | 2 octets | 46 à 1500 octets | 4 octets |

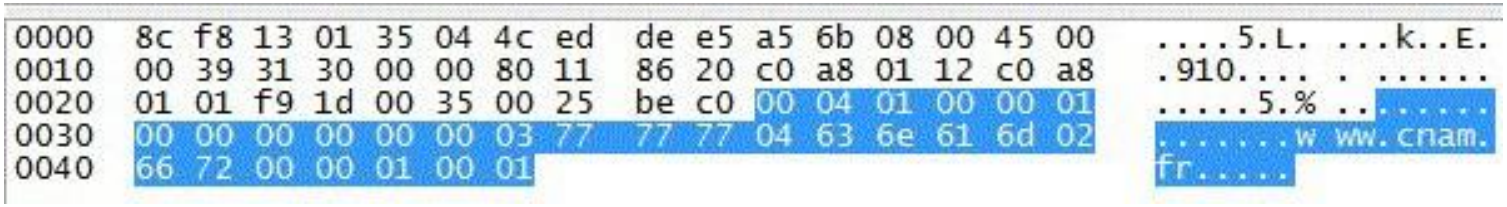
On donne la structure de l'entête IP, consulté le 23 décembre 2013, Source http://www.tcpipguide.com/free/t_IPDatagramGeneralFormat.htm :



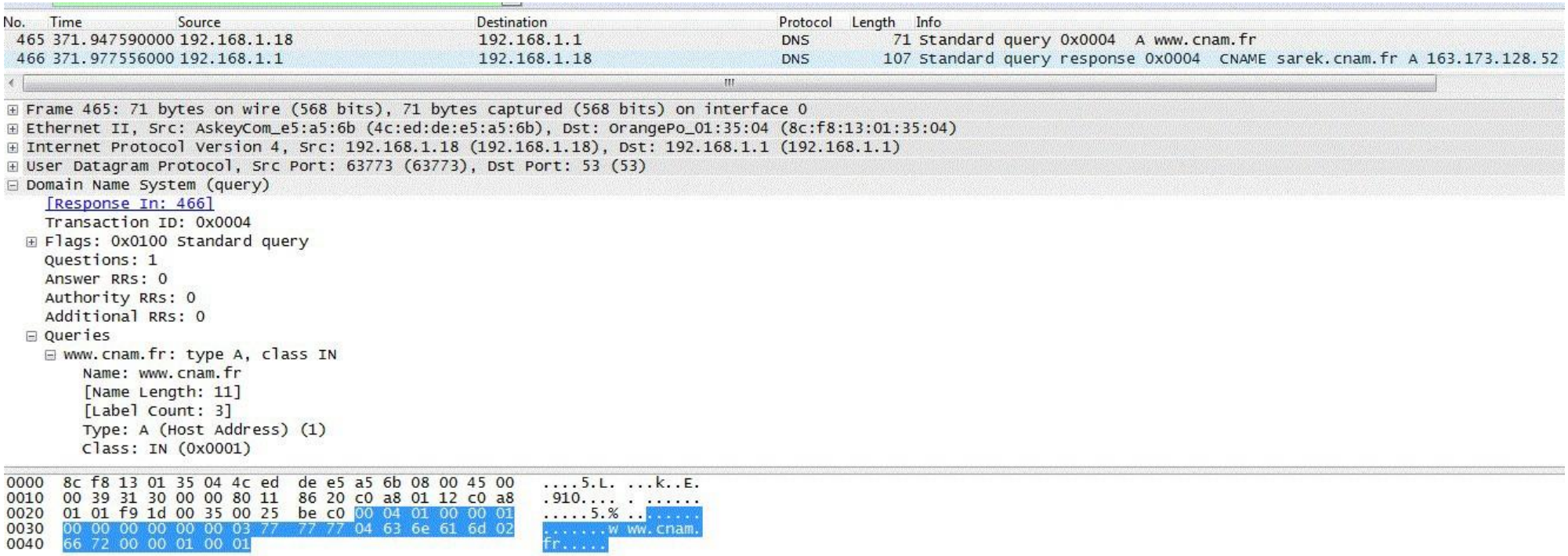
On donne la structure de l'entête UDP :



User Datagram Protocol Header Format




Vous pourrez vous aider de la trace extraite de l'affichage issu de l'outil Wireshark ci-après pour confronter ce que vous trouvez dans la trame avec ce que Wireshark affiche.




On s'intéresse à la trace en hexadécimal ci-après. Donner la valeur et retrouver dans la trace en encadrant sa position :

- l'adresse Ethernet destination en **hexadécimal**
- l'adresse Ethernet source en **hexadécimal**
- le type de la trame en **hexadécimal** et à quel protocole de couche 3 transporté cela correspond,
- la version du protocole IP en **décimal**
- la longueur de l'entête IP en **décimal**
- l'adresse IP source en **hexadécimal**
- l'adresse IP destination en **hexadécimal**
- le protocole transporté en couche 4 dans le datagramme IP en **héxadécimal**
- le numéro de port source en **héxadécimal**
- le numéro de port destination en **héxadécimal**

**Liens pour aller plus loin, c'est une vive recommandation :**
Chris Geer. Wireshark Masterclass. En anglais mais bien fait et plus compréhensible que les séries américaines en VO si vous en suivez sur Netflix !!! Ce cours a la vertu de vous faire travailler votre anglais, ce n'est pas un mal car les informations les plus fiables en réseaux et sur Internet sont souvent en anglais sur le Web ou dans les documents de référence. Mais attention, toujours s'interroger sur ses sources Web. Par exemple Wikipedia, même si ce n'est pas une référence absolue, reste plus fiable en anglais qu'en français pour ce qui concerne le domaine des réseaux. Les vidéos de cette Masterclass sont courtes, moins de 20mn pour ce que j'ai un peu exploré.

"***Intro to Wireshark Tutorial***" :

- 25 Avril 2021, //Lesson 1// Wireshark Setup Free Tutorial, https://www.youtube.com/watch?v=OU-A2EmVrKQ (29/08/2021)
- 5 Avril 2021, //Lesson 2// How to Capture Network Traffic, https://www.youtube.com/watch?v=nWvscuxqais (29/08/2021)
- 29 Avril 2021, //Lesson 3// Capturing Packets with Dumpcap, (tshark est souvent mentionné comme outil en lignes de commande) https://www.youtube.com/watch?v=DAtyzE1TUlI (29/08/2021)
- 11 Mai 2021, //Lesson 4// Where do we capture network traffic? How? https://www.youtube.com/watch?v=Atde35_9AAc (29/08/2021)
- 25 Mai 2021, //Lesson 5// How To filter Traffic, https://www.youtube.com/watch?v=-HDpYR_QSFw (29/08/2021)

Les vidéos suivantes sont intéressantes, mais un peu plus avancés. Le nom change en "***Wireshark Tutorial***" :

- 21 Juillet 2021, //Lesson 6// Name Resolution, https://www.youtube.com/watch?v=gfxxCBCKvMU (29/08/2021)
- 3 Août 2021, //Lesson 7// Using the Time Column, https://www.youtube.com/watch?v=SllJu5MdkAg (29/08/2021)

Chris Geer aborde d'autres sujets sur les réseaux en s'aidant de Wireshark, globalement, c'est très bien ce qu'il fait. Mais c'est un avis personn