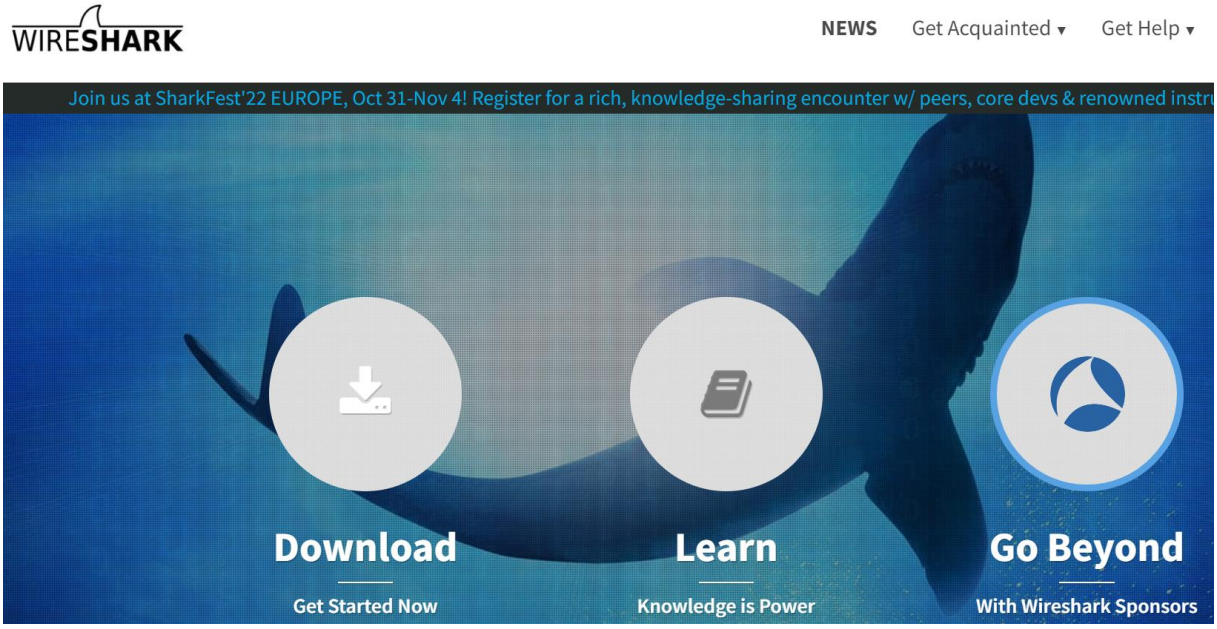
Module R3.06 **Architecture des Réseaux**	**Travaux dirigés**	TD2
Programme de BUT 3		
Séquence : Révision partie 2 **Transferts de données dans le modèle OSI ou TCP/IP**	***Acquis en fin de séance*** *Le Modèle OSI* *Le Modèle TCP-IP* *Passage dans les couches* *Analyse d'une trame* *Datagramme IP* *Segment TCP ou UDP* *ICMP* *ARP*	
Outils	***Wireshark*** ***Cours TCP-IP***	

Présentation de Wireshark

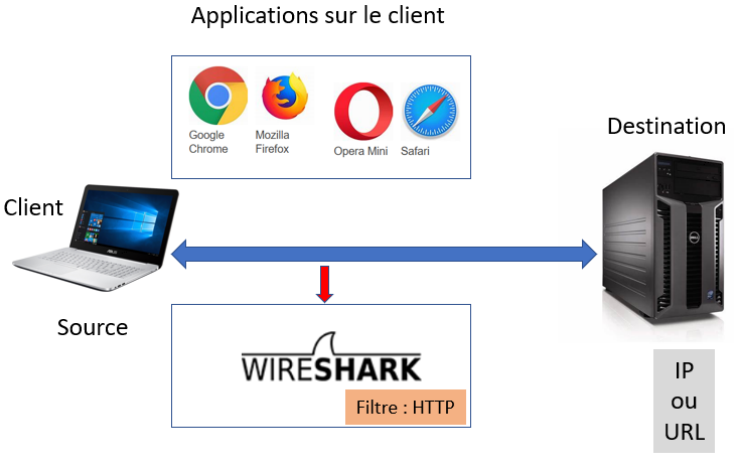
Stable Release (3.6.8) • September 7, 2022



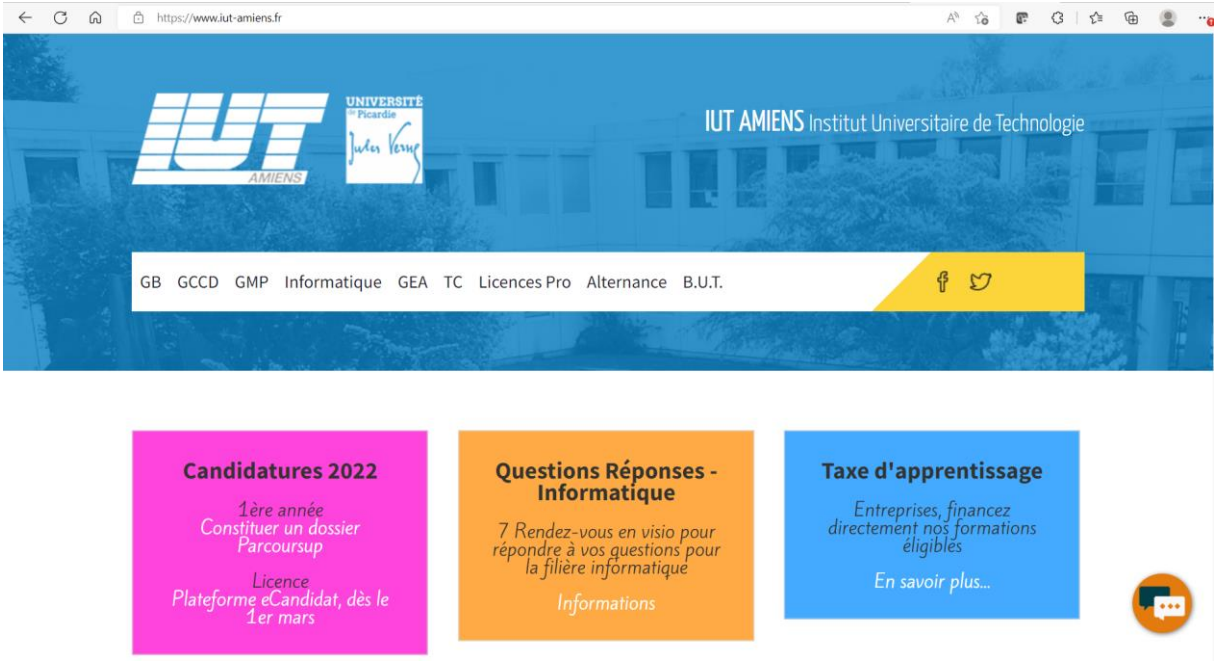
Présentation orale de l'outils (Rappel)

- https://www.wireshark.org/
- Version : 3.6.5
- Les 3 fenêtres
- Analyse intégrée
- Filtrage

Interception des données :



Site WEB capturé (partie A)



Outils Windows utilisé pour une capture

Méthode 1 : (partie B)

```
C:\Users\Eric Brassart>ping www.iut-amiens.fr

Envoi d'une requête 'ping' sur morglum.iut-amiens.fr [194.57.109.129] avec 32 octets de données :
Réponse de 194.57.109.129 : octets=32 temps=375 ms TTL=51
Réponse de 194.57.109.129 : octets=32 temps=233 ms TTL=51
Réponse de 194.57.109.129 : octets=32 temps=273 ms TTL=51
Réponse de 194.57.109.129 : octets=32 temps=291 ms TTL=51

Statistiques Ping pour 194.57.109.129:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 233ms, Maximum = 375ms, Moyenne = 293ms
```

Méthode 2 : (partie C)

```
C:\Users\Eric Brassart>ping 194.57.109.129

Envoi d'une requête 'Ping'  194.57.109.129 avec 32 octets de données :
Réponse de 194.57.109.129 : octets=32 temps=338 ms TTL=51
Réponse de 194.57.109.129 : octets=32 temps=234 ms TTL=51
Réponse de 194.57.109.129 : octets=32 temps=332 ms TTL=51
Réponse de 194.57.109.129 : octets=32 temps=343 ms TTL=51

Statistiques Ping pour 194.57.109.129:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 234ms, Maximum = 343ms, Moyenne = 311ms
```

Outils Windows utilisé pour une capture (partie D)

```
C:\Users\Eric Brassart>nslookup www.iut-amiens.fr
Serveur :   bbox.lan
Address:  192.168.1.254

Réponse ne faisant pas autorité :
Nom :    morglum.iut-amiens.fr
Address:  194.57.109.129
Aliases:  www.iut-amiens.fr
          proxy.iut-amiens.fr


C:\Users\Eric Brassart>ping www.iut-amiens.fr
```

Mécanisme arp **(partie E)**

Attention l'écran ci-dessous n'est pas un résultat réseau mais le résultat d'une commande arp exécuté sur une machine.

```
C:\Users\Eric Brassart>arp -a

Interface : 10.16.6.25 --- 0x10
  Adresse Internet      Adresse physique      Type
  10.16.2.140           48-4d-7e-e7-5e-52     dynamique
  10.16.7.254           44-aa-50-c1-9d-81     dynamique
  10.16.7.255           ff-ff-ff-ff-ff-ff     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique
```

Autre site (partie F) - optionnelle

Vous devez montrer à partir de la source de données correspondant à la capture jointe :

capture_11_09_2022 11/09/2022 18:25 Wireshark capture ... 13 650 Ko

Qui est disponible dans le Moodle UPJV, l'interprétation explicite qui en est faite par le logiciel wireshark.

Les étapes successives que vous avez à analyser sont standards en réseaux et passent par ces phases successives :

- Logiciel ou outils utilisé sur le client,
- Protocole associé au logiciel ou à l'outil,
- Niveau d'interprétation dans les couches OSI ou TCP/IP,
- Interprétation des données dans chaque niveau.

Pour simplifier la recherche des informations correspondant à l'outils utilisé, on peut orienter la recherche des trames en identifiant :

- La source (@IP ou @MAC suivant si on considère le LAN ou l'INTERNET)
- La destination (@IP ou @MAC)
- Le protocole
- Le service
- Le port
- Les RFCs
- URLs
- Etc…

Les machines possèdent des outils réseaux qui vont vous permettre d'identifier facilement certaines de ces informations.

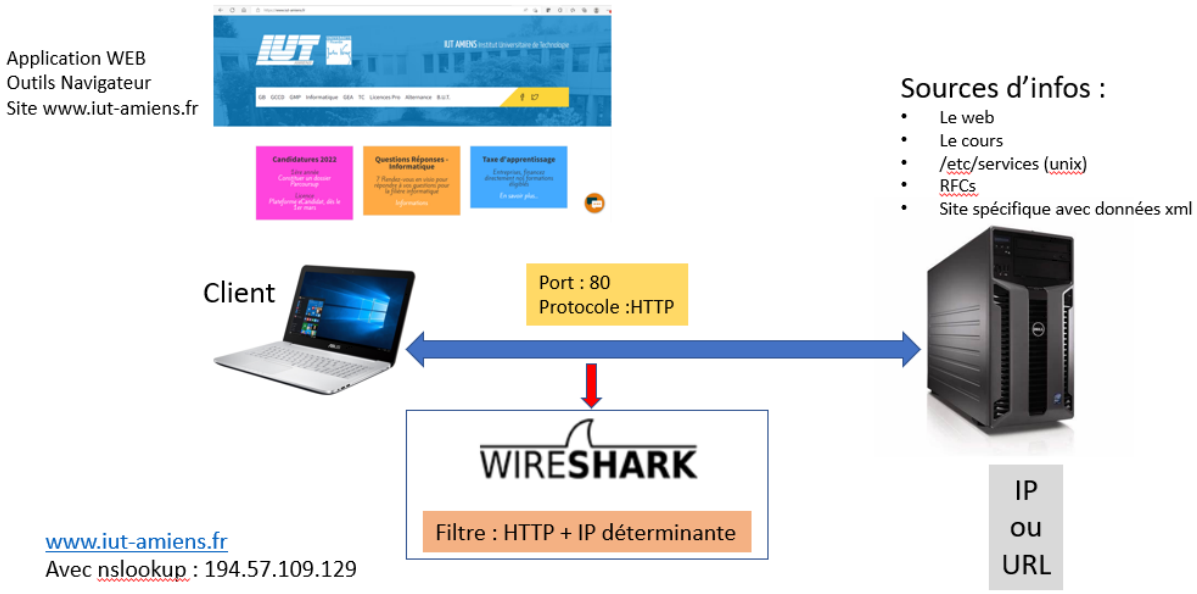
- ipconfig
- ipconfig /all

- nslookup
- arp -a

Ou des sites sur lesquels vous pourrez identifier des services et les protocoles associés.

- https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
- https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

Partie A :



- La source :
- La destination : 194.57.109.129 outils nslookup
- Le protocole : TCP moyen URL
- Le service : HTTP moyen URL
- Le port : 80 moyen URL
- Les RFCs : 2145-2616-2817 … Recherche Google
- URLs : www.iut-amiens.fr visible dans le navigateur

Recherche dans la capture fournie

Il y a 20732 trames capturées.

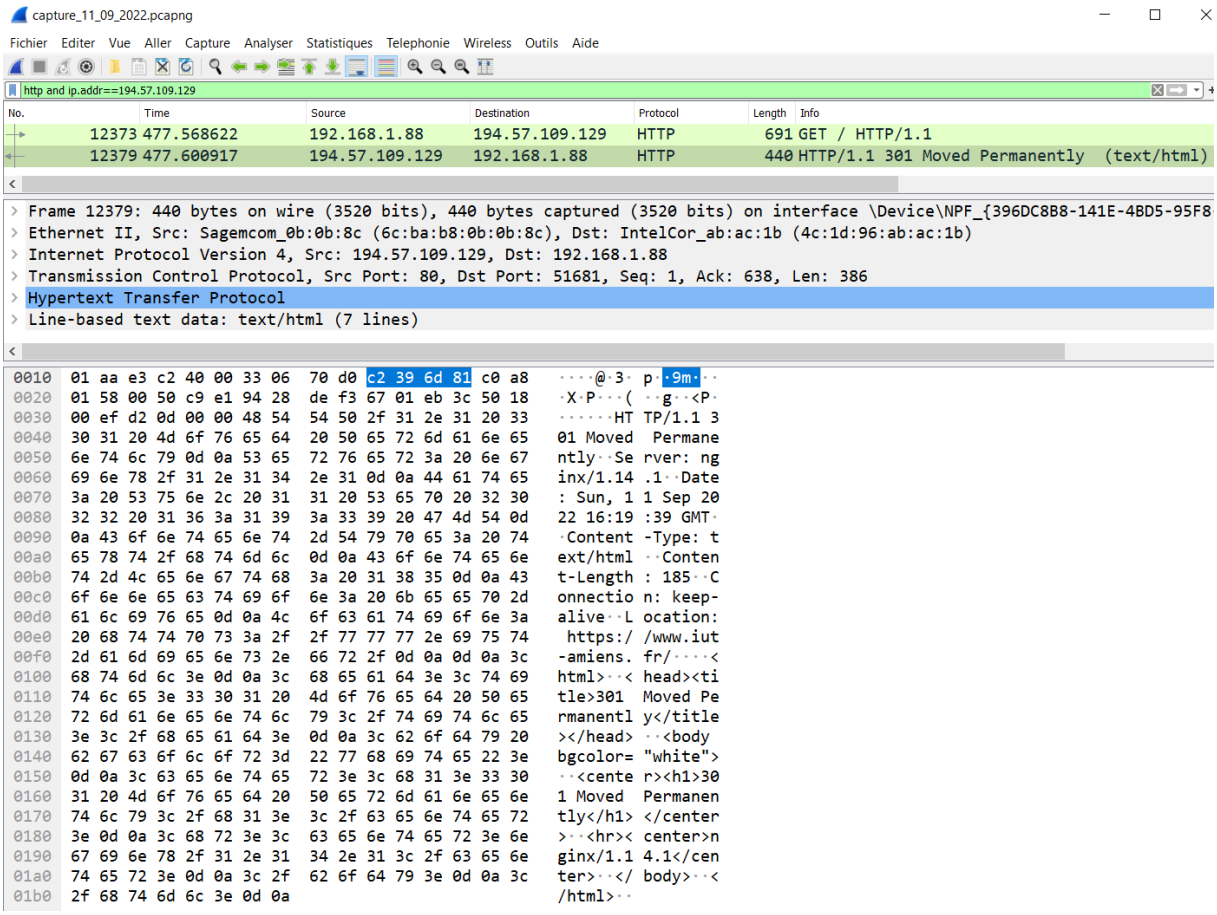
Pour retrouver une ou plusieurs trames correspondant à la capture partie 1, on prends quelques critères de recherche :

Positionnement du filtrage : le protocole + adresse de la destination (URL).

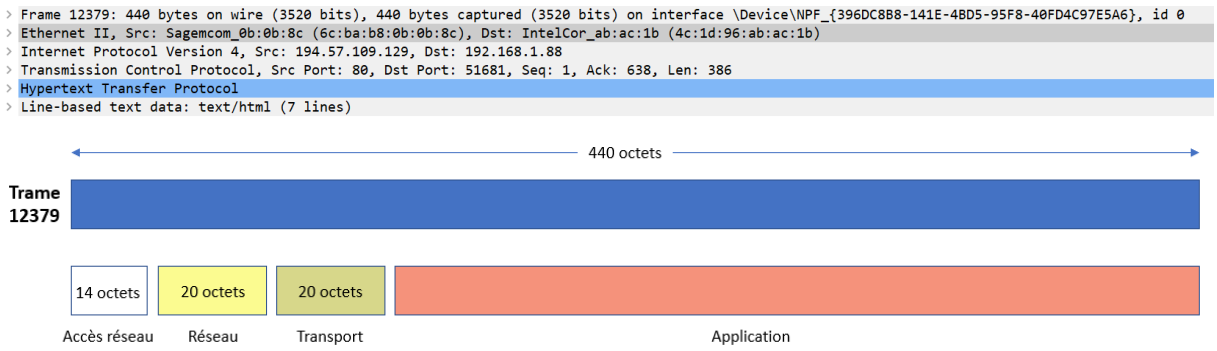
Protocole : http

URL (->@IP) : 194.57.109.129

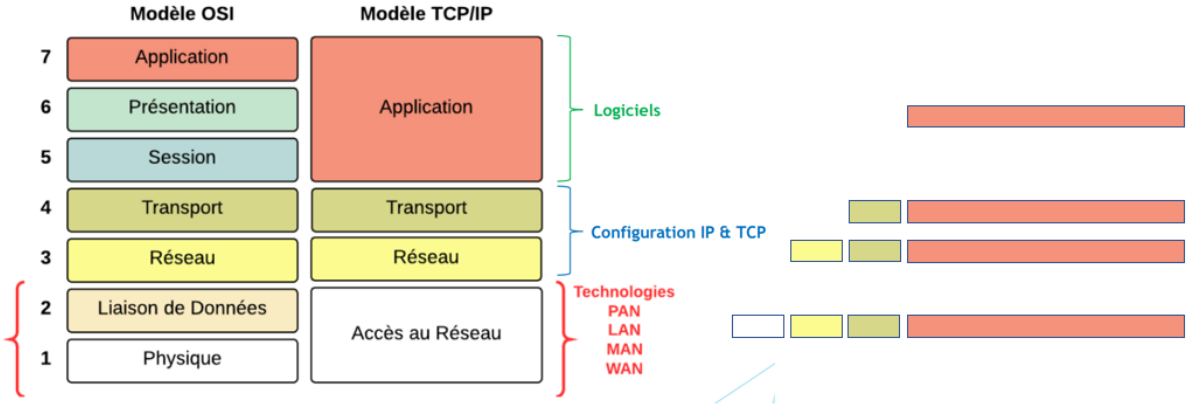
http and ip.addr==194.57.109.129



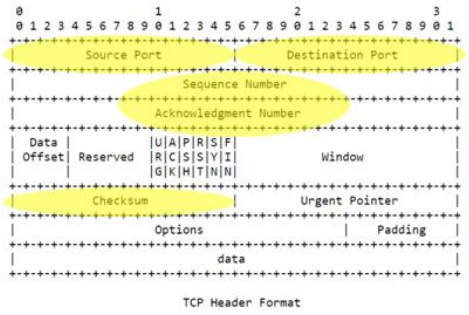
L'encapsulation de la trame



Interprétation TCP/IP



RFC 793

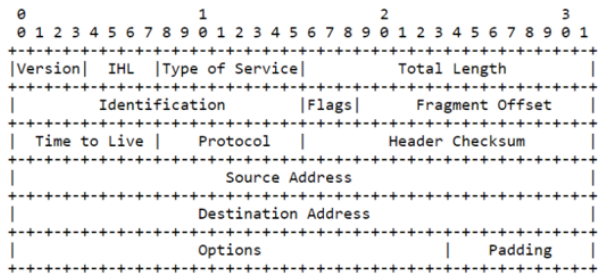


TCP Header Format

```
00 50 c9 e1
94 28 de f3
67 01 eb 3c
50 18 00 ef
d2 0d 00 00
```

```
Transmission Control Protocol, Src Port: 80, Dst Port: 51681, Seq: 1, Ack: 638, Len: 386
  Source Port: 80
  Destination Port: 51681
  [Stream index: 120]
  [TCP Segment Len: 386]
  Sequence Number: 1    (relative sequence number)
  Sequence Number (raw): 2485706483
  [Next Sequence Number: 387    (relative sequence number)]
  Acknowledgment Number: 638    (relative ack number)
  Acknowledgment number (raw): 1728179004
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
  Window: 239
  [Calculated window size: 30592]
  [Window size scaling factor: 128]
  Checksum: 0xd20d [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
  TCP payload (386 bytes)
```

RFC 791




```
45 00 01 aa
e3 c2 40 00
33 06 70 d0
c2 39 6d 81
c0 a8 01 58
```

```
Internet Protocol Version 4, Src: 194.57.109.129, Dst: 192.168.1.88
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 426
  Identification: 0xe3c2 (58306)
> Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 51
  Protocol: TCP (6)
  Header Checksum: 0x70d0 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 194.57.109.129
  Destination Address: 192.168.1.88
```