

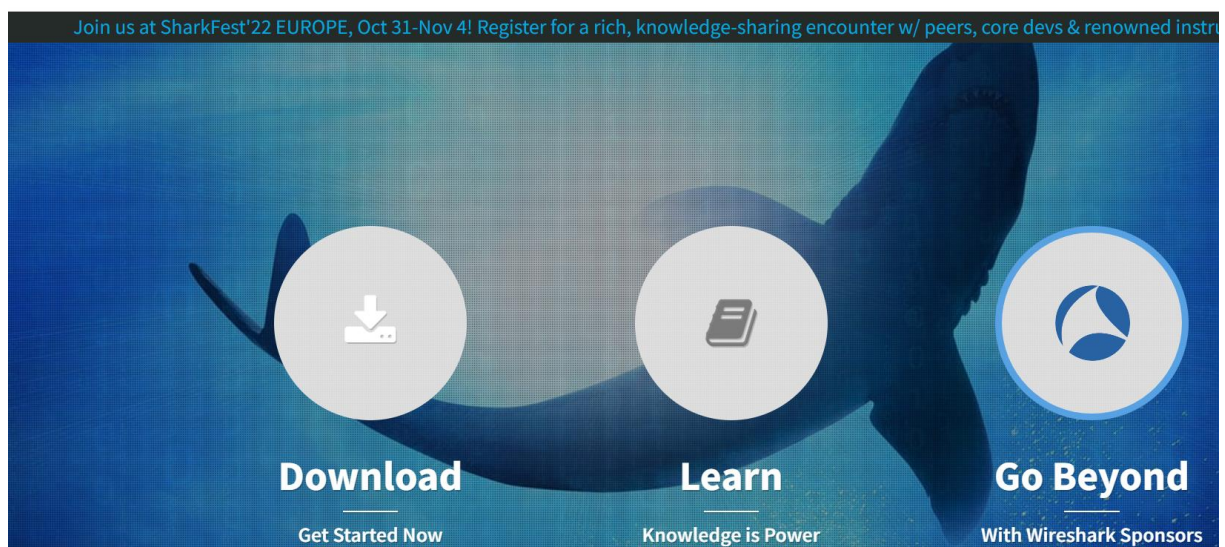
Module R3.06 Architecture des Réseaux	Travaux dirigés	TD2
Programme de BUT 3		
Séquence : Révision partie 2 Transferts de données dans le modèle OSI ou TCP/IP	Acquis en fin de séance <i>Le Modèle OSI</i> <i>Le Modèle TCP-IP</i> <i>Passage dans les couches</i> <i>Analyse d'une trame</i> <i>Datagramme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

Présentation de Wireshark

Stable Release (3.6.8) • September 7, 2022



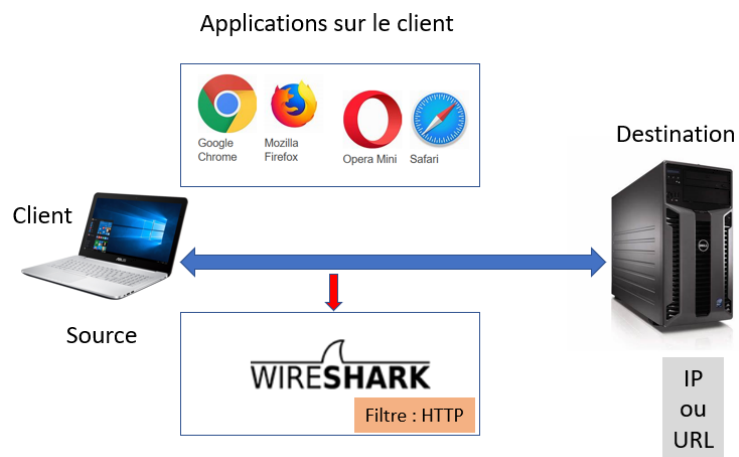
NEWS Get Acquainted ▾ Get Help ▾



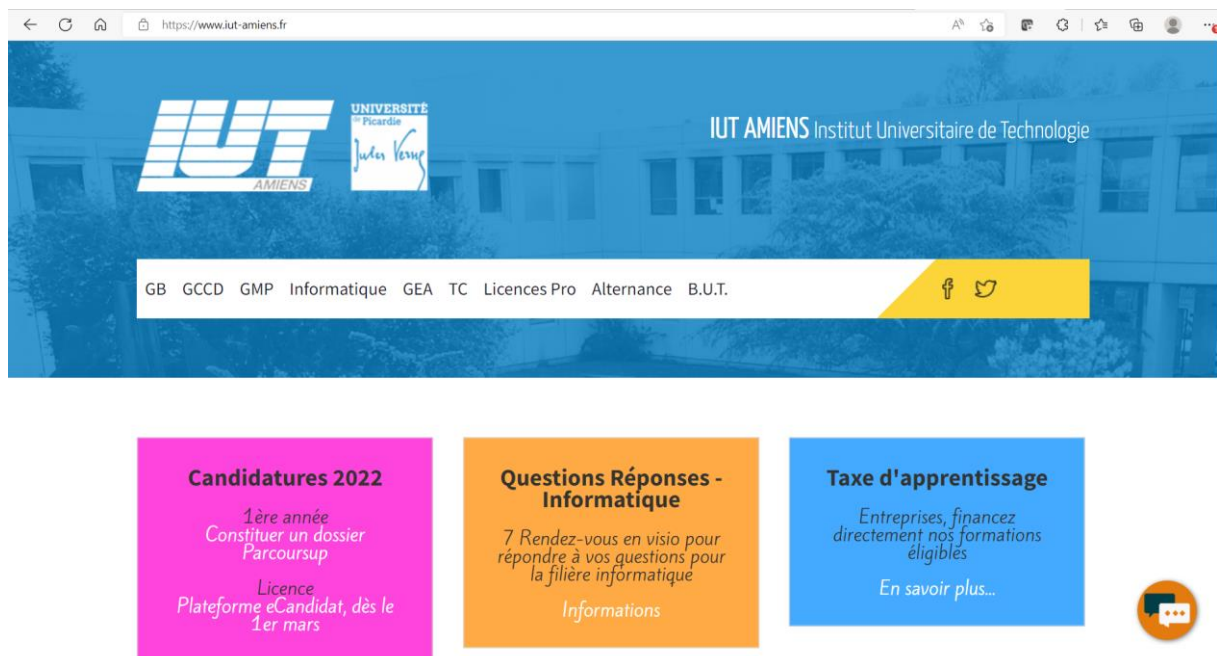
Présentation orale de l'outils (Rappel)

- <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 : bbbox.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'outil 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.

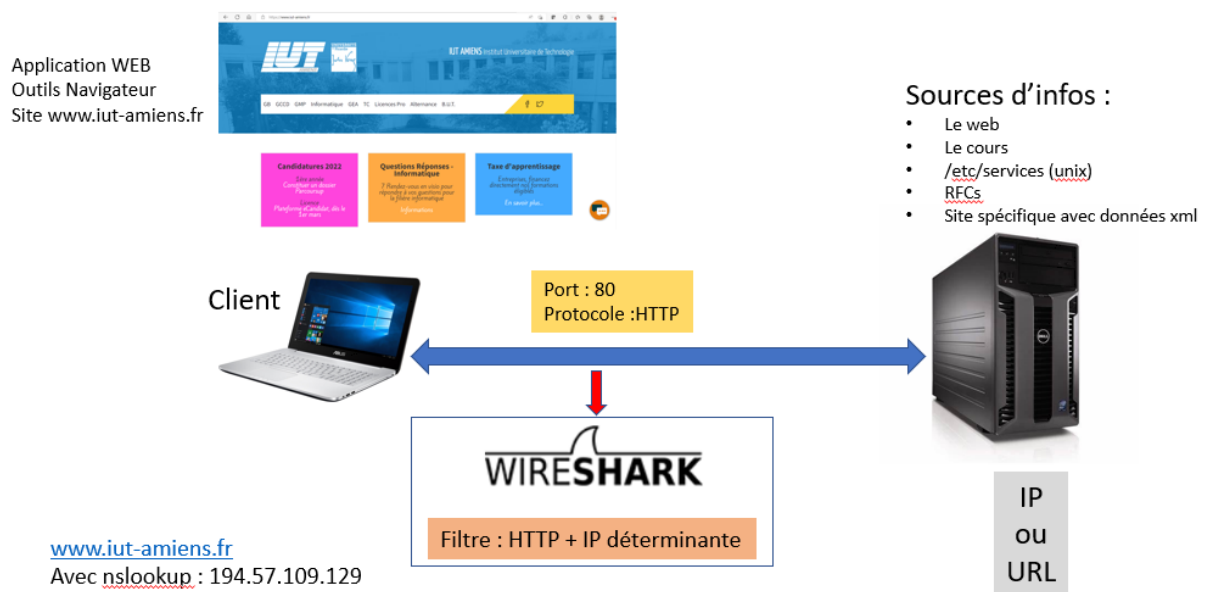
- ipconfig
- ipconfig /all

- 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

capture_11_09_2022.pcapng

Fichier Editor Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

http and ip.addr==194.57.109.129

No.	Time	Source	Destination	Protocol	Length	Info
12373	477.568622	192.168.1.88	194.57.109.129	HTTP	691	GET / HTTP/1.1
12379	477.600917	194.57.109.129	192.168.1.88	HTTP	440	HTTP/1.1 301 Moved Permanently (text/html)

<

> Frame 12379: 440 bytes on wire (3520 bits), 440 bytes captured (3520 bits) on interface \Device\NPF_{396DC8B8-141E-4BD5-95F8-40FD4C97E5A6}, id 0

> Ethernet II, Src: Sagemcom_0b:0b:8c (6c:ba:b8:0b:0b:8c), Dst: IntelCor_ab:ac:1b (4c:1d:96:ab:ac:1b)

> Internet Protocol Version 4, Src: 194.57.109.129, Dst: 192.168.1.88

> Transmission Control Protocol, Src Port: 80, Dst Port: 51681, Seq: 1, Ack: 638, Len: 386

> Hypertext Transfer Protocol

> Line-based text data: text/html (7 lines)

<

```
0010 01 aa e3 c2 40 00 33 06 70 d0 c2 39 6d 81 c0 a8 ....@.3.p.9m...
0020 01 58 00 50 c9 e1 94 28 de f3 67 01 eb 3c 50 18 .X.P...(.g.<P.
0030 00 ef d2 0d 00 00 48 54 54 50 2f 31 2e 31 20 33 .....HT TP/1.1 3
0040 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 01 Moved Permane
0050 6e 74 6c 79 0d 0a 53 65 72 76 65 72 3a 20 6e 67 ntly..Se rver: ng
0060 69 6e 78 2f 31 2e 31 34 2e 31 0d 0a 44 61 74 65 inx/1.14 .1..Date
0070 3a 20 53 75 6e 2c 20 31 31 20 53 65 70 20 32 30 : Sun, 1 1 Sep 20
0080 32 32 20 31 36 3a 31 39 3a 33 39 20 47 4d 54 0d 22 16:19 :39 GMT.
0090 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 .Content -Type: t
00a0 65 78 74 2f 68 74 6d 6c 0d 0a 43 6f 6e 74 65 6e ext/html ..Conten
00b0 74 2d 4c 65 6e 67 74 68 3a 20 31 38 35 0d 0a 43 t-Length : 185..C
00c0 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d onnectio n: keep-
00d0 61 6c 69 76 65 0d 0a 4c 6f 63 61 74 69 6f 6e 3a alive..L ocation:
00e0 20 68 74 74 70 73 3a 2f 2f 77 77 77 2e 69 75 74 https:/ /www.iut
00f0 2d 61 6d 69 65 6e 73 2e 66 72 2f 0d 0a 0d 0a 3c -amiens. fr/....<
0100 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 html>...< head><ti
0110 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 tle>301 Moved Pe
0120 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 rmanentl y</title
0130 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 ></head> ...<body
0140 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e bgcolor= "white">
0150 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 ...<cente r><h1>30
0160 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 1 Moved Permanen
0170 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 tly</h1> </center
0180 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e >...<hr>< center>n
0190 67 69 6e 78 2f 31 2e 31 34 2e 31 3c 2f 63 65 6e ginx/1.1 4.1</cen
01a0 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c ter>...</ body>...<
01b0 2f 68 74 6d 6c 3e 0d 0a
```

L'encapsulation de la trame

> Frame 12379: 440 bytes on wire (3520 bits), 440 bytes captured (3520 bits) on interface \Device\NPF_{396DC8B8-141E-4BD5-95F8-40FD4C97E5A6}, id 0

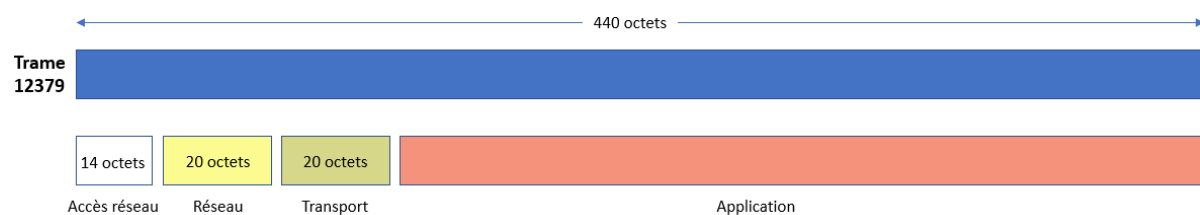
> Ethernet II, Src: Sagemcom_0b:0b:8c (6c:ba:b8:0b:0b:8c), Dst: IntelCor_ab:ac:1b (4c:1d:96:ab:ac:1b)

> Internet Protocol Version 4, Src: 194.57.109.129, Dst: 192.168.1.88

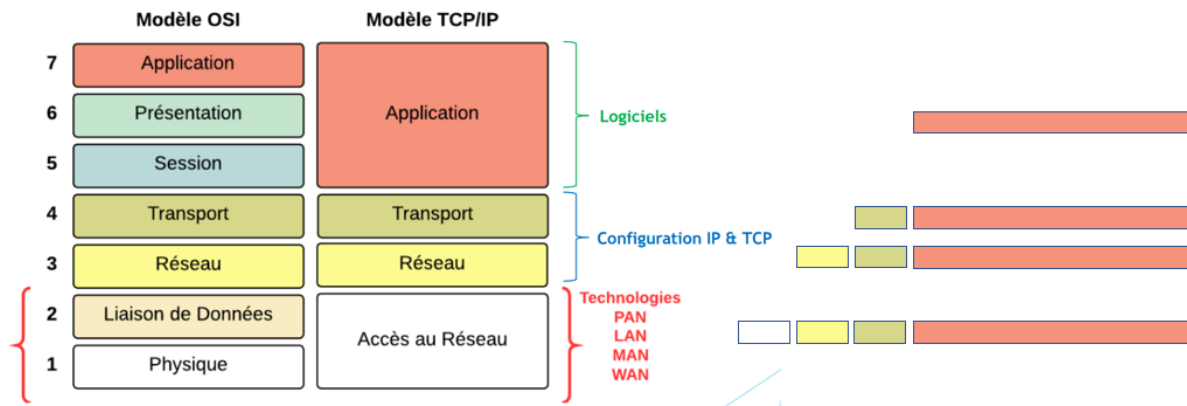
> Transmission Control Protocol, Src Port: 80, Dst Port: 51681, Seq: 1, Ack: 638, Len: 386

> Hypertext Transfer Protocol

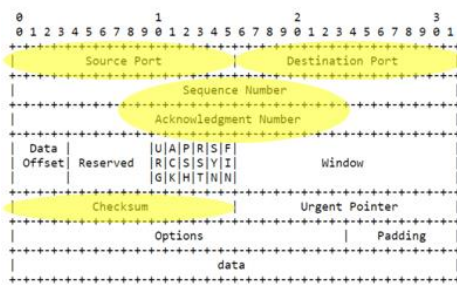
> Line-based text data: text/html (7 lines)



Interprétation TCP/IP



RFC 793

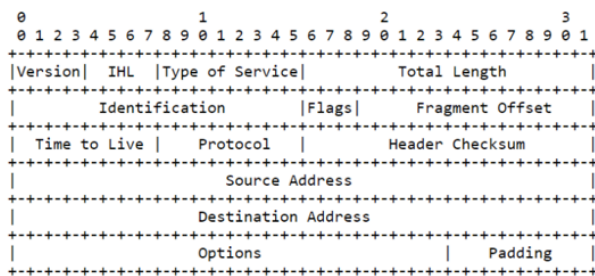


TCP Header Format

```
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): 2485786483
[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
```