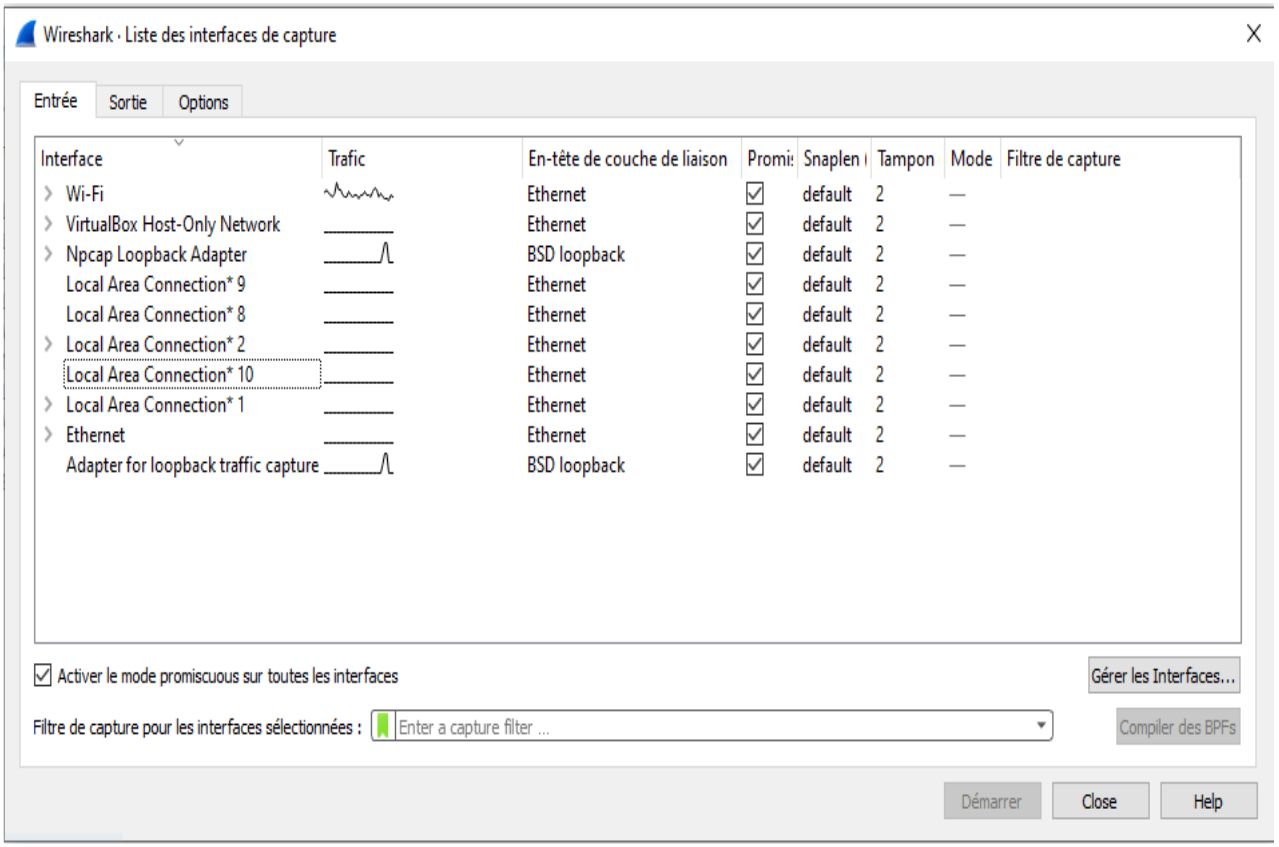
Ecole Supérieure de Technologie Essaouira
1ère année DUT IDSD1 2019-2020

المدرسة العليا للتكنولوجيا الصويرة
L'ÉCOLE SUPÉRIEURE DE TECHNOLOGIE – ESSAOUIRA

Administration Réseaux et Systèmes

TP N^0 1 : Simulateur Wireshark

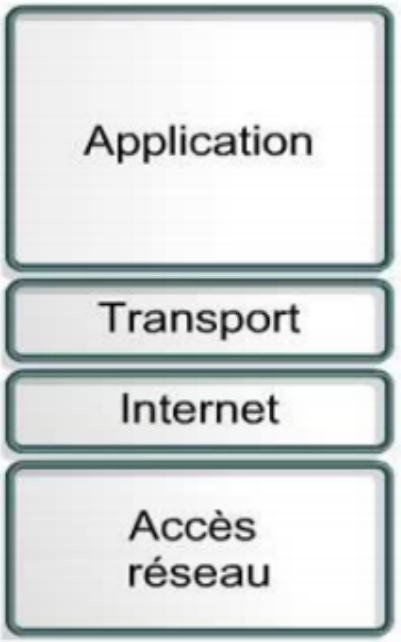
1. _____...
2. _____...
3. Lancer Wireshark et sélectionner Capture/ Interfaces…



4. Pourquoi on appelle TCP/IP une pile ? indiquez brièvement les fonctionnalités de chaque couche.

Le modèle TCP/IP comporte les quatre couches suivantes :

- **La couche application**
- **La couche transport**
- **La couche Internet**
- **La couche d'accès au réseau**



⇨ On appelle TCP/IP une pile parce qu'il empile plusieurs couches dans une seule couche

Couche Accès réseau :

Objectif :

Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion.

Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination.

Unité d'échanges : **Trame**

Couche Internet:

Objectif :

Réalise l'interconnexion des réseaux hétérogènes distants

permettre l'injection de paquets dans n'importe quel réseau et acheminement de ces paquets indépendamment les uns des autres jusqu'à destination

Gère le routage des paquets au travers des réseaux empruntés

Unité d'´echanges : **Datagramme**

Les protocoles :

- IP : Internet Protocol
- ICMP : Internet Control and Error Message Protocol
- ARP : Address Resolution Protocol
- RARP : Reverse Address Resolution Protoco

L'Architecture du modele TCP/IP

Couche Transport :

Objectif :
Même rôle que la couche Transport du modèle OSI
Transport correct de messages de manière fiable et de bout en bout entre l'émetteur et le récepteur.

Unité d'échanges : **Paquet.**

Les protocoles :

➢TCP : Transmission Control Protocol

- Protocole à remise garantie, orienté connexion, qui permet un acheminement sans erreur des messages.

➢UDP : User Datagram Protocol

- Plus simple que TCP mais non fiable (remise non garantie)
- Plus rapide que TCP

Couche Application :

Objectif :
La couche application fournit les protocoles et les fonctions nécessaires pour les applications clients. Il existe un nombre important de services fournis par la couche d'application.

Unité d'échanges : **Message.**

Quelques protocoles :

➢FTP : File Transfer Protocol
➢SMTP : Simple Mail Transfer Protocol
➢TFTP : Trivial File Transfer Protocol
➢DHCP : Dynamic Host Configuration Protocol
➢http : pour le web

5. Donner les couches et les rôles des protocoles réseau que vous connaissez indiqués dans la fenêtre affichée.

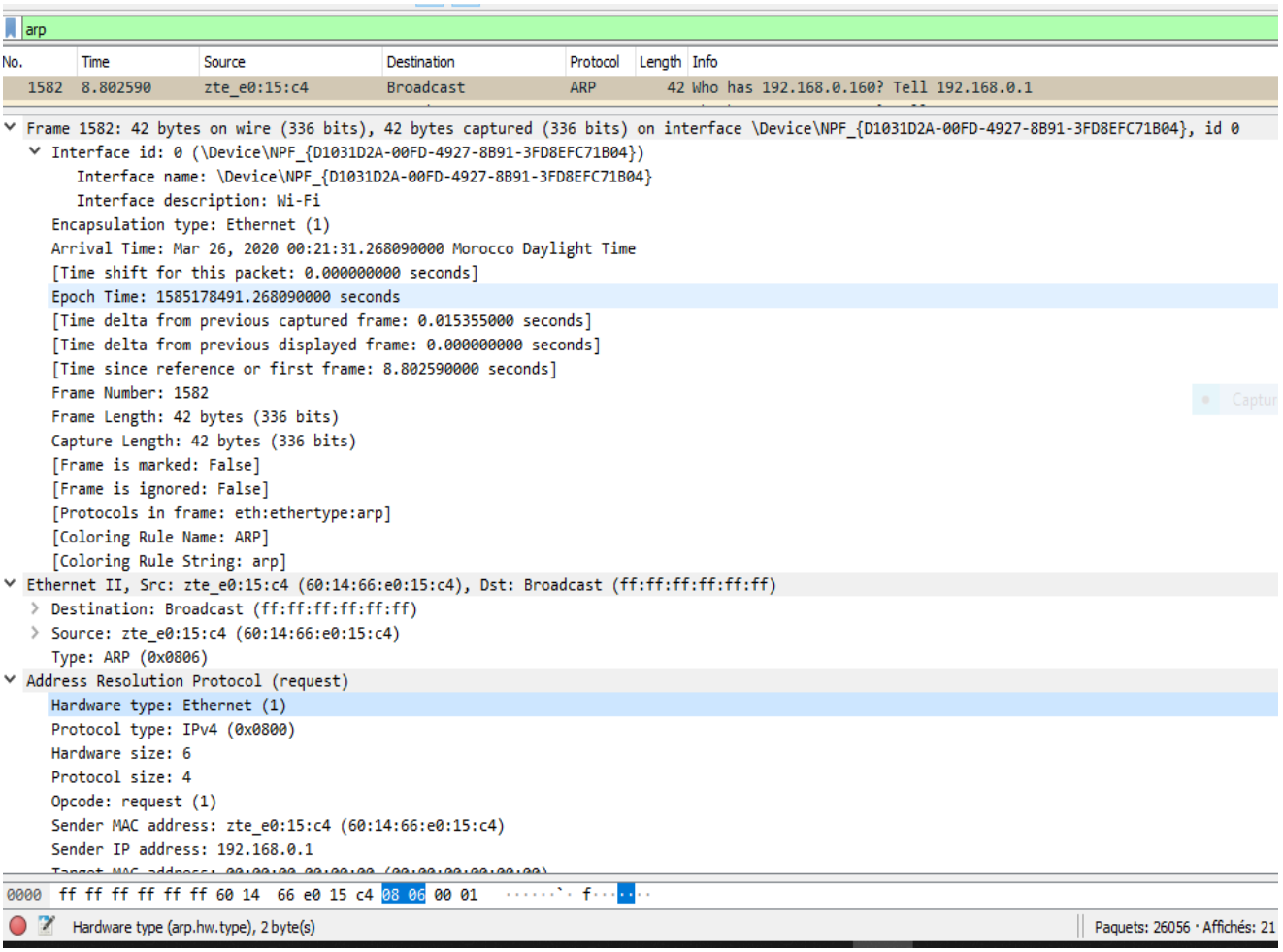
IP (Internet Protocol) : permet l'élaboration et le transport des datagrammes **IP** (les paquets de données), sans toutefois en assurer la « livraison ».

ICMP (Internet Control Message Protocol) : permet le contrôle des erreurs de transmission.

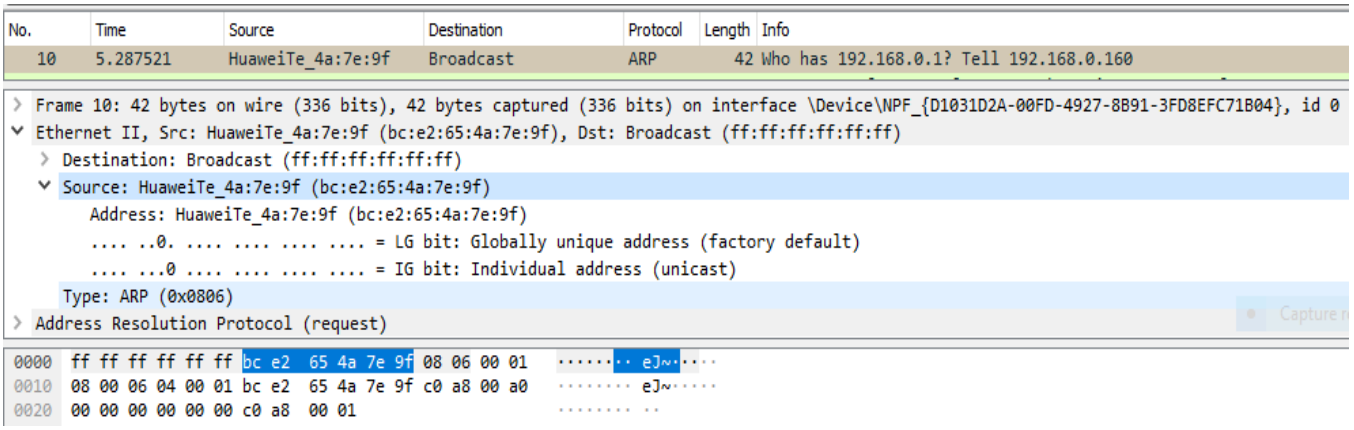
IGMP (Internet Group Management Protocol) : permet à des routeurs IP de déterminer de façon dynamique les groupes multicast qui disposent de clients dans un sous-réseau.

ARP (Adresse Résolution Protocol) : permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP

6. Sélectionner un exemple d'un paquet et analyser en détails ses divers champs



7. Sélectionner 3 paquets et visualiser leur contenu en hexadécimale. Calculer leurs équivalents binaires.

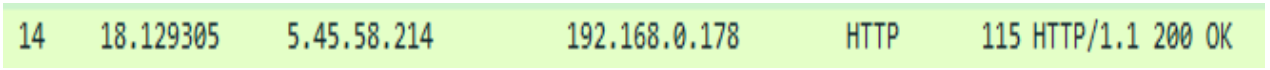


(bc e2 65 4a 7e qf) = (10111100111000100110010101001010011111101001111100001000000000110)2

8. Indiquer le rôle joué par Adresse MAC. Peut-on avoir plusieurs ordinateurs avec une même adresse MAC ?

 Le MAC (Media *Access Control*) : Est un identifiant physique d'une seule machine, et on ne peut pas avoir la même adresse MAC dans plusieurs machines.

9. Quels sont les protocoles supportés par les paquets : 14, 23, 101 et 134.



⇨ HTTP (HyperText Transfer Protocol) : protocole de communication client-serveur.

⇨ TCP (Transmission Control Protocol) : protocole de transport fiable, en mode connecté

⇨ ARP (**Adresse Résolution Protocol**) : utilisé pour traduire une adresse de **protocole** de couche réseau (typiquement une adresse IPv4) en une adresse de **protocole** de couche de liaison (typiquement une adresse MAC).

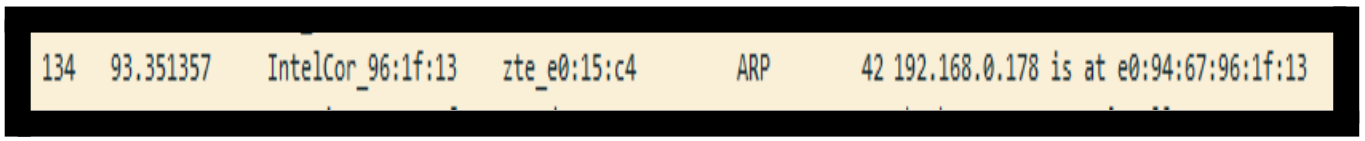
Wireshark fournit deux possibilités de filtrage : l'une au moment de la capture et l'autre au moment de l'affichage.

10. Quelle est la différence entre les deux en faisant des tests

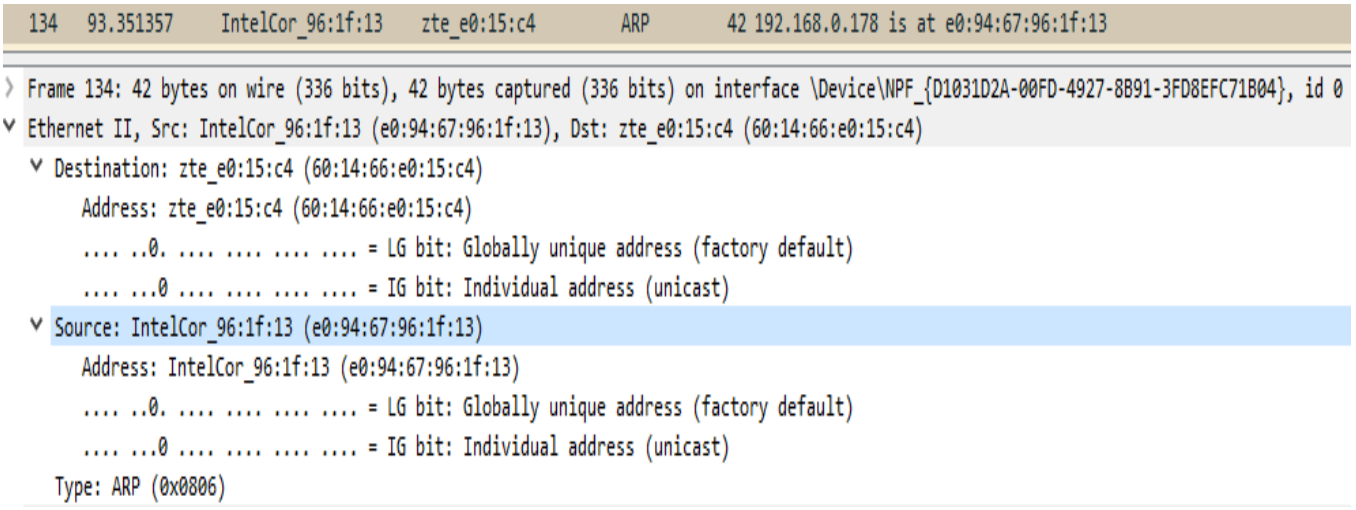
 Au moment de capture on bloque les autres ports et on prendra le seul Protocol sélectionné

 Au moment d'affichage on prendra tous les protocoles après on va sélectionner un seul pour afficher

11. Retrouver un paquet ARP. Indiquer la correspondance entre une adresse IP et une adresse MAC pour deux machines.



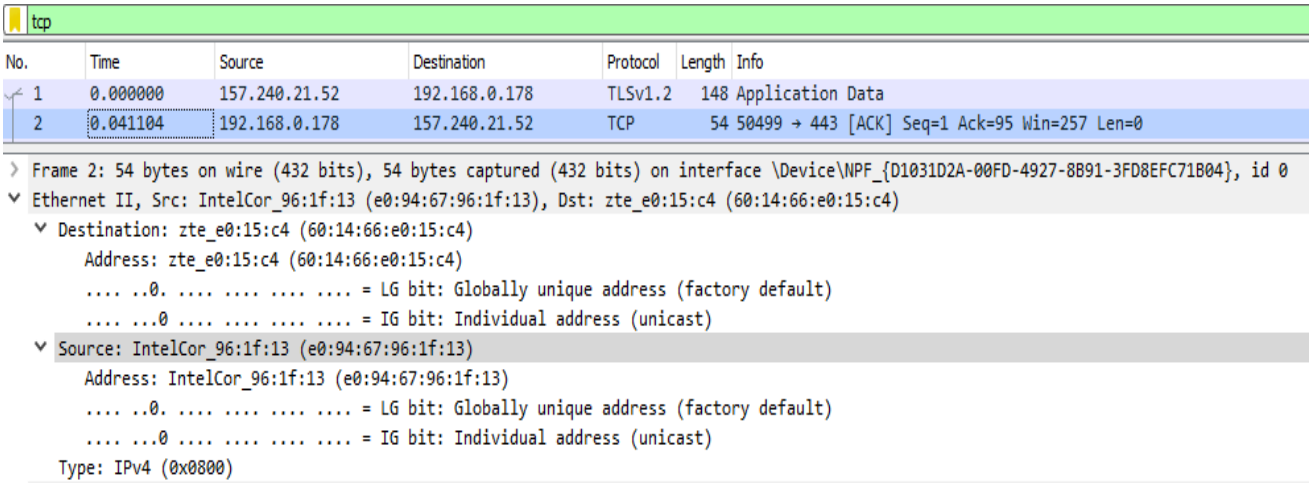
12. Interpréter le champ Destination pour un paquet ARP



13. Réaliser les filtres pour : IP, TCP, UDP, HTTP, ICMP et DHCP. Décrivez leurs caractéristiques et leurs champs.

IP (Internet Protocol) c'est un Protocol de la couche 3 (réseau) permettent un service d'adressage unique pour l'ensemble des terminaux connectés

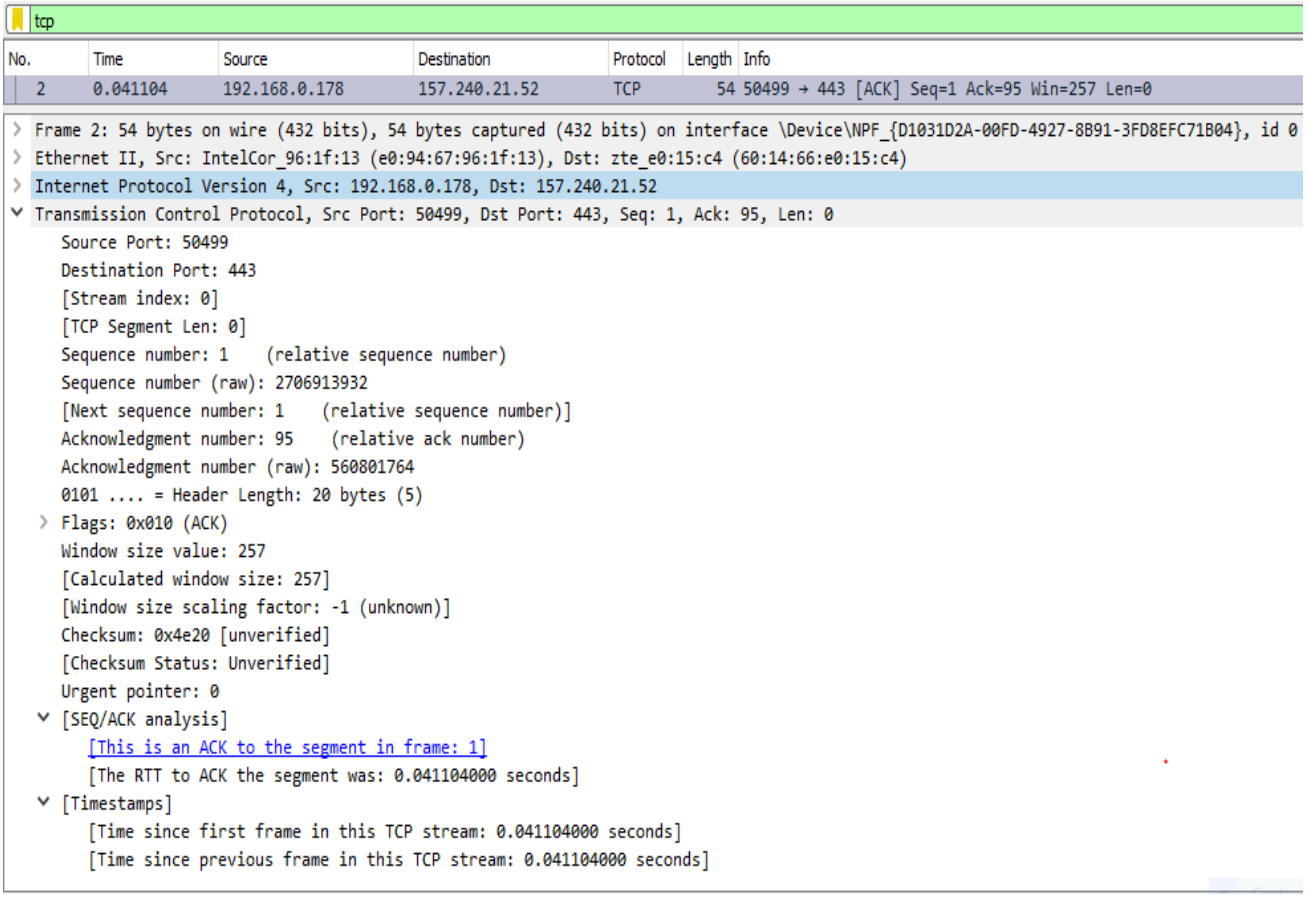
TCP (Transmission Control Protocol) : c'est un Protocol de la couche 4 (transport) protocole de transport fiable, en mode connecté.



UDP (User Datagram Protocol) : un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport du modèle OSI, quatrième couche

Mode déconnecté

14. Analyser le champ Continuation Data pour un paquet TCP.


tcp
No. Time Source Destination Protocol Length Info
2 0.041104 192.168.0.178 157.240.21.52 TCP 54 50499 → 443 [ACK] Seq=1 Ack=95 Win=257 Len=0
Frame 2: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{D1031D2A-00FD-4927-8B91-3FD8EFC71B04}, id 0
Ethernet II, Src: IntelCor_96:1f:13 (e0:94:67:96:1f:13), Dst: zte_e0:15:c4 (60:14:66:e0:15:c4)
Internet Protocol Version 4, Src: 192.168.0.178, Dst: 157.240.21.52
Transmission Control Protocol, Src Port: 50499, Dst Port: 443, Seq: 1, Ack: 95, Len: 0
Source Port: 50499
Destination Port: 443
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 2706913932
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 95 (relative ack number)
Acknowledgment number (raw): 560801764
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window size value: 257
[Calculated window size: 257]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x4e20 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[This is an ACK to the segment in frame: 1]
[The RTT to ACK the segment was: 0.041104000 seconds]
[Timestamps]
[Time since first frame in this TCP stream: 0.041104000 seconds]
[Time since previous frame in this TCP stream: 0.041104000 seconds]