Université de Tunis El Manar

Faculté des Sciences de Tunis

Département des Sciences de l'Informatique

Compte Rendu TP WIRESHARK

Étudiants : Houcem Hbiri,
Salim Brahem, Salim Nahdi, Mohamed Habib Manai

Matière : Cryptographie et sécurité informatique

Filière : 4ème année cycle ingénieur en Génie Logiciel

Année Universitaire : 2024-2025

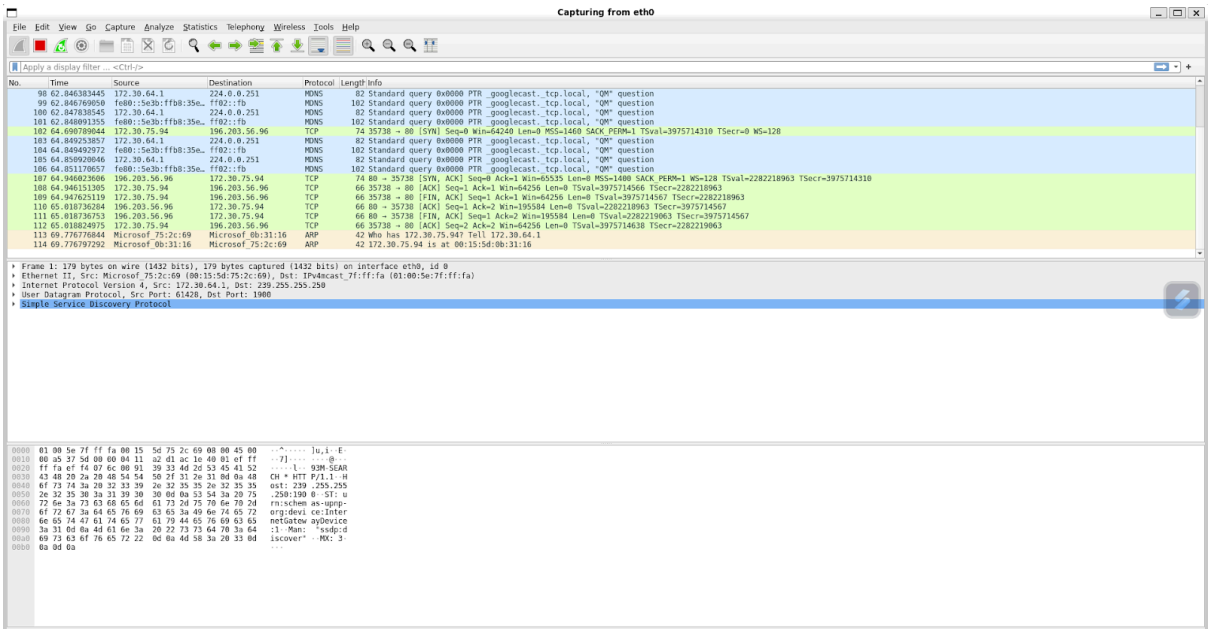
1) **Installez Wireshark en tapant la commande suivante : sudo apt-get install wireshark.**

```
houcem@ASUS Code sudo apt-get install wireshark
[sudo] password for houcem:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbcg729-0 libdouble-conversion3 libinput-bin libinput10 liblua5.2-0
  libmd4c0 libminizip1 libmtdev1 libnl-route-3-200 libqt5core5a
  libqt5dbus5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5
  libqt5printsupport5 libqt5svg5 libqt5widgets5 libsbc1 libsmi2ldbl
  libsnappy1v5 libspandsp2 libspeexdsp1 libssh-gcrypt-4 libwacom-bin
  libwacom-common libwacom9 libwireshark-data libwireshark15 libwiretap12
  libwsutil13 libxcb-icccm4 libxcb-image0 libxcb-keysyms1
  libxcb-render-util0 libxcb-util1 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate
  geoip-database geoip-database-extra libjs-leaflet
  libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libbcg729-0 libdouble-conversion3 libinput-bin libinput10 liblua5.2-0
  libmd4c0 libminizip1 libmtdev1 libnl-route-3-200 libqt5core5a
  libqt5dbus5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5
  libqt5printsupport5 libqt5svg5 libqt5widgets5 libsbc1 libsmi2ldbl
  libsnappy1v5 libspandsp2 libspeexdsp1 libssh-gcrypt-4 libwacom-bin
  libwacom-common libwacom9 libwireshark-data libwireshark15 libwiretap12
  libwsutil13 libxcb-icccm4 libxcb-image0 libxcb-keysyms1
  libxcb-render-util0 libxcb-util1 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common
  wireshark-qt
0 upgraded, 45 newly installed, 0 to remove and 65 not upgraded.
Need to get 40.1 MB of archives.
After this operation, 183 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 libdouble-conver
sion3 amd64 3.1.7-4 [39.0 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libqt5co
re5a amd64 5.15.3+dfsg-2ubuntu0.2 [2006 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy/main amd64 libmtdev1 amd64 1.1.
```

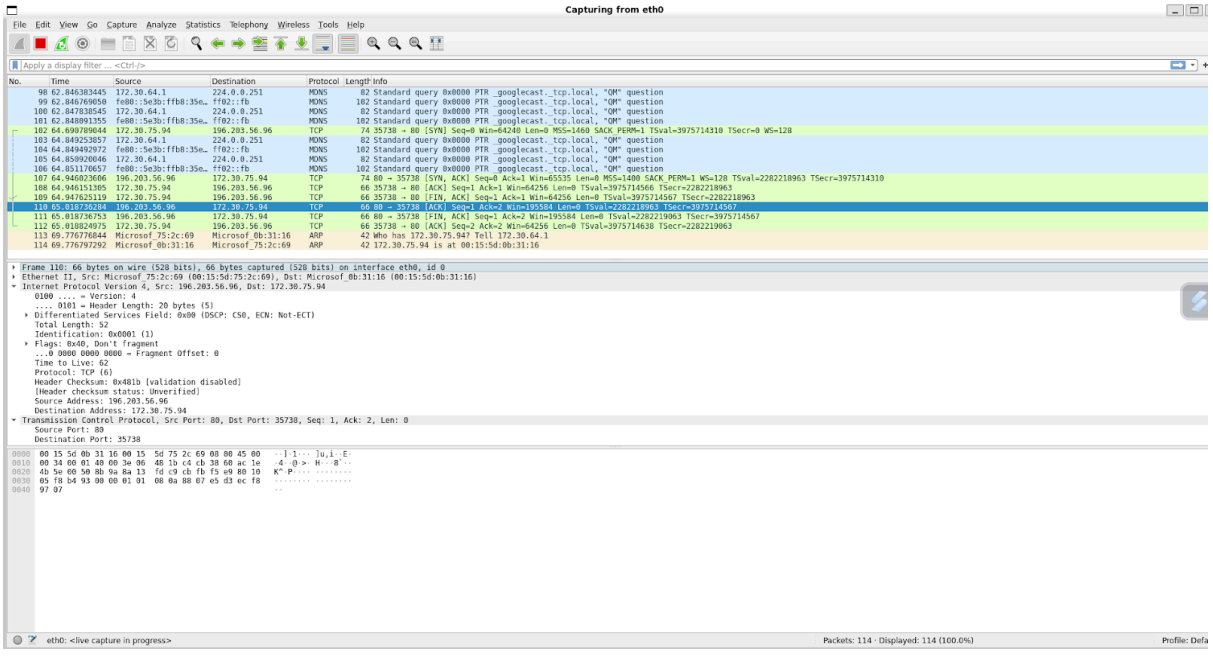
```
Setting up libqt5multimedia5-plugins:amd64 (5.15.3-1) ...
Setting up libqt5svg5:amd64 (5.15.3-1) ...
Setting up wireshark-qt (3.6.2-2) ...
Setting up wireshark (3.6.2-2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for shared-mime-info (2.1-2) ...
Processing triggers for udev (249.11-0ubuntu3.12) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
/sbin/ldconfig.real: /usr/lib/wsl/lib/libcuda.so.1 is not a symbolic link

houcem@ASUS Code
```

2) Démarrez une capture de trame sur l'interface WLAN en allant dans le menu Capture, en sélectionnant l'interface correspondante.



3) Interprétez l'interface de l'analyseur.



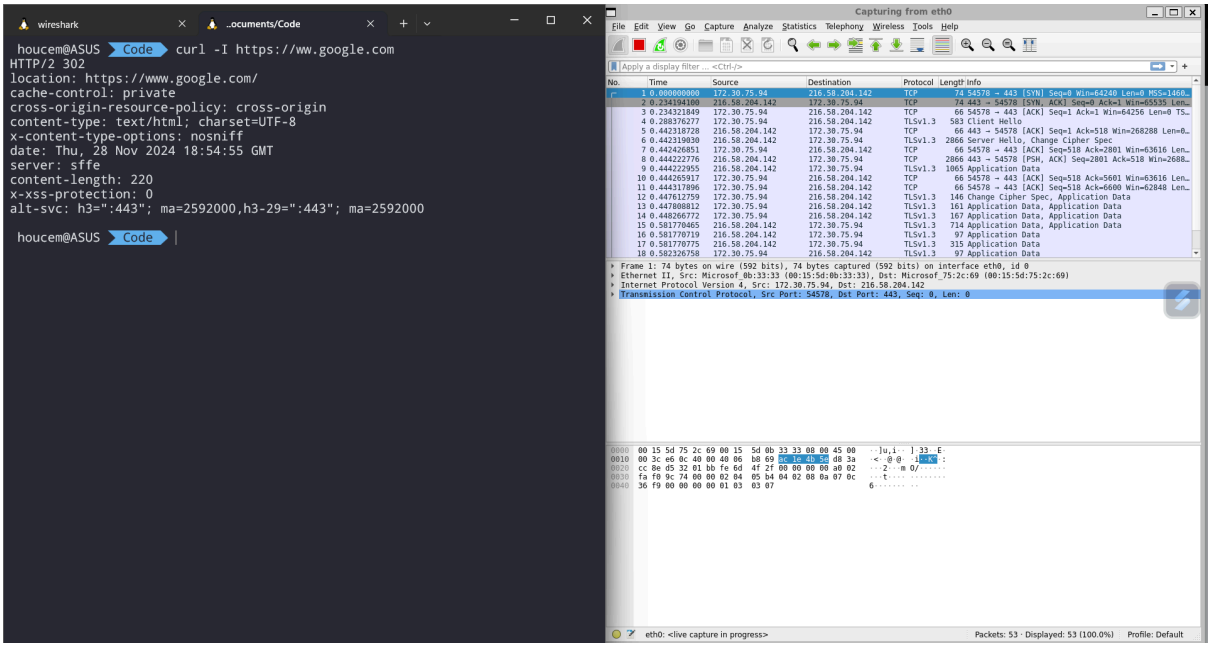
L'interface de l'analyseur Wireshark présentée permet d'examiner en détail les paquets réseau capturés. La fenêtre principale est divisée en plusieurs sections.

En haut, une liste des paquets affiche des informations essentielles telles que le numéro du paquet, l'heure de capture, les adresses IP source et destination, le protocole utilisé, la longueur des paquets, et un résumé des données échangées.

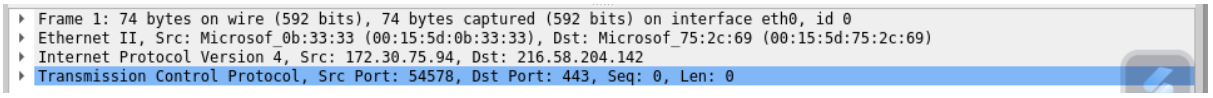
La section centrale donne des détails approfondis sur les couches réseau et transport (Ethernet, IP, TCP/UDP, TLS, etc.), permettant d'explorer chaque trame selon son contexte technique.

Enfin, la partie inférieure montre les données brutes du paquet en hexadécimal et ASCII, utile pour une analyse fine ou un décryptage des échanges. Cette interface facilite l'identification des communications réseau, des anomalies ou des configurations spécifiques.

4) Connectez-vous à un site web quelconque et identifier les paquets ayant comme destination votre adresse IP. Utilisez la commande ifconfig pour identifier votre adresse
IP.

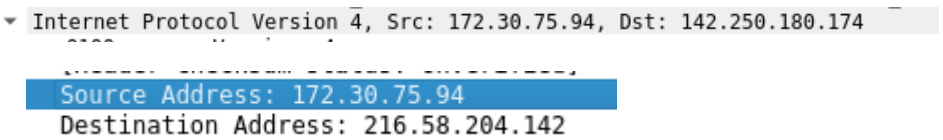


5) Indiquez les couches empilées qui ont été utilisées pour la transmission d'un paquet donnée. la zone centrale permet de visualiser clairement les différentes couches d'encapsulation du paquet.



6) Analysez l'un des paquets qui vous appartient :

a. Quelles sont les adresses source et destination ?



b. Quelle est la version de protocole réseau (Internet Protocol) utilisé ?

```
Internet Protocol Version 4, Src: 172.30.75.94, Dst: 216.58.204.142
```

c. Quelle est la taille l'en-tête IP ?

```
.... 0101 = Header Length: 20 bytes (5)
```

d. Quel est le protocole utilisé par la couche transport ?

```
Protocol: TCP (6)
```

e. Quels sont les ports utilisés ?

```
Transmission Control Protocol, Src Port: 54578, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 54578
    Destination Port: 443
```

f. Quelle est la taille de données transmises ?

```
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0,
```

7) A quoi consiste le filtrage des paquets ?

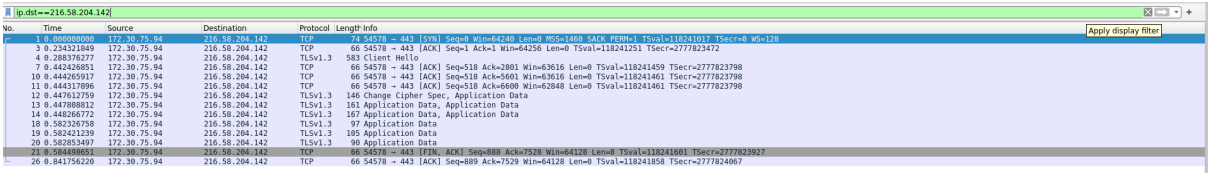
Le **filtrage des paquets** consiste à sélectionner uniquement les paquets pertinents selon des critères (protocole, IP, port, contenu) pour simplifier l'analyse et éliminer les données inutiles.

8) Comment s'effectue la mise en place d'un filtre ?

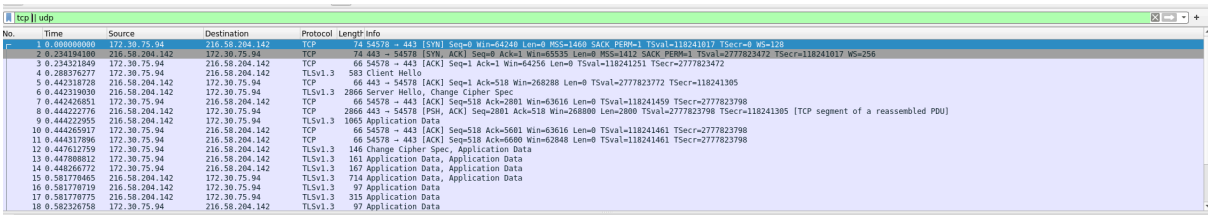
Dans la barre de filtrage au top (en vert dans la capture ci dessous)

9) Appliquez des filtres sur des adresses IP, des protocoles de routage, des protocoles de transport selon votre choix.

- sur l'adresse IP :



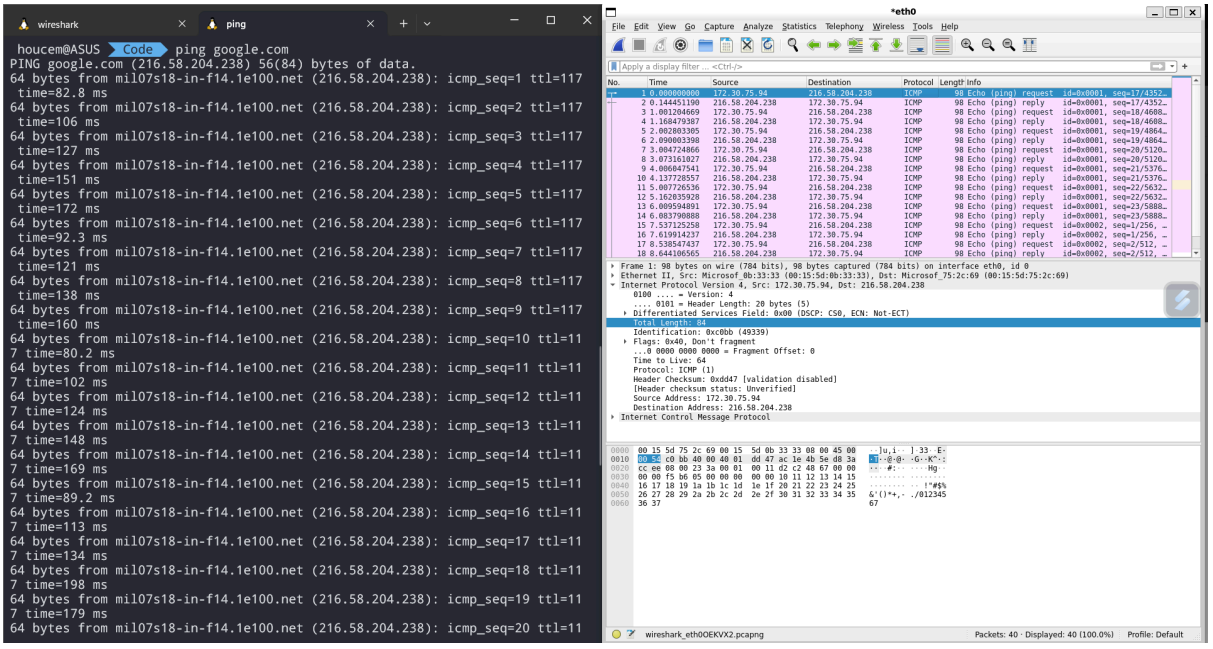
- sur le protocol (tcp ou udp)



10) A quoi consiste un Ping et quel est le protocole réseau utilisé pour faire le Ping ?

Un **Ping** consiste à tester la connectivité entre deux machines sur un réseau en envoyant des paquets pour mesurer la réponse.

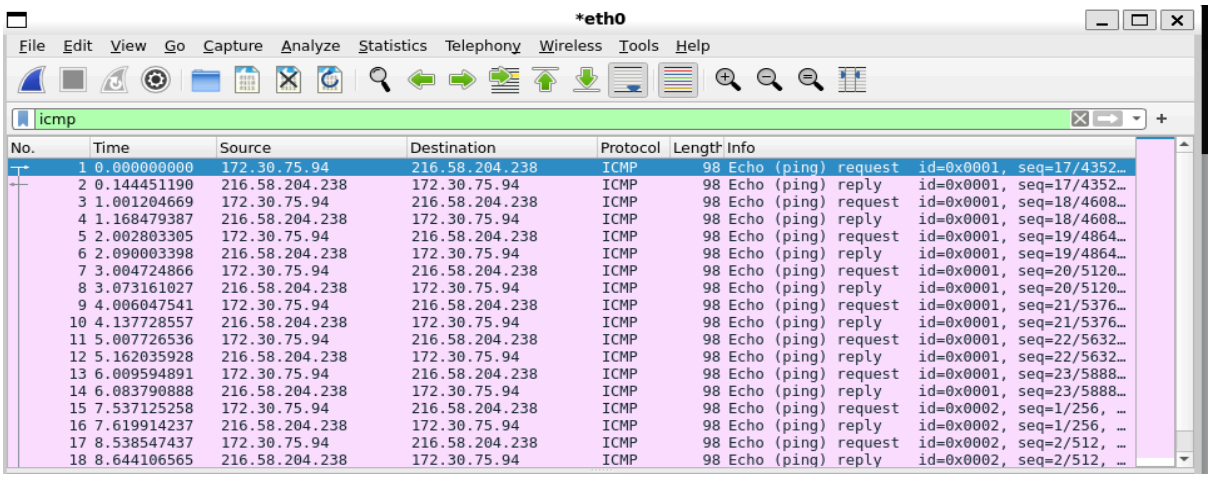
- **Protocole utilisé** : **ICMP** (Internet Control Message Protocol).



11) Utilisez un filtre d'affichage permettant de visualiser uniquement les trames correspondant à une commande Ping.

Pour afficher uniquement les trames correspondant à une commande **Ping** dans Wireshark, utilisez ce filtre

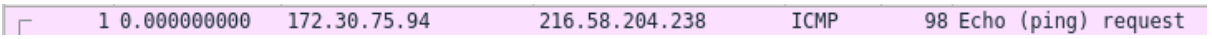
- icmp pour toutes les trames correspondant à une commande Ping
- icmp.type == 8 : Requête Ping (Echo Request).
- icmp.type == 0 : Pour les réponses (Echo Reply)



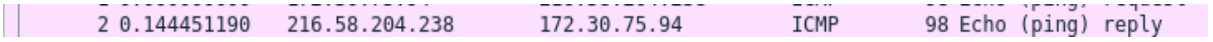
12) Analysez les trames visualisées. Combien trouvez-vous de trames ? A quoi correspondent-elles. Quels sont les protocoles présents dans une trame Ping ?

Nombre de trames :

- Chaque Ping génère **2 trames** :
  - Une requête **Echo Request** envoyée par l'émetteur. (`icmp.type == 8`).



  - Une réponse **Echo Reply (**réponse de la destination). (`icmp.type == 0`).



Protocoles présents dans une trame Ping :

- **ICMP** : Gère la requête et la réponse.
- **IP** : Encapsule ICMP pour l'acheminement.
- **Ethernet** : Utilisé pour la transmission sur le réseau local.