| **UF1. Introducció a les xarxes**  *NF1. Conceptes bàsics de xarxes i configuració inicial de dispositius*  NF1.3. Protocols i models Laboratori1. Veure el tràfic de la xarxa amb Wireshark |
| --- |

| Nom: | Nicola | Cognoms: | Roca Mühlemann |
| --- | --- | --- | --- |

**Índex de la pràctica**

[Entrega 1](#_30j0zll)

[Introducció 2](#_1fob9te)

[Tasques a realitzar 2](#_3znysh7)

# Entrega

* Format PDF amb el nom del fitxer: **UF1\_NF1.3\_L2\_Cognom\_Nom.pdf**
* Es valorarà positivament que l'activitat sigui ordenada, estructurada i ben documentada, amb captures de pantalla quan sigui el cas.
* Es valorarà positivament que documentis els inconvenients que trobis i la solució que hagis donat.
* Es valorarà negativament aquelles activitats que es presenten incompletes.

# Introducció

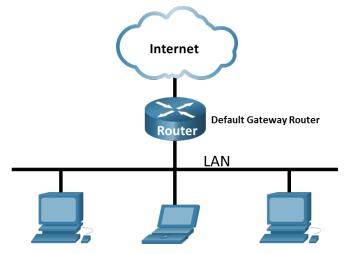
Wireshark és un analitzador de protocols software o també un "sniffer" de paquets que s'utilitza per a solucionar problemes de xarxa, anàlisis, desenvolupament de protocols i software, i en l'àmbit de l'educació. Mentre el flux de dades viatja per la xarxa, l'sniffer captura cada unitat de dades del protocol (PDU) i pot decodificar-la i analitzar el seu contingut segons la RFC correcta (estàndard) o altres especificacions.

És una eina útil si treballes al món de les xarxes, i es pot utilitzar en la majoria de les pràctiques

que realitzàrem per a l'anàlisi de les dades i la solució de problemes. En aquesta activitat

utilitzarem Wireshark per a capturar @IP del paquet de dades ICMP i @MAC de la trama Ethernet.

# Topologia



# Recursos necessaris

* 1 PC (windows o linux amb el programa wirshark instal·lat i connexió a internet)
* Un i varis PC de la mateixa xarxa local per a respondre a les sol·licituds de ping.

# Tasques a realitzar

## APARTAT 1. Captura i anàlisis de dades ICMP locals amb Wireshark

**En aquesta part, farem ping a un altre PC de la LAN i capturarà sol·licituds i respostes ICMP amb**

**Wireshark. També veurem dins de les trames capturades informació específica. Aquest anàlisi ens**

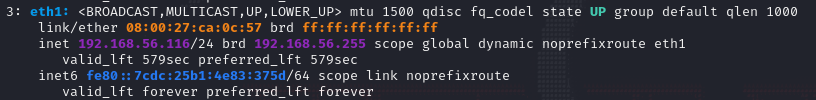
**ha d'ajudar a aclarir de quina manera s'utilitzen les capçaleres dels paquets per a transmetre**

**dades al destí.**

*Pas1: Esbrinar les direccions de interface del PC*

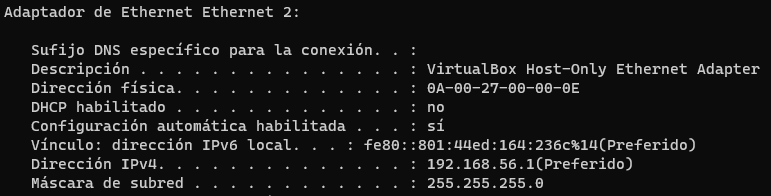
**1. En una finestra d'un terminal, introdueix la comand ifconfig (linux) o ipconfig /all (windows), obtindrem la @IP i @MAC.**

Màquina 1, Kali linux amb Wireshark: IP: 192.168.56.116



**2. L’altre component del grup haurà d’executar la mateixa comanda al seu PC. Us informareu de les dades obtingues (@IP i @MAC dels dos PCs)**

Màquina 2, Windows 11 per fer pings: IP: 192.168.56.1

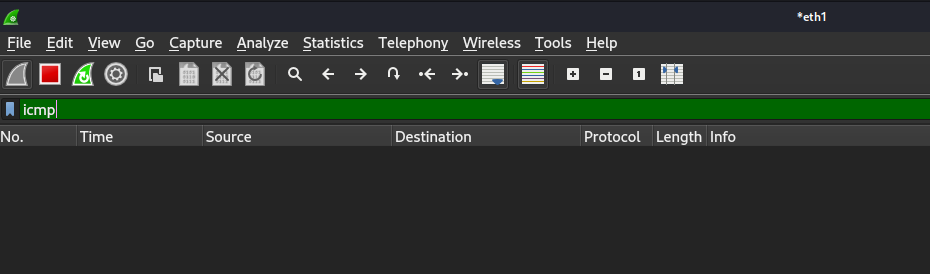


*Pas2: Iniciar wireshark i començar a capturar dades*

**1. Inicia wireshark. Fes doble clic a la interface desitjada per a iniciar la captura de paquets, assegurat que la interface escolida té tràfic.**

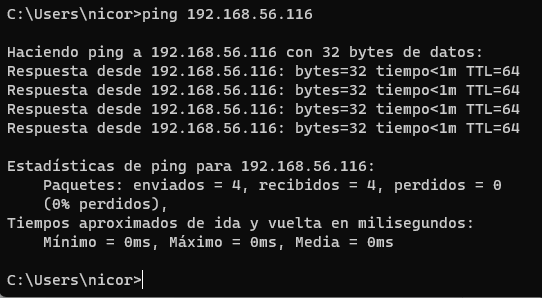
**2. La informació començarà a aparèixer, les línies de dades es podran veure en diferents colors segons el protocol.**

**3. En aquesta activitat només ens interessa mostrar les Pdus de ICMP (ping), per tant, escriurem icmp al quadre Filter a la part superior de Wirshark i pitjarem Enter, o farem clic al botó Apply per a veure només les Pdu ICMP (ping).**

****

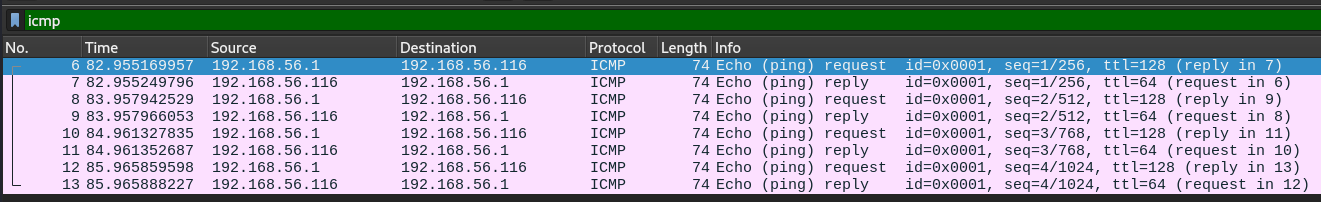
**4. El filtre anterior farà desaparèixer totes les dades de la finestra superior, però el programa segueix capturant el tràfic de la targeta. Obrirem un terminal i farem un ping a la @IP del nostre company/a**

Amb la màquina windows faré un ping a la màquina que te wireshark:

****

**5. Començarem a veure que apareixen un altre cop dades a la finestra superior de Wireshark**

Podem veure tots els paquets (icmp filtrats) amb wireshark, source (pc windows) d’es d’on s’originen, i destination (kali amb wireshark) on aniràn:

****

**6. Para la captura de dades fent clic a la icona Stop Capture**

****

*Pas3: Examinar les dades capturades*

**En aquest apartat examinarem les dades que s'han generat les sol·licituds de ping que hem fet. Les dades a wireshark es mostren en tres seccions:**

* **La secció superior mostra la llist de trames PDU capturades amb un resum de la informació de paquets IP numerats.**
* **La secció intermitja indica informació de la PDU per a la trama que s'ha seleccionat en la secció anterior, i separa les dades de la trama PDU capturada per la capa del protocol.**
* **La secció inferior mostra les dades de cada capa sense processar. Estan en format hexadecial i decimal.**

**1. Fes clic a les primeres trames PDU de la sol·licitud ICMP a la secció superior. Observa que la columna Source conté la @IP del teu PC i la columna destination conté la @IP del PC del teu company/a al que has fet ping.**

**2. Amb aquesta trama PDU seleccionada, accedeix a la secció central. Fes clic al signe que està a l’esquerra de la fila Ethernet II per a poder veure les @MAC origen i destí.**

****

1. **La direcció MAC origen coincideix amb la de la targeta de xarxa del teu PC?**

Podem veure que la mac d’origen (pc windows) coincideix amb la capturada

1. **La direcció MAC de destí coincideix amb la @MAC del PC del teu company/a?**

La direcció MAC de desti (pc kali) també coincideix.

1. **De quina manera el teu PC obté la @MAC del PC al que has fet ping?**

Amb el protocol ARP, en cas de desconèixer quina MAC té cada IP, s’envia un paquet ARP a la IP de broadcast preguntant a quina MAC correspón l’IP on volem arribar.

## APARTAT 2. Captura i analitza dades ICMP remots amb Wireshark

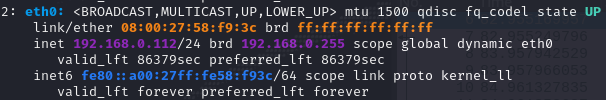
**En aquest apartat farem pings a hosts remots (hosts que no estan a la LAN) i examinarem les dades generades a partir d'aquests pings. Finalment compararem aquestes dades amb les capturades a l'apartat 1.**

*Pas1: Comencem capturant dades a la interface*

**1. Torna a iniciar la captura de dades**

Nota: he tingut de canviar la captura de dades a l’interfície eth0, aquesta correspón a una interfície bridge de virtualbox, ja a que abans estava utilitzant una interfície host-only.

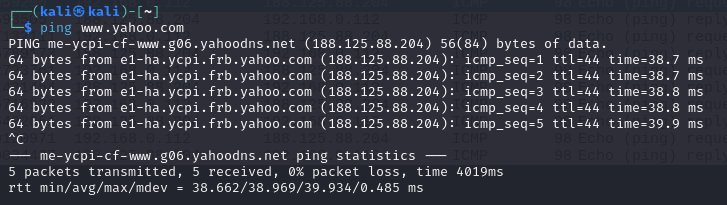
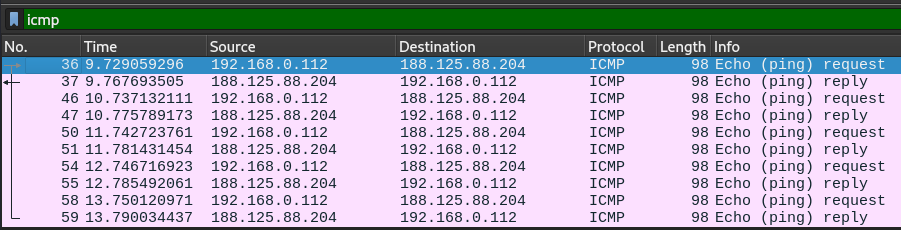
Aquestes són les dades de la interfície



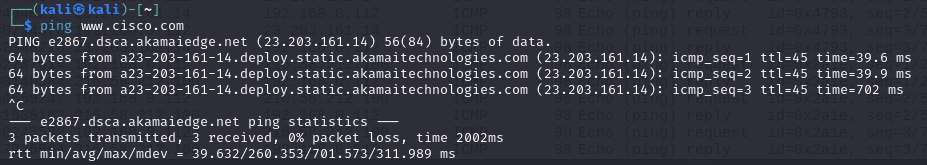
**2. S’obrira una finestra que et demana guardar les dades capturades anteriorment abans de començar una altra captura, no és necessari, fes clic a Continue without Saving.**

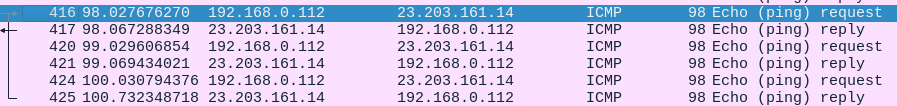
**3. Amb la captura activa, fes ping a les següents URL de llocs web des d’un terminal de Linux o símbol del sistema de Windows.**

1. [www.yahoo.com](http://www.yahoo.com)

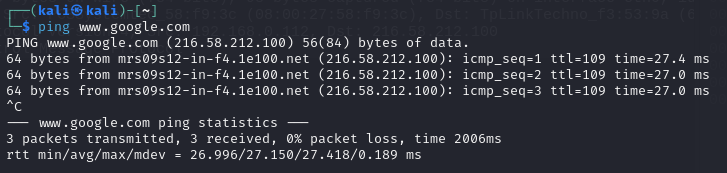
******

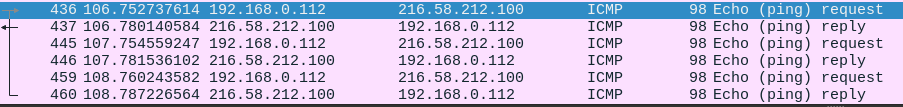
1. [www.cisco.com](http://www.cisco.com)





1. [www.google.com](http://www.google.com)



**

**4. Para la captura de dades fent clic a la icona Stop Capture.**

*Pas2: Inspecciona i analitza les dades dels hosts remots*

**1. Revisa les dades capturades a Wireshark i examina les @IP i @MAC dels tres llocs web als que has fet fet ping.**

1. **Indica les @IP i @MAC destí per als tres llocs web**

Per a yahoo.com és 188.125.88.204, MAC: 60:32:b1:f3:53:9a

Per a cisco.com és 23.203.161.14, MAC: 60:32:b1:f3:53:9a

I per google.com és 216.58.212.100, MAC: 60:32:b1:f3:53:9a

1. **De les dades anteriors quina informació t’ha semblat important o t’ha cridat l’atenció.**

Podem veure que la MAC es manté, ja a que ha de canviar de lan i passar per una gateway, aquesta serà la ultima MAC que el nostre ordinador podrà veure.

1. **Tenint en compte aquesta informació que t’ha cridat l’atenció, en que es diferència si la comparem amb el ping local que has fet a l’apartat 1?**

Com al ping local no teniem de canviar de lan, la mac de destí era el pc al que feiem ping en aquest cas serà la gateway.