

## Presentación del tema: Parámetros de Red en Equipos Terminales y Captura de Tramas

### Introducción:

Esta práctica está diseñada para familiarizarse con los parámetros de red de equipos terminales con sistema operativo Linux (AlmaLinux en este caso), así como para utilizar herramientas de análisis de protocolos como Wireshark. Además, se busca entender las diferencias en el comportamiento de la red cuando se utilizan concentradores (hubs) y conmutadores (switches).

### Objetivos:

1. **Identificar parámetros de red** en equipos con AlmaLinux, tales como dirección MAC, IP, máscara de red, pasarela, y DNS.
2. **Capturar y analizar tramas** de red utilizando Wireshark, observando las diferentes capas de la pila de protocolos.
3. **Comparar el funcionamiento** de una red basada en hubs con una red basada en switches, en cuanto al manejo y filtrado de tramas.

### Resultados Esperados:

- **Identificación clara** de parámetros de red en AlmaLinux mediante comandos como `ifconfig`, `hostname`, y `ip route`.
- **Captura y análisis de tramas** en Wireshark, observando la operación de protocolos como ICMP y FTP.
- **Diferencias visibles** entre el tráfico en una red con hub y una con switch, donde el hub transmite las tramas a todos los dispositivos, mientras que el switch lo hace de manera más controlada.
- **Inseguridad de FTP**: Observación de la falta de cifrado en protocolos como FTP, donde la información sensible (como usuarios y contraseñas) puede ser fácilmente capturada.

# Práctica 1

## Parámetros de red en equipos terminales y captura de tramas

---

### *Objetivos*

1. Identificar los parámetros de red y los comandos para su configuración en equipos terminales (hosts) con sistema operativo Alma Linux (Linux).
2. Conocer las funcionalidades básicas de un analizador de protocolos
3. Identificar algunas diferencias entre la operación de una red basada en concentradores (hubs) y otra basada en conmutadores (switches)

### *Marco Teórico*

Para que un equipo terminal (Host, PC) pueda utilizar los servicios de una red de computadoras, debe ser configurado con una serie de parámetros, como sus identificadores en la red local y en la subred IP<sup>1</sup> (las direcciones MAC e IP respectivamente). Cada sistema operativo tiene su propio conjunto de comandos (y de menús, si el sistema tiene una interfaz gráfica) para configurar y conocer el valor de estos parámetros. Los parámetros de red brindan información para identificar la topología lógica y física de la red.

Los monitores y analizadores de protocolos son herramientas muy valiosas para comprender el funcionamiento de la red; capturan las tramas que circulan por su segmento de red local y las despliegan en distintos formatos y capas. El analizador de protocolos de redes (*Wireshark*) que se utilizará en esta práctica permitirá identificar las distintas capas de la pila de protocolos que conforma la red.

### *Recursos de hardware, software e información por equipo de trabajo*

- Este documento está en Canvas
- Dos PCs con *AlmaLinux* como sistema nativo, por cada equipo de trabajo.
- Analizador de protocolos *Wireshark*
- Un conmutador (switch) 2960 y un concentrador (hub) por cada equipo de trabajo, ambos con puertos RJ45
- Cables UTP

### *Reporte*

---

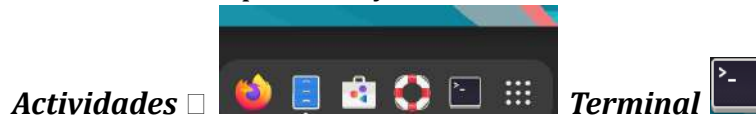
<sup>1</sup> Estos conceptos se estudiarán a profundidad en las sesiones de teoría.

- Se deben seguir las indicaciones de la Guía de Reporte

## Desarrollo

### I. *Parámetros de red en Linux*

1. Encienda su computadora y abra dos ventanas de terminal:



2. (En Linux, el comando **man** <comando> invoca el manual de ayuda para el comando correspondiente. Puede revisar el comando, la forma de invocar sus parámetros, etc. Para salir del manual, presione la tecla **q** [quit]). Para conocer la configuración de sus dos equipos con AlmaLinux, aplique los comandos **hostname** e **ifconfig**

¿Qué parámetros tiene su equipo?

Nombre de host **localhost.localdomain**

Identificador de la interfaz que está conectada a la red del laboratorio **eno1**

Dirección MAC de la interfaz ethernet (NIC) **d8:cb:8a:47:e8:c1 (ether)** Network Interface Card.

Dirección IP de su computadora **148.205.37.164 (inet)**

Máscara de red **255.255.252.0 (netmask)**

Dirección de difusión IP **148.205.39.255 (broadcast)**

Dirección y máscara de red de la interfaz de loopback **127.0.0.1 , 255.0.0.0**

3. Con cualquiera de los comandos *more*, *less* o *cat*, despliegue el contenido del archivo ***/etc/resolv.conf***. (Puede utilizar el manual para conocer más acerca de este archivo).

¿Cuáles son las direcciones del DNS primario y secundario? **148.205.228.11 , 148.205.228.17**

4. Encuentre la dirección de la pasarela por omisión con ayuda del comando ***ip route*** o de ***netstat -rn***.

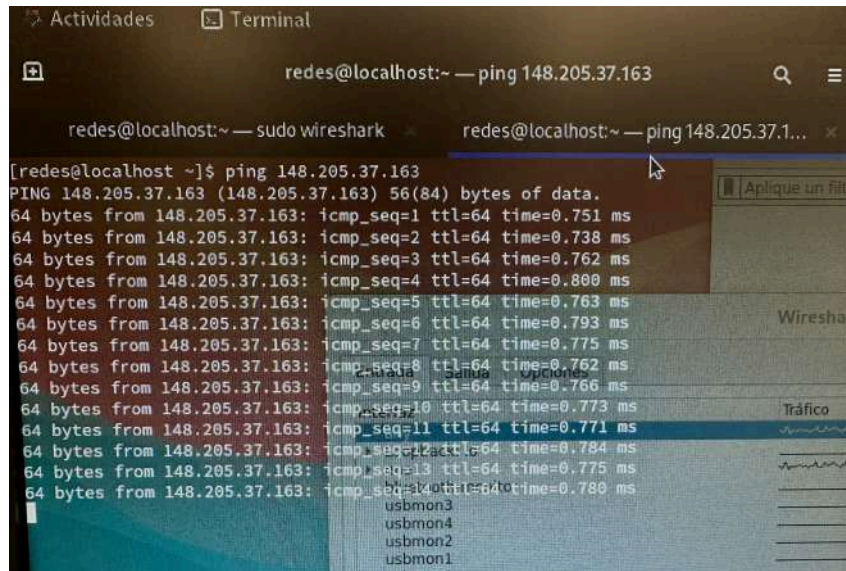
Dirección IP de la Pasarela (gateway) por omisión **192.168.3.1**

### II. *Captura de tramas con Wireshark, desde Linux.*

Anote los nombres y las direcciones IP de las dos computadoras del otro equipo de trabajo **148.205.37.164 , 148.205.37.163**

5. Lance un **ping** desde su computadora a la de al lado

Muestre el comando utilizado y el resultado obtenido.



The screenshot shows a terminal window with the title bar 'Actividades Terminal'. The prompt is 'redes@localhost:~ — ping 148.205.37.163'. The user has entered the command 'ping 148.205.37.163'. The output shows 13 successful ping responses from 148.205.37.163 to 148.205.37.163, each with 56(84) bytes of data and a TTL of 64. The response times range from 0.751 ms to 0.784 ms. A second terminal window titled 'redes@localhost:~ — sudo wireshark' is partially visible in the background.

```
[redes@localhost ~]$ ping 148.205.37.163
PING 148.205.37.163 (148.205.37.163) 56(84) bytes of data.
64 bytes from 148.205.37.163: icmp_seq=1 ttl=64 time=0.751 ms
64 bytes from 148.205.37.163: icmp_seq=2 ttl=64 time=0.738 ms
64 bytes from 148.205.37.163: icmp_seq=3 ttl=64 time=0.762 ms
64 bytes from 148.205.37.163: icmp_seq=4 ttl=64 time=0.800 ms
64 bytes from 148.205.37.163: icmp_seq=5 ttl=64 time=0.763 ms
64 bytes from 148.205.37.163: icmp_seq=6 ttl=64 time=0.793 ms
64 bytes from 148.205.37.163: icmp_seq=7 ttl=64 time=0.775 ms
64 bytes from 148.205.37.163: icmp_seq=8 ttl=64 time=0.762 ms
64 bytes from 148.205.37.163: icmp_seq=9 ttl=64 time=0.766 ms
64 bytes from 148.205.37.163: icmp_seq=10 ttl=64 time=0.773 ms
64 bytes from 148.205.37.163: icmp_seq=11 ttl=64 time=0.771 ms
64 bytes from 148.205.37.163: icmp_seq=12 ttl=64 time=0.784 ms
64 bytes from 148.205.37.163: icmp_seq=13 ttl=64 time=0.775 ms
64 bytes from 148.205.37.163: icmp_seq=14 ttl=64 time=0.780 ms
```

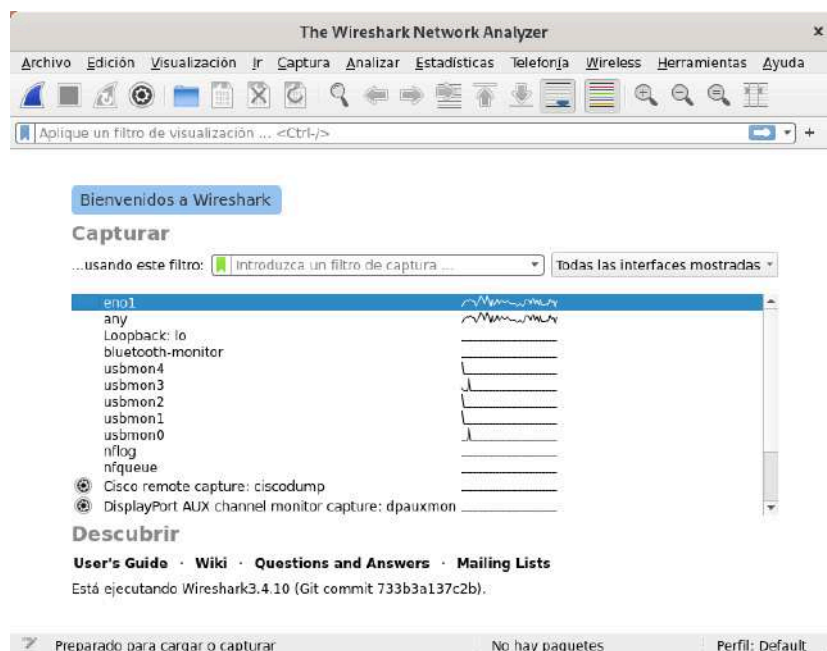
6. En esta sección se hará la conexión de las cuatro computadoras entre dos equipos de trabajo a través de un CONCENTRADOR o HUB (Brasilia, CdMexico, Brisbane, Tokio, Rennes, Creta).

¿Concentrador (HUB) a utilizar? **TOKYO**


Antes que nada, anote el número de las Rosetas (en el faceplate) a la que están conectadas sus computadoras. Rosetas **LI6-05 y LI6-11.**

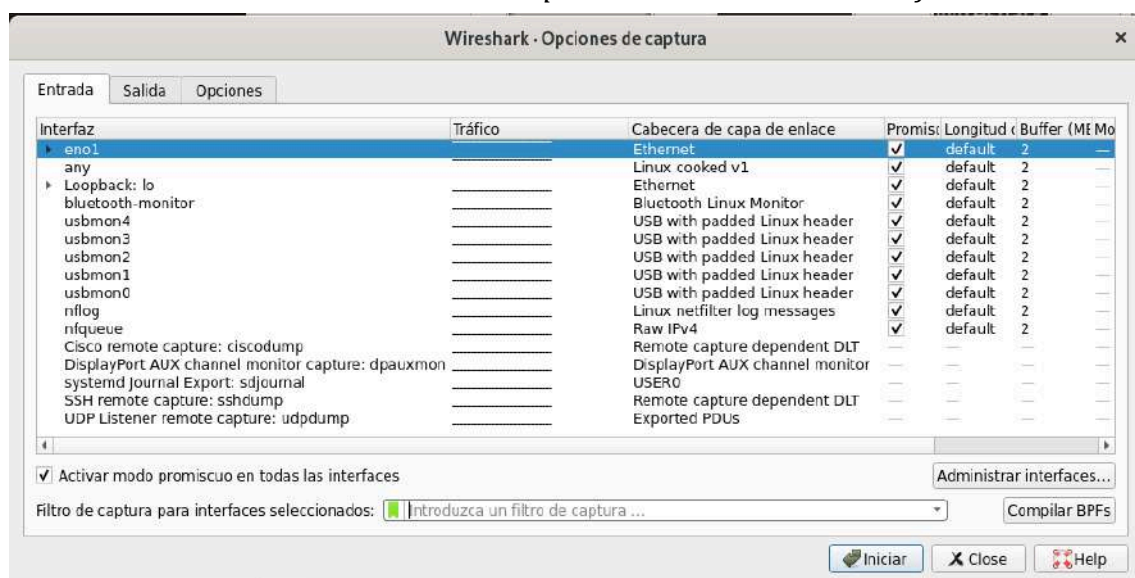
Desconecten los cables de las rosetas de su isla, al que están conectadas sus computadoras y conéctelos al HUB que le corresponda. POR FAVOR TRATE CON CUIDADO LOS CABLES. EVITE ROMPER LA PESTAÑA QUE FIJA EL CONECTOR.

7. Lance nuevamente un **ping** desde su computadora a la de al lado y verifique que se mantiene la conexión. También el otro equipo de trabajo debe hacerlo al mismo tiempo.
8. Para lanzar, desde la segunda terminal, *WireShark*, aplicando el comando “*sudo wireshark*”  
Se desplegará:



Este analizador de protocolos copia todas las tramas que pasan por la tarjeta NIC de la computadora, y las despliega.


9. Una vez en Wireshark, seleccione el menú *Capture-> Options*, o de click en . Se abrirá la ventana “*Capture Options*”, asegúrese de que este seleccionada la pestaña “*Entrada*”. También active “*Activar modo promiscuo en todas las interfaces*”.



En la ventana “*Capture Options*”, verifique que se encuentra seleccionado el adaptador de red de su equipo (*eno1*).



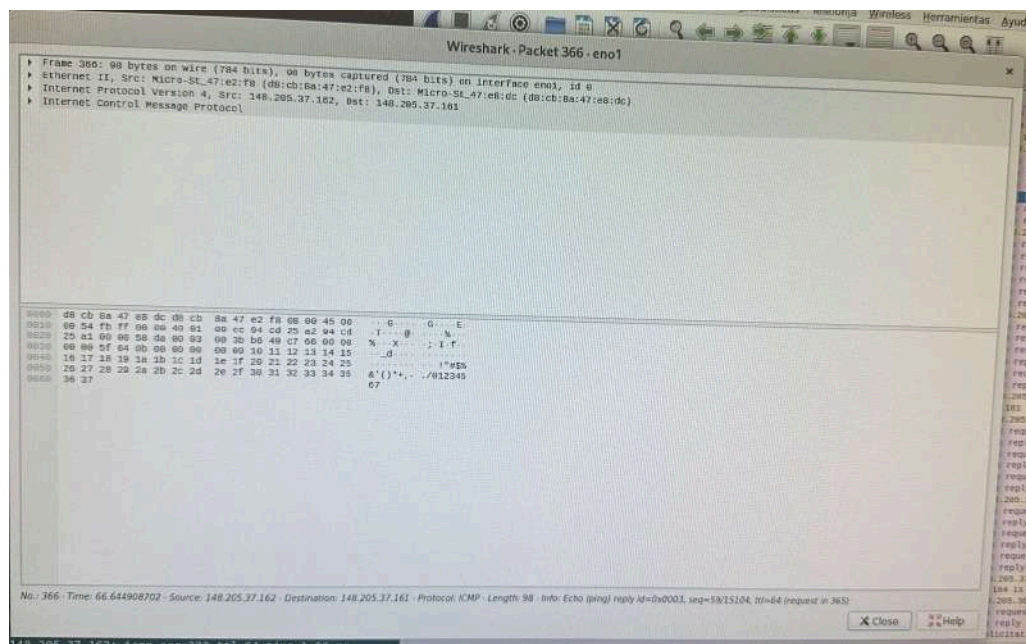
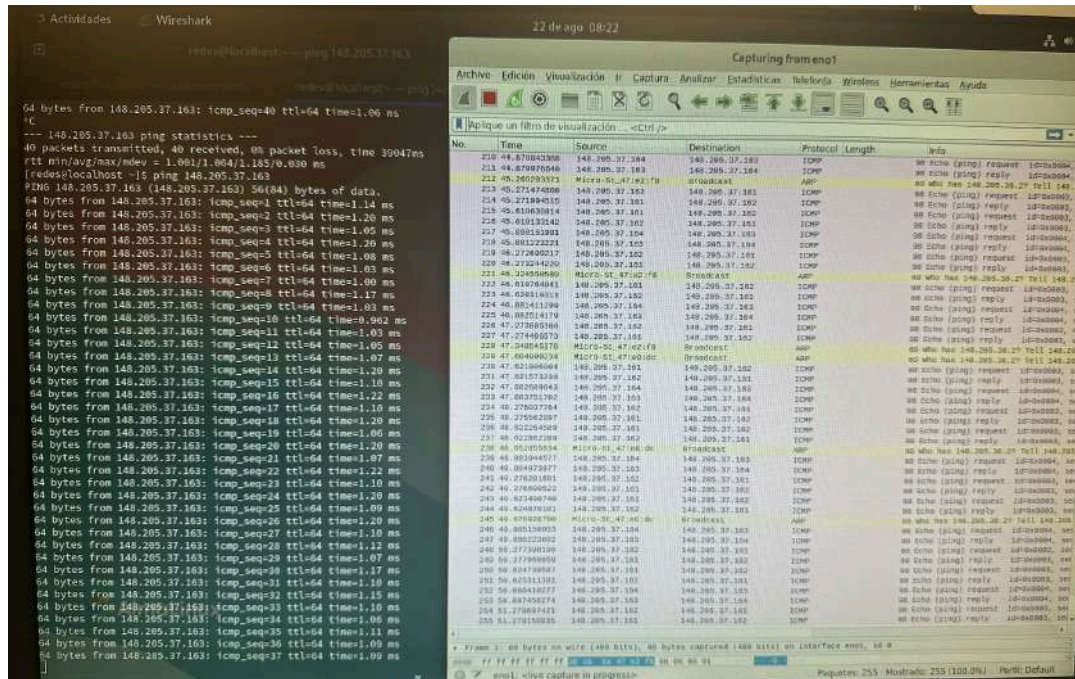
10. Para iniciar la captura de tráfico en el adaptador *eno1* dé clic en el botón “Start”, o 

Nota: Detenga la captura mediante el botón , después de un rato.

Puede reiniciar la captura de tráfico.

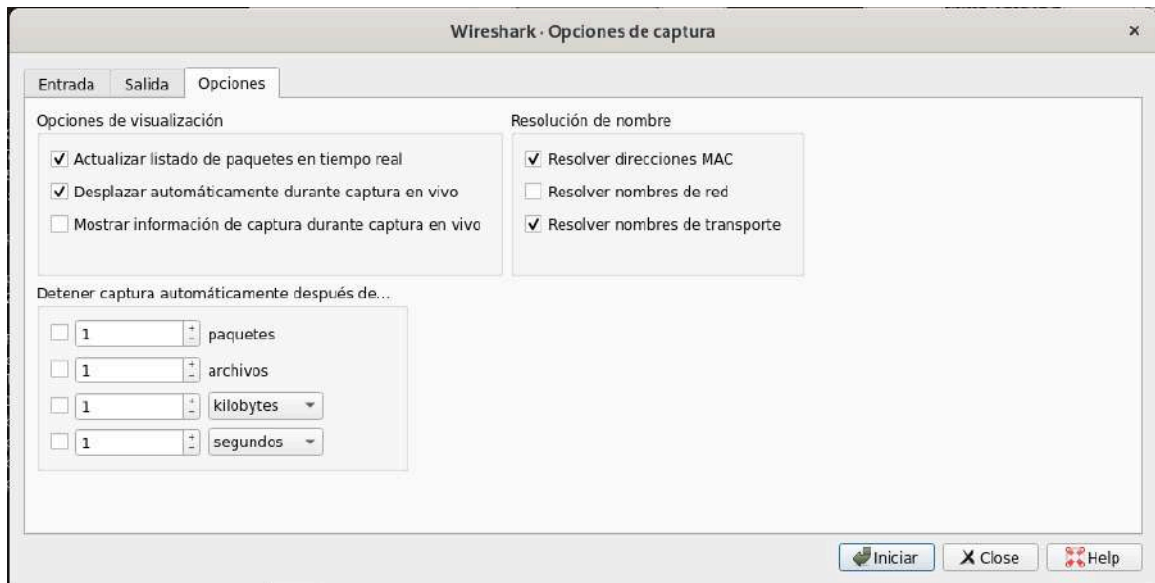
Muestre la captura de una trama y resalte los protocolos que utiliza *ping*. ¿Son consistentes con los que reportó al preparar esta práctica?

Si son consistentes, se utiliza el protocolo ICMP



¿La tramas que aparecen son comunicaciones entre sus dos hosts o también aparecen las de los hosts del otro equipo de trabajo? **también aparecen las del otro equipo, debido a que no hay filtro.**

En Wireshark, vuelva a seleccionar el menú *Capture-> Options*. Ahora seleccione la pestaña “*Opciones*”. Mostrándose:

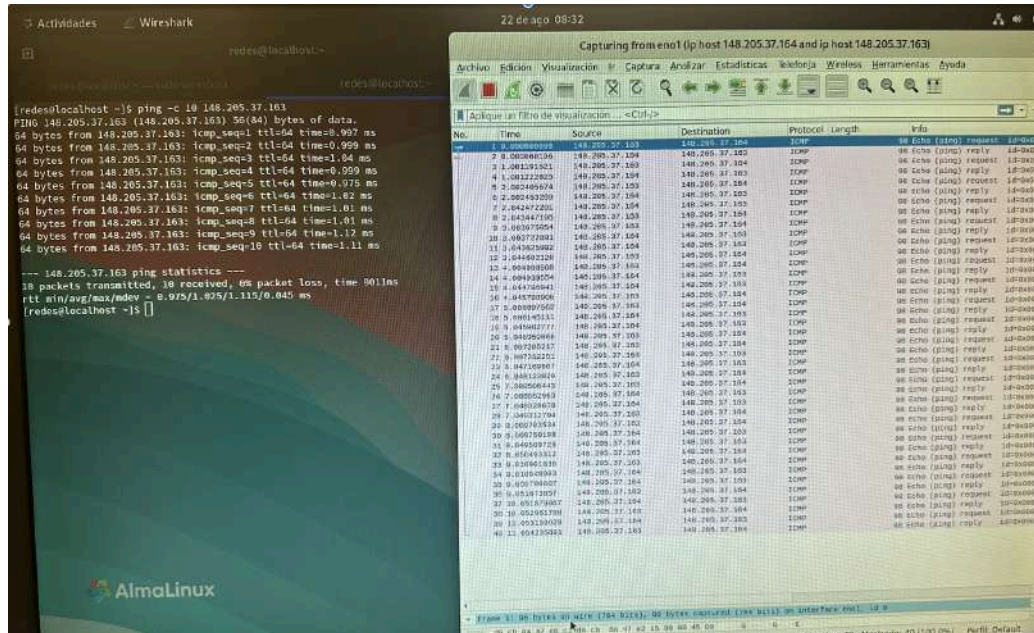


Deberá activar las opciones de visualización y Resolución de nombre, tal y como aparecen en la ventana. También, deberá dejar desactivadas las dos que se muestran como tal.

11. Regresando a la pestaña “*Entrada*”, defina filtros de captura:

- En el cuadro de texto “*Capture Filter for selected interfaces*” escriba (apareciendo seleccionando *eno1*)  
`ip host [IP_mi_maquina] and ip host [IP_maquina_compañero]`
- Seleccione el botón “*Iniciar*” -> “*Continue without savings*”, cerrándose la ventana.

12. Vuelva a lanzar un **ping -c** con un total de 10 repeticiones y capture las tramas en el analizador, junto con el otro equipo de trabajo.



¿La tramas que aparecen son comunicaciones entre sus dos hosts o también aparecen las de los hosts del otro equipo de trabajo? **Solo aparecen la de nuestro equipo, ya que se aplicó un filtro**

¿Para qué sirven los filtros de captura? **Para mostrar solo las tramas que cuenten con ciertas características según el filtro que se aplique**

¿Cuál es el objetivo del filtro que se definió en el punto anterior? **Mostrar solo las tramas que se envían entre las direcciones ip de nuestro equipo de trabajo**

Remueva el filtro anterior.

13. Seleccione una de sus computadoras como Servidor de FTP, y sobre ella:

- ¿Dirección IP del que será Servidor FTP, una de sus PCs? **148.205.37.164**
- Deshabilite el FIREWALL de la computadora (ver Apéndice A)
- Habilite al servidor de FTP (ver Apéndice A)

14. En *Wireshark* cambie el filtro de captura por el siguiente:

`ip host [IP_Servidor_FTP]`

### PUNTO DE SINCRONIZACIÓN.

Espere a que sus compañeros en el puesto vecino hayan terminado.



15. Inicie nuevamente la captura de tráfico
16. Desde la línea de comandos, de su otra computadora, inicie una conexión *ftp* al servidor indicado anteriormente. Como nombre de usuario escriba *redes* y la contraseña correspondiente *adminRedes*.
17. Liste el contenido del directorio (comando *dir*) y cierre la sesión.

```

64 bytes from 148.205.37.164: ftp_seq=60 ttl=64 time=1.12 ms
64 bytes from 148.205.37.164: ftp_seq=61 ttl=64 time=1.07 ms
64 bytes from 148.205.37.164: ftp_seq=62 ttl=64 time=1.13 ms
64 bytes from 148.205.37.164: ftp_seq=63 ttl=64 time=1.11 ms

redes@localhost:~$ ftp 148.205.37.164
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (148,205,37,164,104,243).
150 Here comes the directory listing.
drwxr-xr-x  3 1000 1000  127 Feb 09 2024 Descargas
drwxr-xr-x  2 1000 1000   6 Aug 16 2023 Escritorio
drwxr-xr-x 12 1000 1000   6 Aug 16 2023 Imágenes
drwxr-xr-x  2 1000 1000   6 Aug 16 2023 Música
drwxr-xr-x  2 1000 1000   6 Aug 16 2023 Plantillas
-rwxr-xr-x  1 1000 1000  110 Apr 19 18:29 Practica-11.sh
drwxr-xr-x  2 1000 1000   6 Aug 16 2023 Público
drwxr-xr-x  2 1000 1000   8 Oct 27 2023 miArchivoA.txt
-rw-r--r--  1 1000 1000  10 Oct 27 2023 miArchivoC.txt
drwxr-xr-x  6 1000 1000  129 Mar 15 19:18 pt
drwxr-xr-x  2 1000 1000   6 Aug 25 2023 re03des10
-rwxr-xr-x  1 1000 1000  115 Apr 19 19:42 return_default_values_of
_eno1.sh
-rw-r--r--  1 1000 1000  1612 Nov 17 2023 show-running-config.txt
226 Directory send OK.
ftp>

```

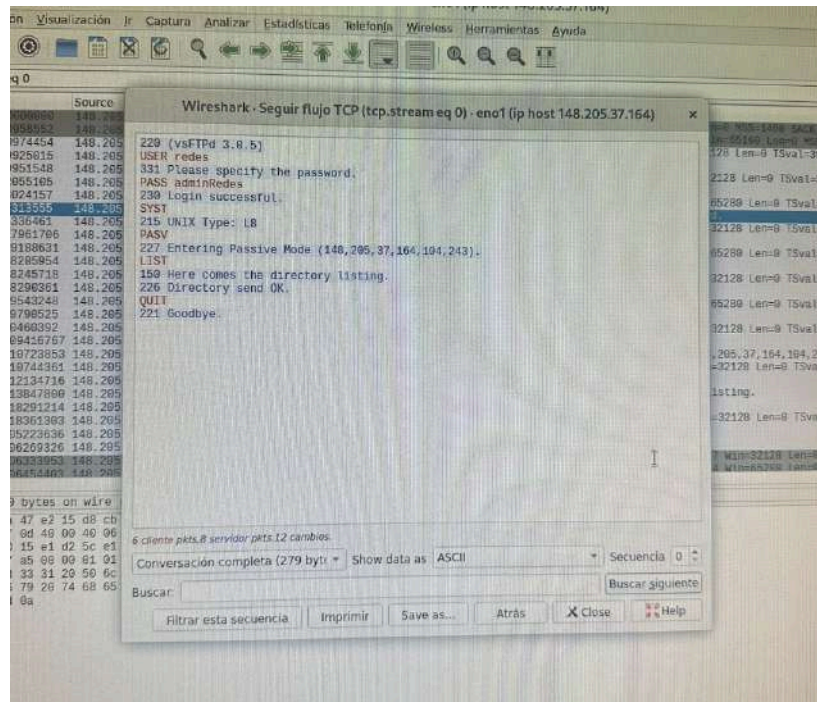
Esta foto muestra los archivos de la computadora que se estableció como servidor.

18. Detenga el analizador de protocolos y seleccione la primera trama con la dirección IP de su máquina. De clic con el botón derecho para activar el menú contextual y seleccione la opción *Follow TCP Stream*
19. Analice otras tramas. En particular, busque la trama donde se envían el usuario y la contraseña.

¿En qué trama encontró la contraseña? ¿Estaba cifrada? **En la trama número 6, no se encontraba cifrada**

20. Retire la opción anterior; busque una trama con la dirección IP de la máquina del puesto vecino y active nuevamente el menú contextual y la opción *Follow TCP Stream*

21. Busque la trama donde se envían el usuario y la contraseña.



¿Encontró la trama? ¿Estaba cifrada? Comente sobre los resultados obtenidos  
**En el flujo de la trama 8 nos encontramos con que tampoco había cifrado, lo cual demuestra la inseguridad de esto.**

Ahora se repetirán los últimos puntos, pero enlazando las computadoras a través de un CONMUTADOR o SWITCH (Natal, Merida, Sydney, Osaka, Atenas, Paris).

¿Conmutador (SWITCH) utilizado? **Osaka**

22. Lance nuevamente un **ping** desde su computadora a la del puesto de al lado y verifique que se mantiene la conexión.

### PUNTO DE SINCRONIZACIÓN.

Espera a que sus compañeros en el puesto vecino hayan terminado.

23. En *Wireshark* borre el filtro de captura e inicie nuevamente la captura de tráfico provocado por *ping*.

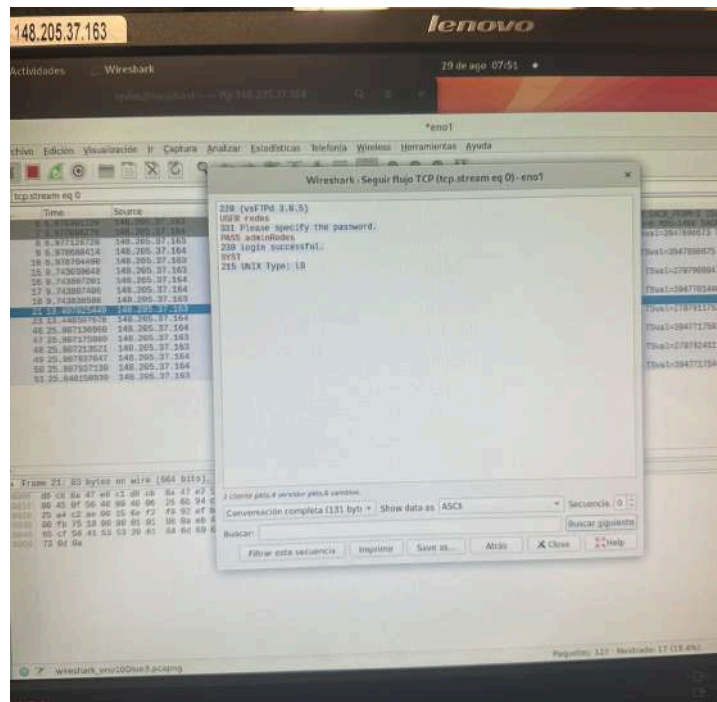
¿La tramas que aparecen son comunicaciones entre sus dos hosts o también aparecen las de los hosts del otro equipo de trabajo? **No, solo se ven las tramas donde**

**interviene mi computadora. Y es la diferencia entre un hub y un switch. El switch revisa el destino de los paquetes, es inteligente**

**PUNTO DE SINCRONIZACIÓN.**

Espera a que sus compañeros en el puesto vecino hayan terminado.

24. Arrancando nuevamente *Wireshark* inicie la captura de tráfico. Desde la línea de comandos, inicie una conexión *ftp* al servidor indicado anteriormente. Como nombre de usuario escriba *redes* y la contraseña correspondiente.
25. Detenga el analizador de protocolos, busque la trama donde se envían el usuario y la contraseña.
26. Analice otras tramas. En particular, busque la trama donde se envían el usuario y la contraseña.



**¿En qué trama encontró la contraseña? ¿Estaba cifrada? Se encontró en la trama 21, no se encontraba cifrada**

27. Retire la opción anterior, busque una trama con la dirección IP de la máquina del puesto vecino

¿Encontró la trama? ¿Estaba cifrada? Comente sobre los resultados obtenidos.

**Si, fue la trama 48. Y no se encontraba cifrada.**

**Con esto podemos ver que no es que el switch o el hub sean inseguros, el problema es el protocolo FTP.**

Deshabilite al servidor de FTP desde otra ventana (ver Apéndice A).

También, habilite el FIREWALL de la computadora (ver Apéndice A).

**28. Regrese el cable de la computadora a la roseta en la cual estaba conectada inicialmente y muestre al profesor con un explorador dicho regreso.**

## Anexo A

---

DESHABILITACIÓN del FTP servidor, desde el home directory.

- cd
- sudo service vsftpd stop

HABILITACIÓN del FTP servidor, desde el home directory.

- cd
- sudo service vsftpd start

DESHABILITACIÓN del FIREWAL, desde el home directory.

- cd
- sudo systemctl stop firewalld.service

HABILITACIÓN del FIREWAL, desde el home directory.

- cd
- sudo systemctl start firewalld.service

### NOTAS CLASE:

Enrutador: divide redes

Firewall: barrera que impide que lleguen ataques desde afuera y monitorear comportamiento sospechoso desde adentro.

Administrador de cargas: asigna a las distintas redes cierto ancho de banda.

Switch principal:

IDF: intermedia data frame: es el cuarto donde llegan todos los cables de otros switches.