**ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO**

**Laboratorio No. 2 – Alistamiento S.O, Shell y Software de apoyo en redes.**

**Ana Gabriela Silva – Juan Sebastián Mina.**

**EXPERIMENTOS**

1. **CONOCIENDO PACKET TRACER.**

**Responda las siguientes preguntas**

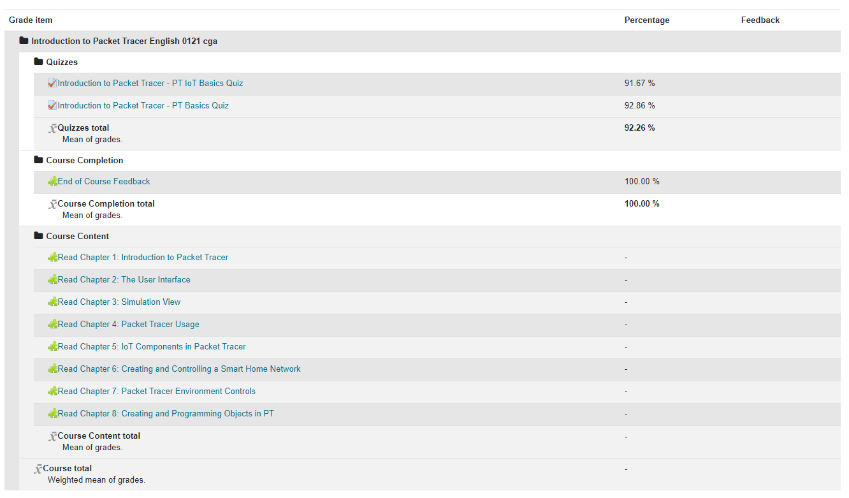
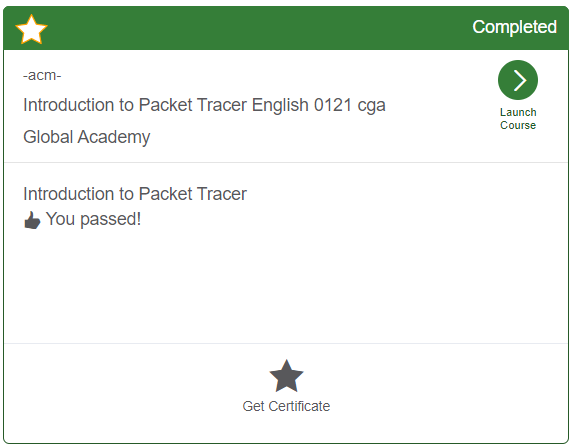
* **¿Qué versión de Packet Tracer se encuentra instalada en el Lab?**

r. La versión instalada en el laboratorio es la 7.3.1

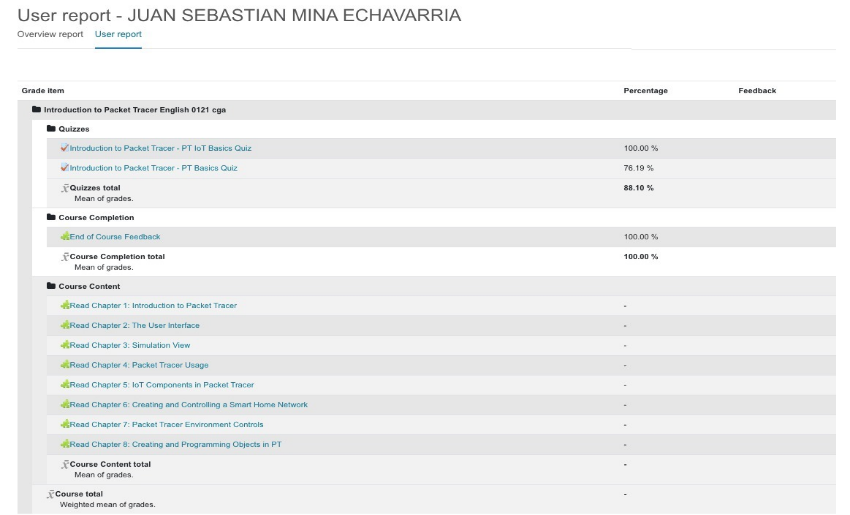
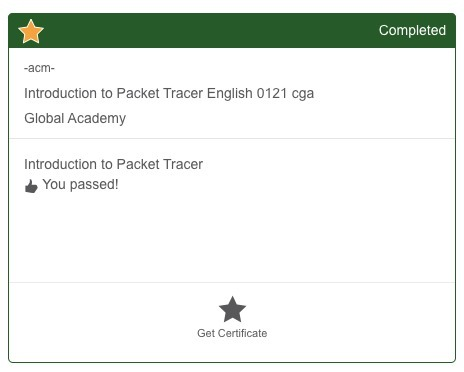
* **A través de la plataforma de Cisco inscribase en el curso Introduction to Packet Tracer v1.1. muestre con un video hecho por el grupo un resumen del curso. Máximo 5 min.**

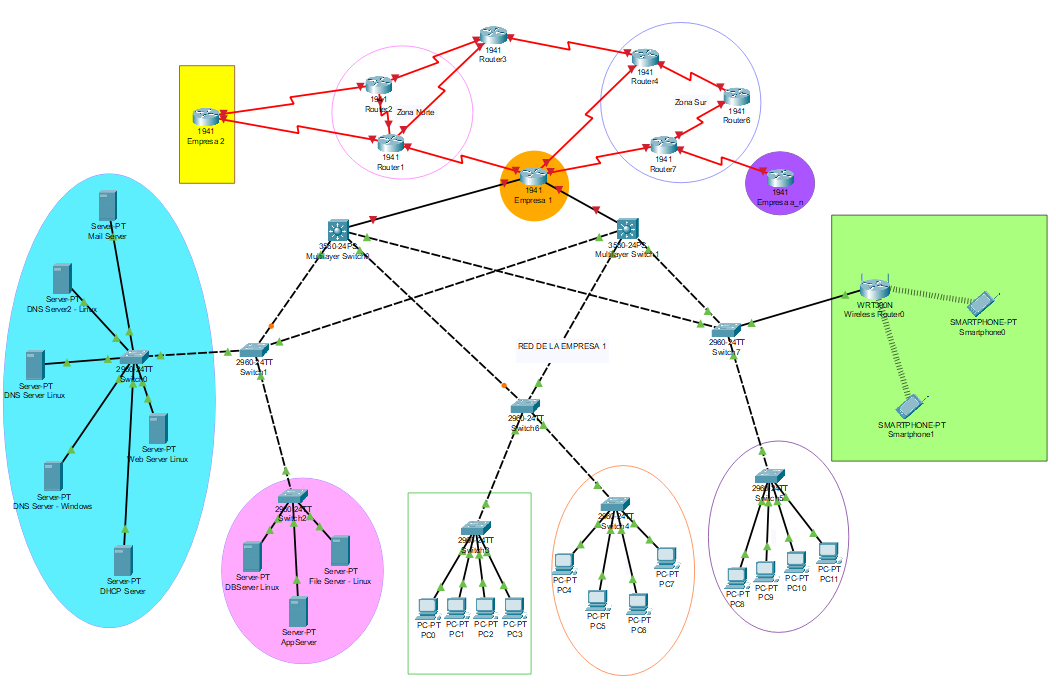
r. El vídeo está en los archivos del canal “AnaGabrielaSilva\_JuanSebatianMina” en Microsoft Teams.

* **Realice la evaluación del curso y tome un pantallazo del resultado de la evaluación.**

Ana Gabriela Silva

Juan Sebastián Mina



* **Usando Packet Tracer haga el diagrama de red que se presenta en la página siguiente.**

**Conexiones negras continuas (Copper Straight – Through):** es un cable estándar que se utiliza para conectar dos dispositivos que operan en diferentes capas del modelo OSI (como concentrador a enrutador). Se puede utilizar con los tipos de puerto Ethernet, Fast Ethernet y Gigabit Ethernet.

**Conexiones negras discontinuas (Copper Cross – Over):** Este cable funciona para las conexiones entre el equipo de la misma capa de acuerdo al modelo OSI, de igual manera, para las conexiones HUB – HUB, PC – PC, SWITCH – SWITCH.

1. **SIGUIENDO MENSAJES CON PACKET TRACER**

* Seleccione dos servidores ubicados en el ovalo azul agua marina (izquierda-abajo en el

dibujo). Póngales la siguiente configuración

Servidor 1

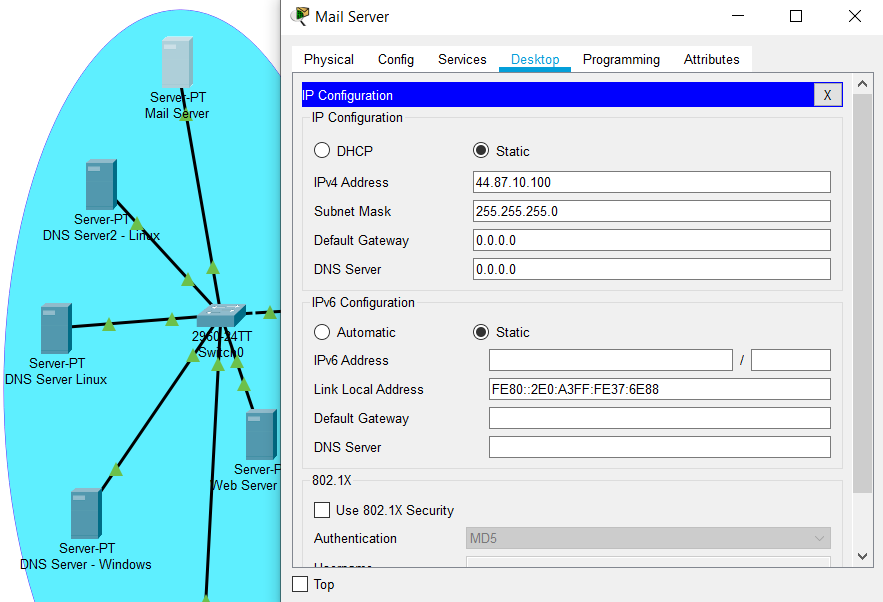
IP 44.87.10.100

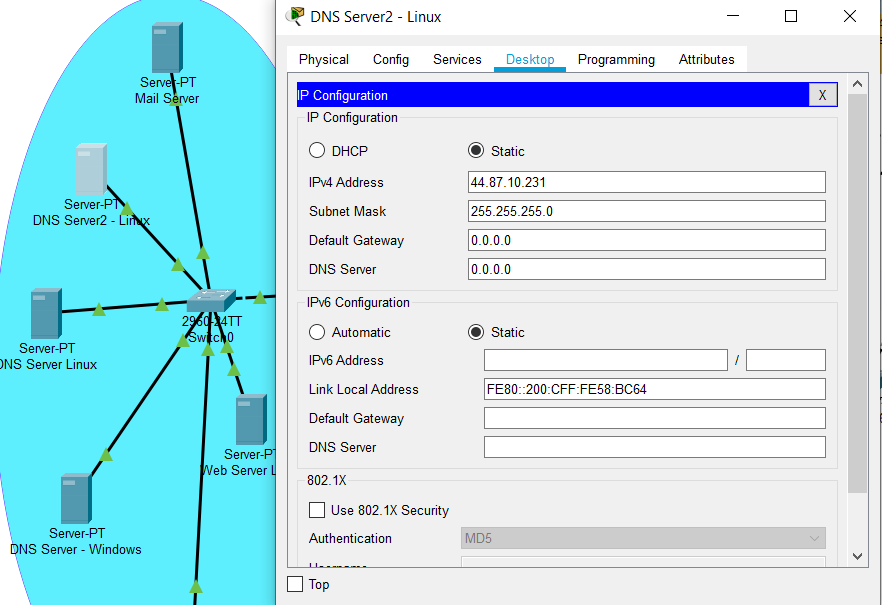
Máscara: 255.255.255.0

Servidor 2

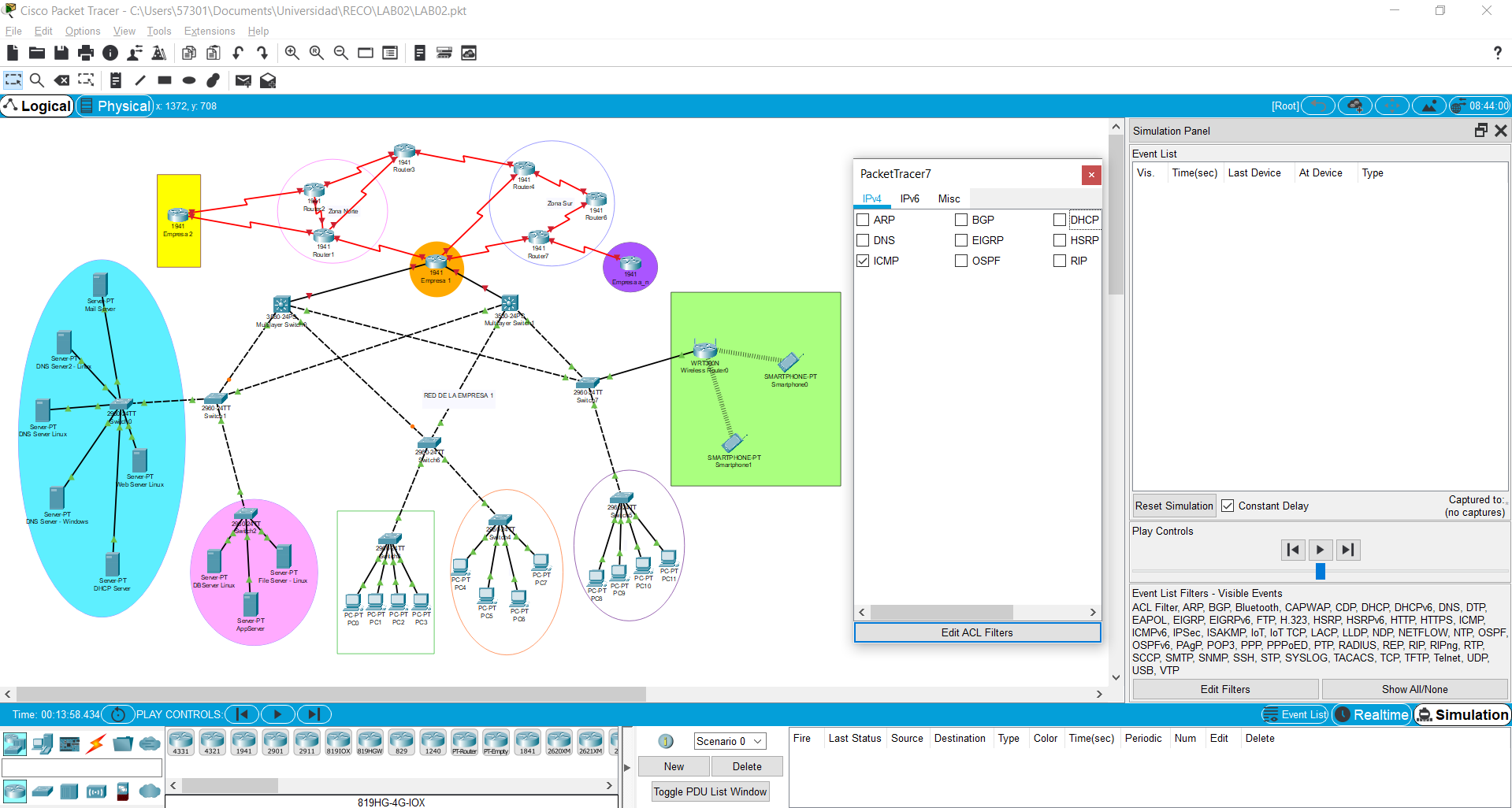
IP 44.87.10.231

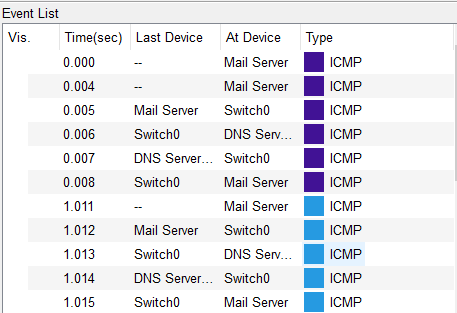
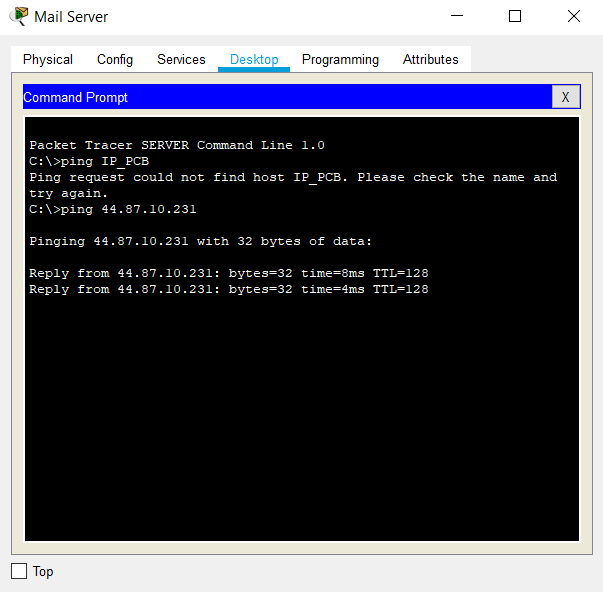
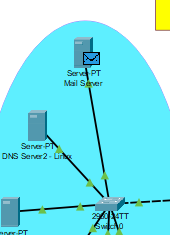
Máscara 255.255.255.0

****

****

* Run the simulation and capture the traffic.
* In the far lower right of the PT interface is the toggle between Realtime and Simulation mode. Click on Simulation mode.
* Click in the Edit filters button and select only ICMP.
* Click in PCA. Choose the Desktop tab. Open the Command Prompt. Enter the command ping IP\_PCB). Pressing the Enter key will initiate four ICMP echo requests. Minimize the PC configuration window. Two packets appear in the Event List, the first ICMP echo request and an ARP request needed to resolve the IP address of the server to its hardware MAC address.
* Click the Auto Capture / Play button to run the simulation and capture events.
* Click OK when the "No More Events" message is reached.



****

**EN LA RED REAL**

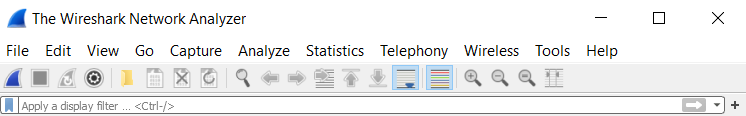
1. **USANDO WIRESHARK**

* **¿Qué es Wireshark?**

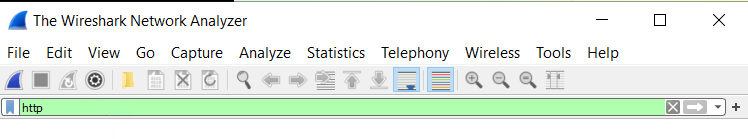
Es una herramienta multiplataforma con interfaz gráfica para el análisis de red, producto de la evolución de Ethereal. Incluye la herramienta Tshark en modo consola para capturas, análisis de red, entre otras posibilidades. Al usar las librerias pcap, su uso es similar a Tcpdump y Windump.

Este permite ver, aun nivel bajo y detallado, consultar todo lo que está ocurriendo en la red. Es open source y multiplataforma. Se utiliza a menudo como mejor opción al momento de auditar redes usualmente redes Ethernet y es compatible con algunas otras.

* **¿Cómo generar filtros?, ¿Para qué se usan? De unos ejemplos**

****

Antes de iniciar el filtro.

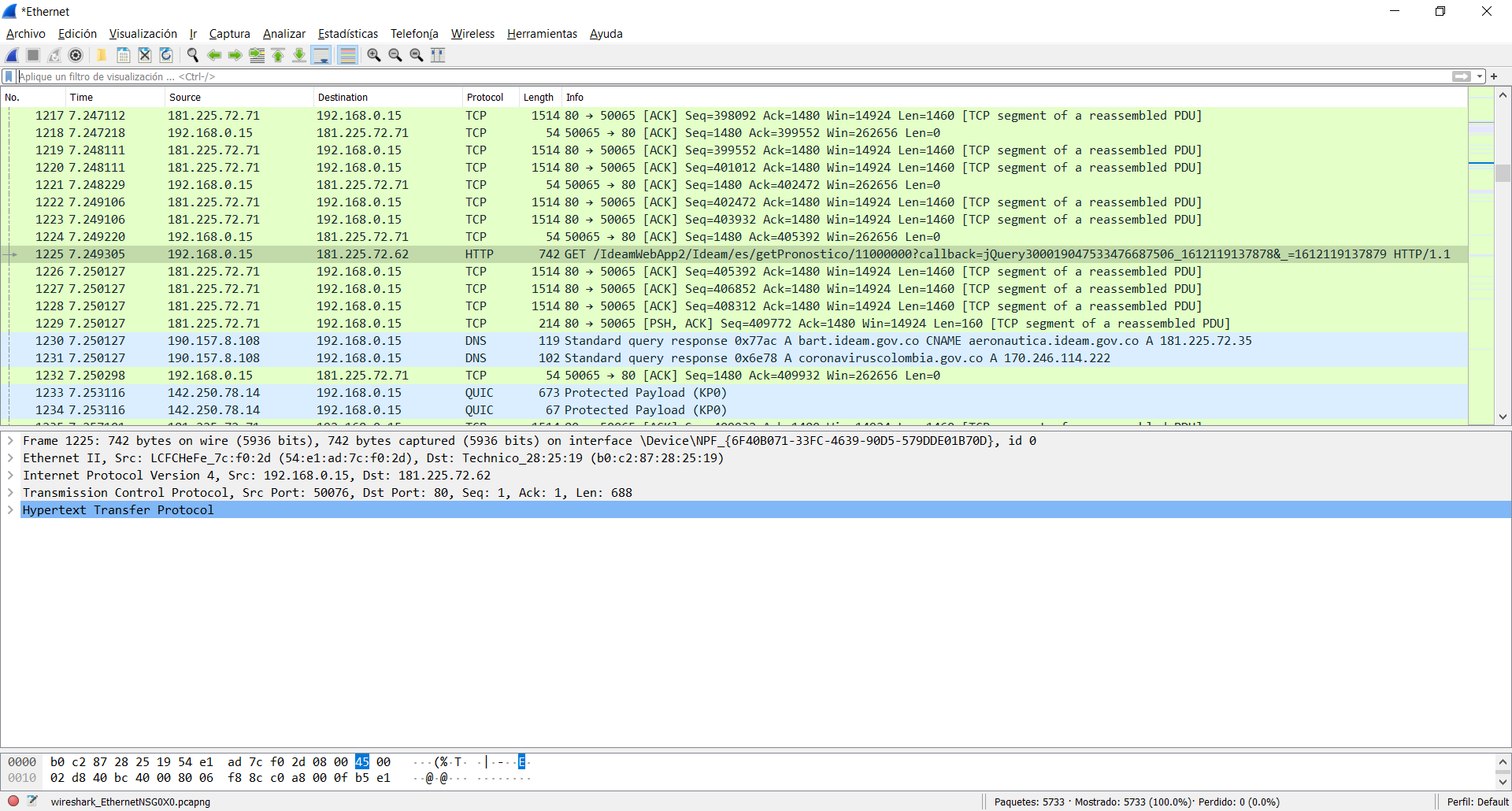
****

Después de iniciar el filtro.

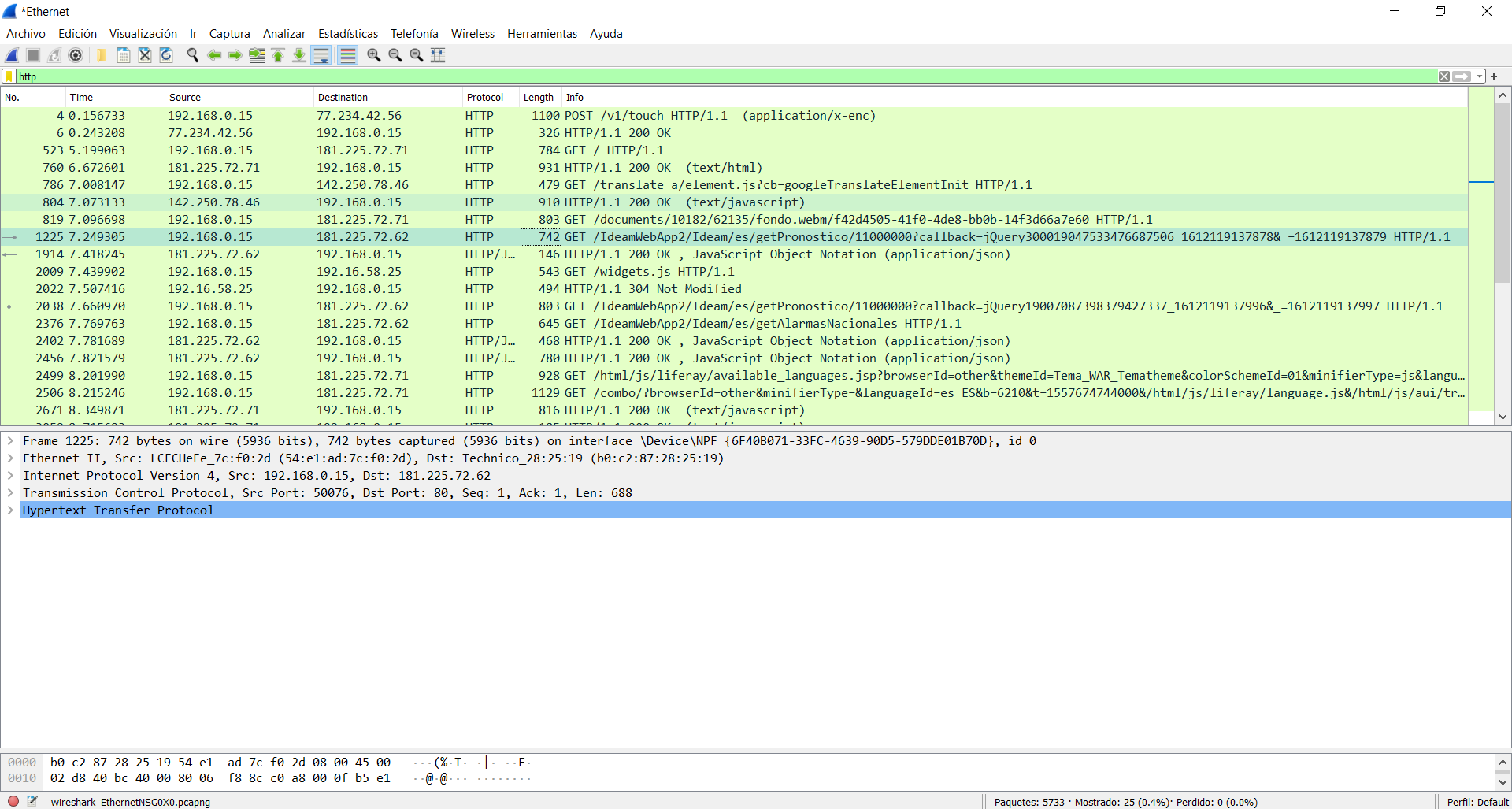
Se usan para reducir la información que se nos muestra al momento de navegar, mostrándonos únicamente lo que queramos ver.

Los filtros son de gran utilidad y pueden ser aplicados en conjunto como parte de operaciones lógicas. Pueden utilizarse sobre la captura o especificarse previamente para que solo capturen lo especificado en el propio filtro. Este tipo de herramientas no solo es utilizado en el análisis de malware sino también en el estudio de protocolos de red, la búsqueda de vulnerabilidades y demás aplicaciones.

* **Realice una consulta web al link http://www.ideam.gov.co/ y capture el tráfico generado.**

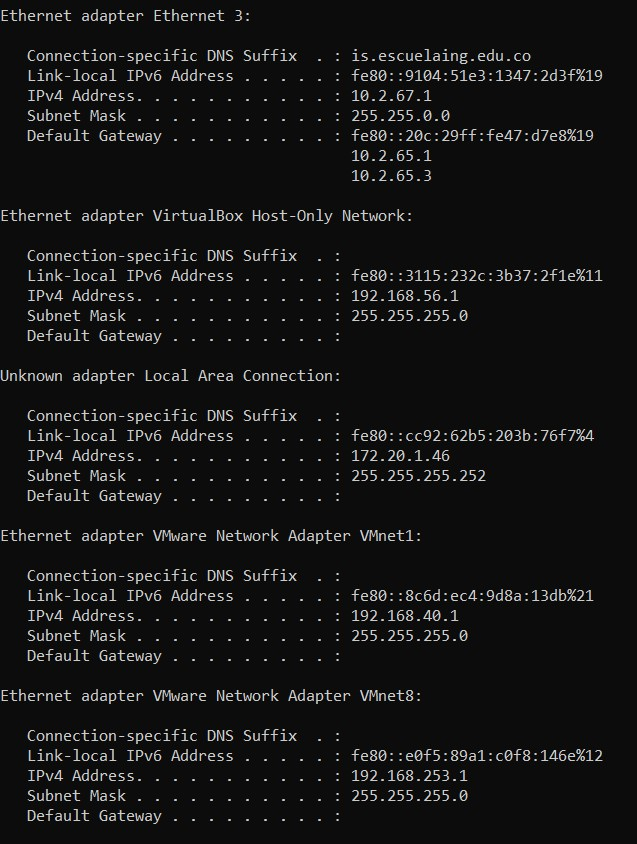


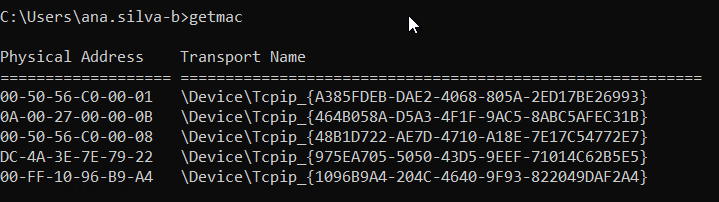
* Analice los datos encontrados en uno de los paquetes capturados. Mire el encapsulamiento y presente capturas del mismo (Use el paquete que contiene una de las solicitudes GET que se realizan).



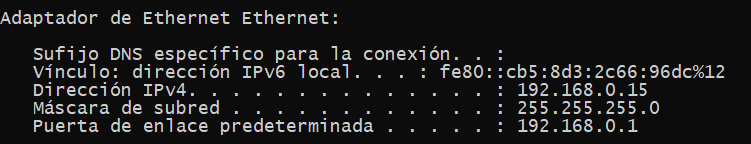
1. **TARJETAS DE RED.**

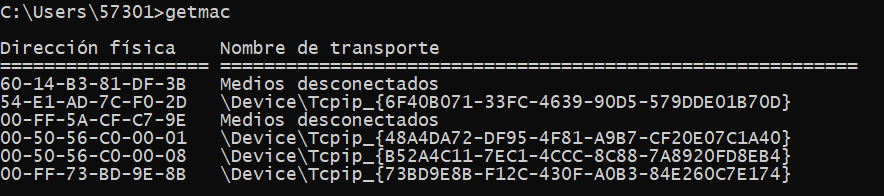
* Sistemas 01.



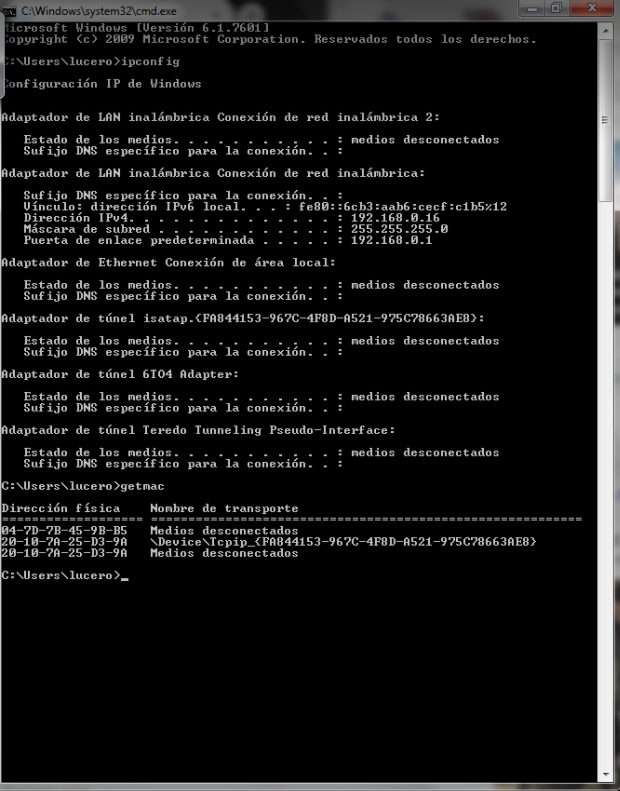


* Computador portátil Ana Gabriela.

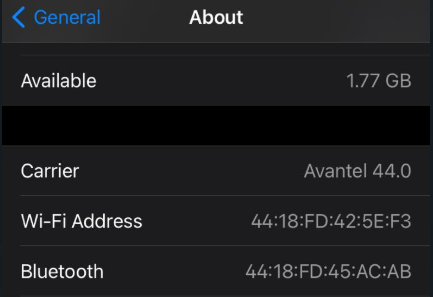




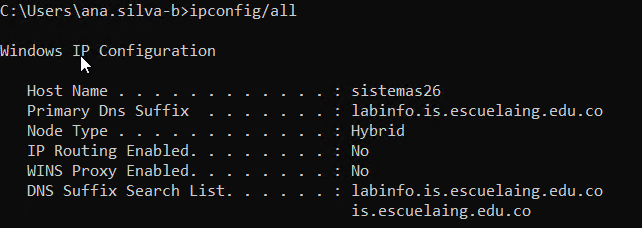
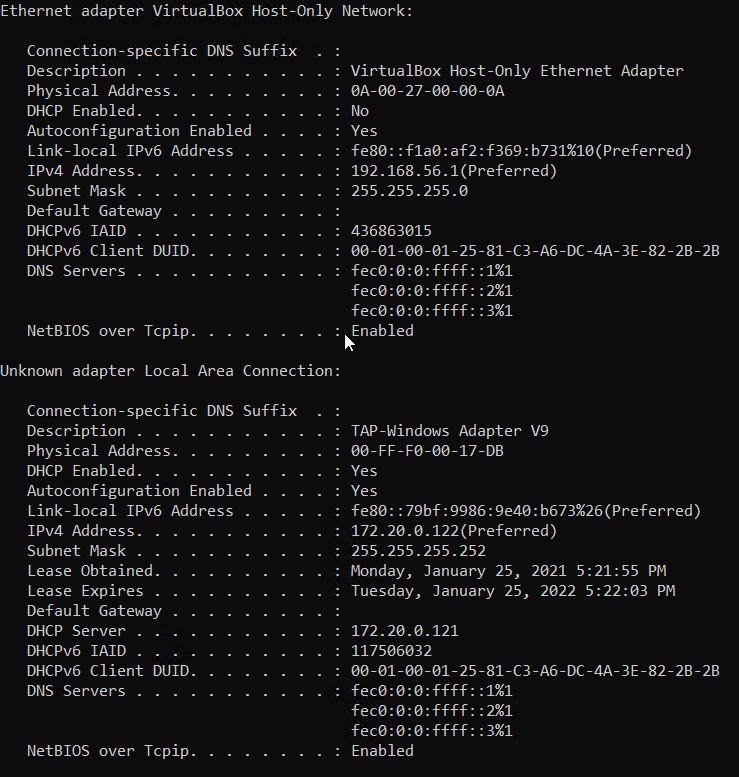
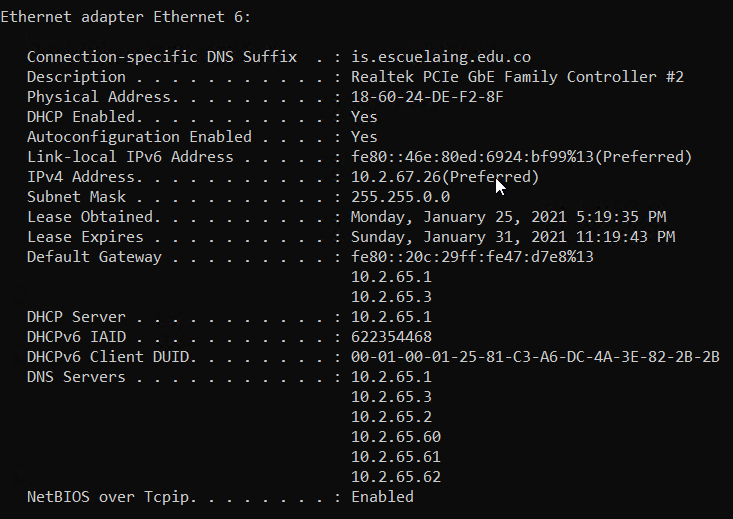
* Computador todo en uno Ana Gabriela.

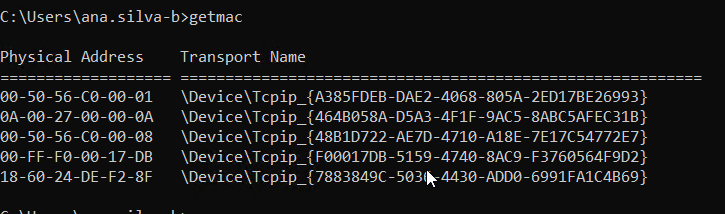


* Teléfono personal Ana Gabriela.



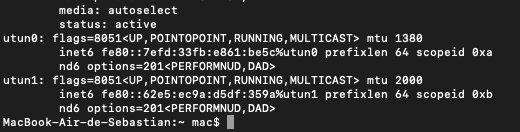
* Sistemas 26

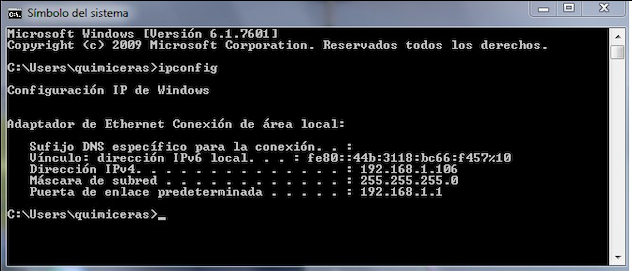
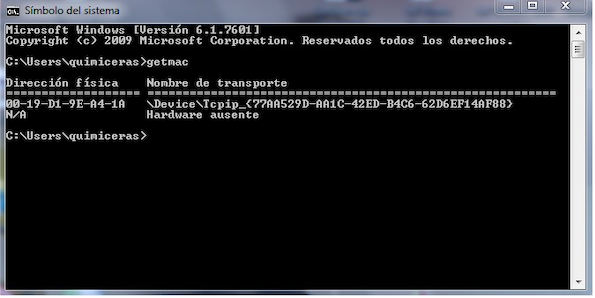


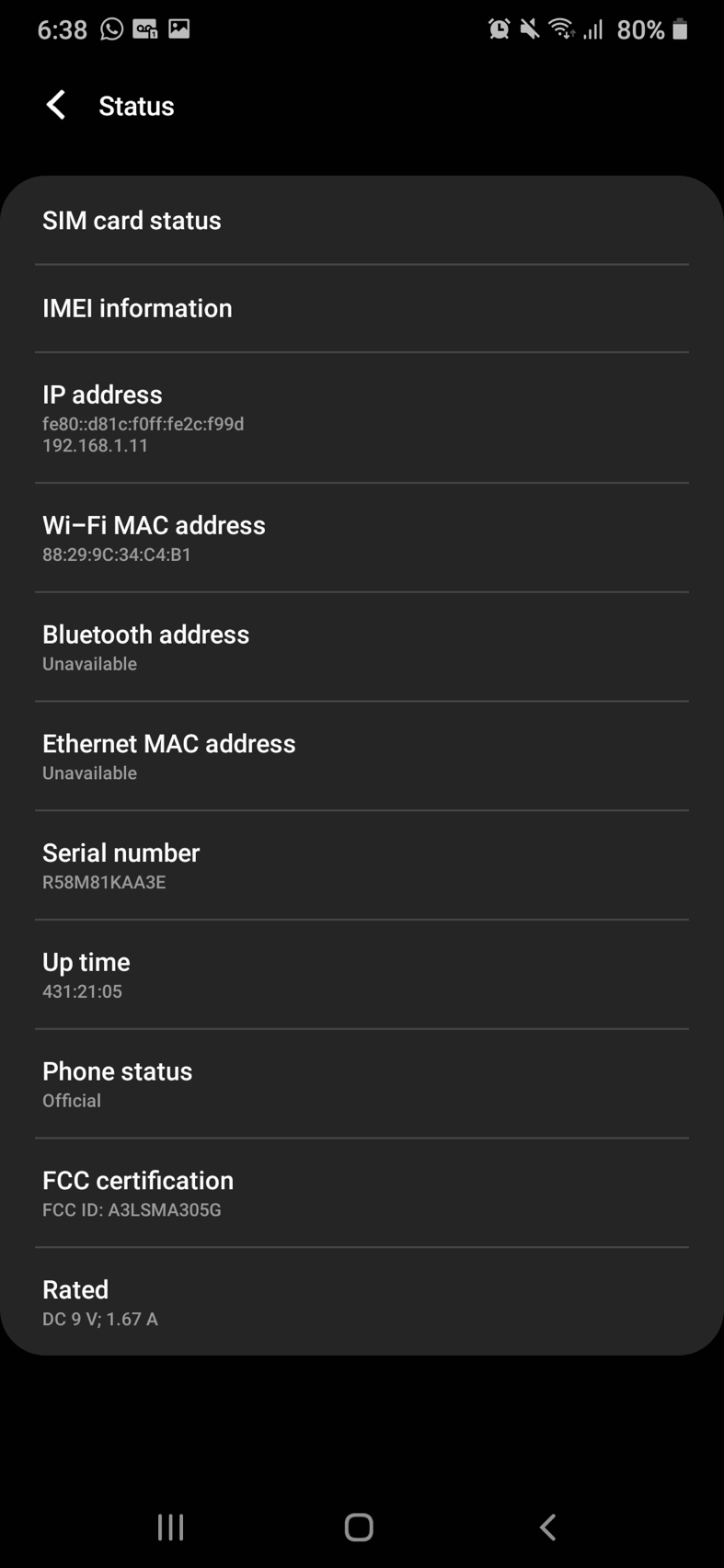


* Portatil Sebastián Mina





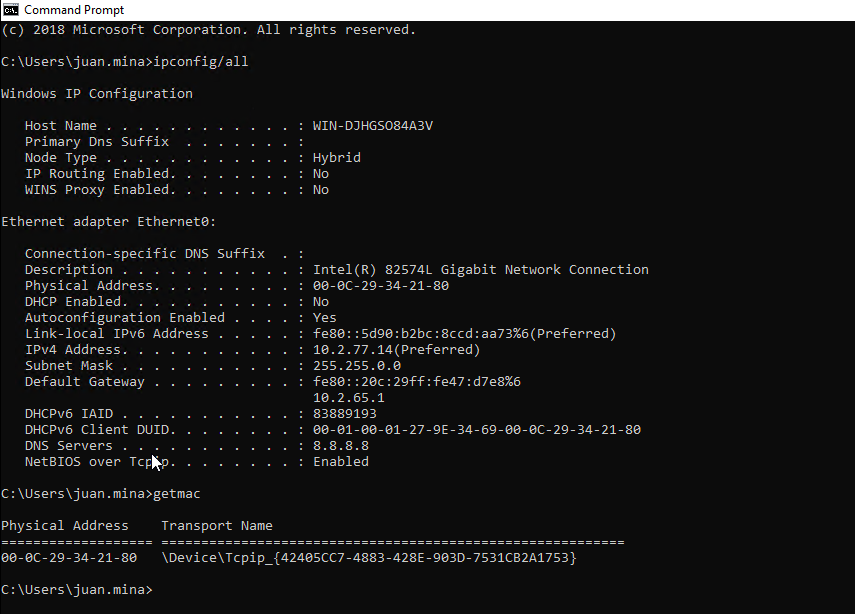
* Computador de torre Sebastián Mina
* Teléfono personal Sebastián Mina



* MV – BSD (VMWare)



* MV – WINDOWS SERVER (VMware)



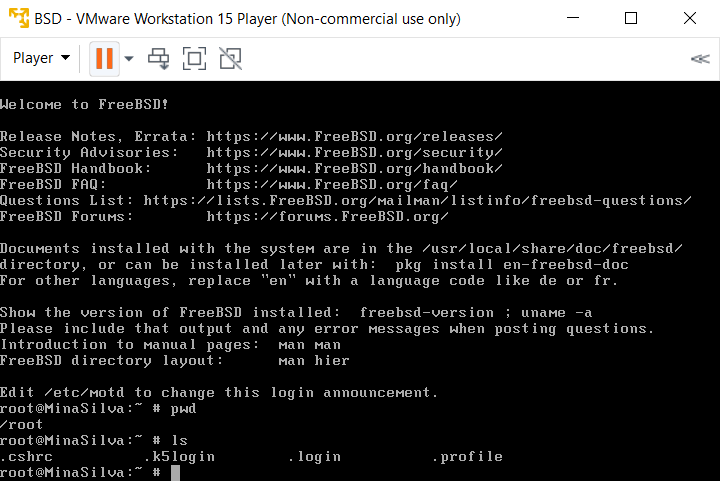
**Diferencias:**

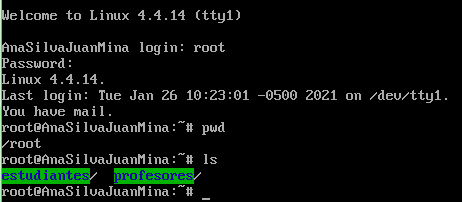
* Otro fabricante.

**Software Base**

1. **SHELL PROGRAMMING- UNIX**
   1. **COMANDO LS Y PWD**

* FREE BSD (VMWare)

****

* Slackware (VMWare)
* **¿Cómo puede utilizar el comando ls para obtener información adicional como por ejemplo fecha y permisos?**

r. ls -l

* **¿Cómo puede utilizar el comando ls para listar los archivos ocultos de un directorio?**   
  r. ls -a
* **¿Cómo puede utilizar el comando ls para listar los archivos ordenados por fecha de modificación?**   
  r. ls -t
* **¿Cómo mostrar el contenido de un directorio en donde uno no se encuentra ubicado usando el comando ls?**

r. ls {opciones} {directorio}

* **Cuando un directorio contiene muchos archivos, ¿cómo hacer para mostrarlo por páginas? (use la ruta /etc)**

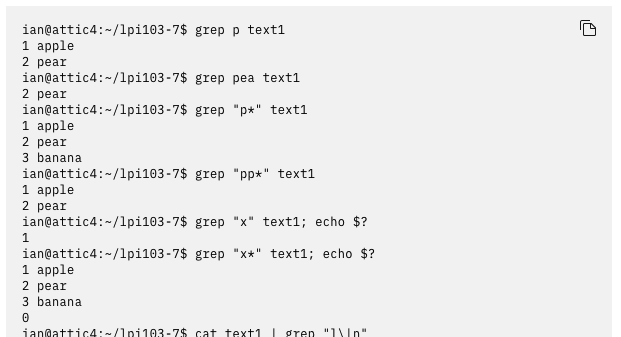
r. ls /etc|mor

* **¿Cómo listar los archivos que comienzan con la letra m?**

r. ls \*m\*

* **¿Qué otros ordenamientos se pueden realizar?**
* ls -r, nos permite ver los ficheros ordenados en orden de Z-A.
* ls -S, ordena los ficheros por tamaño.
* ls -X, organiza los ficheros alfabéticamente por la extensión del fichero.
* **¿Qué es una expresión regular? y ¿en dónde se puede usar dentro del Shell?**

Una expresión regular, es una forma de describir una cadena de texto de forma que un programa pueda hacer coincidir el patrón con otras cadenas de texto, proporcionando una capacidad de búsqueda mejor. También es como conocida como regex o regexp.



* 1. **COMANDO ECHO.**
* **¿Cuál es el objetivo del comando ECHO?**

La función principal del comando ECHO es mostrar mensajes (eco) por pantalla, también puede activar o desactivar la presentación de comandos por pantalla. Si se utiliza el comando echo sin parámetros muestra la configuración actual de echo.

**Parámetros:**

**<mensaje>** Texto que se mostrará en la pantalla.

**<on | off>** Activa o desactiva la presentación por pantalla de comandos. La presentación de comandos está activada por defecto.

**/?** Muestra la Ayuda en el símbolo del sistema.

* **Variable PATH: ¿Para qué sirve la variable PATH?, use el comando ECHO para mostrar su contenido.**

La variable PATH es una variable de entorno que contiene una lista ordenada de rutas que Unix buscará ejecutables al ejecutar un comando. El uso de estas rutas significa que no tenemos que especificar una ruta absoluta al ejecutar un comando.



BSD



SLACKWARE

* **¿Cómo añadir datos al PATH?**

Con el comando *export* seguido del nombre de la variable de entorno, establecemos el contenido de la variable de entorno. La idea es establecer el contenido actual de la variable de entorno PATH, seguido de la ruta que queremos añadir. Recordemos que si queremos añadir una ruta al PATH de forma permanente, bastará con añadir el comando *export* anterior, al final de uno de estos ficheros:

/etc/profile (Para todos los usuarios)

~/.bash\_profile (Para un usuario concreto)

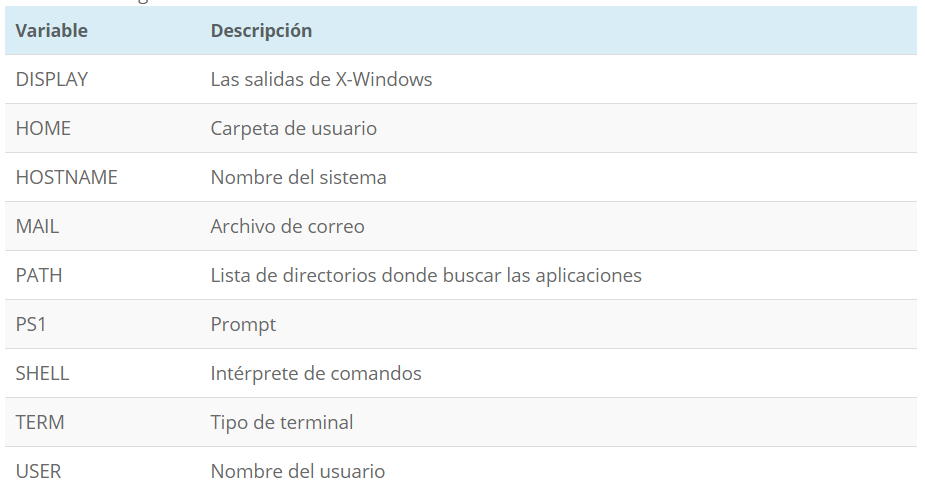
~/.bash\_login (Para un usuario concreto)

~/.profile (Para un usuario concreto

* **¿Qué son las variables de ambiente?, de ejemplos de algunas de ellas.**

Independientemente del sistema operativo que estemos usando, las Variables de Entorno son la forma simple de pasar información de una aplicación a otra.

En linux, tenemos unas variables comunes, y las encontramos en la gran mayoría de distribuciones linux. Son las siguientes:



* 1. **EJECUCIÓN AUTOMÁTICA DE UNA SECUENCIA DE COMANDOS, VARIABLES Y CONDICIONALES.**

r. revisar script1

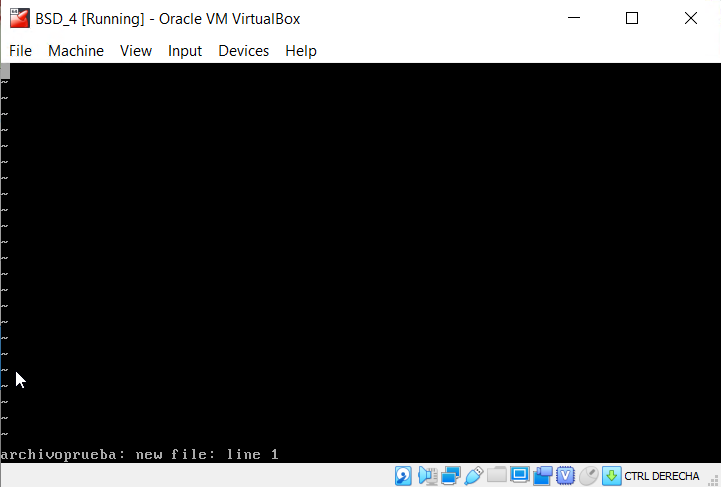
* 1. **REVISIÓN DE LOG.**

r. revisar script2

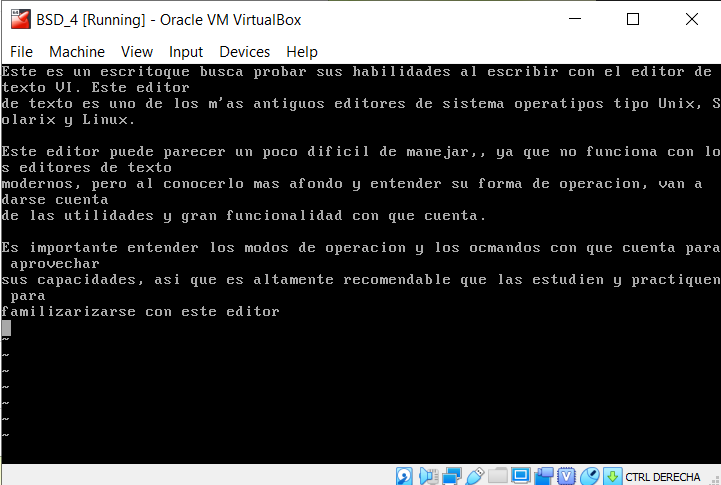
* 1. **CREACIÓN DE USUARIOS.**

r. revisar script3

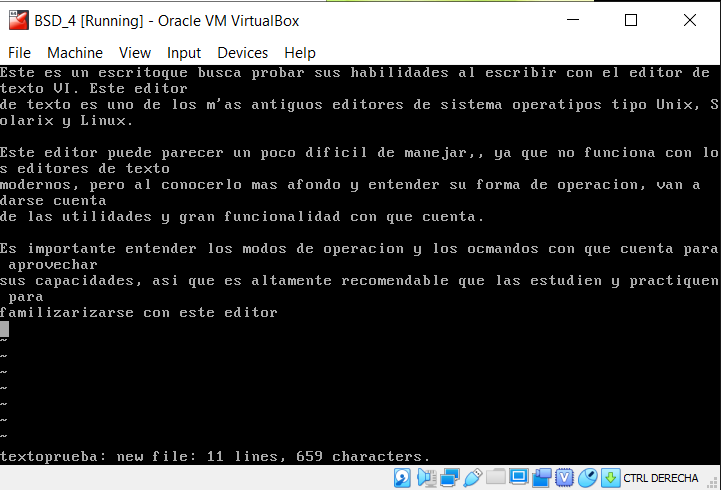
* 1. **EDITOR VI.**
* Utilice el editor VI para crear un archivo. Indique los comandos utilizados.
* Vi (nombre archivo) archivoprueba.

****

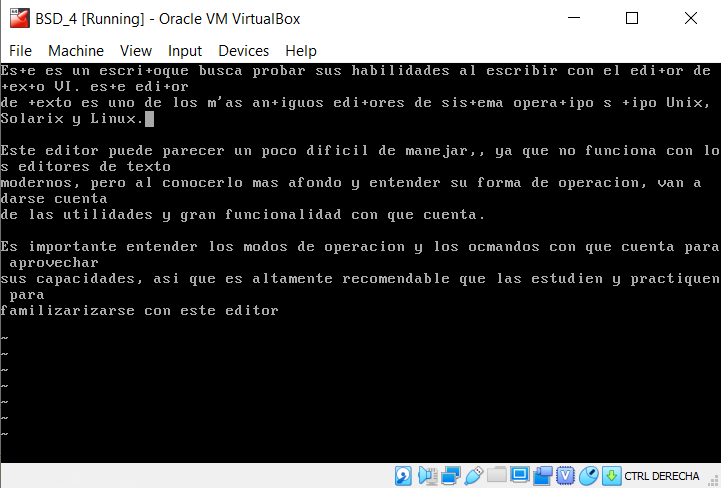
* Digite el siguiente texto y documente los comandos utilizados. Nota: debe quedar en cada línea del editor una línea del texto presentado, es decir, debe digitarse la tecla ENTER al final de cada fin de línea.

****

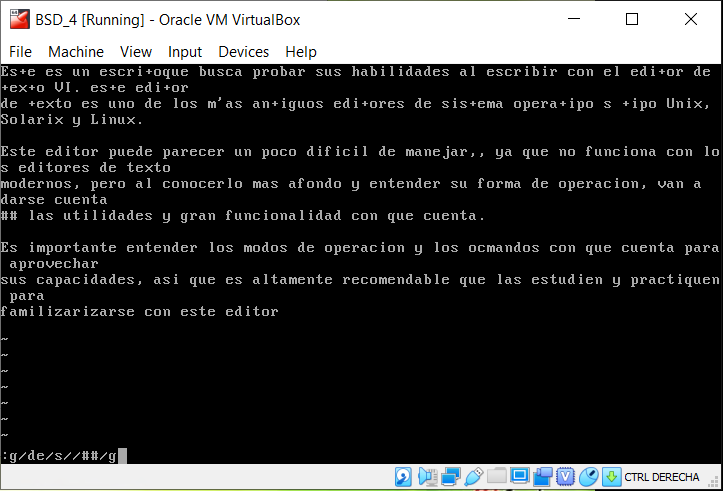
* Grabe el trabajo realizado sin salir del editor. (Esc :w)

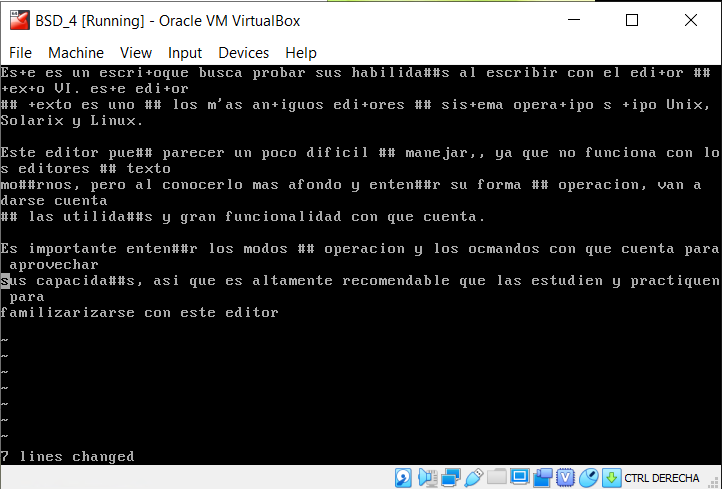


* Cambie las letra ‘t’ del primer párrafo por el símbolo +



* Cambie las palabras ‘de’ de todo el texto por los símbolos ##.

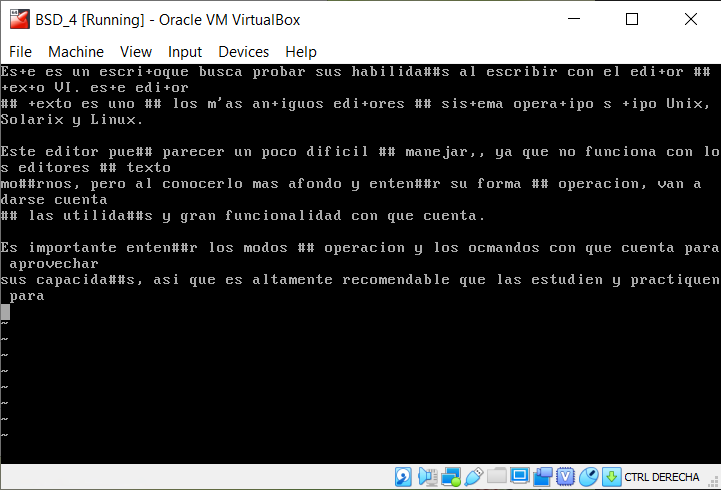


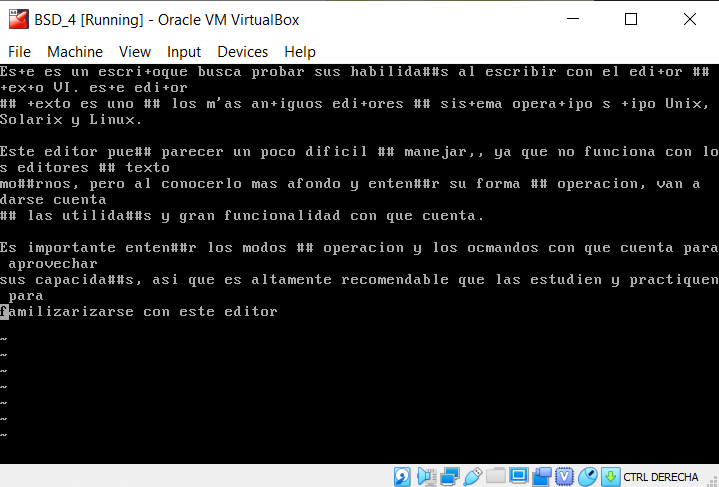
****

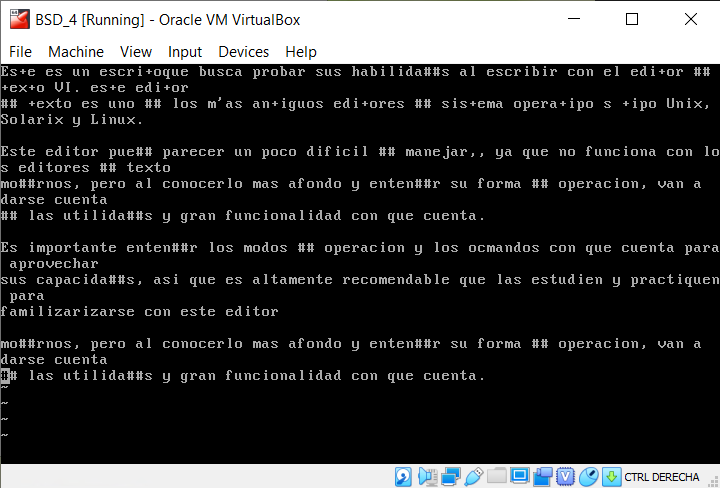
* ¿Qué comando se puede usar para borrar una palabra en VI?

r. dw (Especificación en el cuadro de resumen de los comandos)

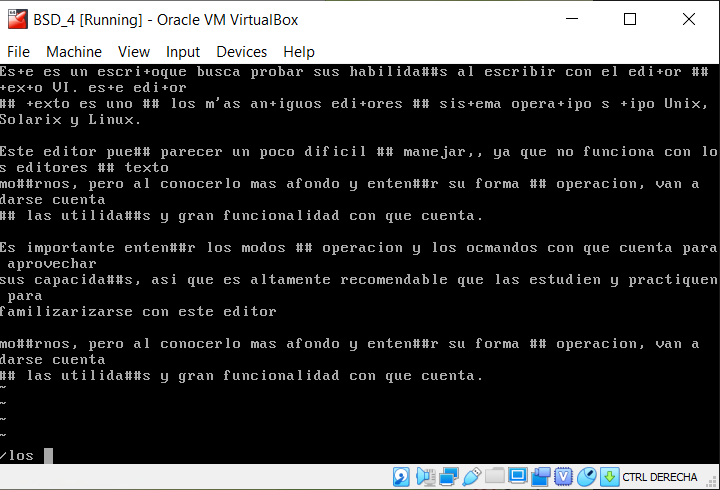
* **Borre la última línea del documento. (el cursor en la línea que se quiere eliminar y se presiona dd)**

****

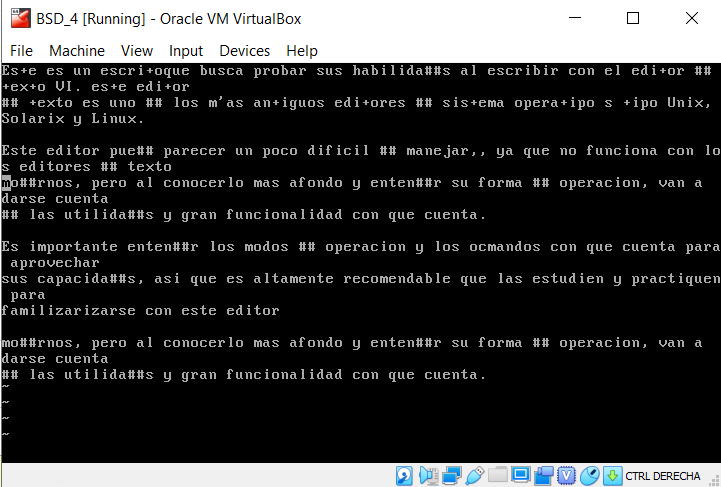
* Deshaga el comando anterior. (u)
* Copie las últimas 2 líneas del segundo párrafo al final del archivo. (yy en la línea que se quiere pegar y en el lugar donde se quiere pegar se presiona p)

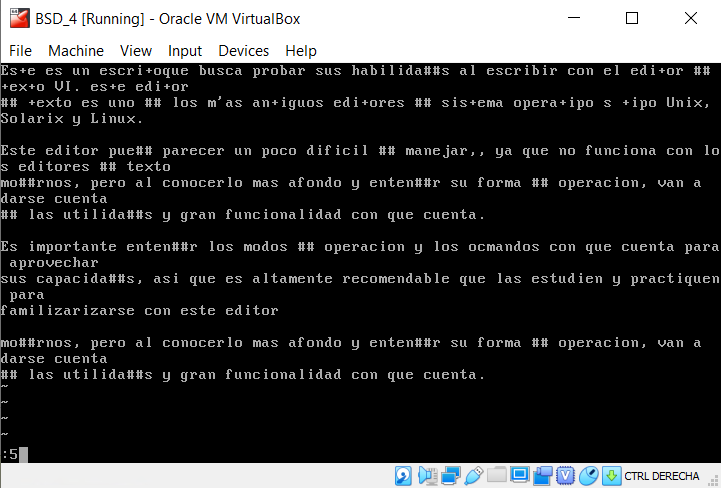


* Busque la palabra los dentro del texto

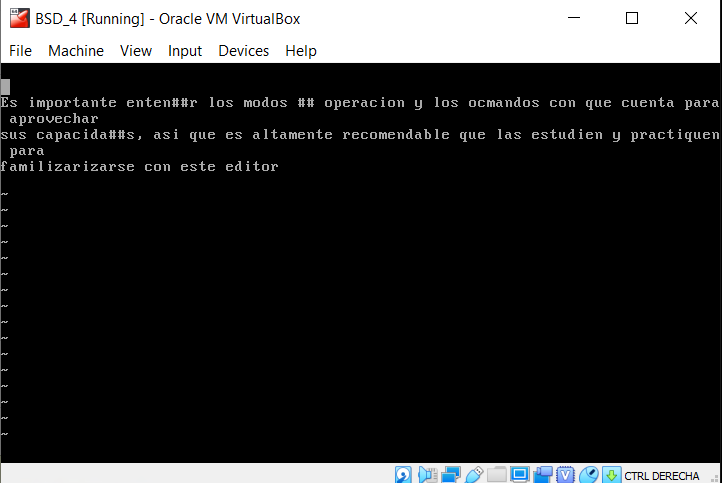


* Ubíquese en la línea 5 del texto usando un comando

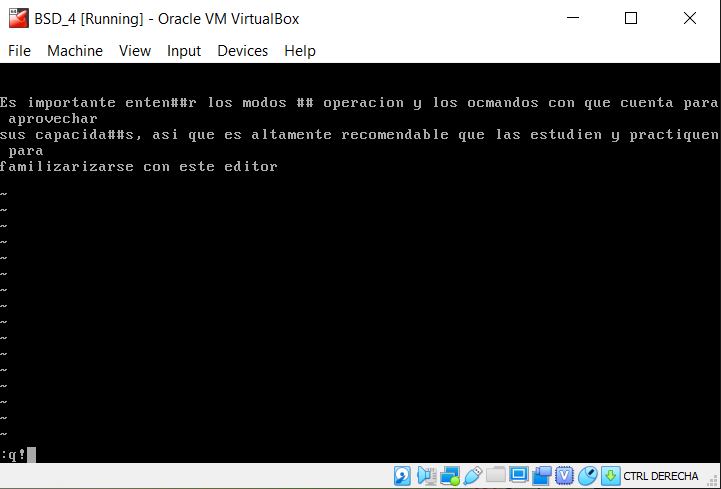




* Vuelva a entrar y borre las primeras 5 líneas



* Salga del archivo sin grabar. (:q!)



* Resumen de comandos utilizados.

|  |  |
| --- | --- |
| COMANDO | USO/SIGNIFICADO |
| **Creación** | |
| vi | Abre la ventana de edición sin abrir ningún archivo. |
| vi (nombre archivo) | Edita el archivo si ya existe, de lo contrario, lo crea |
| **Borrar texto** | |
| x | Borra el carácter bajo el cursor |
| dd | Borra la línea donde se encuentra el cursor |
| ndd | Borra las próximas n líneas |
| D | Borra desde donde se encuentra el cursor hasta el final de la línea |
| dw | Borra desde donde se encuentra el cursor hasta el final de una palabra |
| **Buscar texto** | |
| /[palabra por buscar] | Busca hacia delante la cadena de caracteres buscados. |
| **Copia y pegar texto** | |
| yy | Copiar línea |
| p | Poner la línea pegada por debajo de la línea actual |
| P | Poner la línea pegada por encima de la línea actual |
| **Reemplazar** | |
| :g/[**palabra a reemplazar**]/s//[**palabra para reemplazar**]/g | Reemplazar una cadena de texto por otra |
| s | Sustituir cadena por carácter(es) desde el cursor hacia adelante |

REFERENCIAS:

* Wireshark. (actualizado). Recuperado 31 de enero de 2020, de EcuRed website: <https://www.ecured.cu/Wireshark>
* Aprende a listar tus ficheros en Linux con el comando ls. (actualizado). Recuperado 31 de enero de 2021, de EDteam website: <https://ed.team/blog/aprende-listar-tus-ficheros-en-linux-con-el-comando-ls>
* Busque archivos de texto usando expresiones regulares. (actualizado). Recuperado 31 de enero de 2021, de IBM developer website: <https://developer.ibm.com/es/technologies/linux/tutorials/l-lpic1-v3-103-7/#:~:text=Una%20expresi%C3%B3n%20regular%20>
* Comando ECHO. (actualizado). Recuperado 1 de febrero de 2021, de Tu infomática f@cil website: <https://www.tuinformaticafacil.com/sistemas-operativos/windows/comando-echo>
* Linux PATH Variable. (actualizado). Recuperado 1 de febrero de 2021, de Baeldung website: <https://www.baeldung.com/linux/pathvariable#:~:text=The%20PATH%20variable%20is%20an,path%20when%20running%20a%20command>.
* Linux: Añadir ruta al PATH. (actualizado). Recuperado 1 de febrero de 2021, de Sysadmit website: <https://www.sysadmit.com/2016/06/linux-anadir-ruta-al-path.html>
* Variables de entorno: qué son, para qué sirven . (actualizado). Recuperado 1 de febrero de 2021, de Genbeta website: <https://www.genbeta.com/desarrollo/variables-entorno-que-sirven-como-podemos-editarlas-windows-linux>
* Variables de entorno: ¿qué son y para qué sirven?. (actualizado). Recuperado 1 de febrero de 2021, de soloLinux website: <https://www.sololinux.es/variables-de-entorno-que-son-y-para-que-sirven/>
* EDITOR VI. (actualizado). Recuperado 8 de febrero de 2021, de uniroja website: <https://www.unirioja.es/cu/enriquez/docencia/Quimica/vi.pdf>
* Resumen de los comandos básicos de vi. (2010). Recuperado 8 de febrero de 2020, de Oracle website: <https://docs.oracle.com/cd/E19620-01/805-7644/6j76klopr/index.html>
* Editor Vi: Cómo ir a una línea o palabra en particular en un fichero (actualizado). Recuperado 8 de febrero de 2020, de Ochobitshacenunbyte website: <https://www.ochobitshacenunbyte.com/2018/06/11/editor-vi-como-ir-a-una-linea-o-palabra-en-particular-en-un-fichero/>