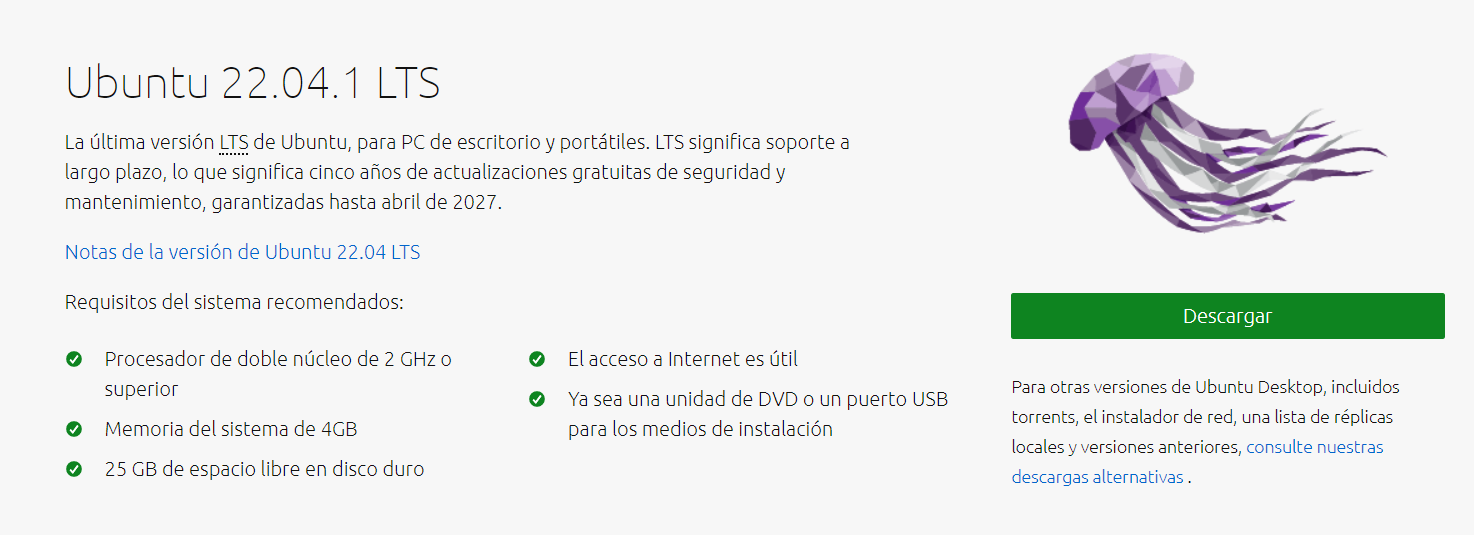
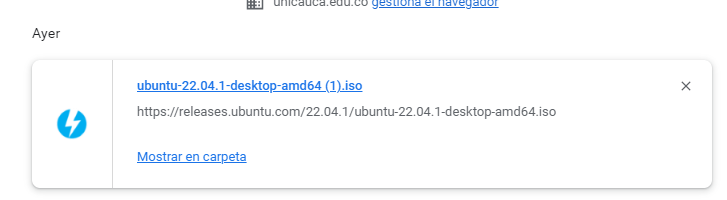
EVIDENCIAS CLASES 15/NOV/2022

Por: Brayan David Ruiz Dorado

Preparamos el entorno para tener una máquina virtual de Linux, en este caso utilizamos UBUNTU en su versión 22.04.1 LTS, el cual da garantía de un soporte a largo plazo.



Obtenemos la imagen iso de Ubuntu



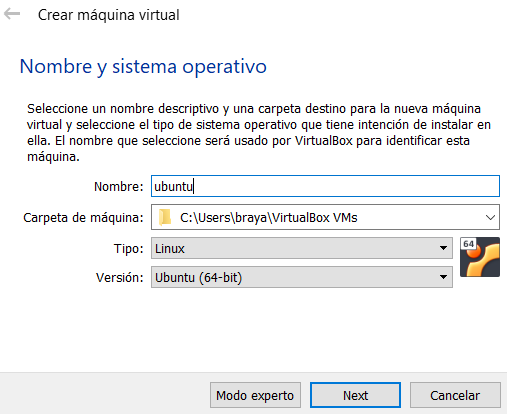
Descargamos e instalamos Oracle VM VirtualBox



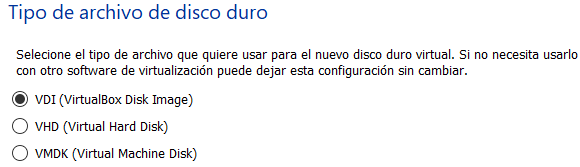
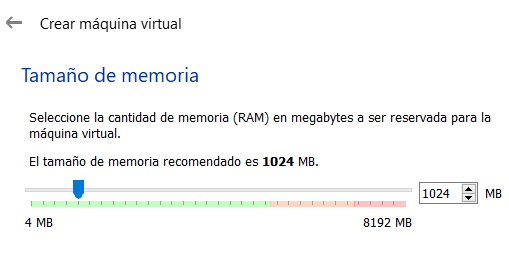
Abrimos Oracle VM VirtualBox y le damos a “Nueva”



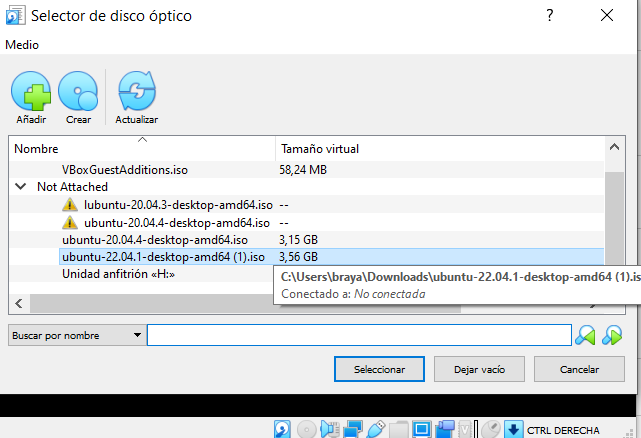
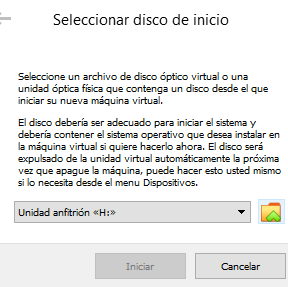
Creamos una nueva máquina virtual llamada ubuntu



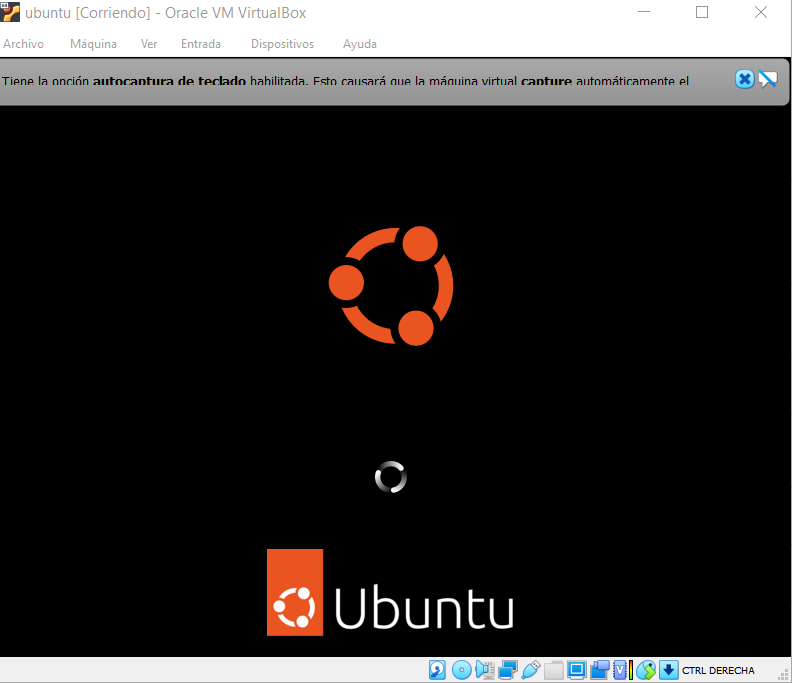
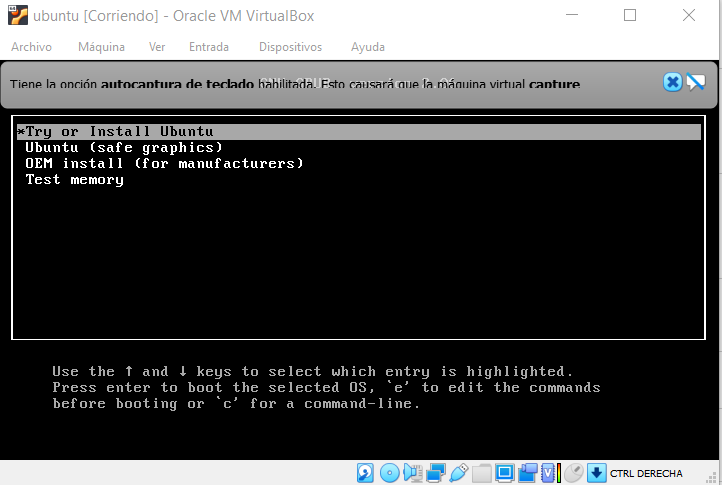
Configuramos la máquina virtual

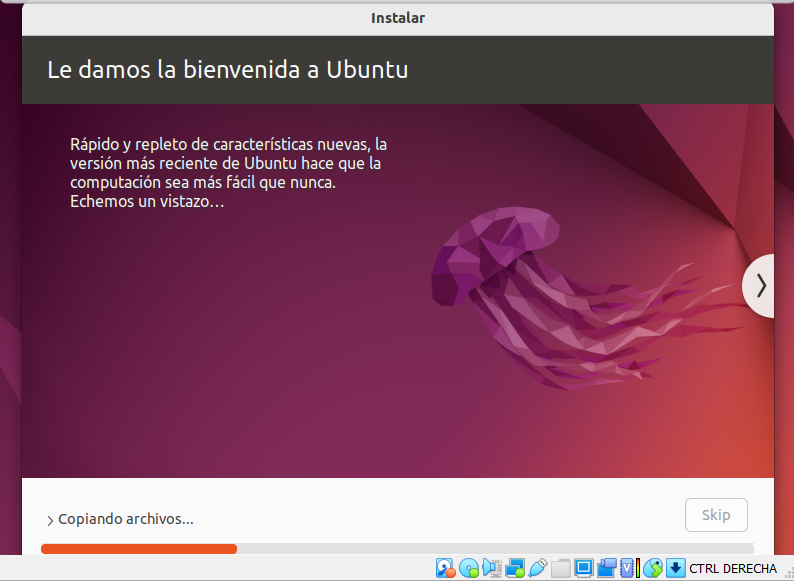


Montamos la imagen iso donde esta el Ubuntu



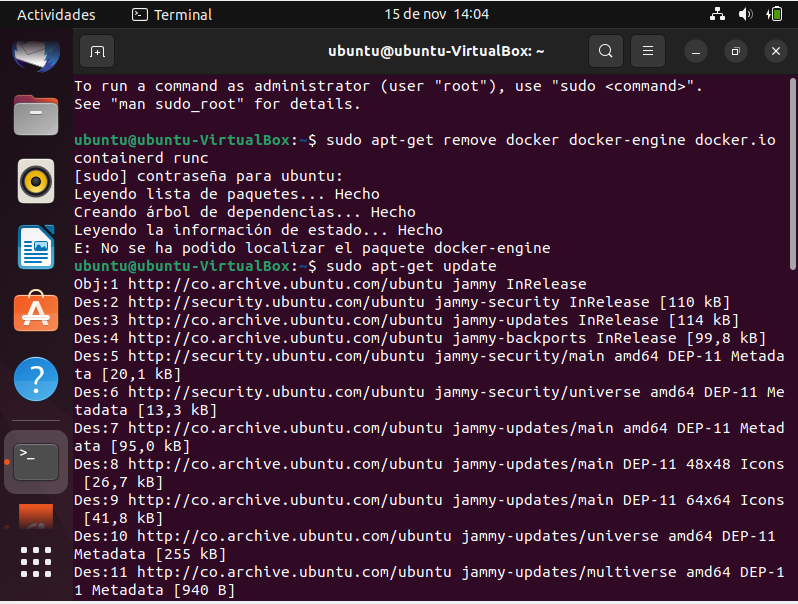
Se realiza la instalación correspondiente



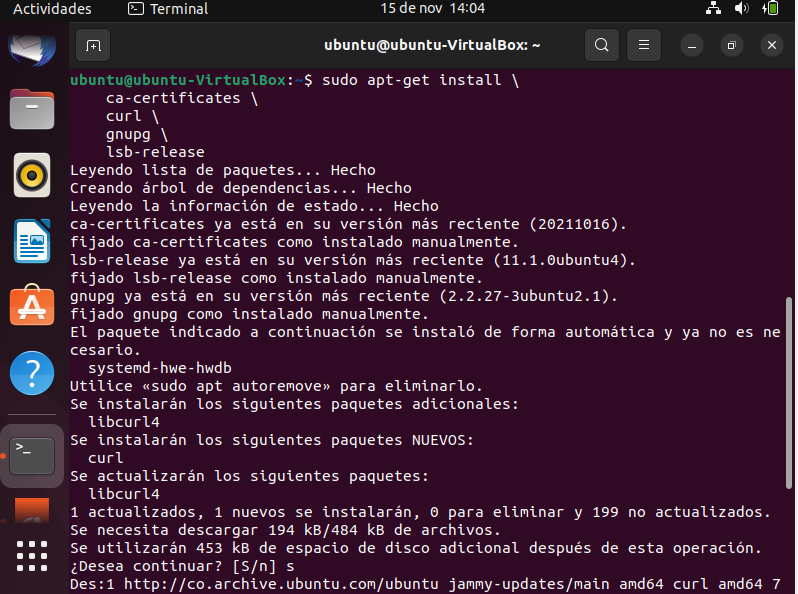


**INSTALACIÓN DE DOCKER EN UBUNTU:**

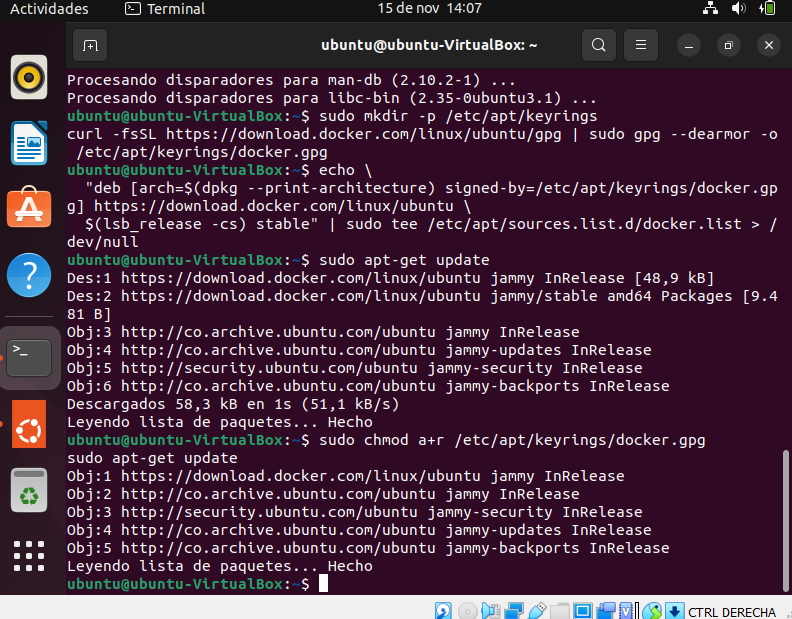
A continuación se instala en linux los dockers



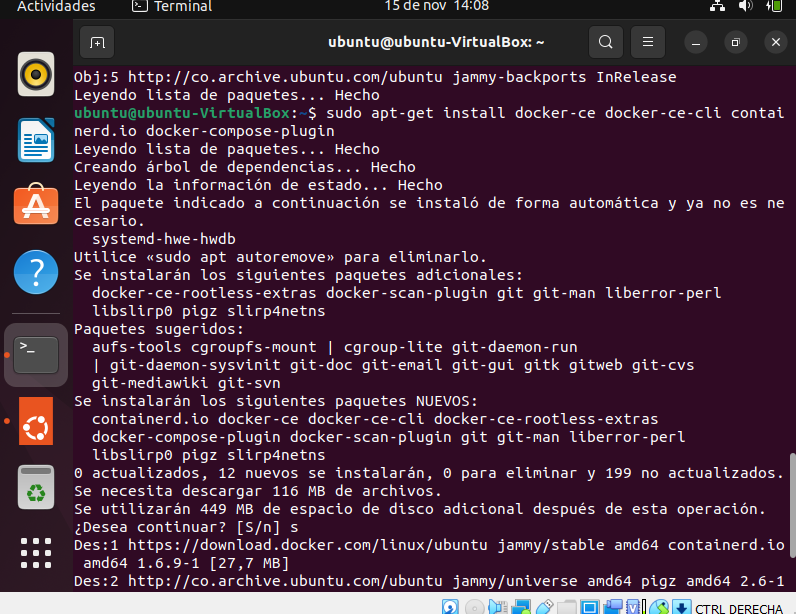
Actualice el aptíndice de paquetes e instale paquetes para permitir aptel uso de un repositorio a través de HTTPS:



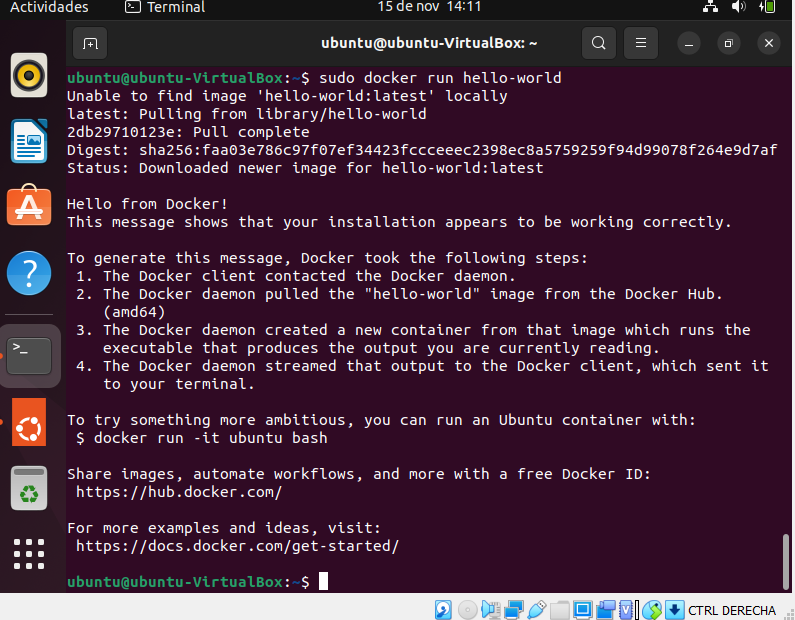
Agregue la clave GPG oficial de Docker:**Instalar el motor Docker**



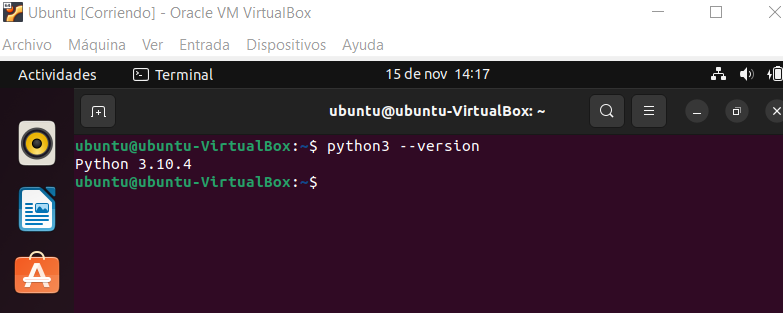
instalando Docker Engine, containerd y Docker Compose.



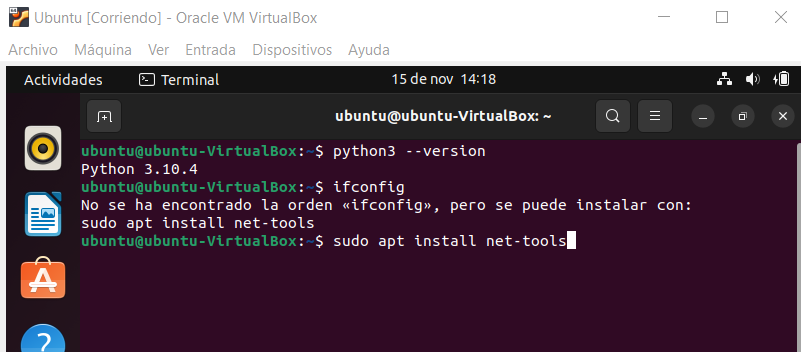
Verifique que la instalación de Docker Engine sea exitosa ejecutando la hello-world imagen:



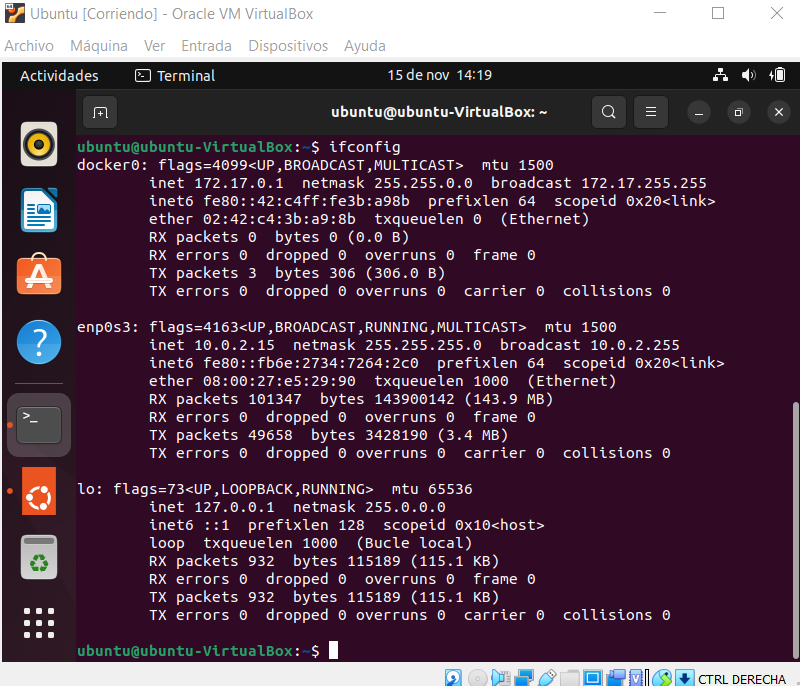
**PYTHON EN UBUNTU:**



Instalamos una serie de herramientas que nos van a permitir ver las redes en linux e identificar servicios y puertos ocupados en el sistema con los comandos ss, netstat y lsof.



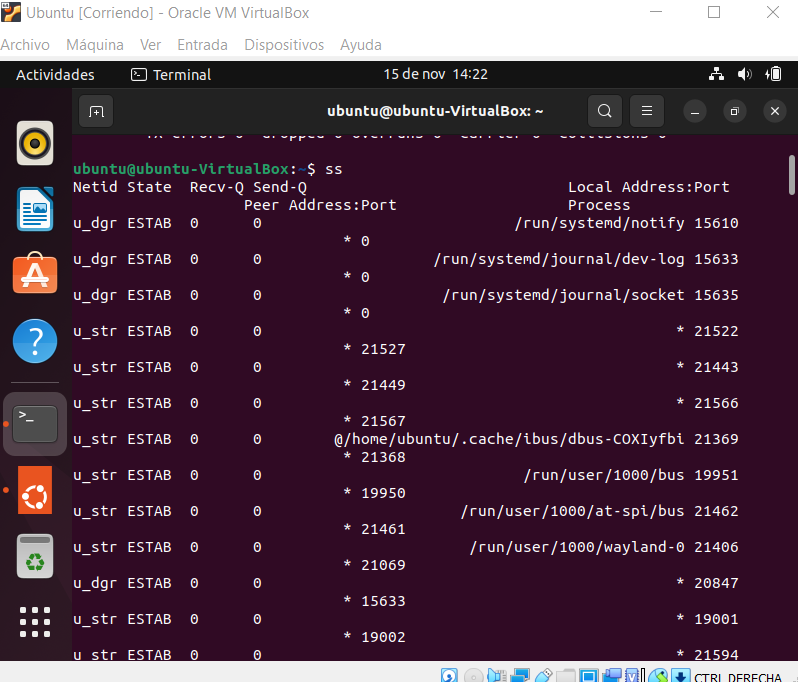
corremos el comando ***ifconfig***



Se puede observar los puertos, direcciones, servicios….. hasta el docker que hemos instalado

**COMANDO SS EN LINUX**

Usando el comando **ss** que nos permitirá observar una gran cantidad de información sobre los puertos, son una lista de [sockets](https://phoenixnap.com/glossary/what-is-a-socket) abiertos que no escuchan con conexiones establecidas.



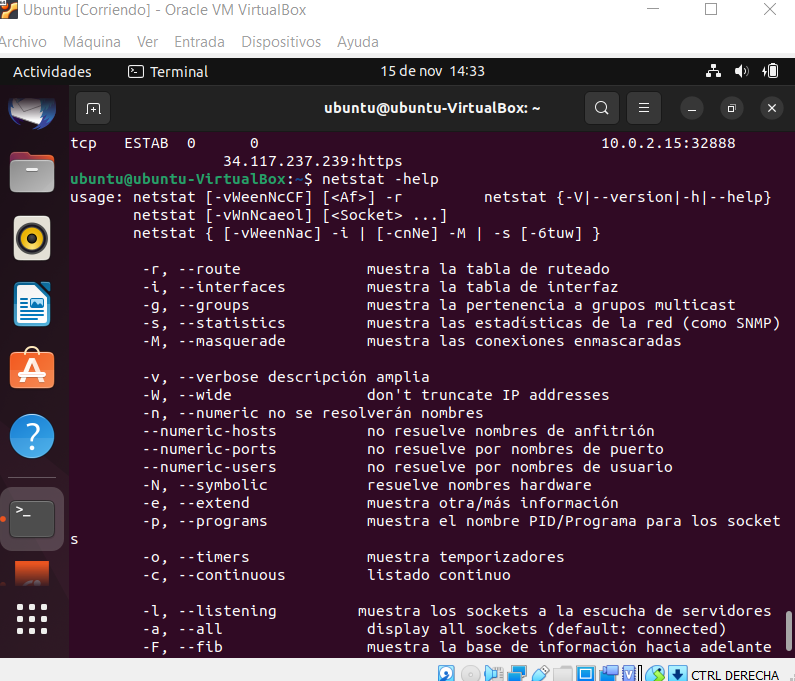
Las columnas muestran los siguientes detalles:

* **Netid** – Tipo de socket. Los tipos comunes son TCP , UDP , u\_str (secuencia Unix) y u\_seq (secuencia Unix).
* **Estado :** estado del zócalo. Más comúnmente ESTAB (establecido), UNCONN (desconectado), LISTEN (escuchando).
* **Recv-Q :** número de paquetes recibidos en la cola.
* **Send-Q :** número de paquetes enviados en la cola.
* **Dirección local: puerto :** dirección de la máquina local y el puerto.
* **Peer address:port** : dirección de la máquina y el puerto remotos.

COMANDO NETSTAT

netstat (estadísticas de red) es una herramienta de línea de comandos que muestra las conexiones de red (entrantes y salientes), tablas de enrutamiento y una serie de estadísticas de interfaz de red.

netstat es potente y puede ser una herramienta útil para solucionar problemas relacionados con la red y verificar las estadísticas de conexión.



## Established Connection

Si está buscando todas las conexiones establecidas desde el servidor.

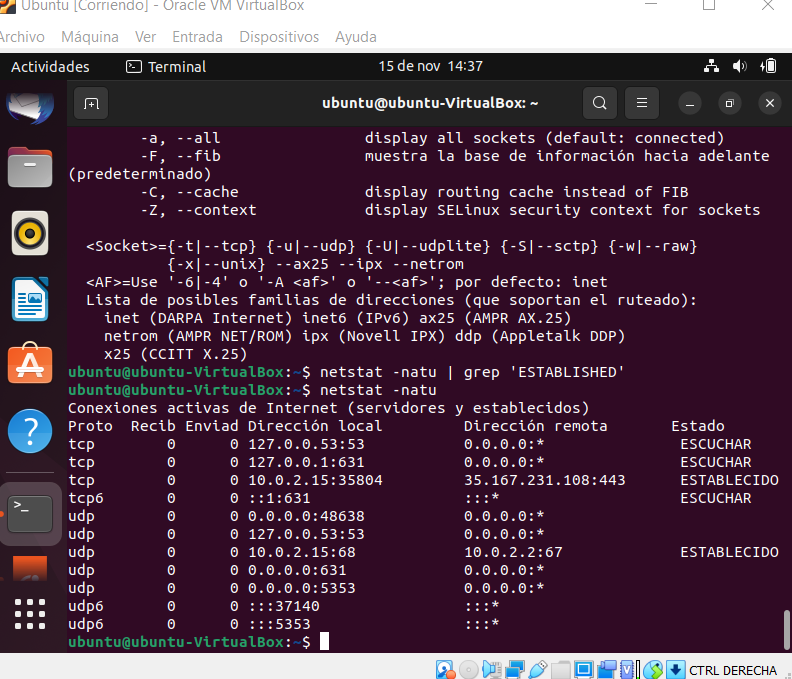


Tabla de enrutamiento

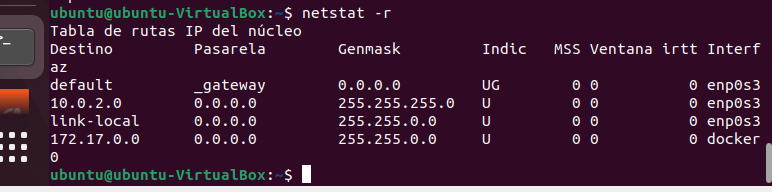
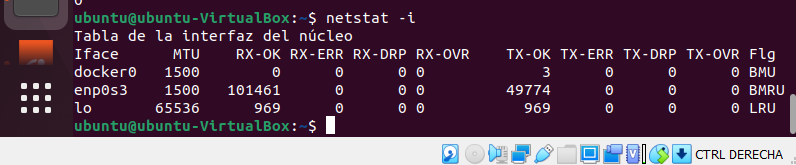


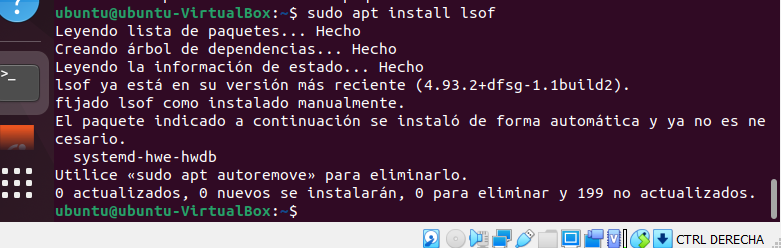
Tabla de interfaces de Ethernet



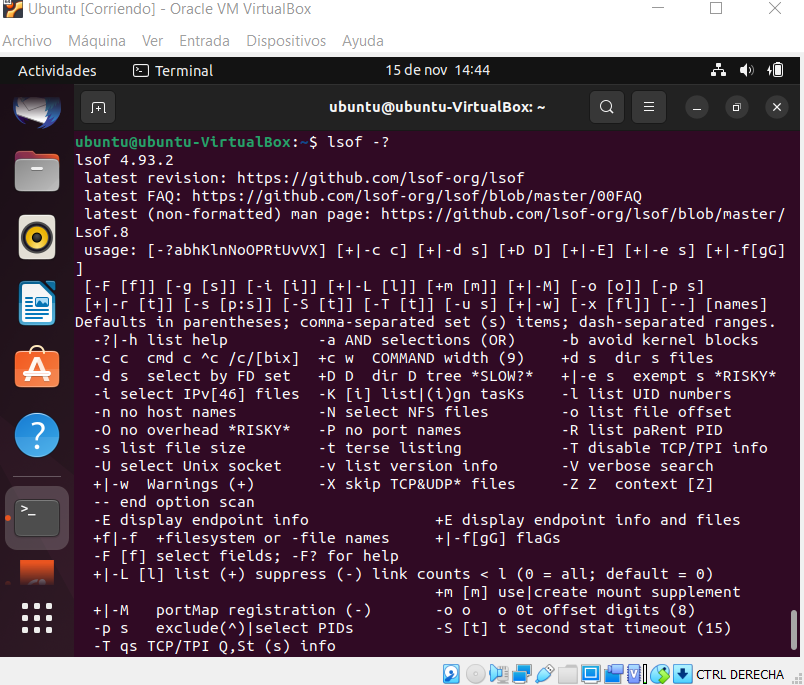
**COMANDO lsof**

Con lsof, puede encontrar diferentes procesos que bloquean un archivo o directorio, un proceso que escucha en un puerto, la lista de procesos de un usuario, todos los archivos que un proceso está bloqueando. Primero cubriremos su instalación y luego algunos comunes ejemplos de uso en este articulo.

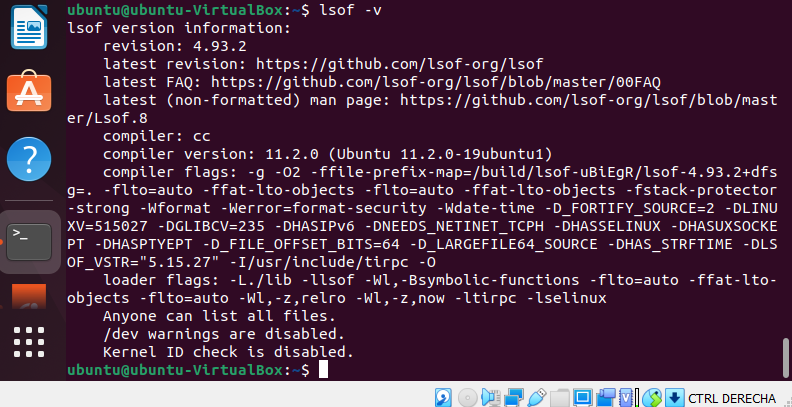
Instalamos:



comando de ayuda lsof

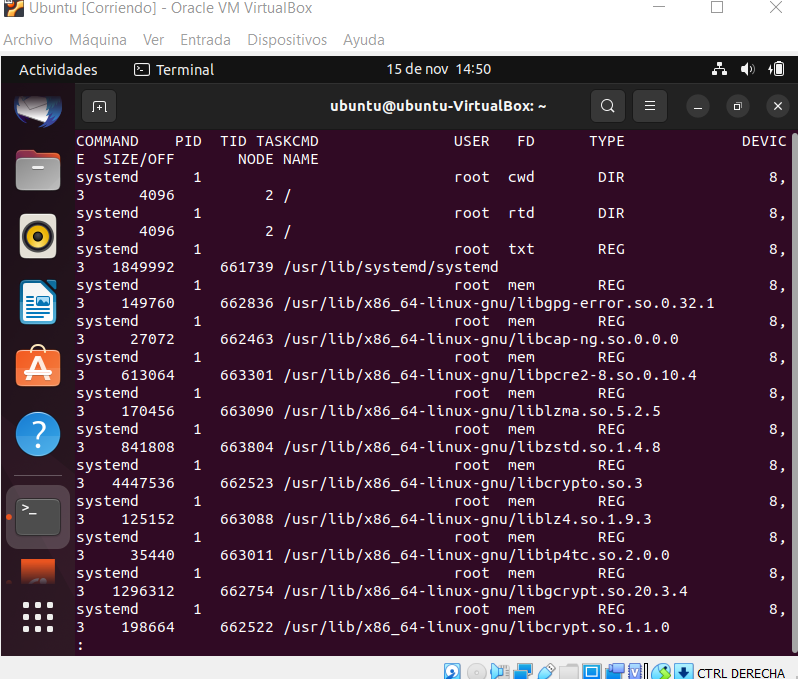


Verificando versión lsof

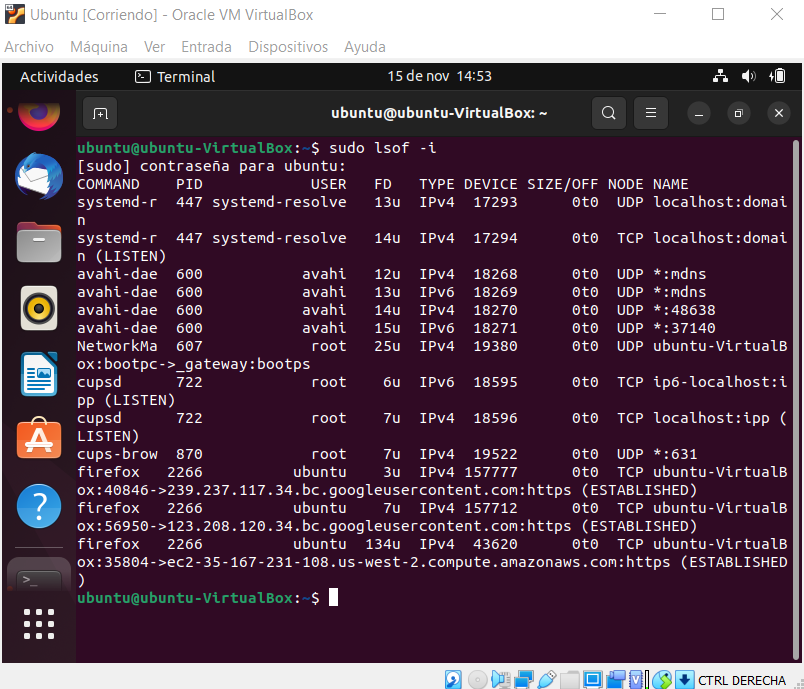


Ejemplo de comando lsof

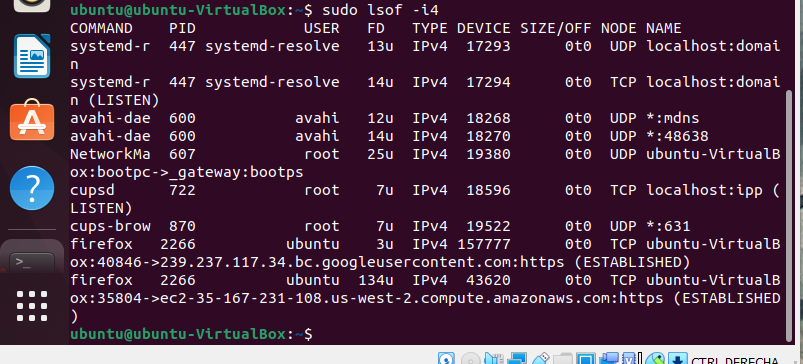
Ejecutar lsof sin ninguna opción mostrará una lista de todos los archivos que están abiertos actualmente por procesos activos.

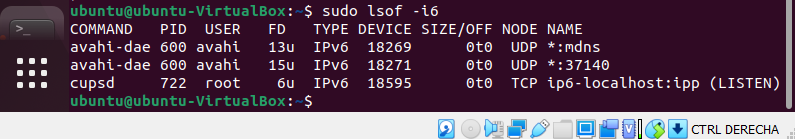


lsof admite la lista de cualquier tipo de archivos de Linux que incluyen sockets de red, etc. Como tal, podemos enumerar los detalles de las conexiones de red abiertas usando -i bandera.



Hay una opción para filtrar la lista de conexiones de red limitándola a IPv4 o IPv6.





**EVIDENCIA PRACTICA 2:**