Índice:

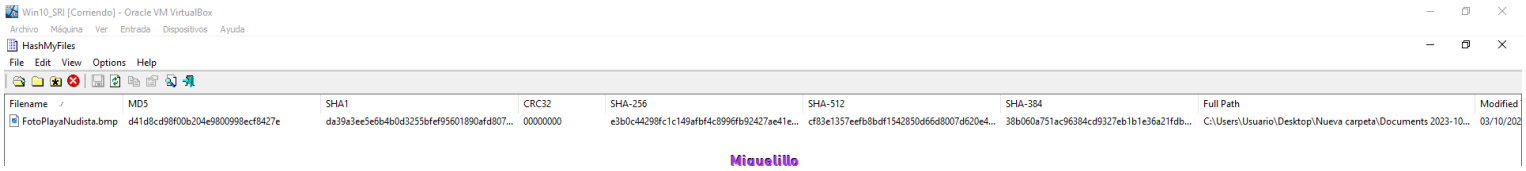
Ejercicio 1

a) Análisis forense y uso de comandos o herramientas de análisis forense.

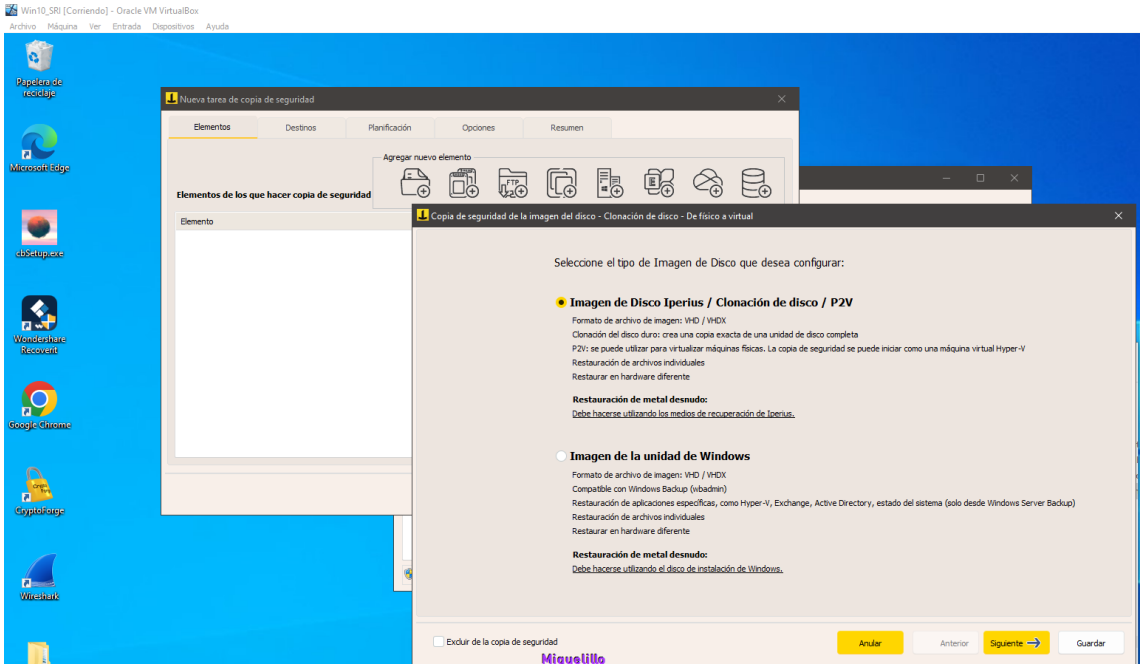
Solución:

A la hora de realizar un análisis forense se utiliza un documento de cadena de custodia lo que indica que las evidencias que han sacado del dispositivo no han sido manipuladas y se pueden presentar como pruebas en un juicio para confirmar que no ha sido confirmado se saca la función Hash del documento

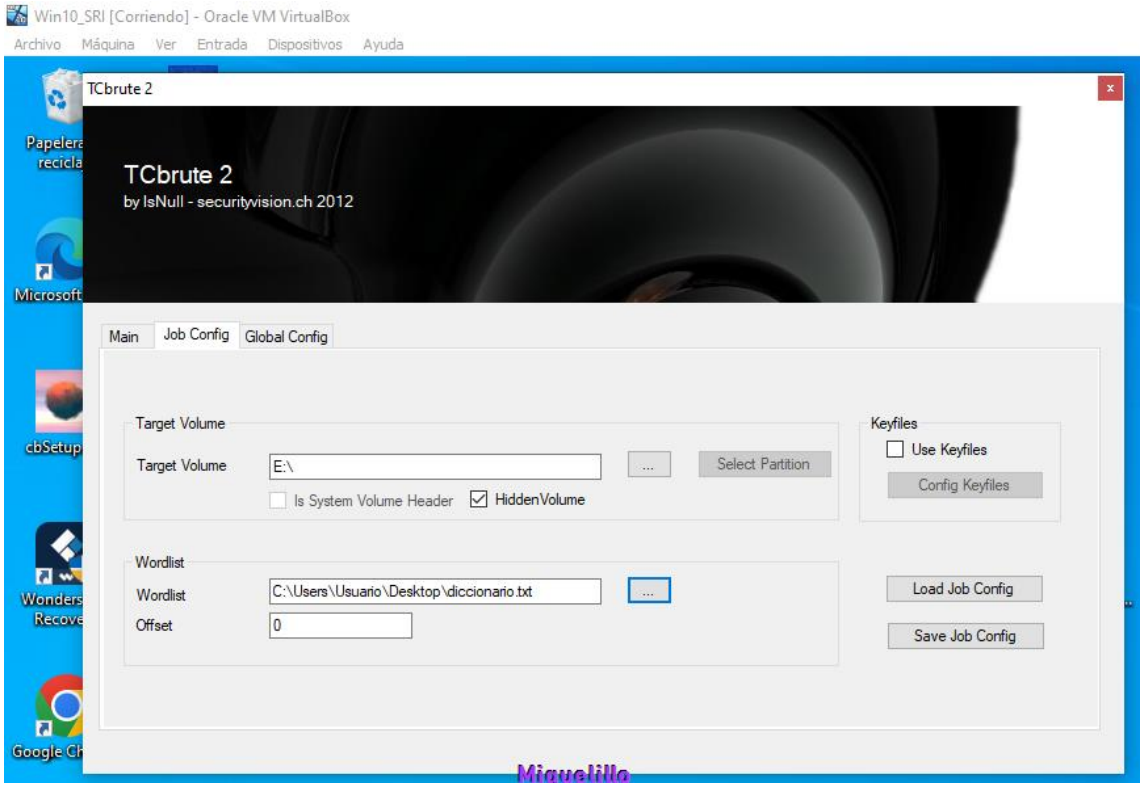
En este caso he usado HashMyFiles



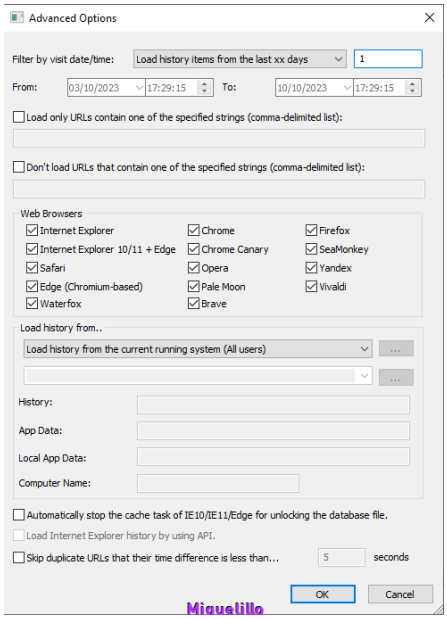
En un análisis forense se suele clonar el disco duro para mantener la integridad del original y se trabaja con el clonado. O bien con una clonadora de discos física con software dedicado como **Iperius Backup**

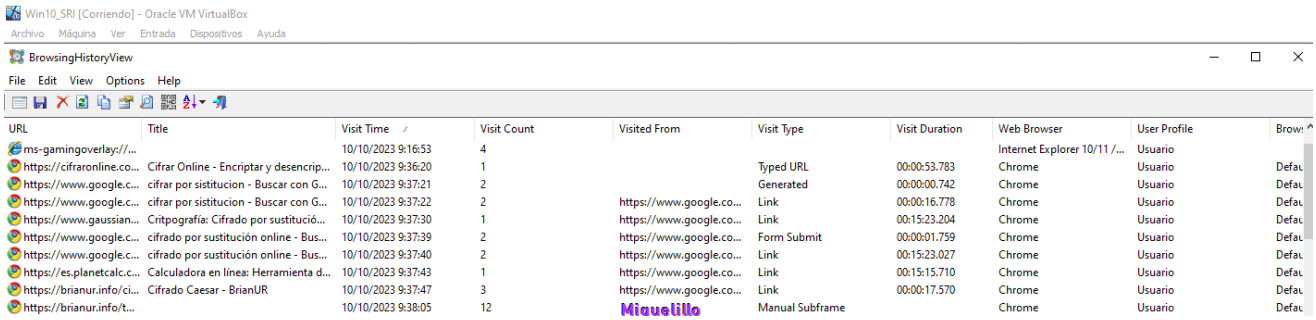


En caso de estar cifrado podemos hacer un ataque de fuerza bruta si tenemos una mínima idea de cómo es la contraseña podríamos no tardar mucho pero si no tenemos la mínima idea y la contraseña no es insegura o de diccionario podríamos tardar cientos de años. Voy a usar TCbrute

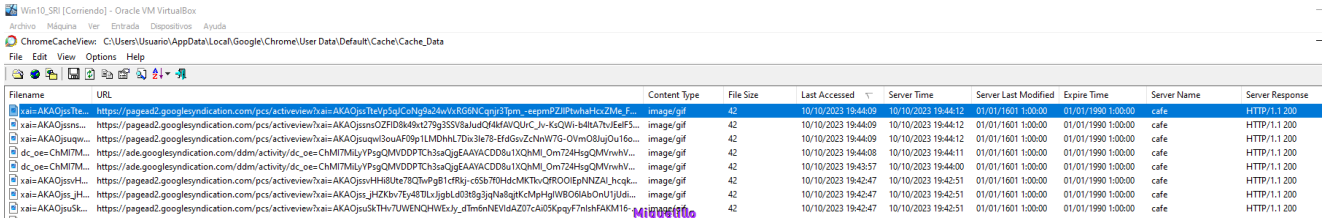


Herramienta para sacar el historial de los buscadores BrowsingHistory, en la configuración podemos seleccionar de cuantos días queremos los registros.

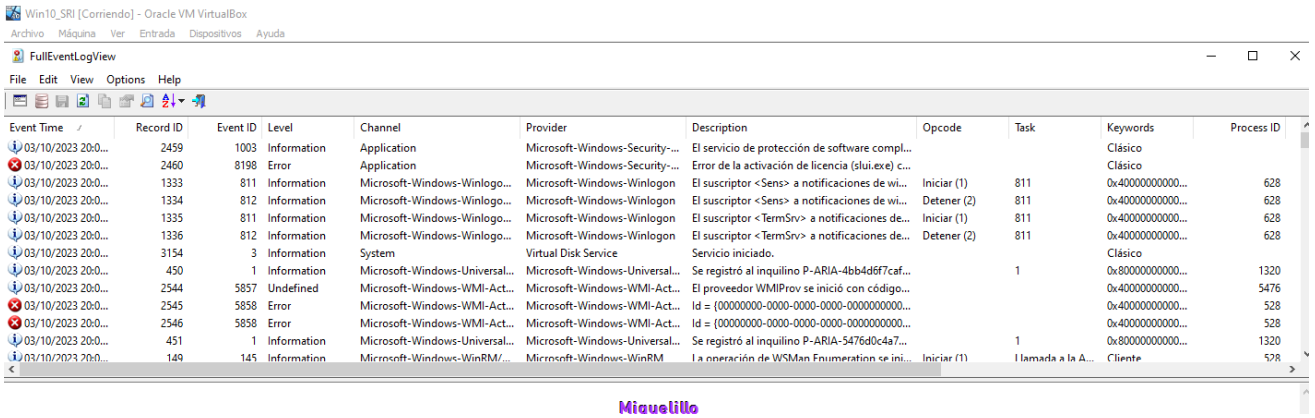




Herramienta para ver el caché de Chrome **ChromeChacheView**

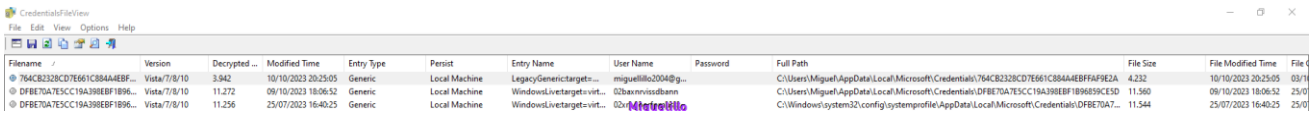


Para ver los registros del sistema **FullEventView**



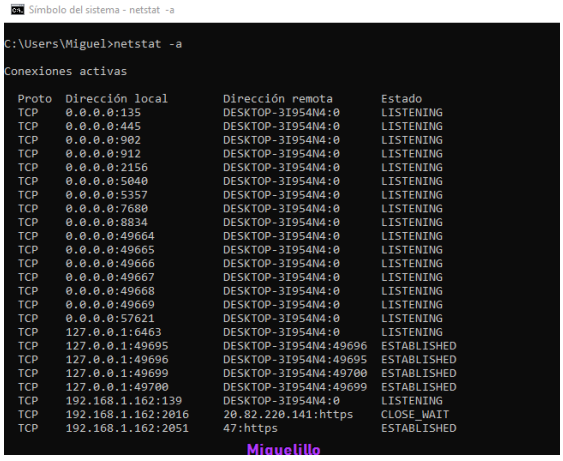
Para ver las redes a las que te has conectado y sus contraseñas **WirelessKeyView**

Para ver las cuentas y sus respectivas contraseñas **CredentialFileView**

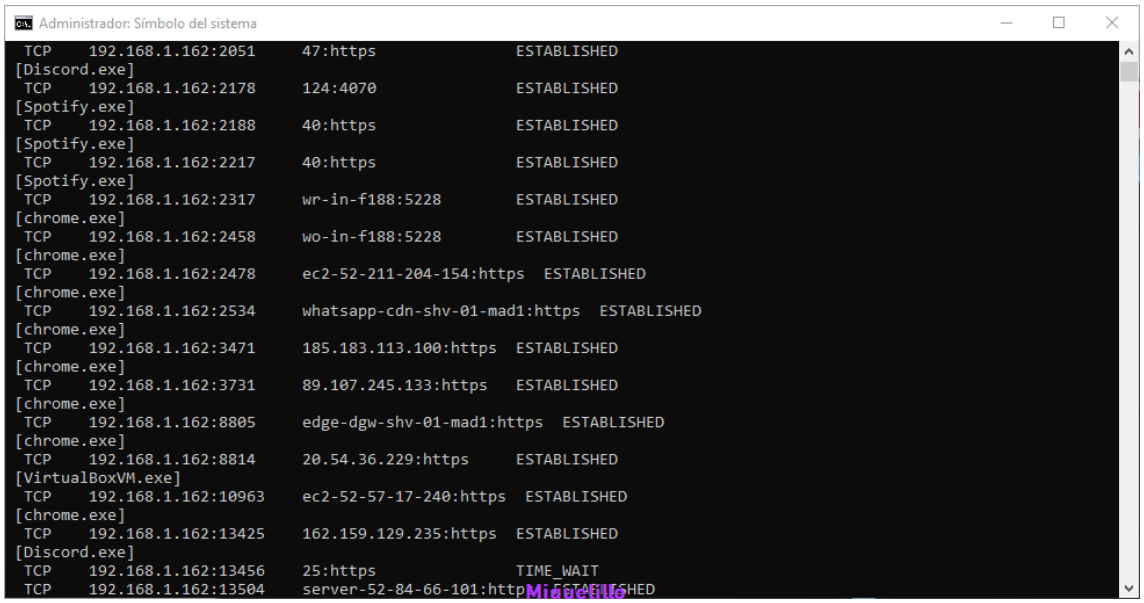


Comandos de Windows para detectar si hay un intruso en la red

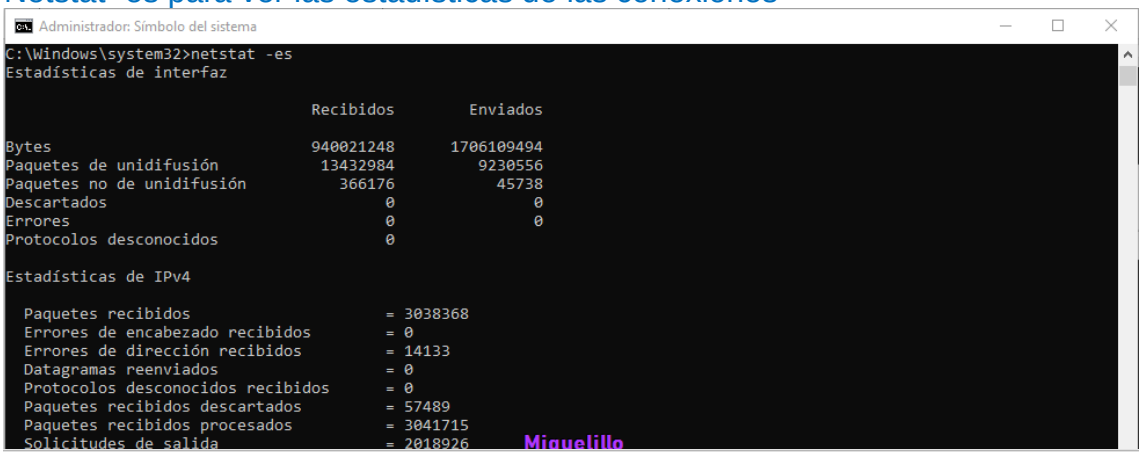
Netstat para ver el estado de los puertos y los protocolos

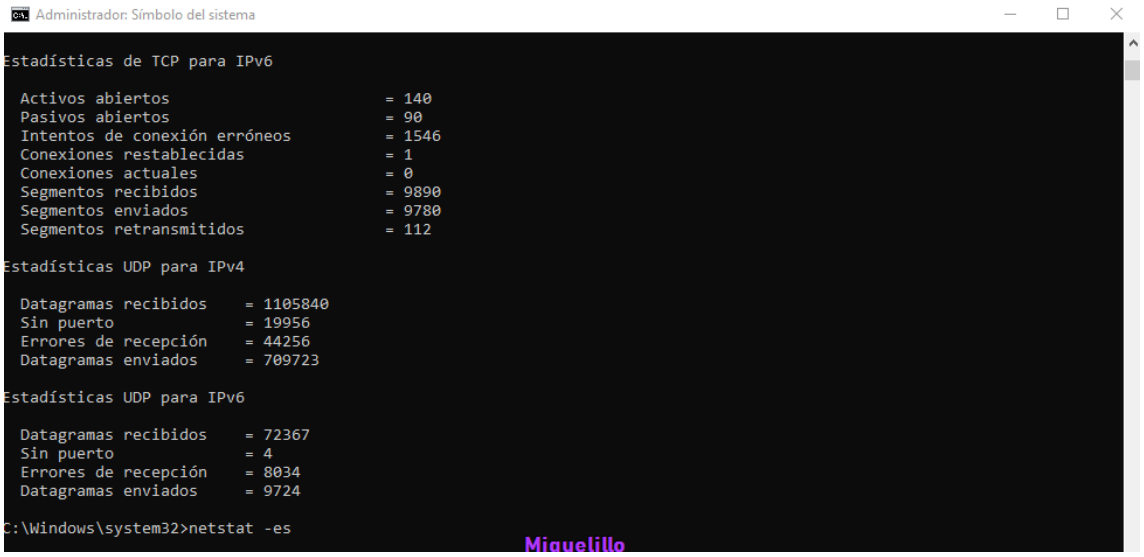


Netstat -b para ver el trafico por proceso

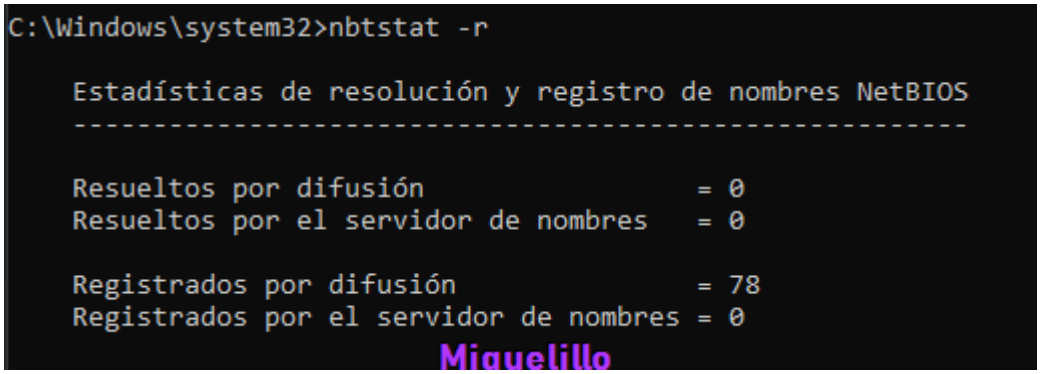


Netstat -es para ver las estadísticas de las conexiones

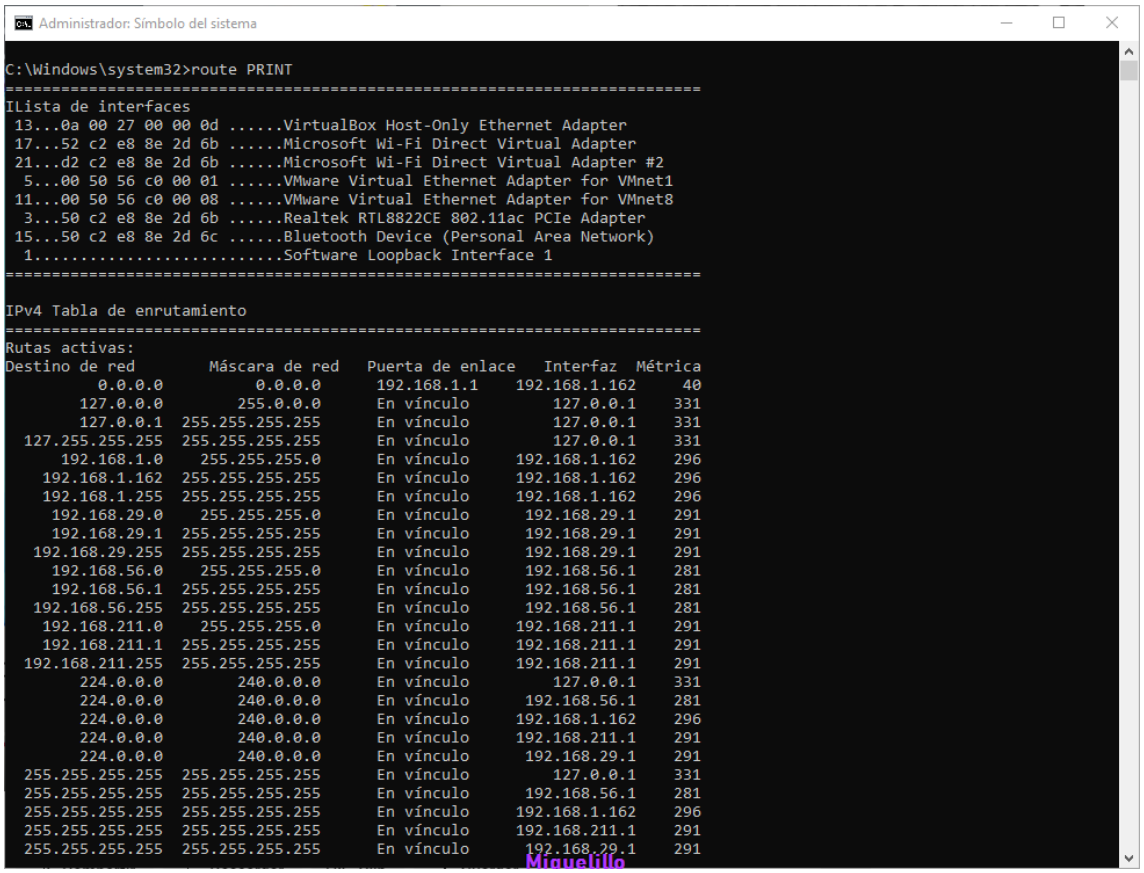




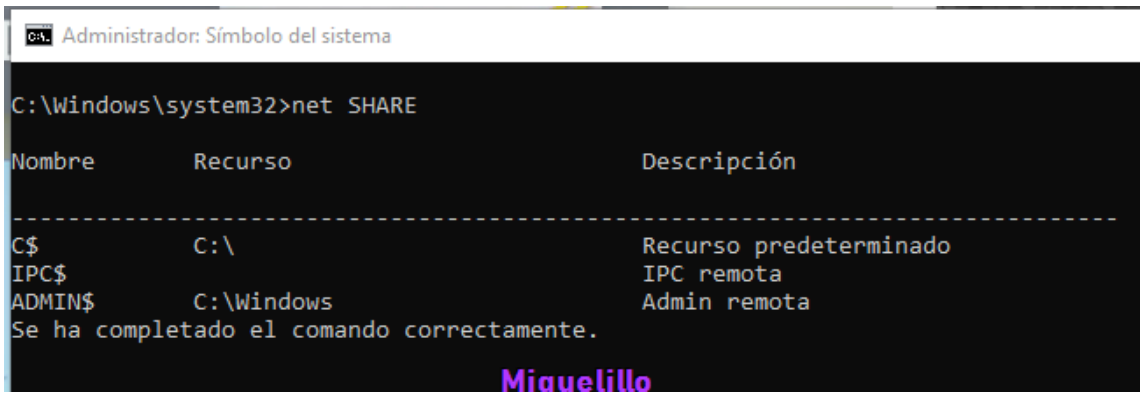
Para ver conexiones por NetBIOS nbtstat -r



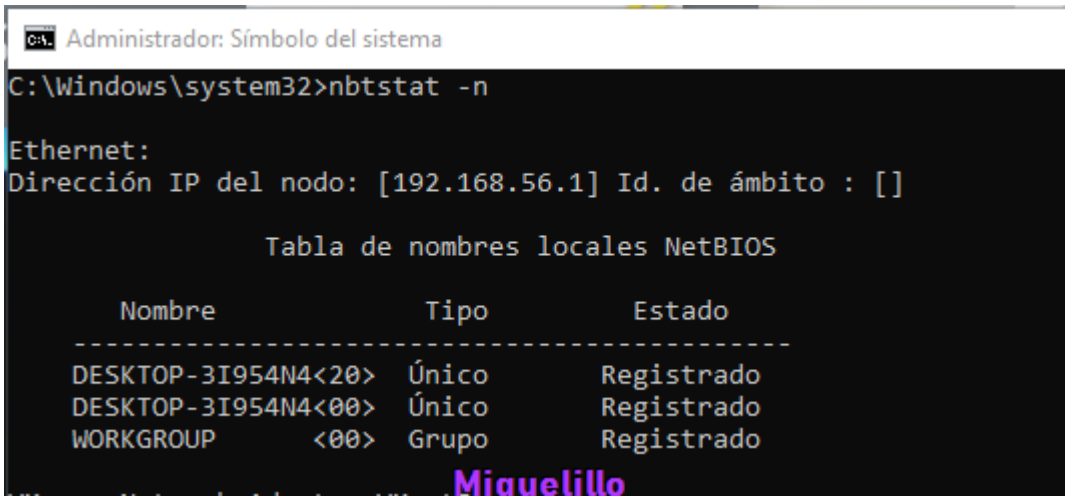
Con route PRINT podemos ver las tablas de enrutamiento en IPv4 y en IPv6



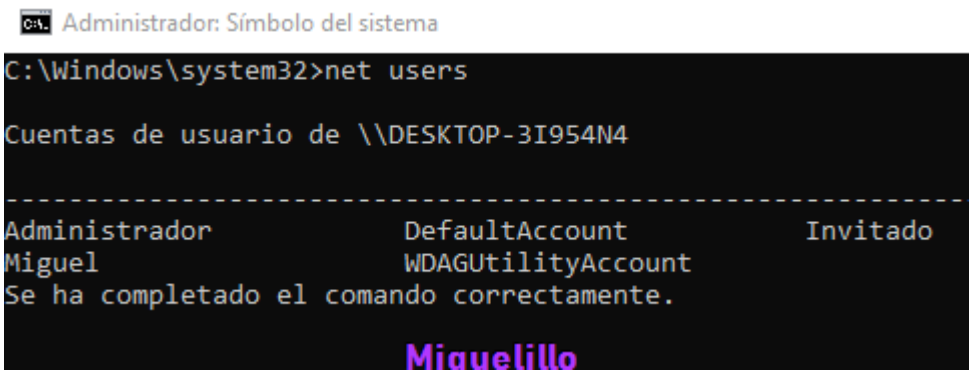
Para ver los recursos compartidos de la red **net share**



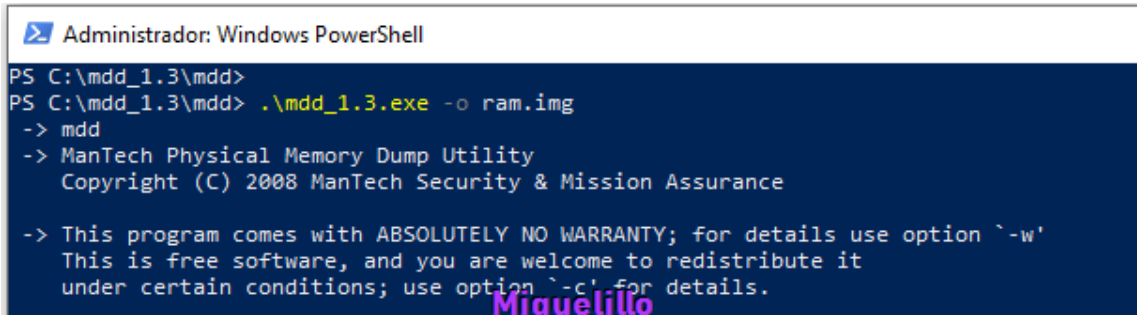
Para ver los usuarios de net bios nbtstat -n



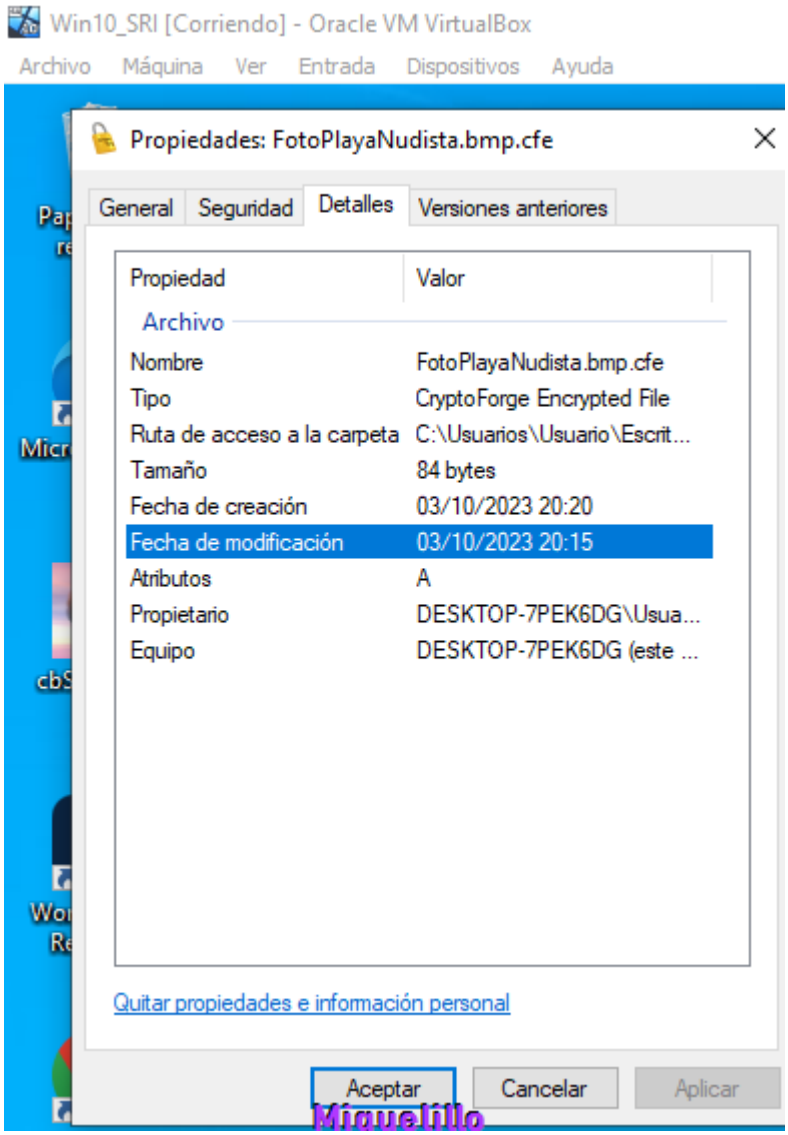
Para ver los usuarios de los recursos compartidos net users



Con la utilidad de mdd compiamos la RAM a un archivo y con Volatility -f interpretamos el archivo



Podemos desde propiedades obtener metadatos, aunque los archivos estén cifrados


Win10_SRI [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Propiedades: FotoPlayaNudista.bmp.cfe
General Seguridad Detalles Versiones anteriores
Propiedad Valor
Archivo
Nombre FotoPlayaNudista.bmp.cfe
Tipo CryptoForge Encrypted File
Ruta de acceso a la carpeta C:\Usuarios\Usuario\Escrit...
Tamaño 84 bytes
Fecha de creación 03/10/2023 20:20
Fecha de modificación 03/10/2023 20:15
Atributos A
Propietario DESKTOP-7PEK6DG\Usua...
Equipo DESKTOP-7PEK6DG (este ...
Quitar propiedades e información personal
Aceptar
Cancelar
Aplicar
Miguelillo