Lab 1.1 Image Mounting

Teoria

Y

Practica

Core Windows Forensics

Comprensión del sistema operativo y las aplicaciones

Un examinador/analista forense debe tener un sólido entendimiento del sistema operativo y la aplicación que está examinando. Solo al entender el sistema operativo y las aplicaciones en el sistema que estás examinando podrás saber dónde buscar evidencia de una acción.

Muchas veces, descubrirás que tendrás que realizar pruebas en tu laboratorio sobre aplicaciones para encontrar qué evidencia crea la aplicación cuando se realiza una acción, y luego ir al disco duro que estás analizando y buscar esa pieza de evidencia.

Como mencionamos antes acerca de simplemente realizar una búsqueda de palabras clave y exportar los resultados para su revisión por parte del agente del caso, ¿crees que un agente o investigador no técnico, no capacitado en forense, entiende lo suficiente sobre sistemas informáticos como para pedir archivos de vínculos (link files) o saber qué en el registro podría ayudar a su investigación? **No.**

Comprensión de la Evidencia Creada

La evidencia de una acción o actividad es creada tanto por el **usuario de la computadora como por el sistema en sí mismo**. Un ejemplo de esto podría ser un directorio creado por un usuario con el nombre que describe el contenido, como "ARCHIVOS PERSONALES". Otro ejemplo de evidencia creada por las acciones de un usuario podría ser la creación de un archivo tipo Shortcut cuando un archivo es abierto por el usuario.

La evidencia creada por una acción del sistema podría ser un **registro de auditoría** que muestre que el mantenimiento del sistema por defecto se ha ejecutado en el tiempo predeterminado, o los tiempos de acceso a archivos que son cambiados por un escaneo antivirus que se ejecuta automáticamente.

Entender qué tipos de evidencia se crean, cómo se crean y por qué, te ayudará a ser un mejor examinador.

Image Mounting

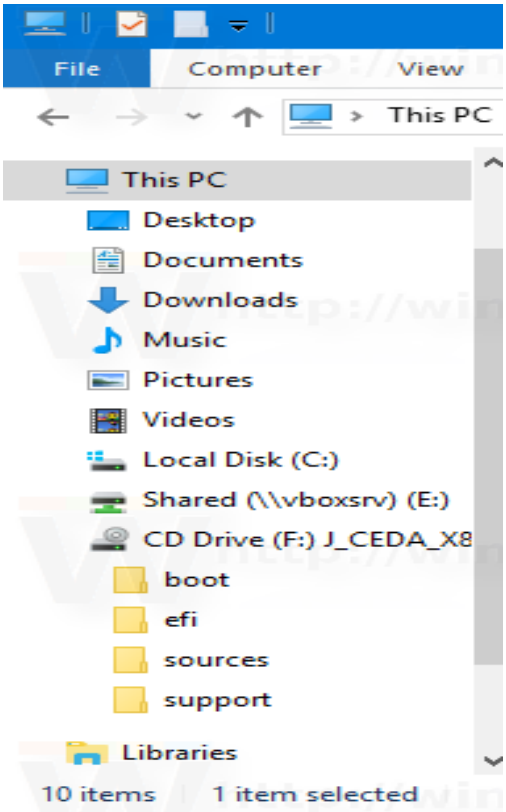
Algunos de los muchos beneficios de montar imágenes forenses son que los examinadores, e incluso investigadores sin entrenamiento forense, pueden ver e interactuar con los archivos montados en su aplicación nativa o la aplicación asociada instalada localmente en la máquina del revisor. Esto permite al revisor copiar archivos fuera del sistema de archivos montado. **Debido a que la imagen se monta en modo de solo lectura**, no hay preocupaciones de que se puedan copiar archivos en la imagen montada o de que la imagen montada se modifique de alguna manera.

Una imagen forense que se monta se ve como otra unidad conectada al sistema principal. Las aplicaciones de detección de antivirus y malware pueden ejecutarse contra el sistema de archivos montado. Esto podría ser

un gran primer paso para determinar si un virus o malware ha infectado el sistema.

De esta forma podemos decir de los beneficios de **Image Mounting** :

1. Interactuar con archivos utilizando su aplicación nativa o asociada.
2. Ejecutar aplicaciones de detección de antivirus y malware.
3. Compartir con computadoras remotas (trabajo en equipo)
4. Copiar archivos fuera de la imagen.
5. **Mantener la integridad forense.**



Arsenal RECON

Arsenal Recon es una suite de herramientas forenses desarrollada por Arsenal Consulting, una empresa especializada en análisis forense digital y ciberseguridad. Arsenal Recon se centra en proporcionar herramientas avanzadas para la adquisición, análisis y presentación de evidencia digital en investigaciones forenses.

Esta suite de herramientas incluye una variedad de utilidades diseñadas para ayudar a los investigadores forenses a realizar tareas como la adquisición forense de datos, el análisis de artefactos de sistemas operativos, la recuperación de datos eliminados y la visualización de información forense de una manera eficiente y efectiva.

Entre sus características:

1. Montar en modo de solo lectura como unidad o dispositivo físico
    - Tipos de montaje:
    - Imágenes RAW/DD, E01, S01, AD1 y L01

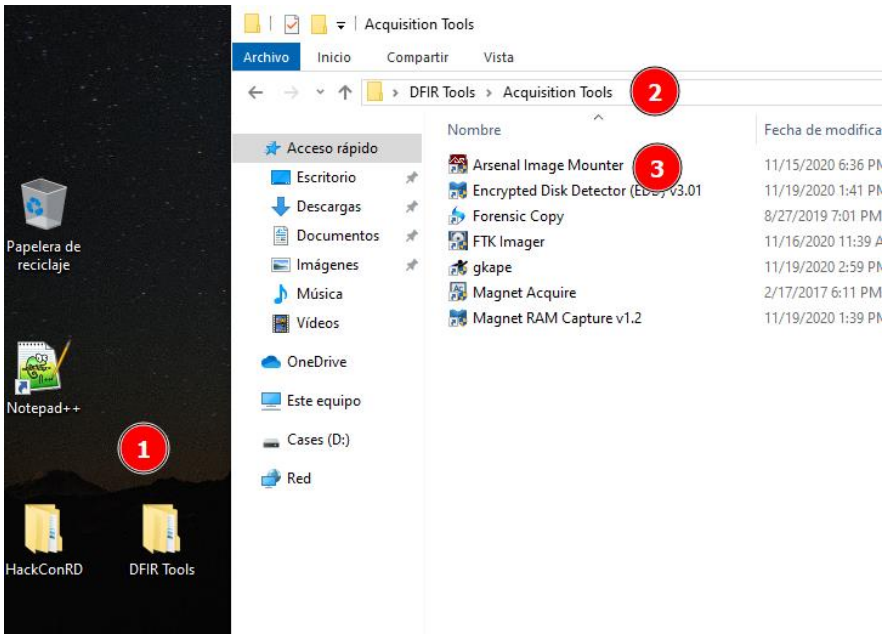
Laboratorio: Montar imágenes de disco usando Arsenal Image Mounter

Una capacidad importante en la informática forense es la capacidad de examinar la evidencia digital contenida dentro de **un formato de imagen forense.**

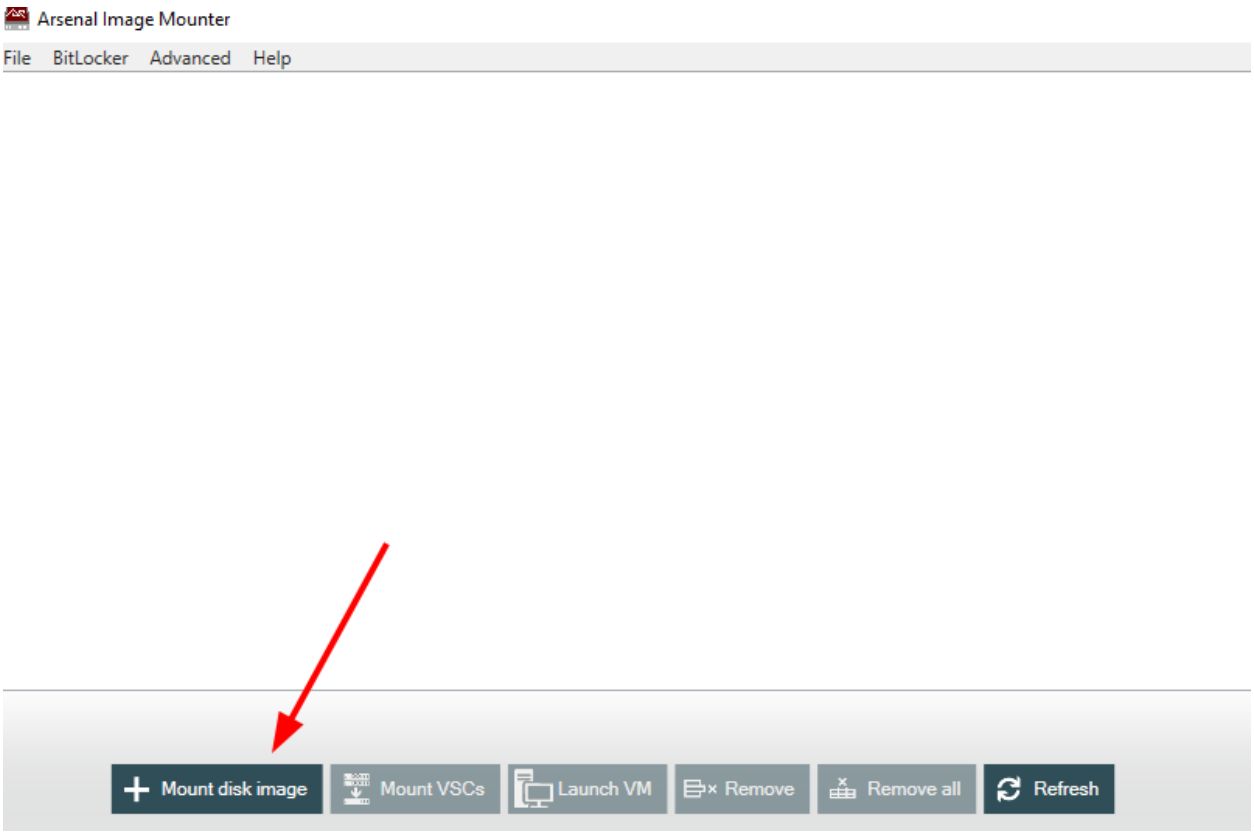
Arsenal Image Mounter (AIM) es una herramienta gratuita (también hay una versión comercial con características adicionales) que se puede utilizar para montar imágenes de disco forense en un sistema de examen forense. AIM puede montar imágenes de disco en formato **E01, Raw (dd), Advanced Forensic Format 4 (AFF4) y formatos de disco de máquina virtual como VMDK, VHD y OVA.**

AIM monta el contenido de las imágenes de disco como discos completos en Windows, no como comparticiones o particiones como lo hacen algunos otros productos. Las capacidades de montaje de bajo nivel de AIM **proporcionan acceso a artefactos especiales de Windows como copias de sombra de volumen y BitLocker que otros productos no tienen.**

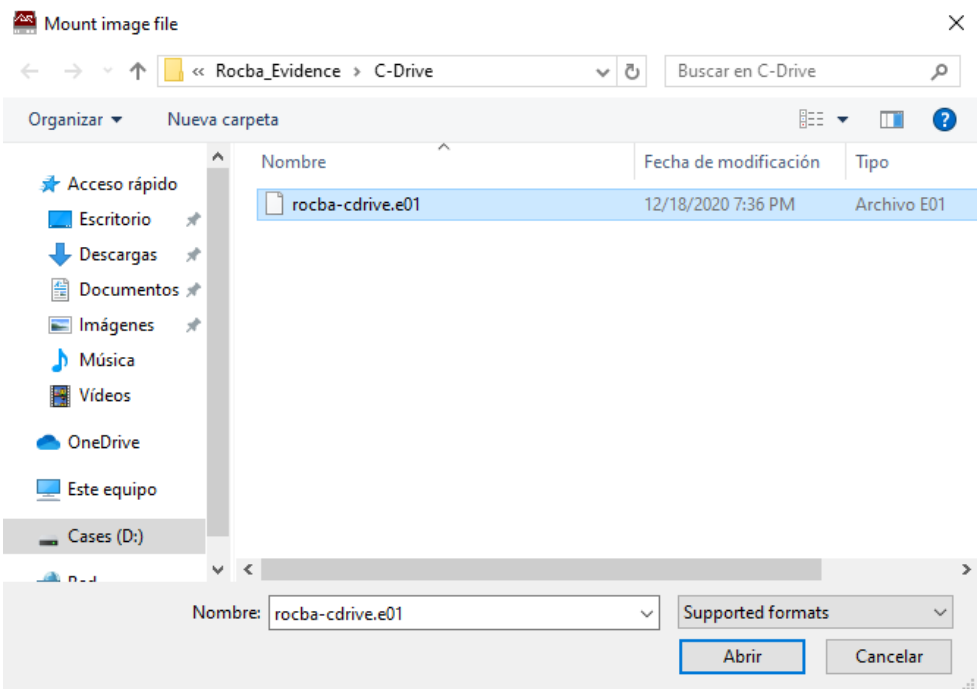
En nuestra máquina virtual, en el Desktop tenemos "DFIR TOOLS", dentro, tenemos una carpeta llamada "Acquisition Tools", y entre las herramientas abrimos Arsenal Image Mounter.



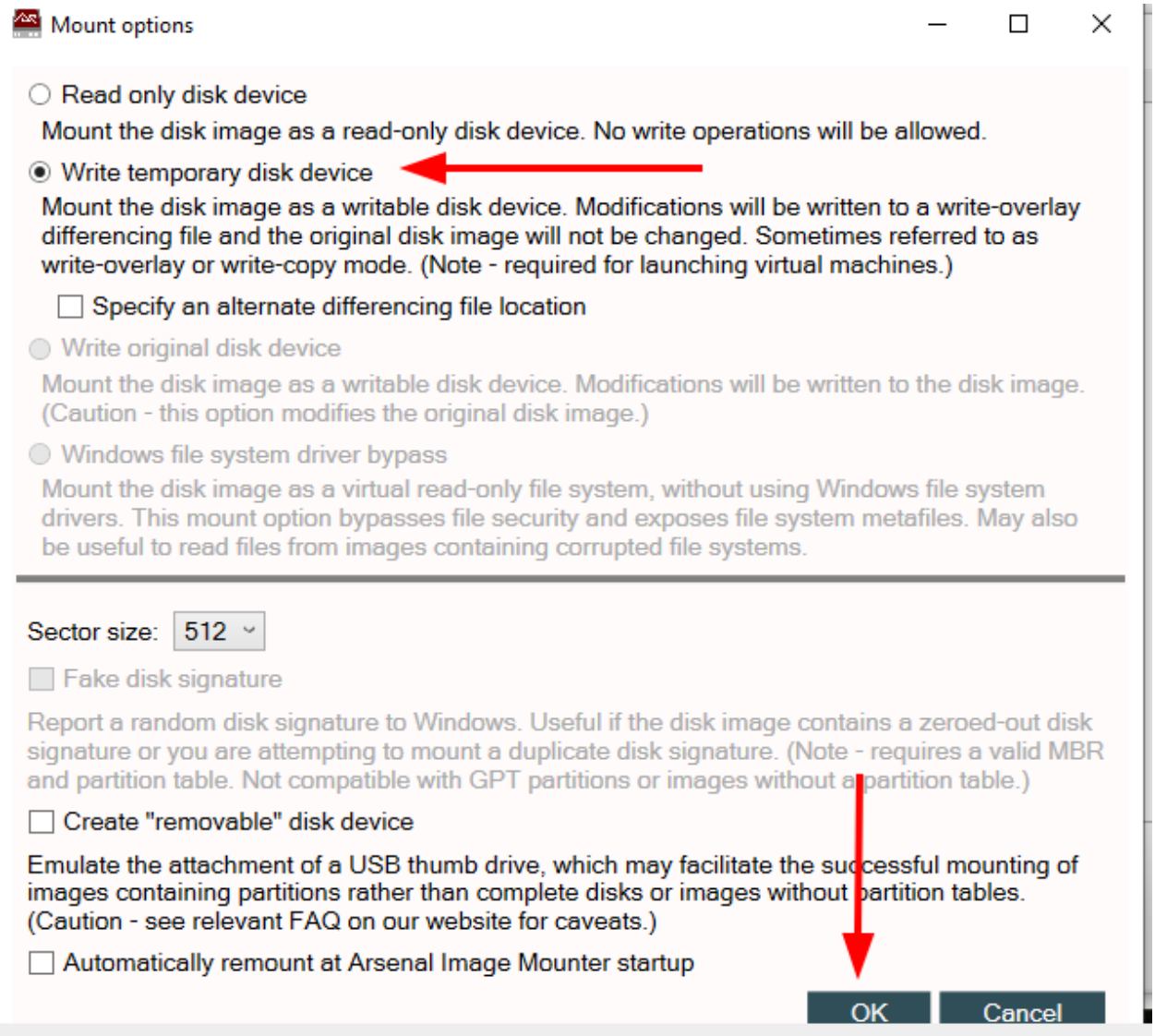
Abrimos el aplicativo



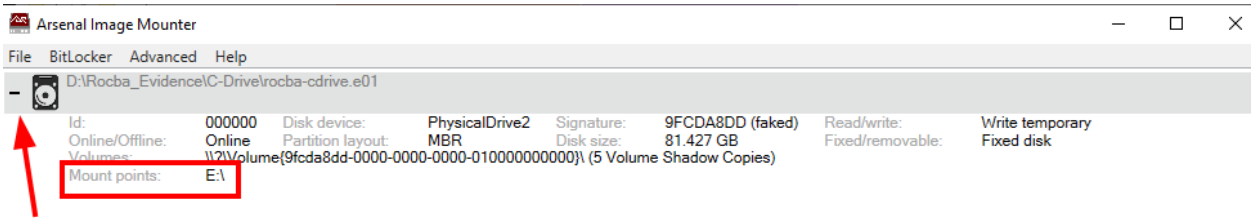
Y buscamos en la ruta: **D:\Rocba_Evidence\C-Drive\rocba-cdrive.e0**



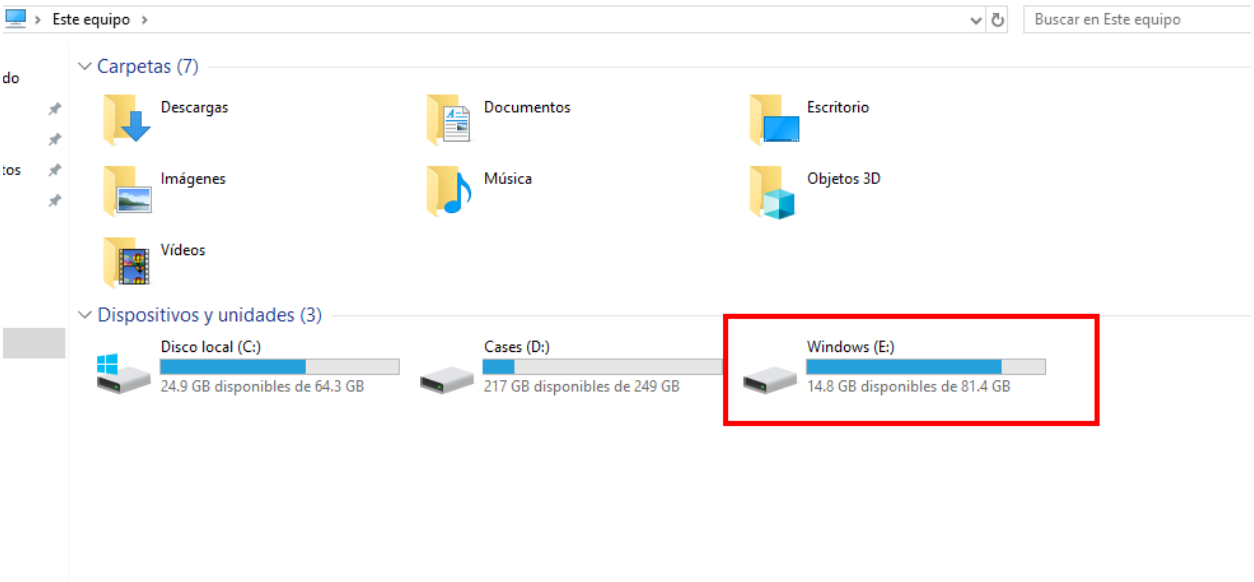
Seleccionamos **Write temporary disk device** en **Mount options**



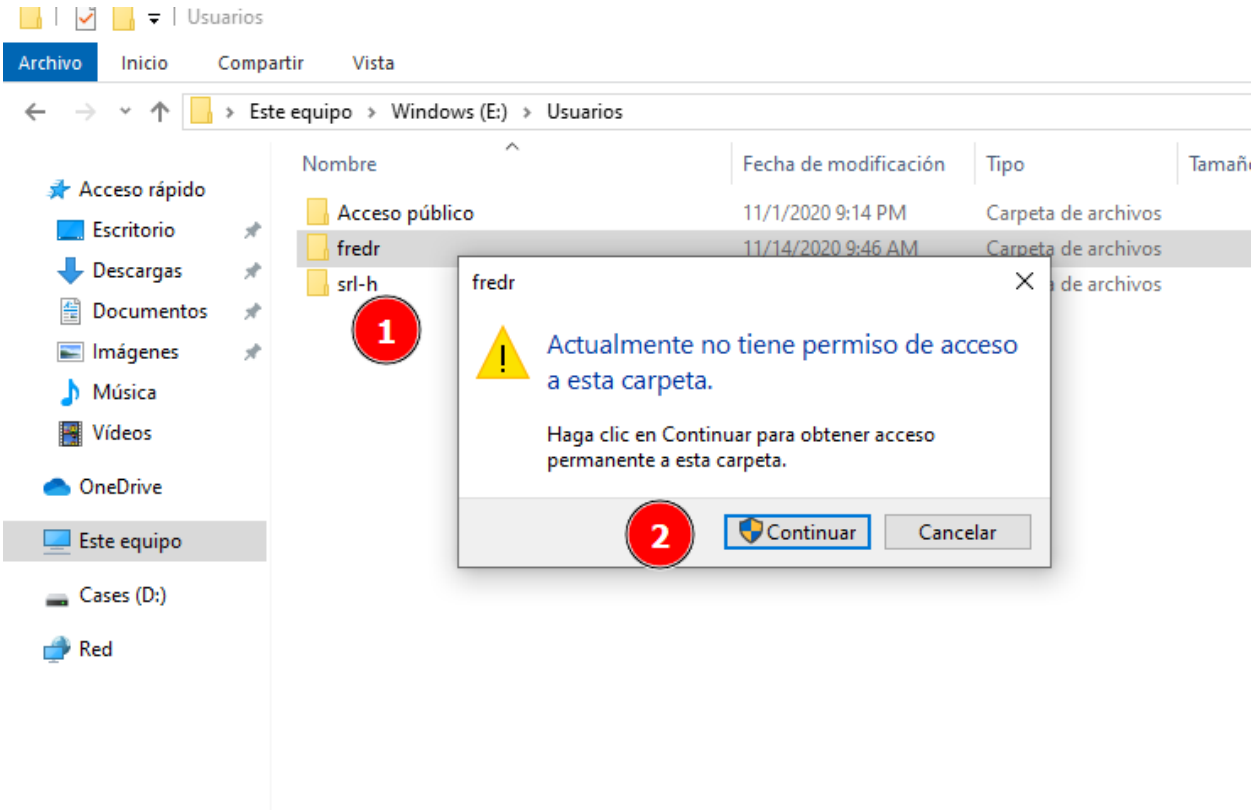
Una vez montada, deberías ver la ventana principal de Arsenal Image Mounter mostrar la siguiente pantalla:



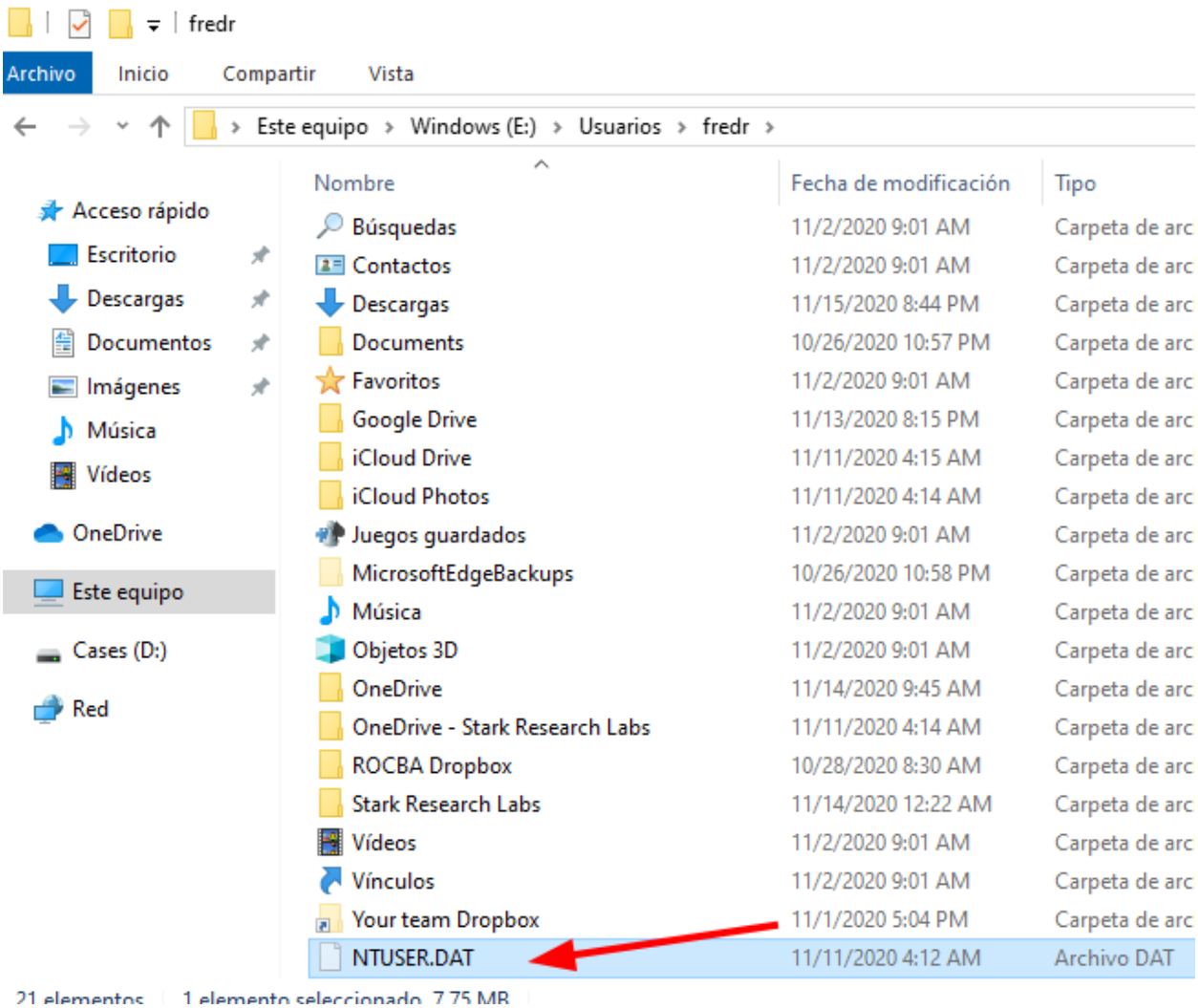
En el Explorador de Windows, la partición montada se mostrará como se muestra a continuación:



Abrimos la carpeta del usuario “fredr” en la ruta **\Usuarios\fredr** y garantizamos permisos



En dado caso de no ver NTUSER.DAT , en la solapa “Vista” habilitamos “ver archivos ocultos”


fredr
Archivo
Inicio
Compartir
Vista
Este equipo › Windows (E:) › Usuarios › fredr ›
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
OneDrive
Este equipo
Cases (D:)
Red
Nombre
Fecha de modificación
Tipo
Búsquedas 11/2/2020 9:01 AM Carpeta de arc
Contactos 11/2/2020 9:01 AM Carpeta de arc
Descargas 11/15/2020 8:44 PM Carpeta de arc
Documents 10/26/2020 10:57 PM Carpeta de arc
Favoritos 11/2/2020 9:01 AM Carpeta de arc
Google Drive 11/13/2020 8:15 PM Carpeta de arc
iCloud Drive 11/11/2020 4:15 AM Carpeta de arc
iCloud Photos 11/11/2020 4:14 AM Carpeta de arc
Juegos guardados 11/2/2020 9:01 AM Carpeta de arc
MicrosoftEdgeBackups 10/26/2020 10:58 PM Carpeta de arc
Música 11/2/2020 9:01 AM Carpeta de arc
Objetos 3D 11/2/2020 9:01 AM Carpeta de arc
OneDrive 11/14/2020 9:45 AM Carpeta de arc
OneDrive - Stark Research Labs 11/11/2020 4:14 AM Carpeta de arc
ROCBA Dropbox 10/28/2020 8:30 AM Carpeta de arc
Stark Research Labs 11/14/2020 12:22 AM Carpeta de arc
Vídeos 11/2/2020 9:01 AM Carpeta de arc
Vínculos 11/2/2020 9:01 AM Carpeta de arc
Your team Dropbox 11/1/2020 5:04 PM Carpeta de arc
NTUSER.DAT 11/11/2020 4:12 AM Archivo DAT
21 elementos
1 elemento seleccionado 7.75 MB

Principales conclusiones:

Montar una imagen de disco con **Arsenal Image Mounter** permite un acceso sin restricciones a través de toda la imagen y será utilizado por muchas de nuestras herramientas que esperan operar en artefactos de Windows, no en imágenes forenses.

Montar una imagen de disco permite el análisis tanto de los archivos y directorios, además de tener un manejo de una representación del disco físico (algunos softwares forenses pueden interactuar con un disco físico).