

DIGITAL FORENSICS MOUNT RAW IMAGES

Contents

Multiple Ways to Mount Raw Images (Windows) . Error! Bookmark not defined.

Introduction	3
Why Mount an Image?	3
Tool #1: Mount Image Pro	3
Tool #2: OSF Mount.....	7
Tool #3: Arsenal Image Mounter	11
Tool #4: Access Data FTK Imager.....	14

Introduction

In the Cyber Forensic world, a forensic image is a complete, sector-by-sector copy of a hard drive or external drive. Generally, a forensic image is used as evidence in forensic investigation. These images include unallocated space, slack space, and boot records. Some computer forensic tools use different formats to generate a forensic image.

Some common forensic image formats are RAW, E01, AFF, etc. We can use a variety of tools to analyse and mount that image to get better investigative results.

Why Mount an Image?

Mounting is the process that converts a RAW logical image into a mounted directory. To better examine a forensic image, mounting is preferred. There are various tools that can be used to mount a RAW image. Let's learn the process of mounting using this variety of tools. Although the basic procedure is the same, there are times when an investigator finds himself in a situation where he/she cannot use their preferred tool. Also, each investigative company uses different tools. So a good investigator should know all the different types of tools available to them to widen their ability and robustness.

Tool #1: Mount Image Pro

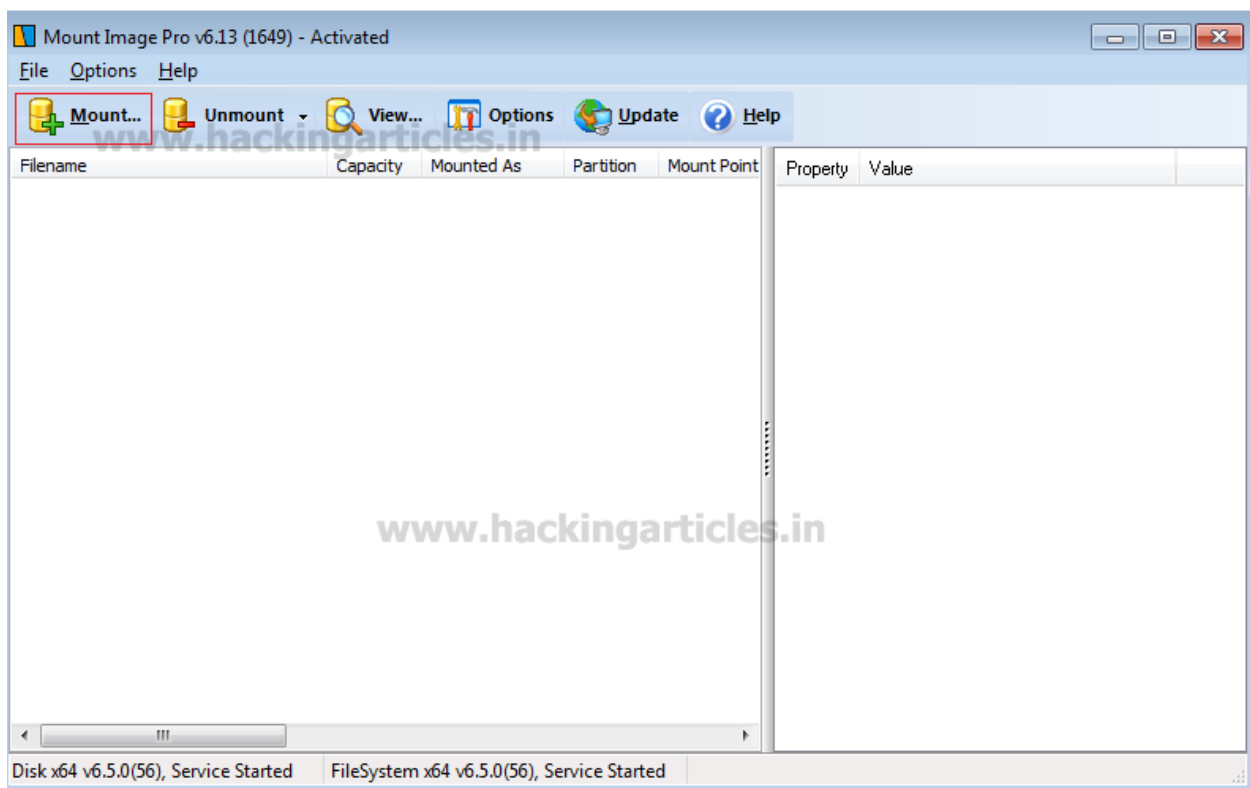
Mount Image Pro is a tool, which is quite useful in Forensic investigations. It enables the mounting image across all the forensic image extensions. Some of them are:

- .RAW
- .E01 (Encase Image)
- .A01
- .dd

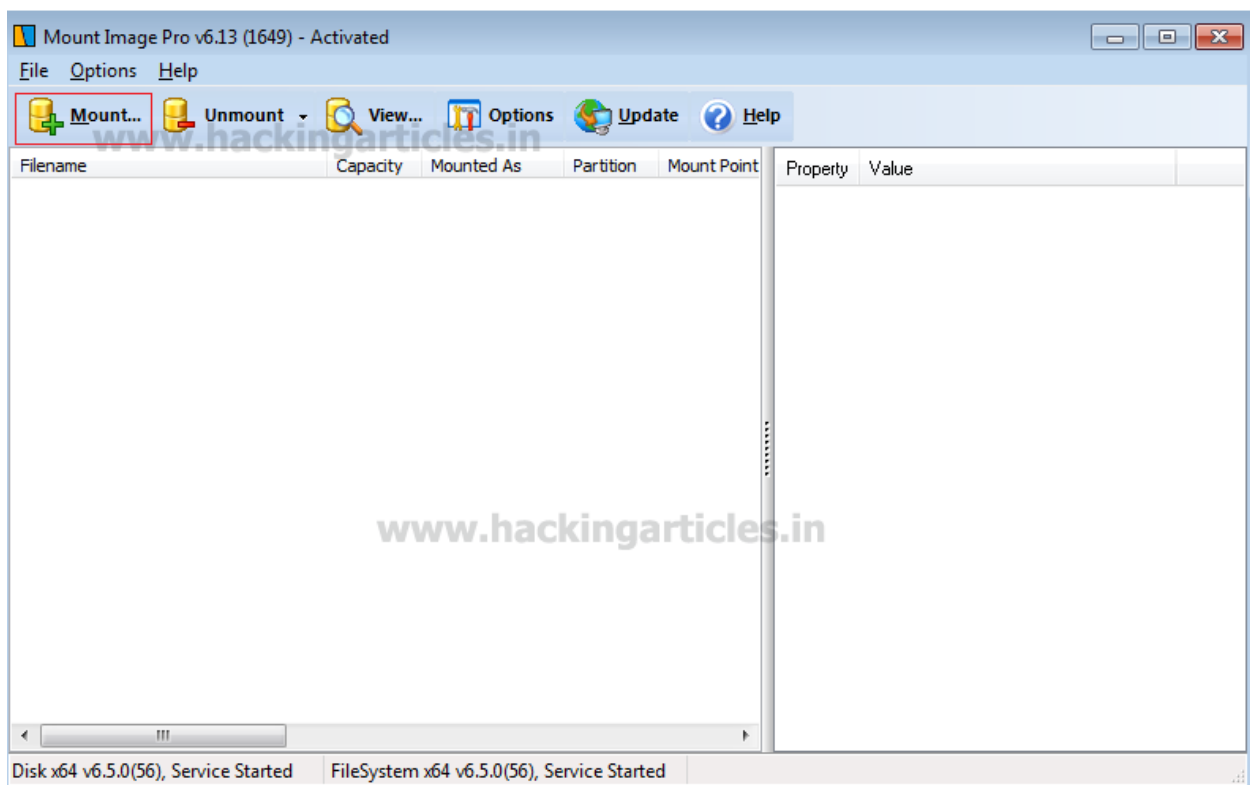
This tool is developed by Get Data. They are Renowned Provider of User-End software. That provides Data Recovery, File Recovery, Computer Forensics and File Previewing. Their products are designed for getting data back from systems and their hard drives.

We can download the mount image pro from [here](#).

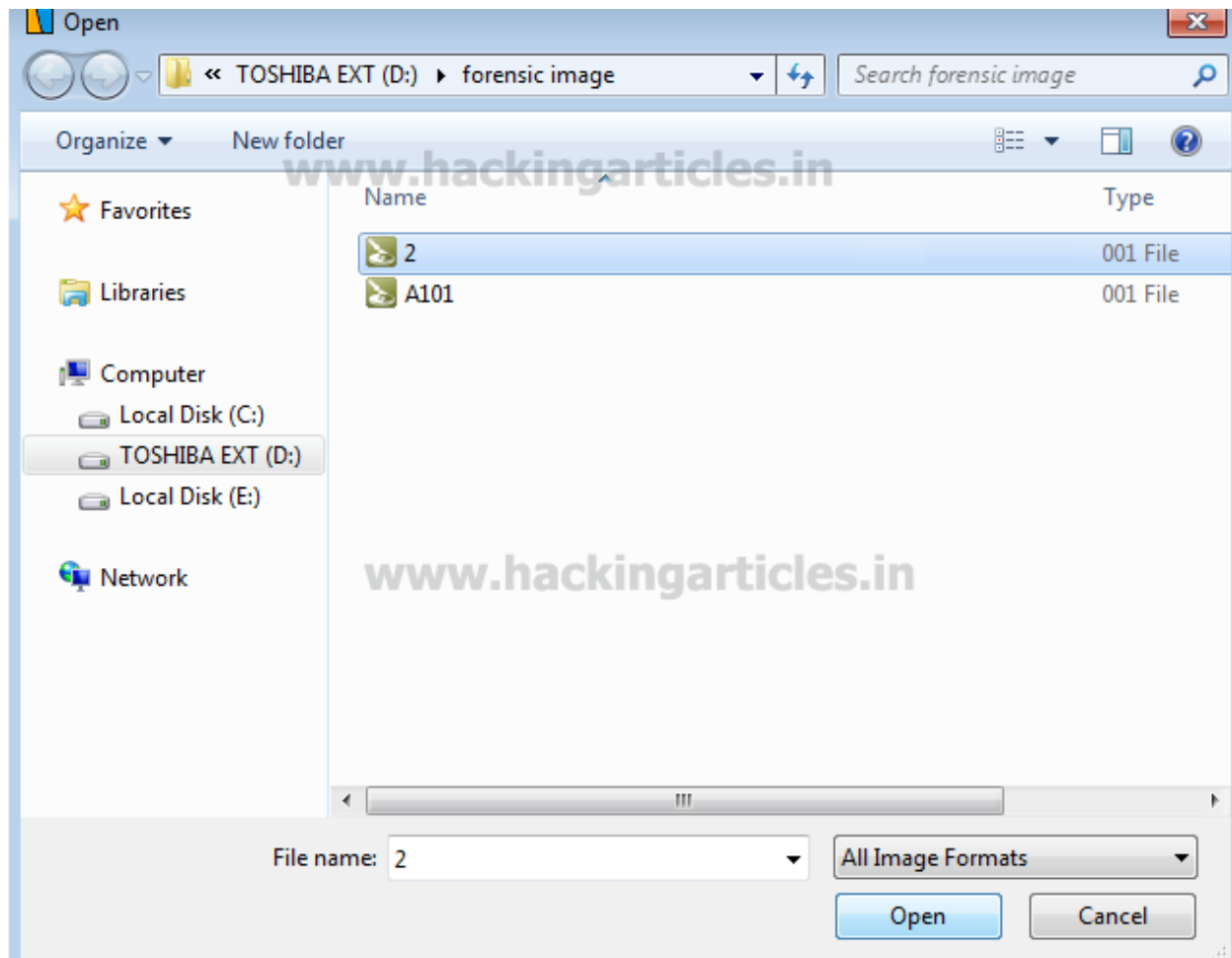
Once downloaded the mount image pro, then launch tool using the Icon created on the Desktop. After launching the app, we need to press the **Mount** icon to get started.



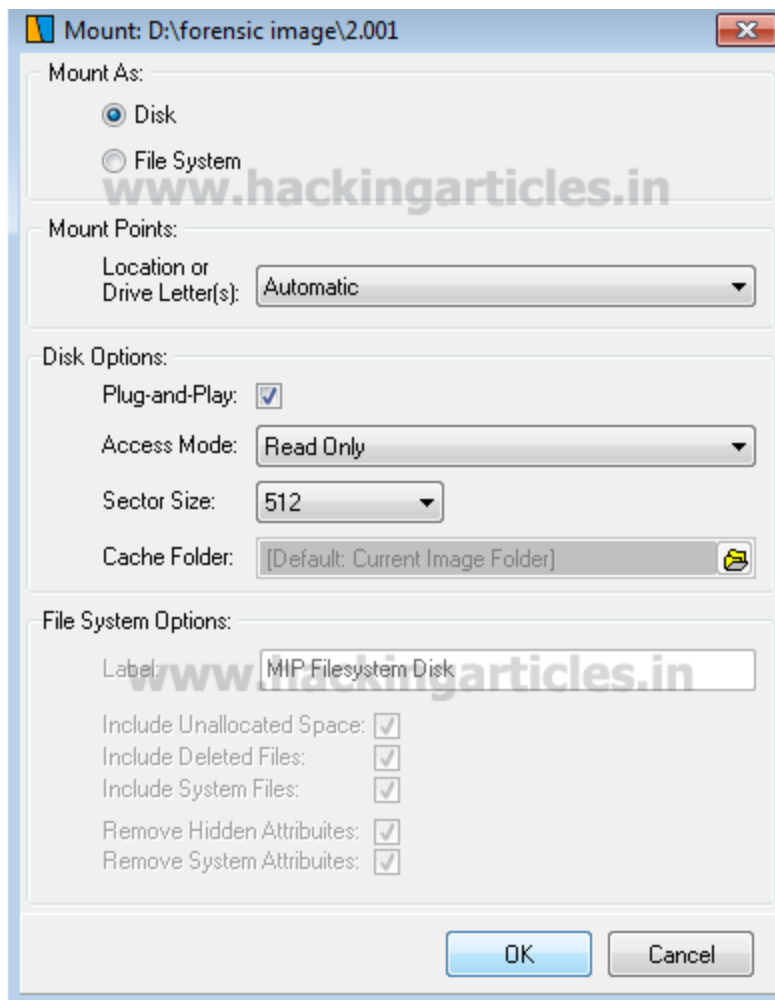
We can also click on the File from the Dropdown menu. Go for the **"Mount Image File"** Option to move ahead.



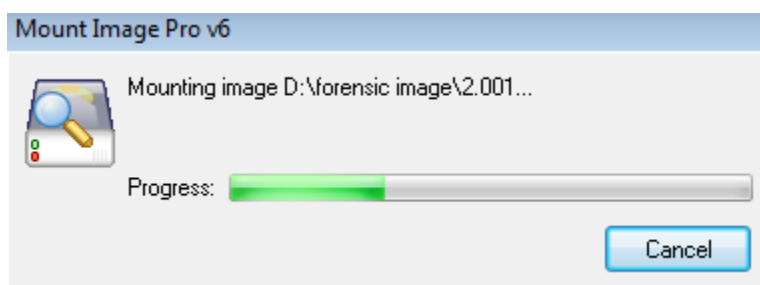
After this, we need to select our digital image file on our hard drive. After selecting the image file, we need to click on the "**Open**" button to open the image file.



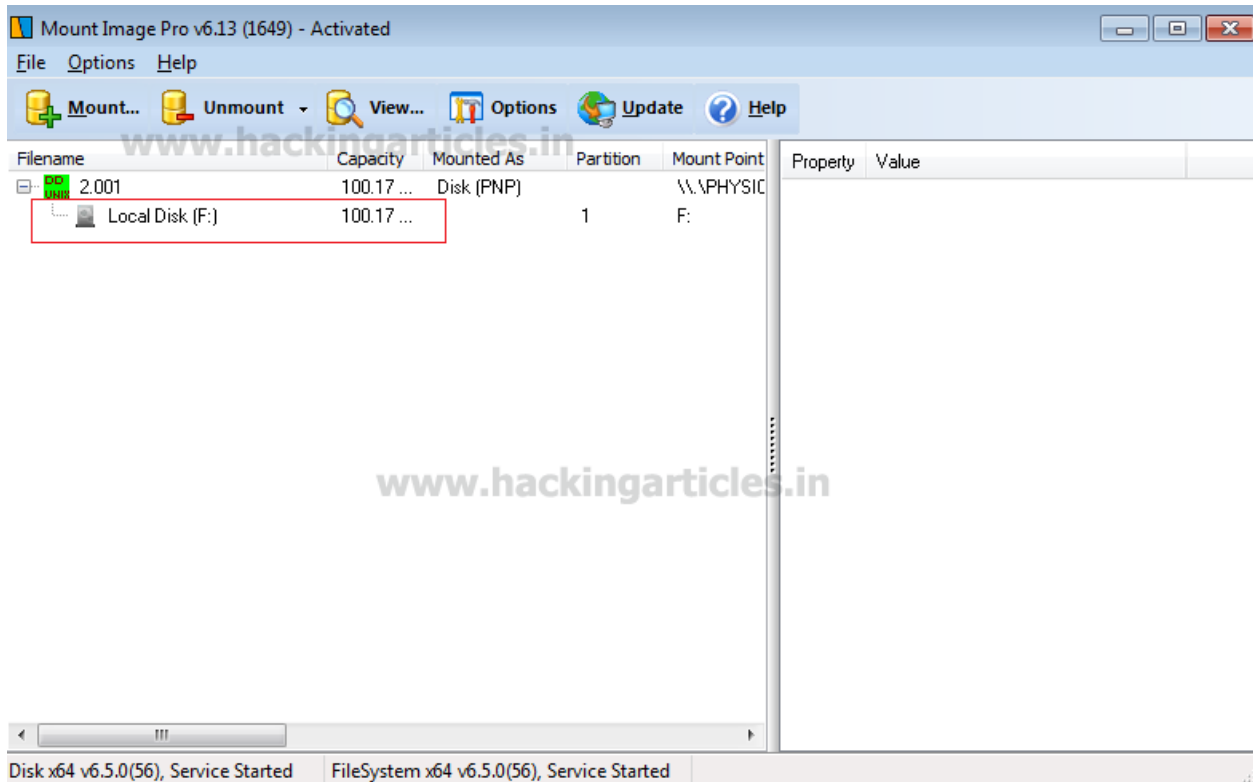
Now, we need to select a bunch of options to get started. The first one is how do we want to mount our image? We want the image to be mounted and shown as a partition in our Explorer. Hence, we chose the disc option. If you want to investigate the image as a directory, choose File System. Following that, this is the location where we want to mount. If we choose the File System Option, we need to specify the destination directory. Here we can choose an alphabet which would act as a drive letter (such as Local Disk D: or E: etc.). Next, we get to the Disk options panel. Here, we checked Plug and Play so that the dismount is easier. Now we select the kind of access that we want to get. We chose Read-Only Access. We can also customise the sector size of the partition. After giving all the required details, press the **OK** button.



After this, mounting will start and we get a live progression of the process through the status bar as depicted below.



After completion, we will get our mounted image and we can start our investigation.



As the screenshot suggests it mounted our forensic image as F drive. Now, we can analyse it and get the same view from the files as its user gets in its system.

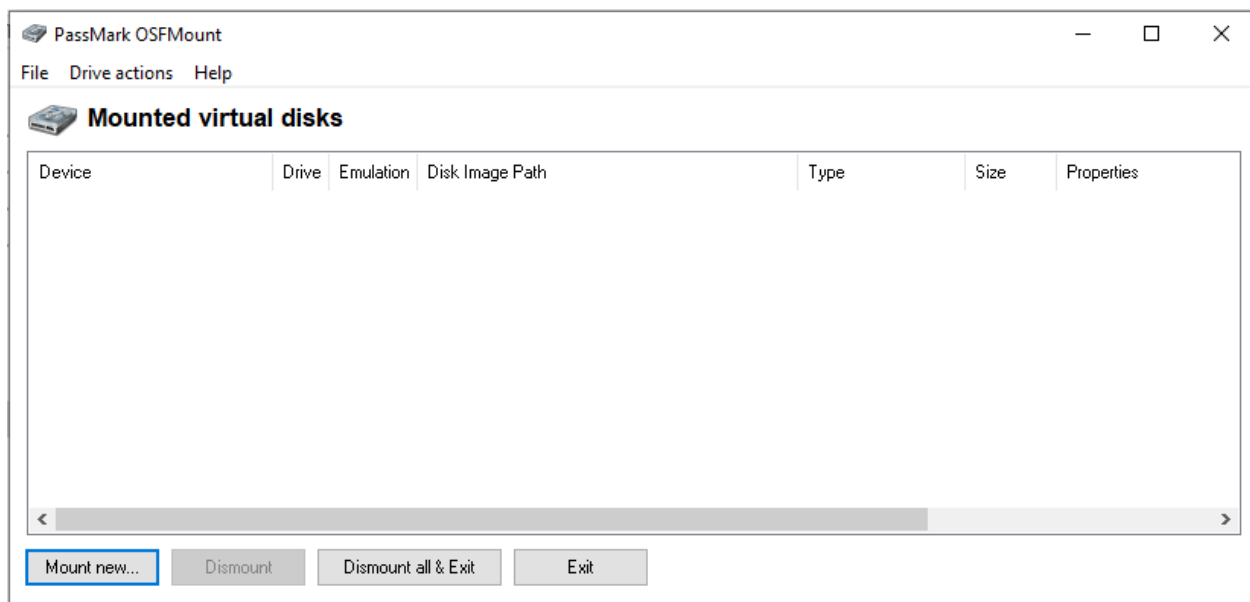
Tool #2: OSF Mount

OSF Mount is the software that allows us to mount local disk image files (sector by sector copies of an entire disk or disk partition) on a Windows system. We can then analyse the disk with its other tool, which is OS Forensics. By default, the image files are mounted as read-only so that our original image files are not altered.

This software supports mounting disk image files in any mode, whether we want them in the read-only mode, the write mode, or the write cache mode.

We can download OSF mount from [here](#).

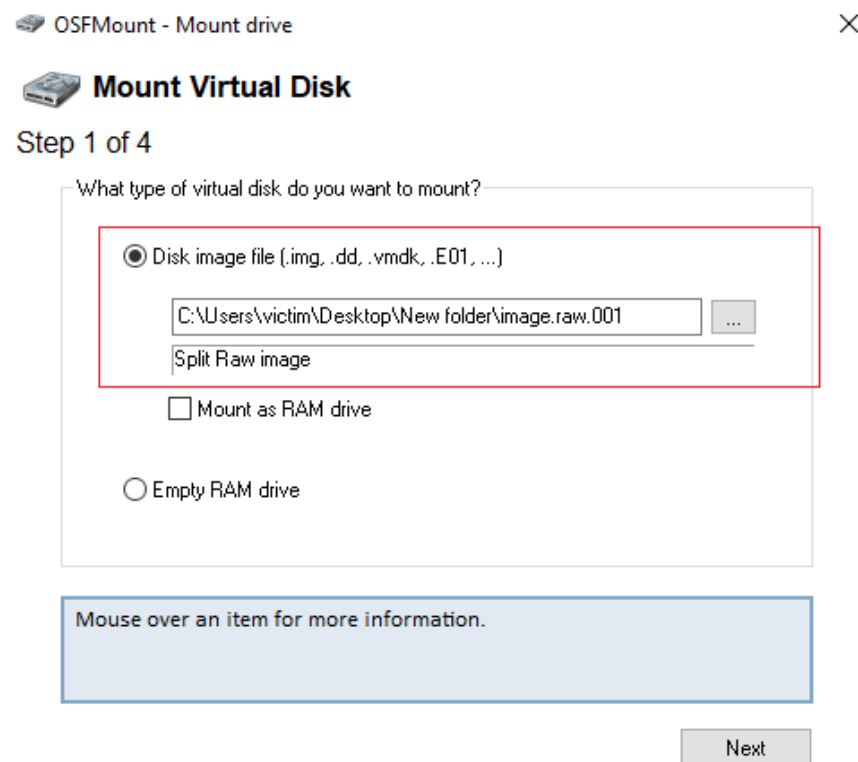
Let's Begin with opening the OSF mount after completing its installation process. The developers at Pass Mark gave us a neat UI to work upon. We have a very minimalistic interface here. To begin with, we will hit the **"Mount New"** Button.



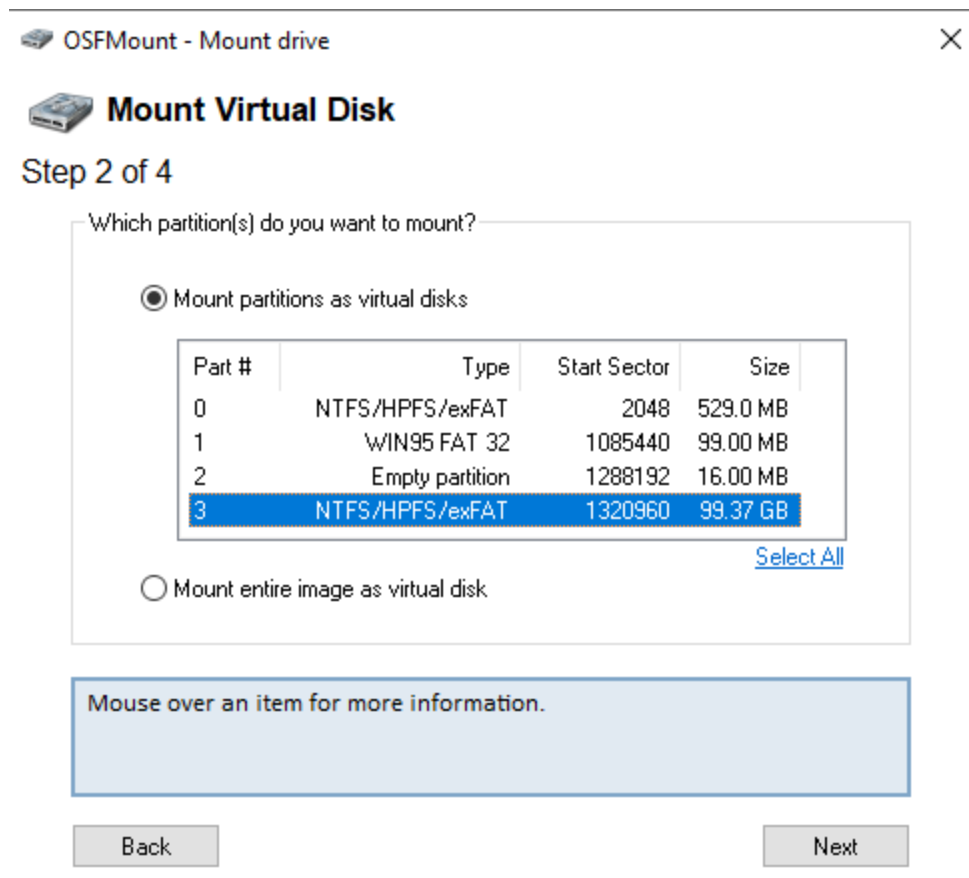
After that, we follow a series of steps where we fill in the required details.

Step #1: We need to provide the source of the image file to mount for our investigation.

After filling in details, we hit the **Next** button.

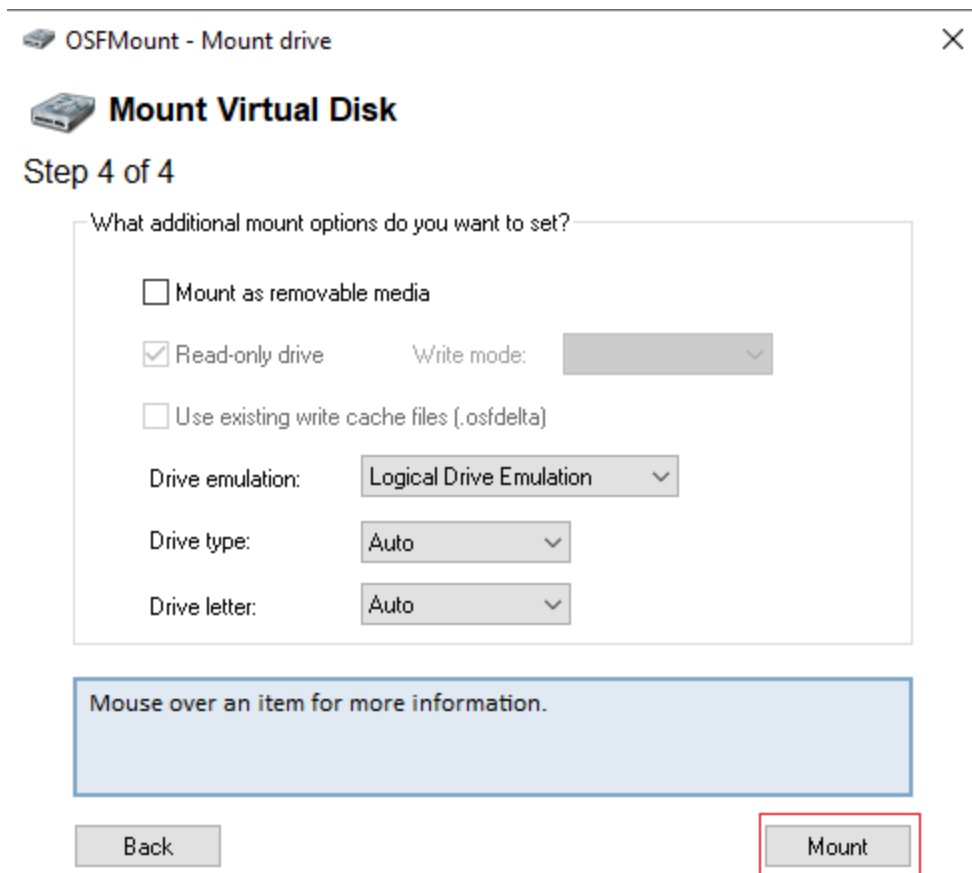


Step #2: We need to select if we want a specific partition or we want the entire image mounted for investigation.

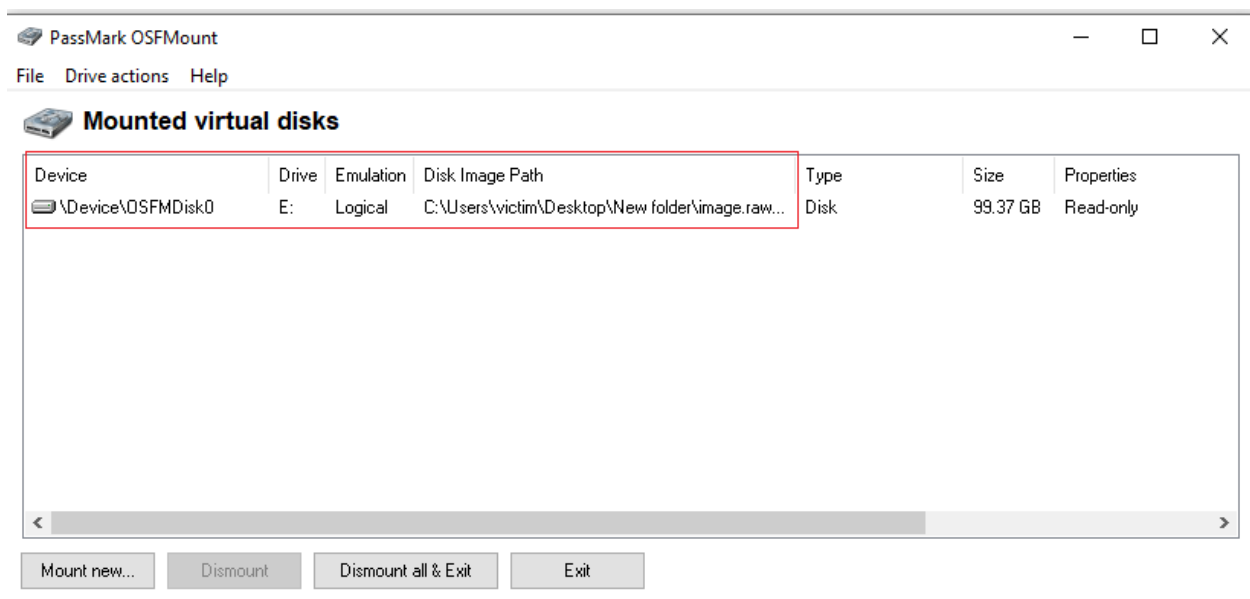


After that step, we need to finalise things. In the last step, we need to select a few details regarding our image. These are some additional features that we want to include in our process or not. These features include whether we want to mount our image as a removable media or not, the drive type, the drive letter, drive emulations, etc.

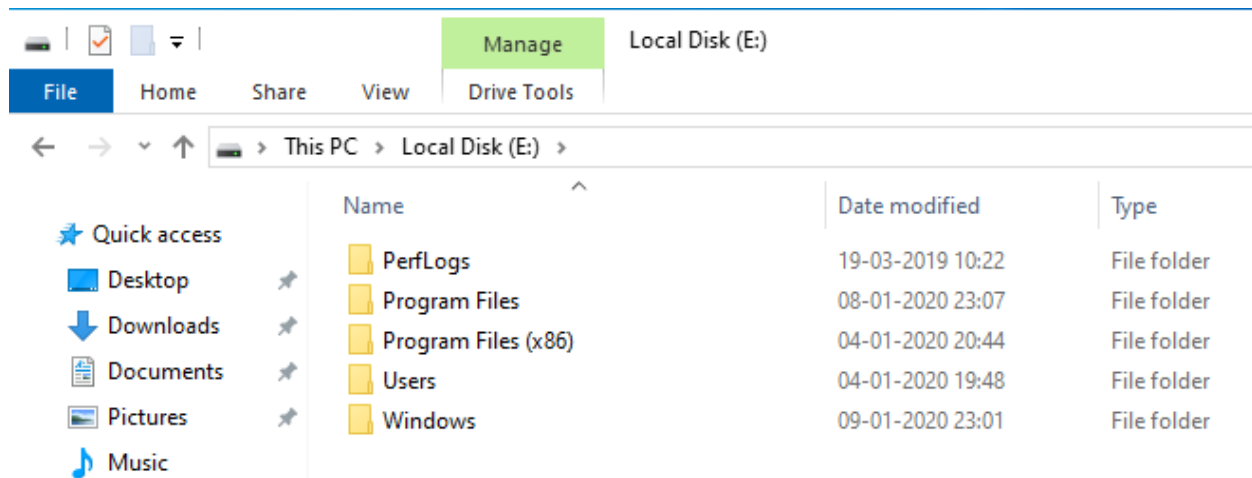
After filling in all the details and completing all the steps, click on the mount button to start mounting the image file.



Now as shown in the image given below we have the image successfully mounted and ready for the analysis.



We can also check the working of the mounted image file by opening the mounted image in the File Explorer as shown in the image given below:



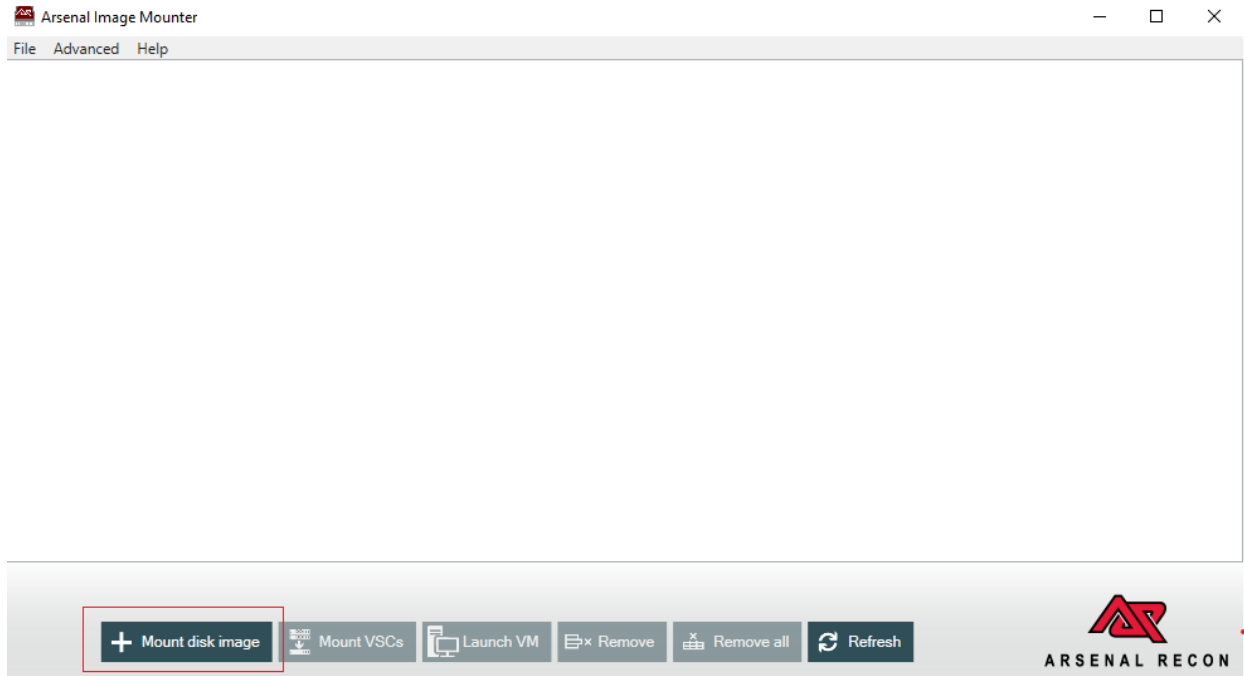
Tool #3: Arsenal Image Mounter

Arsenal image mounter handles the disk images as a whole drive. As far as the Windows system is concerned, the contents of disk images mounted by AIM are real SCSI disk, which allows its users to take advantage of some disk-specific features like integration with Disk Manager, access to volume shadow copies, and much more.

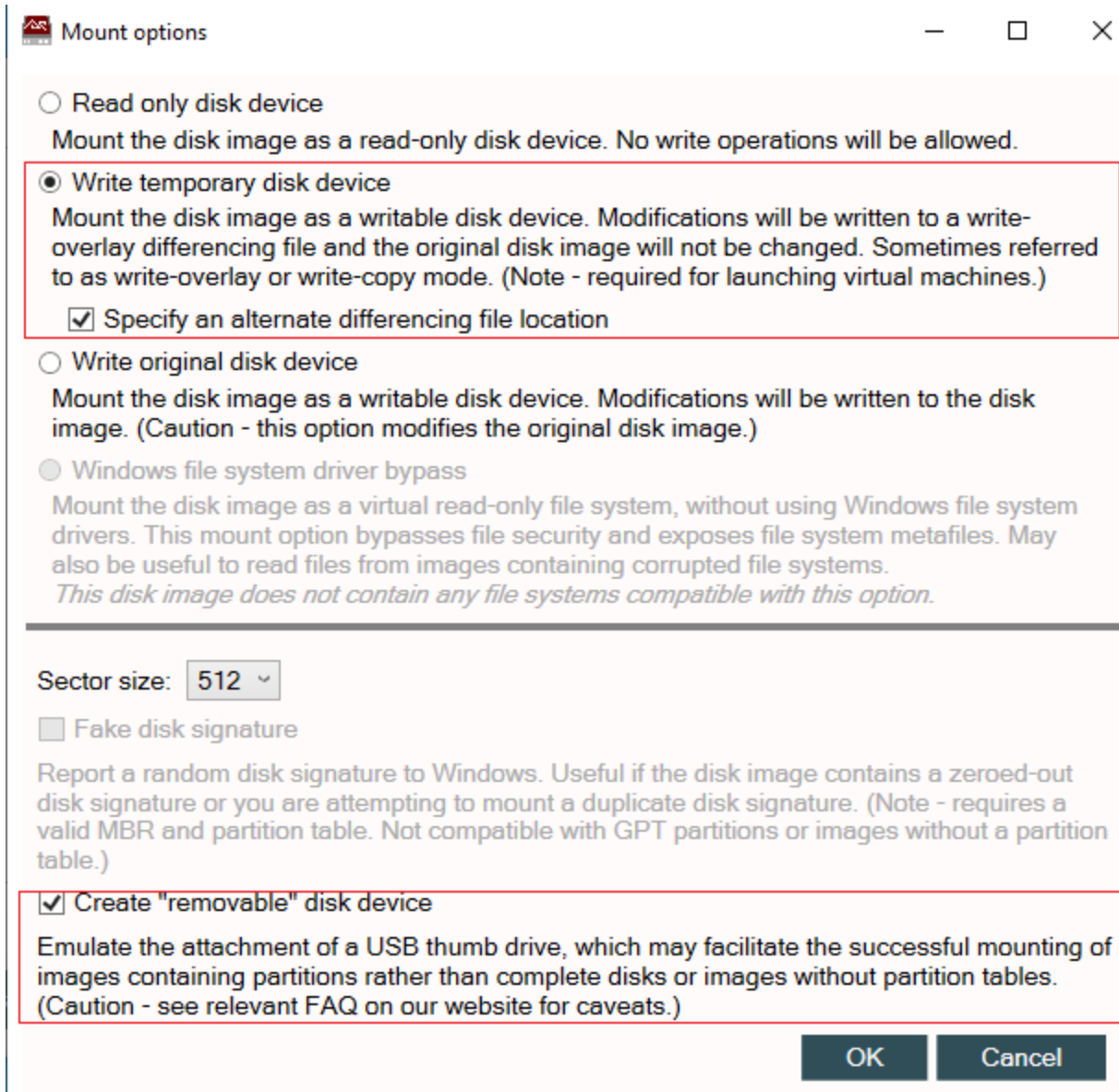
Many of the image mounting solutions on the market contents of disk images as share and partitions rather than complete disk. which sometimes limits their usefulness to digital forensics practitioners or investigators. If AIM is running without a license, it will run in free mode and provide core functionalities. If it is licensed, it will run in professional mode with full functionality enabled.

We can download our Arsenal Image Mounter from [here](#).

After downloading and completing its installation process, we can open this software and start mounting an image file. After opening that software click on the **“Mount disk image”** button.



Now we have some details to fill in. We are asked about the mode in which we want to see our mounted image or what type of device it has to be. We can choose Read Only or Writable, among other options. We are also required to fill in the Sector Size and click on the Create "removable" disk device for a better mounting process. After filling up all the details, click on the **OK** button to move further.

The image shows a 'Mount options' dialog box with a title bar containing a red icon, the text 'Mount options', and standard window controls (minimize, maximize, close). The dialog has a light pink background. It contains three radio button options, each with a description. The first option, 'Read only disk device', is unselected. The second option, 'Write temporary disk device', is selected and highlighted with a red rectangular border; it includes a sub-option 'Specify an alternate differencing file location' which is checked. The third option, 'Write original disk device', is unselected. Below these is a greyed-out option 'Windows file system driver bypass'. Further down is a 'Sector size' dropdown menu set to '512', followed by a greyed-out checkbox 'Fake disk signature'. At the bottom is another red-bordered section containing a checked checkbox 'Create "removable" disk device'. At the very bottom are 'OK' and 'Cancel' buttons.

Mount options

☐ Read only disk device
Mount the disk image as a read-only disk device. No write operations will be allowed.

☒ Write temporary disk device
Mount the disk image as a writable disk device. Modifications will be written to a write-overlay differencing file and the original disk image will not be changed. Sometimes referred to as write-overlay or write-copy mode. (Note - required for launching virtual machines.)
☒ Specify an alternate differencing file location

☐ Write original disk device
Mount the disk image as a writable disk device. Modifications will be written to the disk image. (Caution - this option modifies the original disk image.)

☐ Windows file system driver bypass
Mount the disk image as a virtual read-only file system, without using Windows file system drivers. This mount option bypasses file security and exposes file system metafiles. May also be useful to read files from images containing corrupted file systems.
This disk image does not contain any file systems compatible with this option.

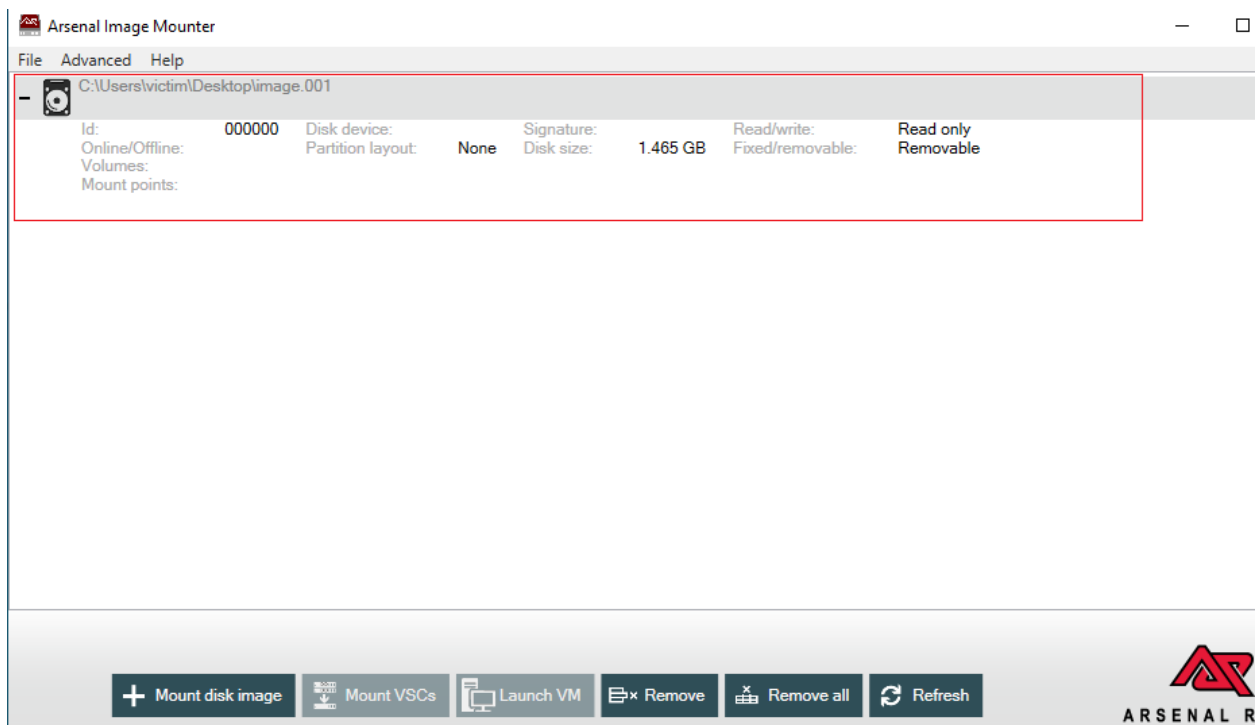
Sector size:

☐ Fake disk signature
Report a random disk signature to Windows. Useful if the disk image contains a zeroed-out disk signature or you are attempting to mount a duplicate disk signature. (Note - requires a valid MBR and partition table. Not compatible with GPT partitions or images without a partition table.)

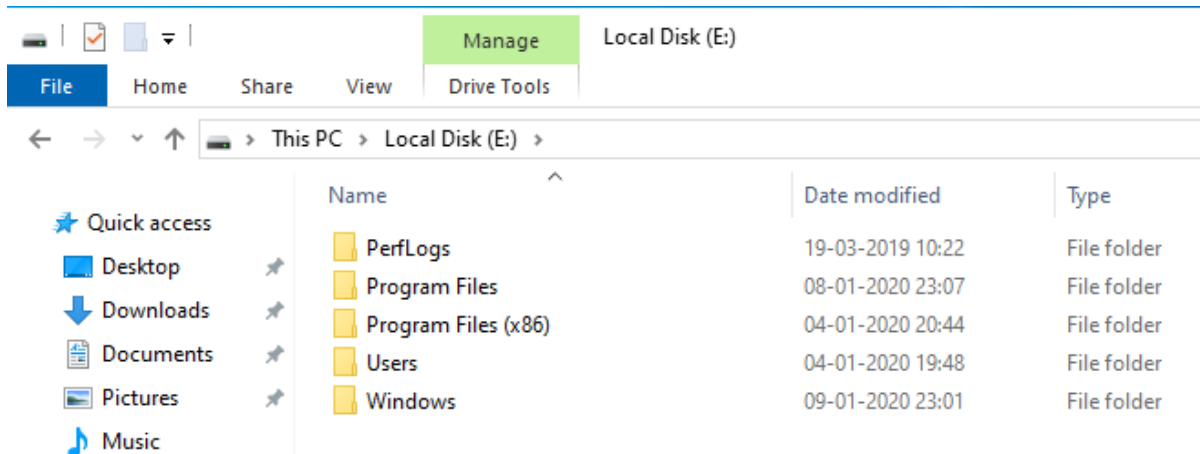
☒ Create "removable" disk device
Emulate the attachment of a USB thumb drive, which may facilitate the successful mounting of images containing partitions rather than complete disks or images without partition tables. (Caution - see relevant FAQ on our website for caveats.)

OK Cancel

After this our disk is mounted successfully, we will get all the details regarding that with that mounted message.



Now we check if our image is successfully mounted as a removable device in our system. After checking that, now we can finally start our investigation process.



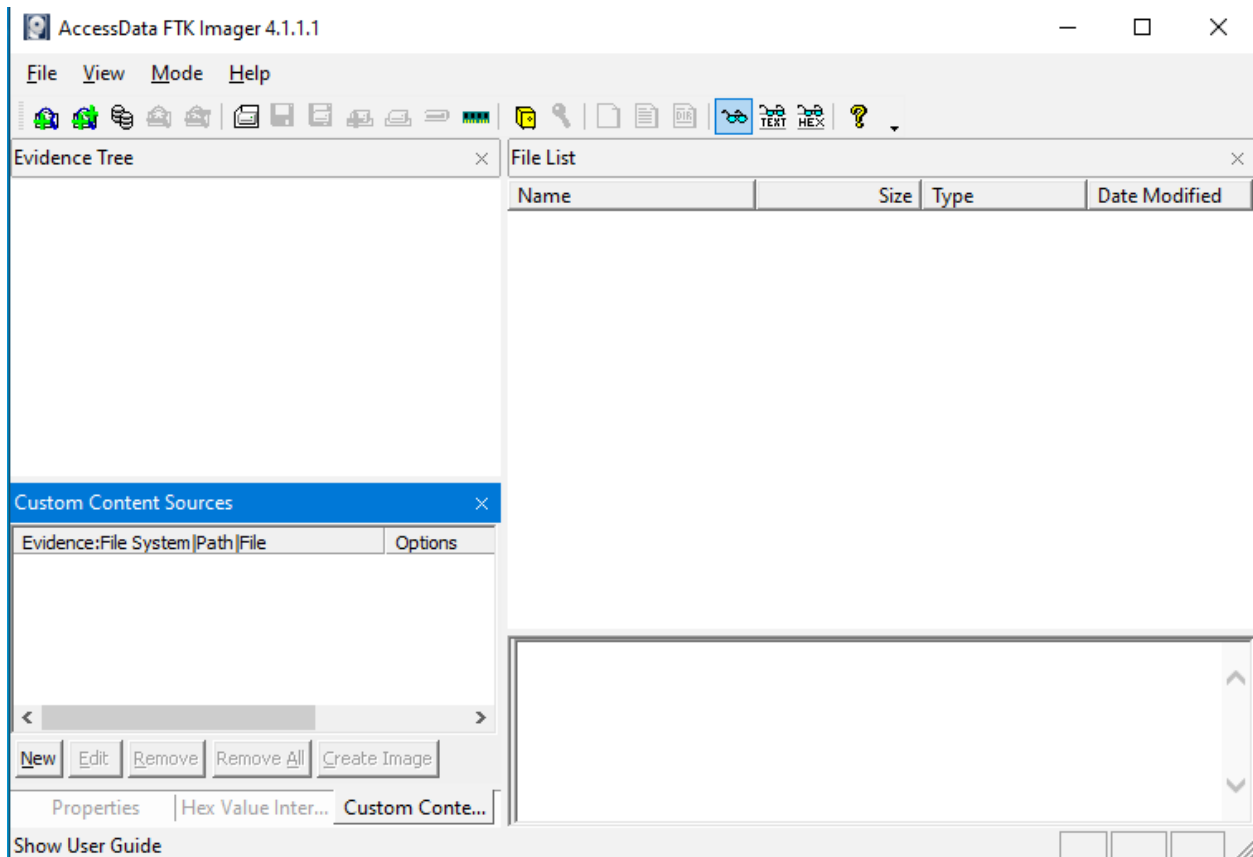
Tool #4: Access Data FTK Imager

Access Data believes that zero is on the relevant evidence quickly, conducts faster searches, and dramatically increases analysis speed with FTK. FTK uses distributed processing and is a solution to fully leverage multi-core and multi-thread computers. While other tools waste the usage of modern hardware solutions. Where FTK tries to use 100 per cent of its hardware resources to try to help in the investigation process.

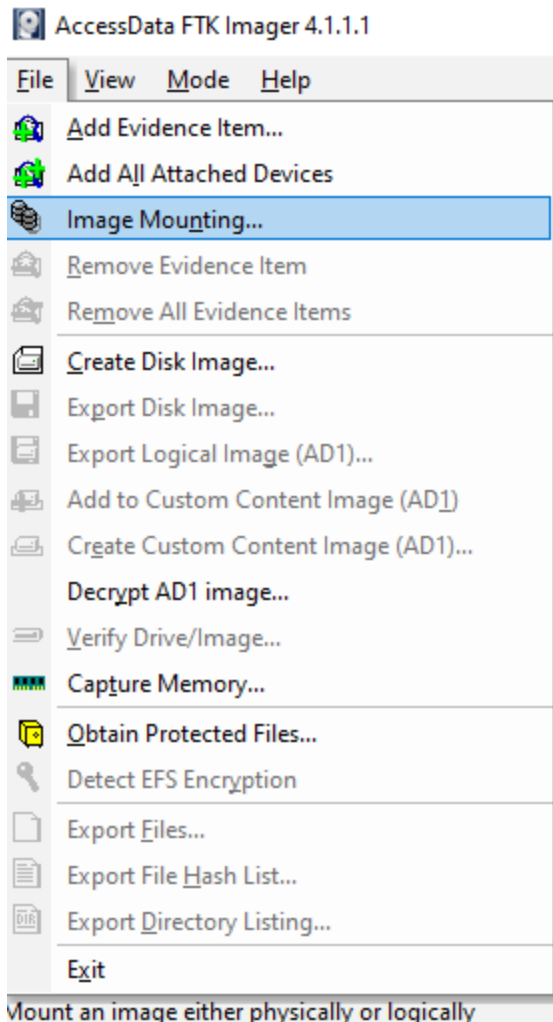
FTK provides faster searching in comparison to other solutions. FTK is truly database-driven. All data is stored securely and centrally, which allows our teams to use the same database, which reduces the cost of creating multiple data sets.

We can download our access data FTK Imager from [here](#).

After finishing up the installation process, open the software to move further ahead.



Now, click on the File option from Menu and Select the “**Image Mounting**” option to start the image mounting process.



Now we explore the Add Image file option. We browse the image file in the system, then fill up the details like image file mount type, its drive letter, and its mount method.

After filling up all mandatory details regarding the process, click on the **Mount** button to start the mounting process.

Mount Image To Drive

It takes some time to mount an image, but after finishing up the process, we will get the details of our mounted image, which comes in the mapped images section. It provides us with some basic information regarding the drive, method, partition, image locations, etc.

Mount Image To Drive

Close

Add Image

Image File:
C:\Users\victim\Desktop\New folder\image.001

Mount Type: Physical & Logical

Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

Write Cache Folder:
C:\Users\victim\Desktop\New folder

Mount

Mapped Image List

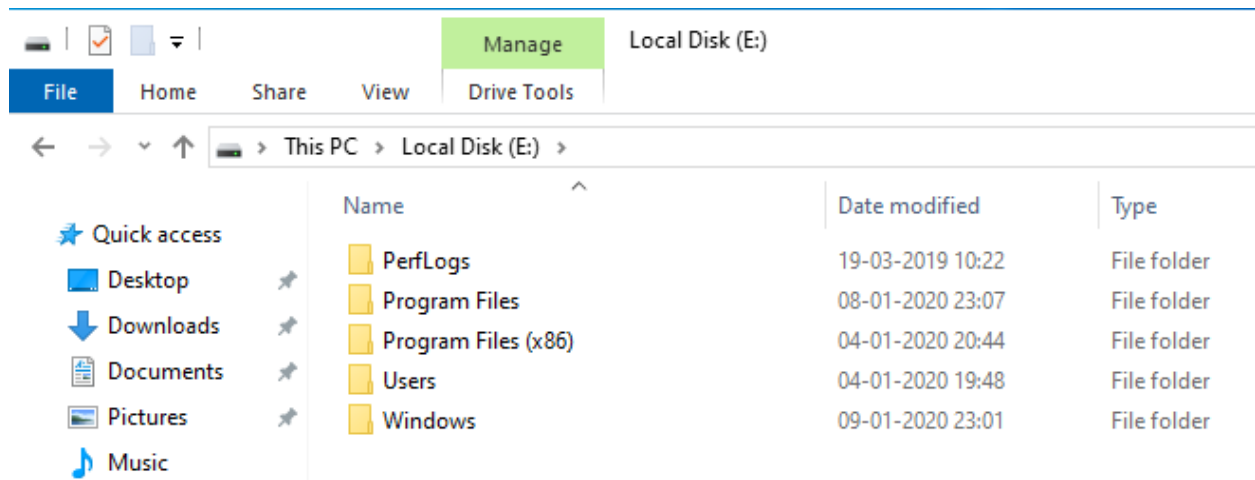
Mapped Images:

Drive	Method	Partition	Image
PhysicalDrive1	Block Device/Read ...	Image	C:\Users\victim\Desktop\New folder\image.001
E:	Block Device/Read ...	Partition 1 [20971...	C:\Users\victim\Desktop\New folder\image.001

Unmount

Close

If we want we check the integrity information we can do so by checking or monitoring this drive physically by reaching this drive location to validate that data information and start our investigation.



These are different ways in which we can mount a forensic image window to help investigators. For a better analysis of the evidence, it will help them in their investigation process.

JOIN OUR TRAINING PROGRAMS

