

## PARA PRACTICAR CREACIÓN DE UNA IMAGEN FORENSE CON FTK IMAGER

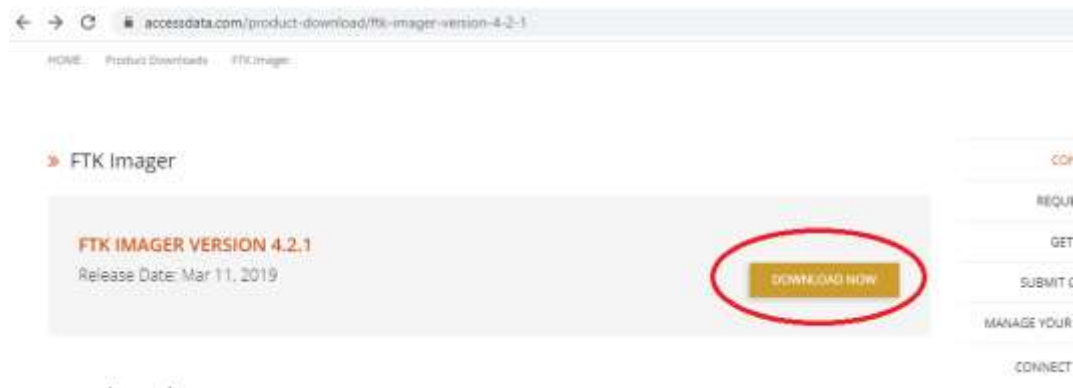
**Objetivo.-** Aprender el uso del software FTK IMAGER para la creación de imágenes forenses de discos de almacenamiento de información.

**FTK Imager** es un software gratuito que se utiliza para crear archivos de imagen de disco o montar imágenes de disco o dispositivos de almacenamiento para poder realizar previsualización de los archivos y análisis de la estructura del disco entre otros.

### DESARROLLO DE LA PRÁCTICA

#### 1) Descargar FTK Imager de la siguiente dirección

<https://accessdata.com/product-download/ftk-imager-version-4-2-1>



- Llenar los datos del formulario

**FTK® Imager 4.2.1**

FTK® Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence. After you create an image of the data, use **Forensic Toolkit® (FTK®)** to perform a thorough forensic examination and create a report of your findings. FTK Imager will:

- **Create forensic images** of local hard drives, CDs and DVDs, thumb drives or other USB devices, entire folders, or individual files from various places within the media.
- **Preview files and folders** on local hard drives, network drives, CDs and DVDs, thumb drives or other USB devices.
- **Preview the contents** of forensic images stored on the local machine or on a network drive.
- **Mount an image for a read-only view** that leverages Windows® Internet Explorer® to see the content of the image exactly as the user saw it on the original drive.

To download FTK Imager, please fill out the form below:

First Name

Last Name

Email

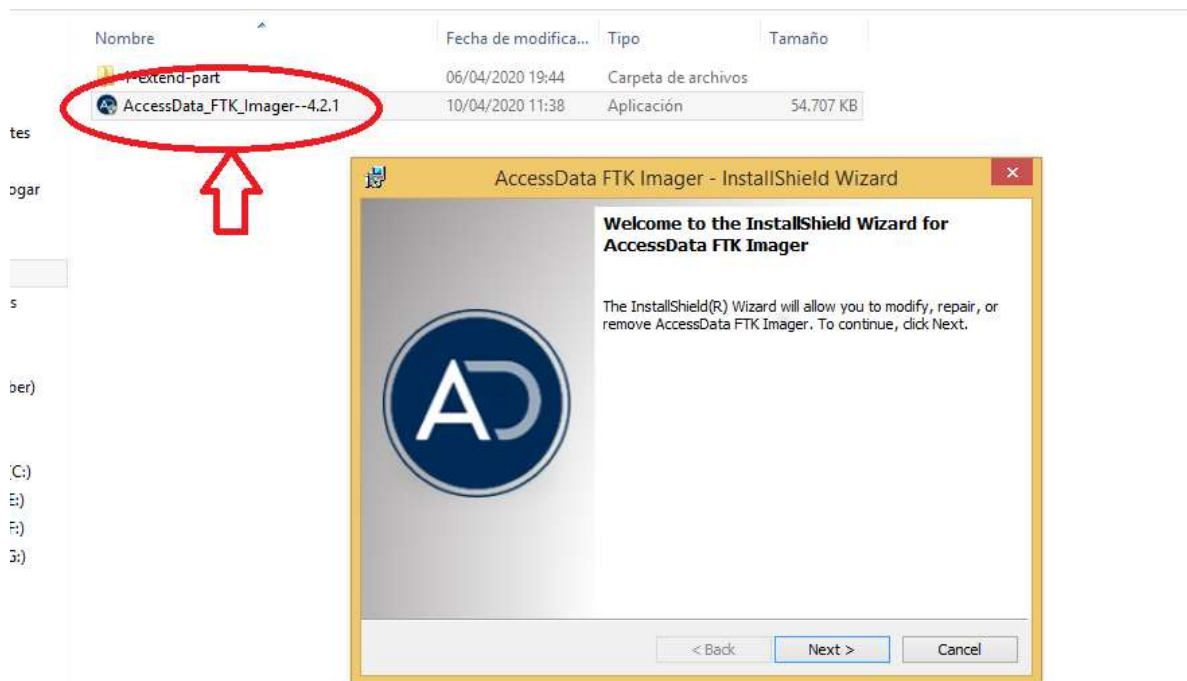
Please input a valid email address from a non-free provider.

Phone

Country

- Ingresar al correo electrónico registrado y desde ahí empezará la descarga.

## 2) Proceder con la instalación del archivo descargado



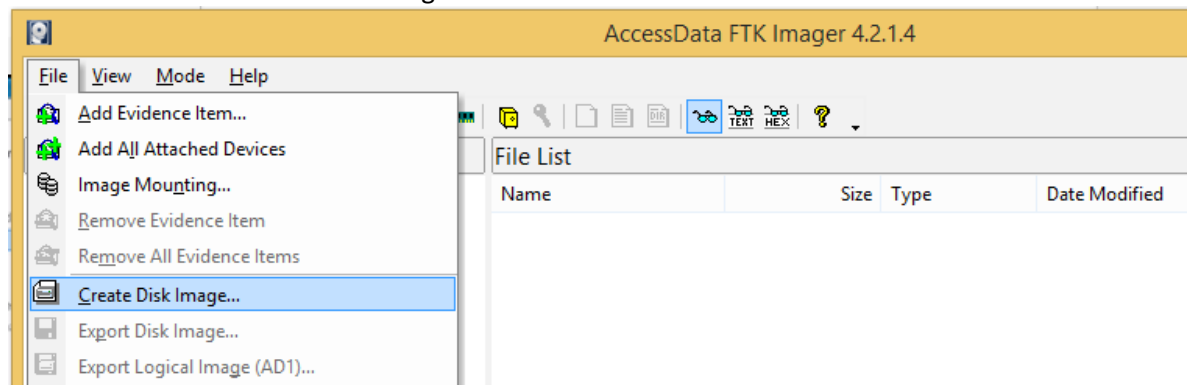
## 3) Iniciar el programa



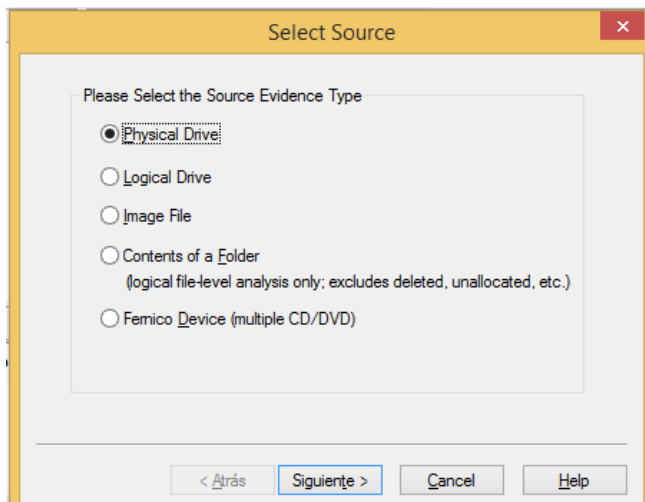
## 4) Conectar un Pendrive

## 5) Cargar el Pendrive desde FTK Imager

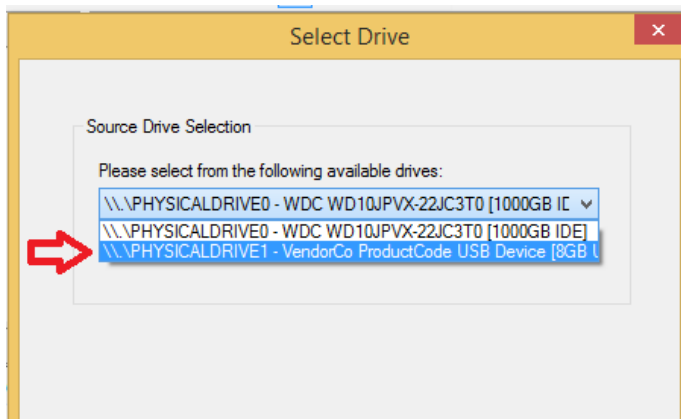
- Ir al Menú File → Create Disk Image



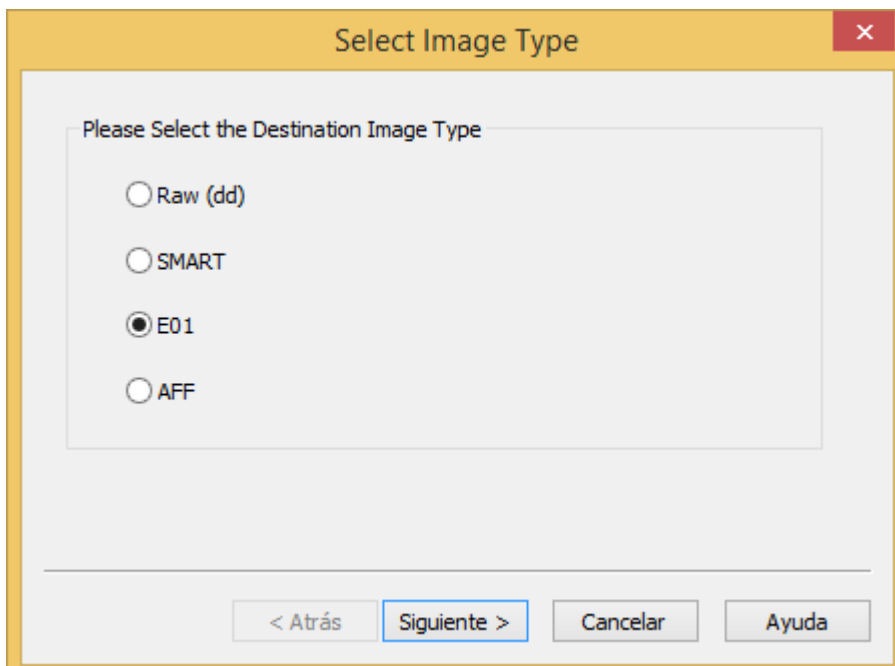
- Seleccionar "Physical Drive"



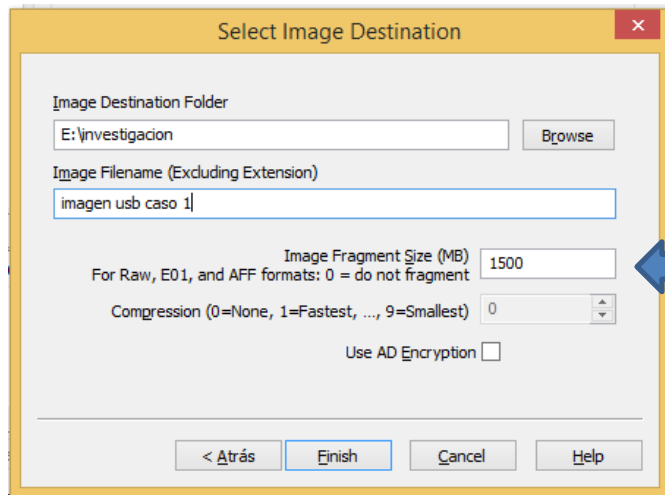
- Seleccionar el dispositivo USB y presionar finish



- Presionar el botón **add** y escoger la opción E01

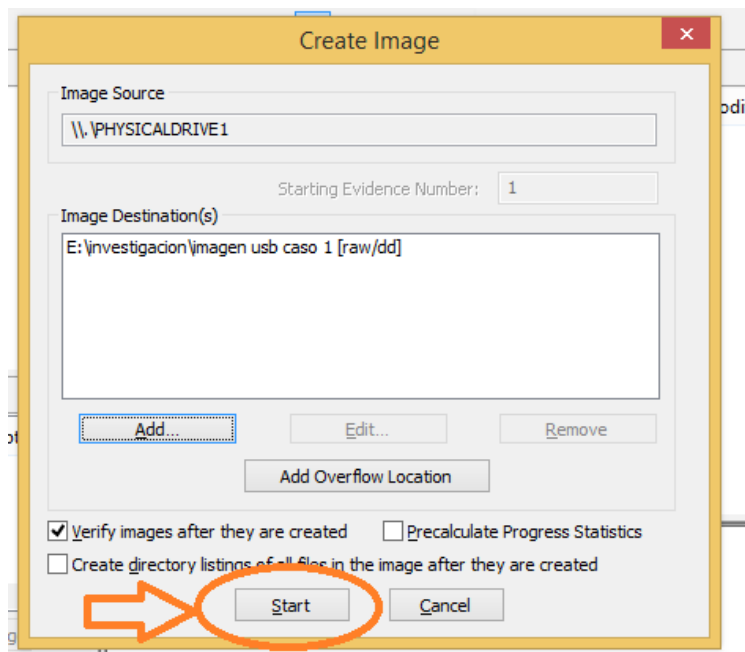


- Llenar el formulario Información de la evidencia
- Seleccionar nombre y destino de la imagen forense – presionar Finish

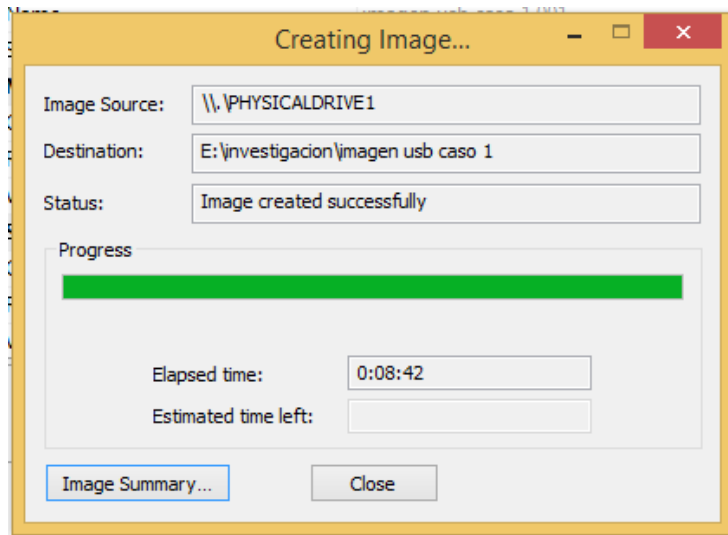


Insertar el tamaño del Pendrive en  
Megabytes

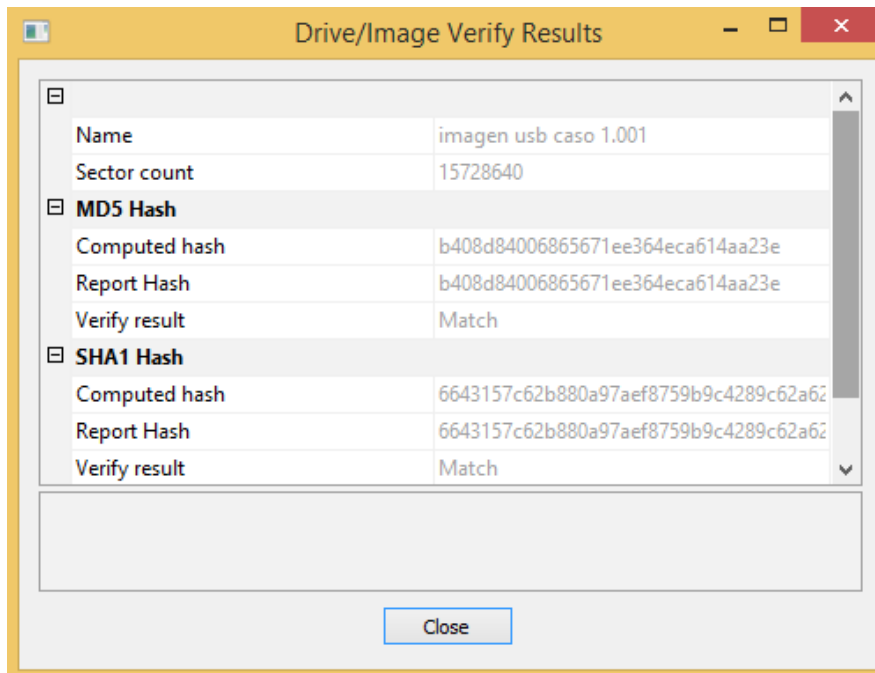
- Iniciar la copia



- Cuando haya terminado la copia, nos mostrará este mensaje

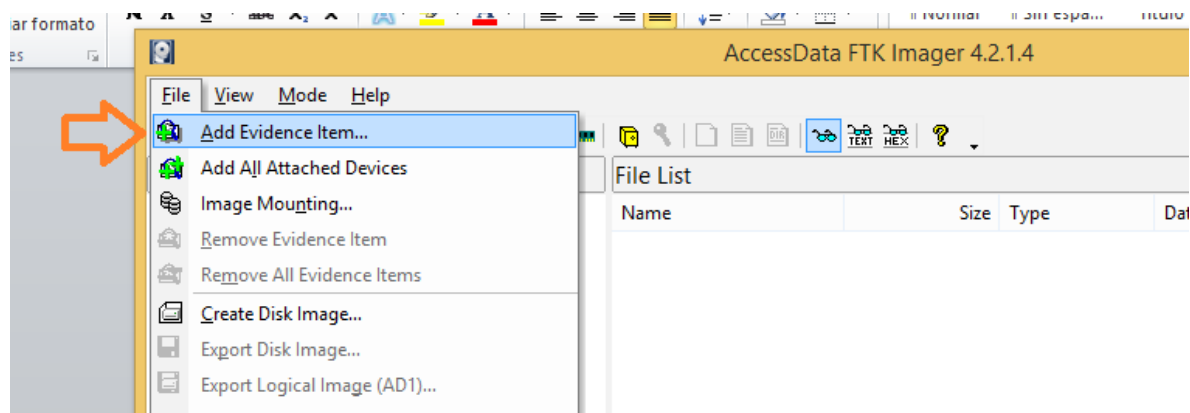


- Y finalmente nos mostrara un resumen de los resultados con los valores hash MD5 y sha1

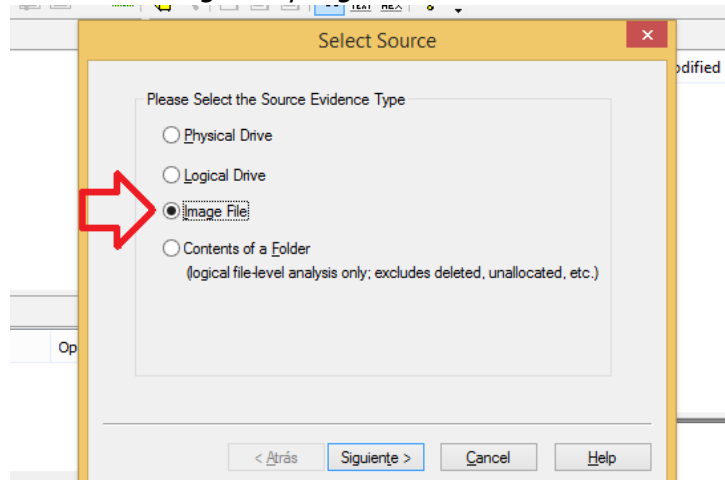


## 6) VISUALIZAR LOS DATOS DE LA IMAGEN

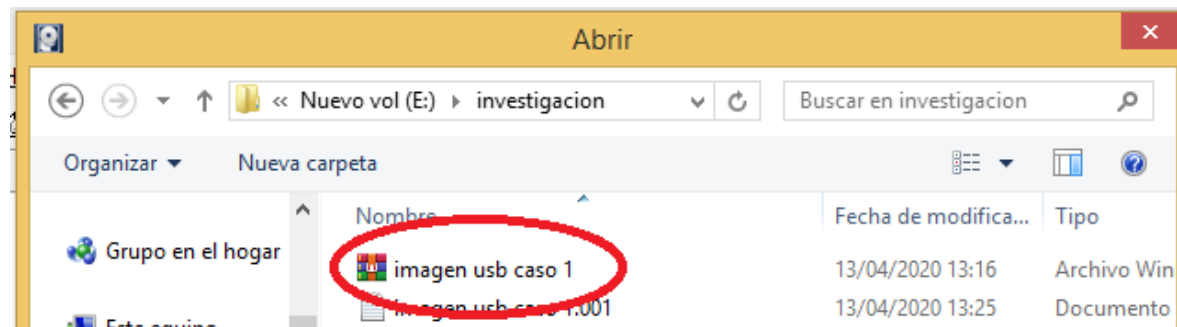
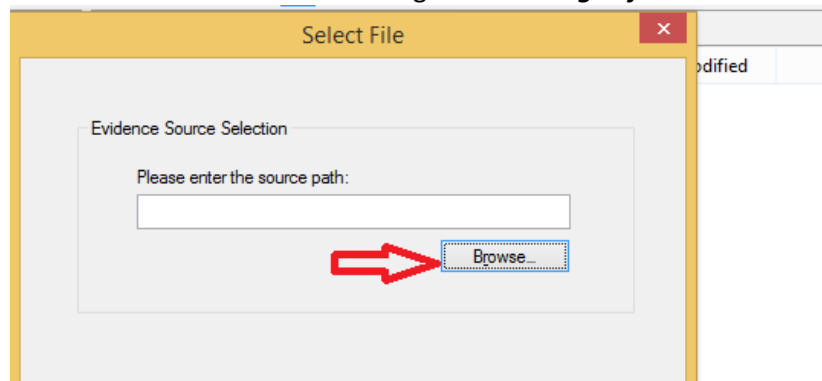
- Ir al Menu File → Add Evidence Item



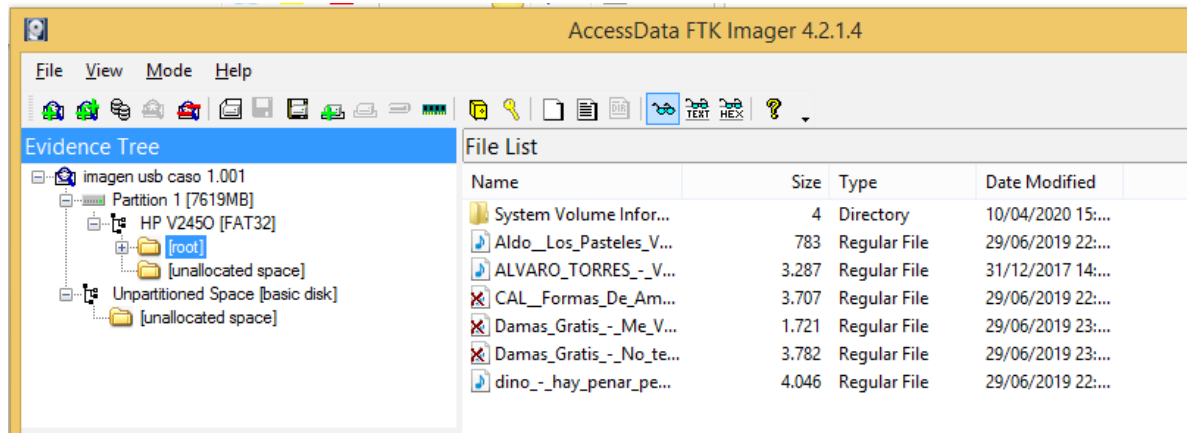
- Seleccionar **Image File** y **siguiente**



- Seleccionar la dirección donde se guardó la **imagen forense**



- Y veremos todos los archivos que tiene la imagen del pendrive como si fuera el mismo pendrive



**Indique cuántos archivos eliminados existen en el Pendrive**