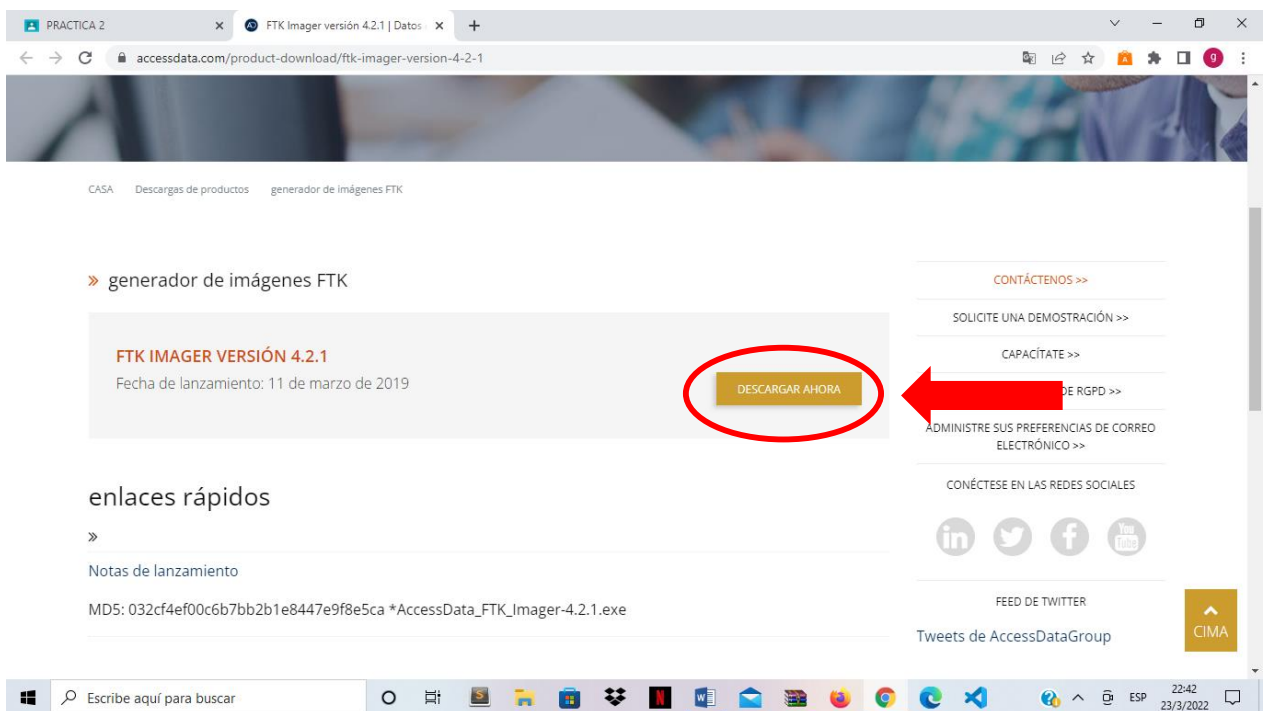


U.A.T.F.	CARRERA: ING. DE SISTEMAS	FECHA:25/03/2022
MATERIA: INFORMATICA FORENSE	LABORATORIO NO 2 (CREACION DE UNA IMAGEN FORENSE CON FTK IMAGER)	
DOCENTE: ING. LIMBERT RUIZ MOLINA		
AUXILIAR:		
NOMBRE: GRACIELA VASQUEZ RELOS		

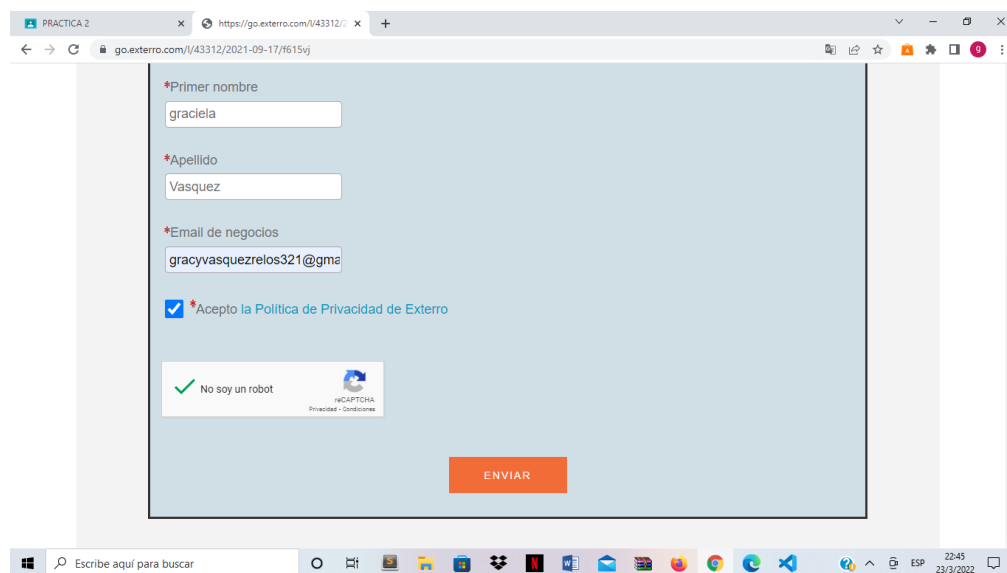
- Se realizó la practica en un Sistema operativo windows con la herramienta FTK imager.

**1) DESCARGAR FTK IMAGER**

- El primer paso es descargar FTK Imager de la siguiente dirección  
<https://accessdata.com/product-download/ftk-imager-version-4-2-1> como se observa se descargara el FTK imager 4.2.1

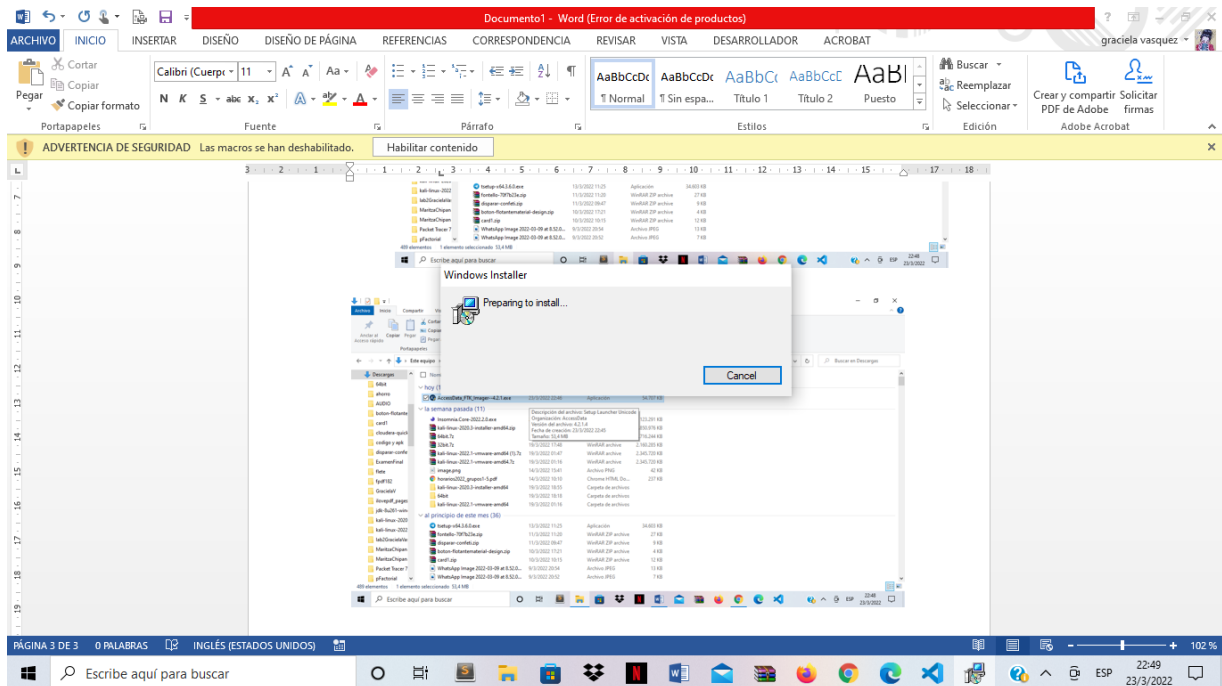


\*Al momento de descargar el FTK nos pide un formulario de registro donde debe ser llenado, y una vez llenado se procederá a la descarga.

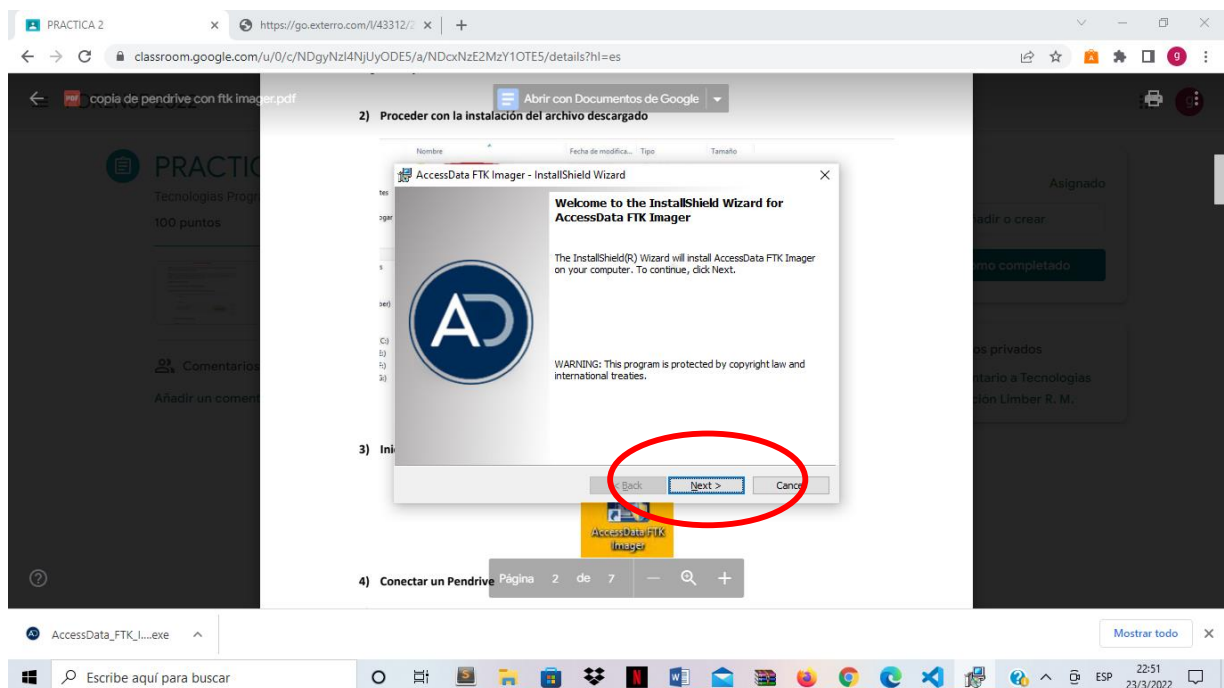


## 2) PROCEDER A LA INSTALACION DEL ARCHIVO DESCARGADO

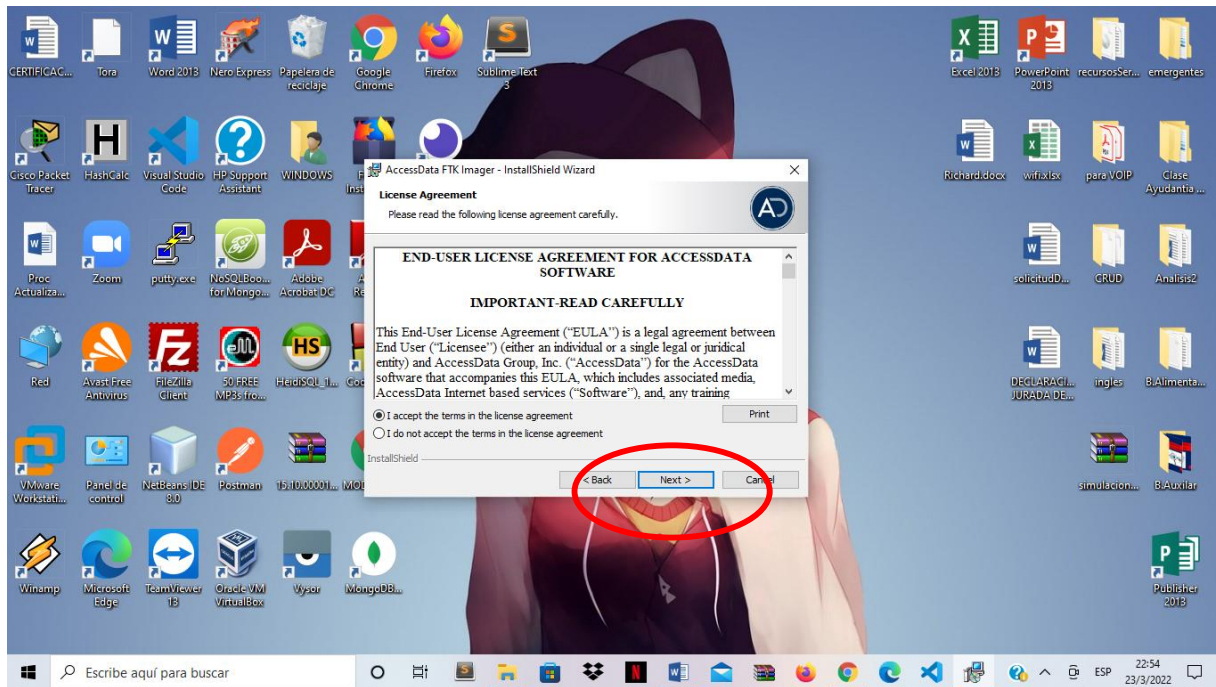
\* Se procede a la instalación, ejecutando el programa descargado.



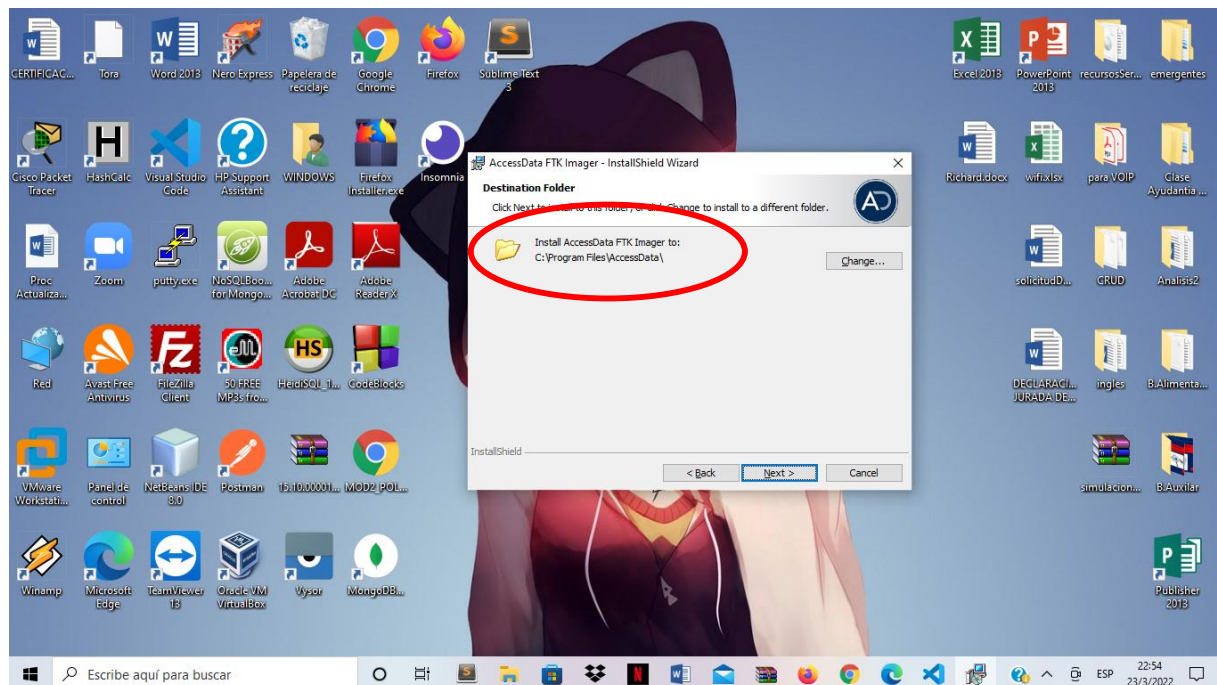
- La siguiente ventana nos da la bienvenida y Poner “next” en dicha ventana.



- Marcar "acepto todos los términos" y "next"

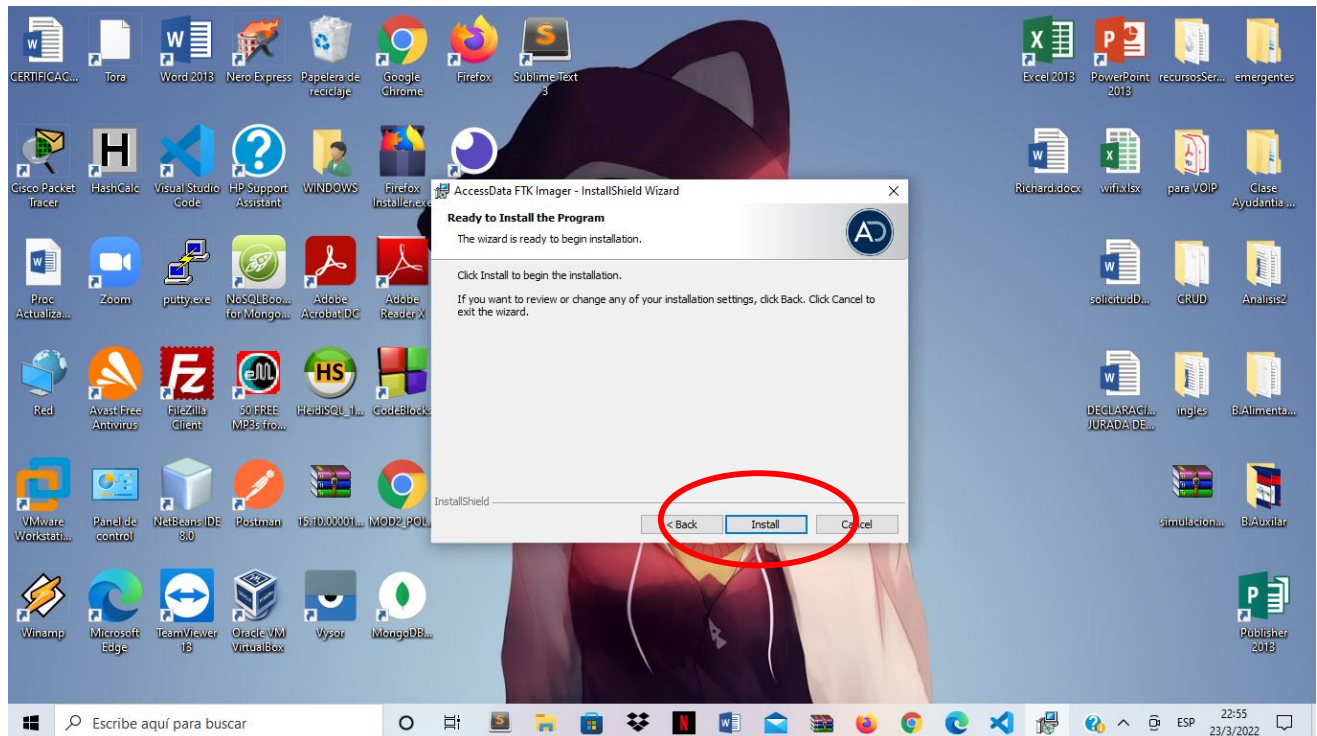


- Nos pregunta en que carpeta se esta guardando, en mi caso lo dejare la carpeta por defecto y poner siguiente "next"

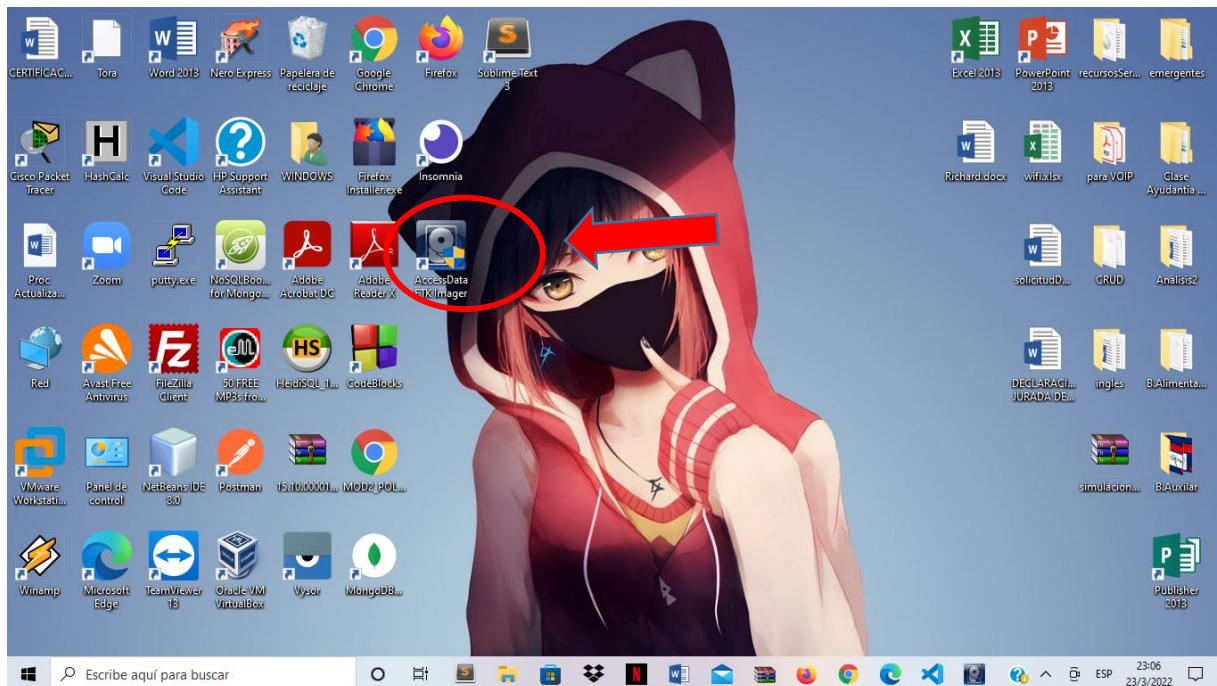




\*Finalmente se pondrá “finish” donde se procederá a la instalación del FTK.

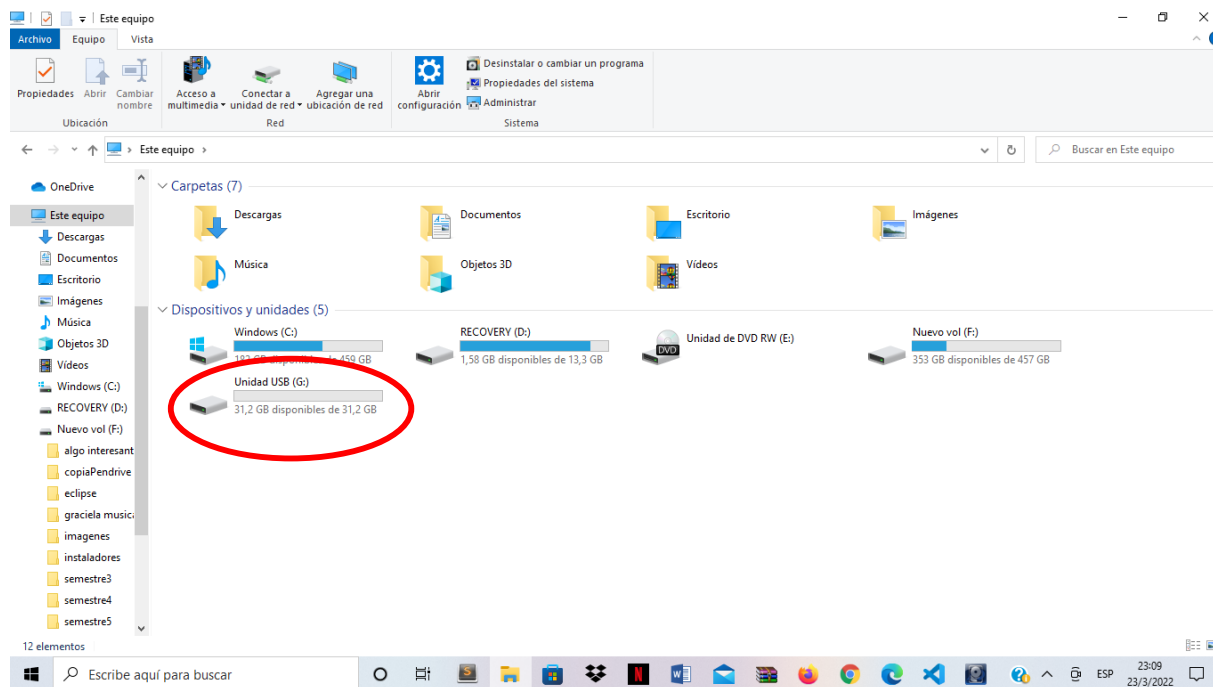


\*Se observa que ya se instaló el FTK en Windows.



### 3) CONECTAR EL PENDRIVE EN WINDOWS

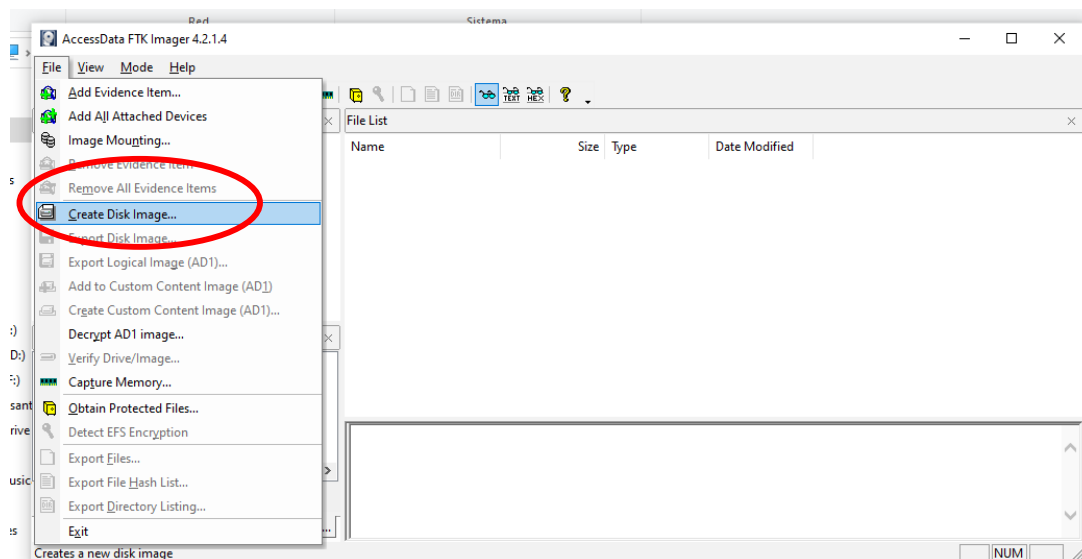
\*Como ya se tiene instalado, se procede a introducir un pendrive.



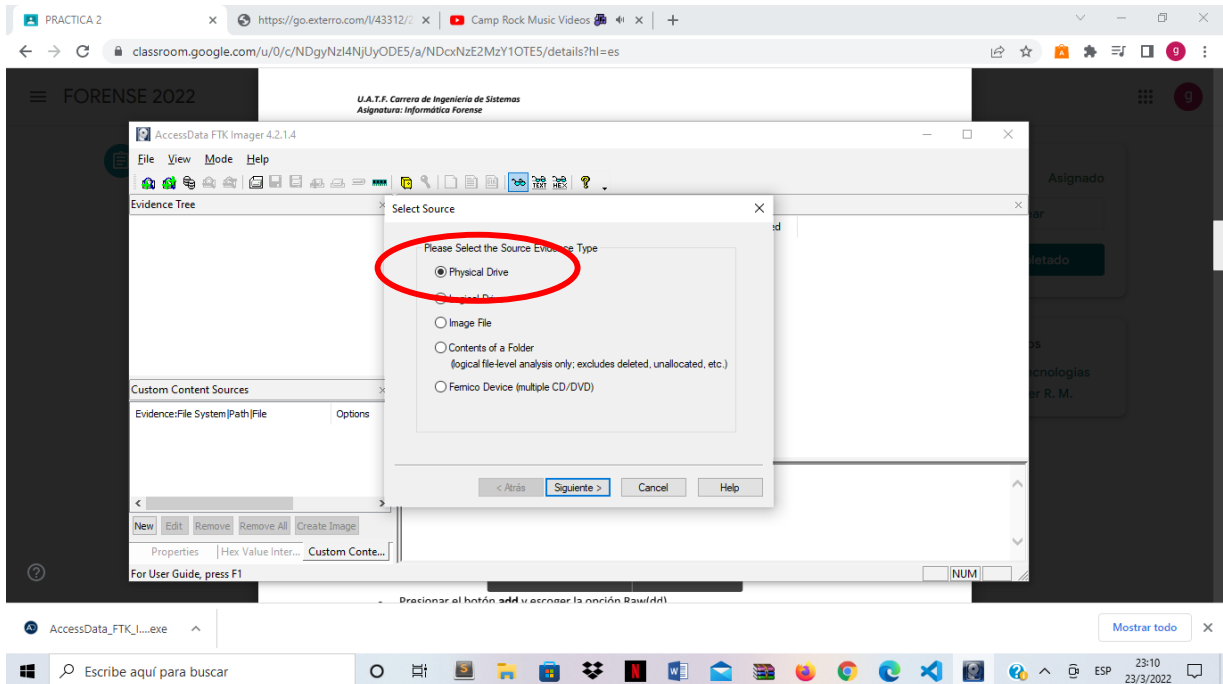
### 4) SE INICIA EL PROGRAMA FTK

\*Ahora ejecutamos FTK ya que ya se tiene instalado

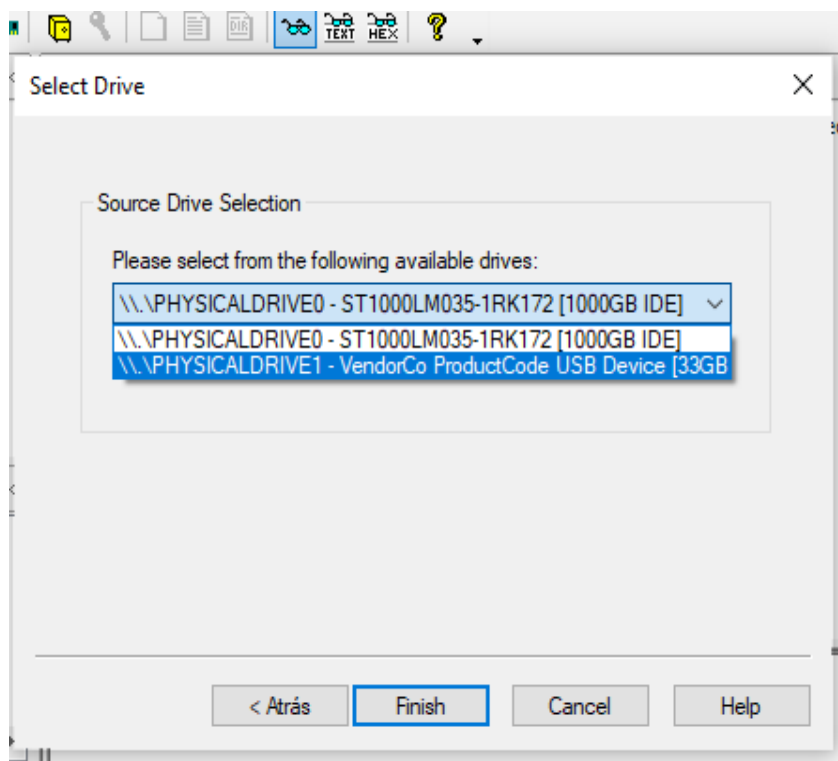
Se muestra una ventana, buscar "File" y "créate Disk Image"



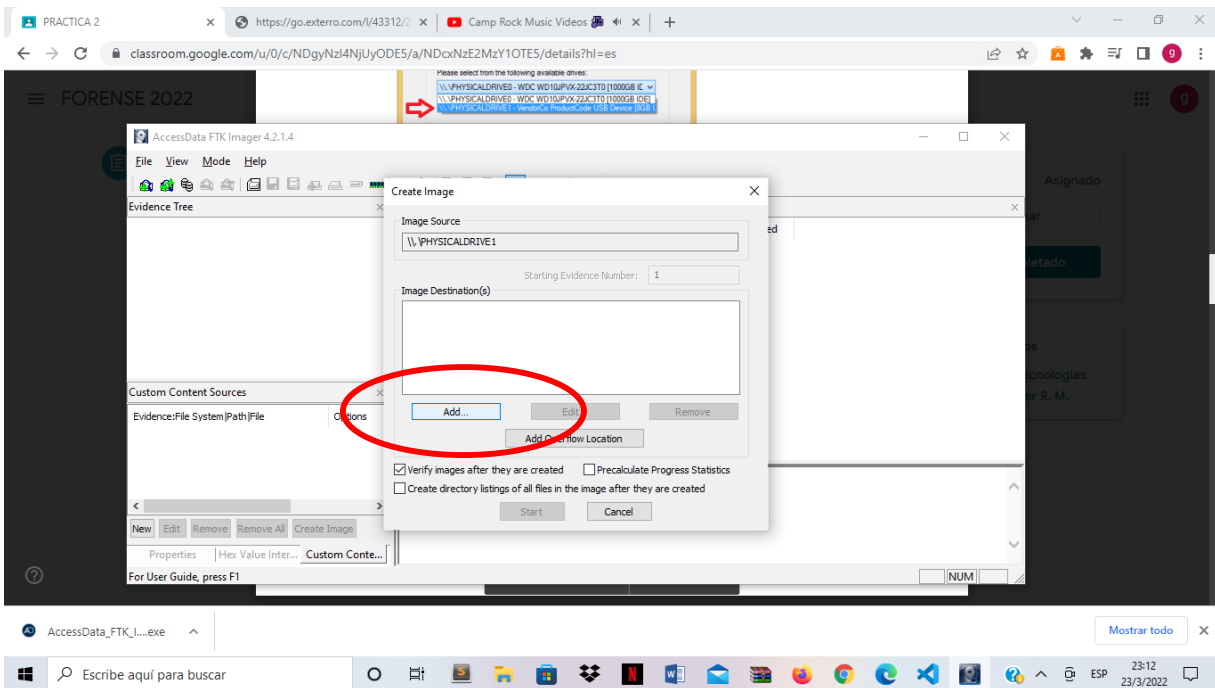
\*Sigüientemente Seleccionar Physical Drive



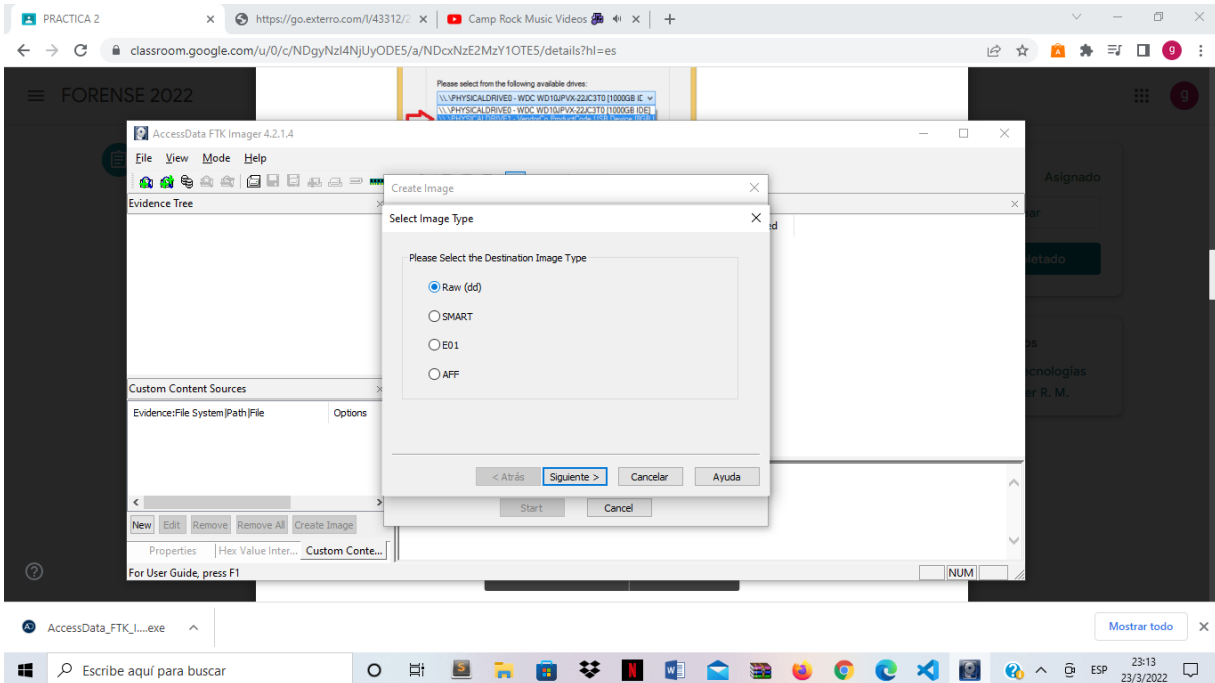
\*Desplegamos, seleccionamos el USB que se insertó a la pc.



- Presionamos “add”

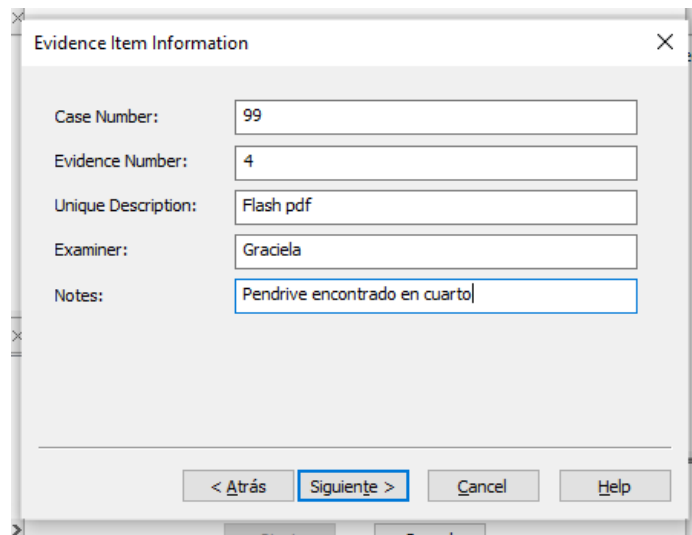


- Ahora presionamos la opcion Raw(dd)





\*Nos aparecerá un formulario, se llenara y después poner “siguiente”

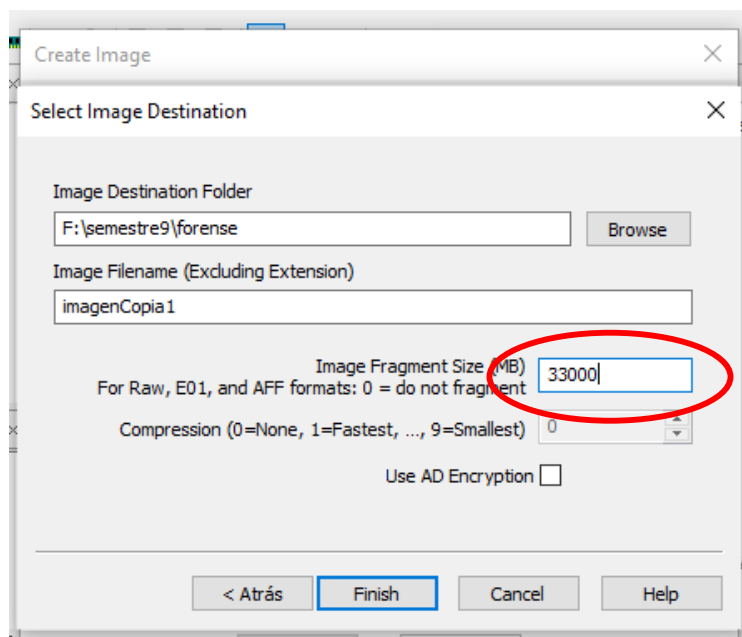


The 'Evidence Item Information' dialog box contains the following fields and values:

Field	Value
Case Number:	99
Evidence Number:	4
Unique Description:	Flash pdf
Examiner:	Graciela
Notes:	Pendrive encontrado en cuarto

At the bottom, there are four buttons: '< Atrás', 'Siguiente >', 'Cancel', and 'Help'. The 'Siguiente >' button is highlighted with a blue border.

- Ahora se selecciona el destino y el nombre de la imagen.  
Algo en tomar encuesta es el tamaño de la imagen, se puso 33000 MB, debido a que se eligió una sola partición y que el pendrive es de 32 GB.
- Al tomar la decisión, finalmente se pondrá finish.

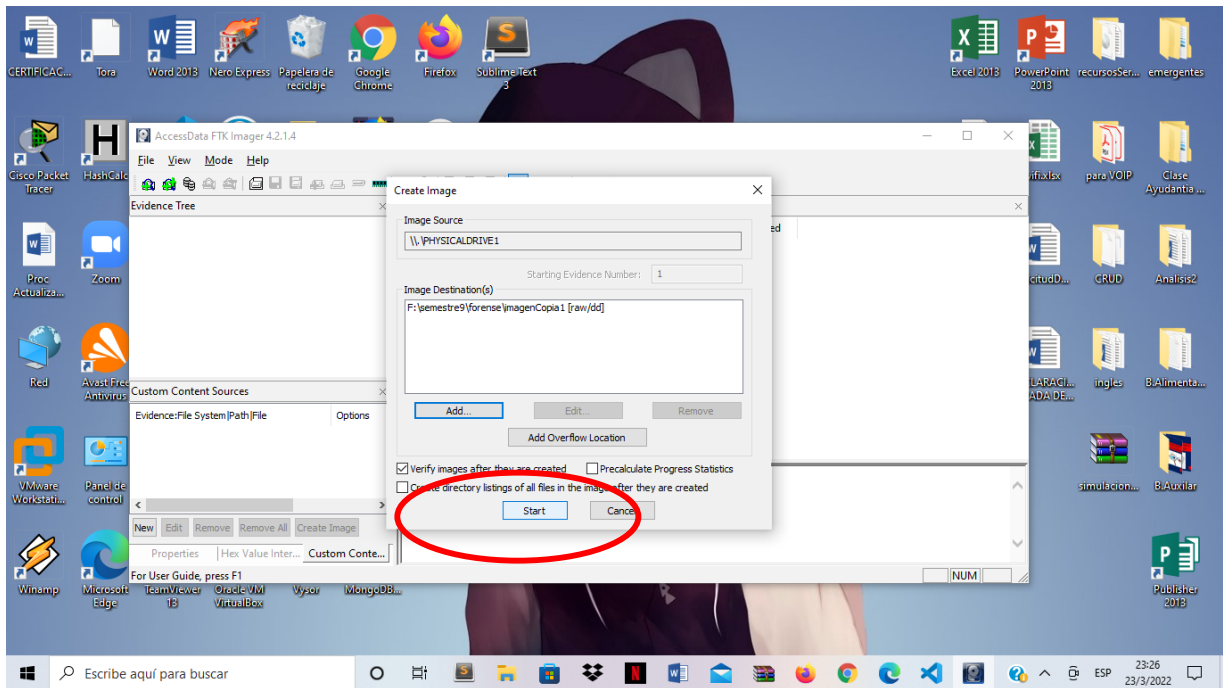


The 'Create Image - Select Image Destination' dialog box contains the following fields and values:

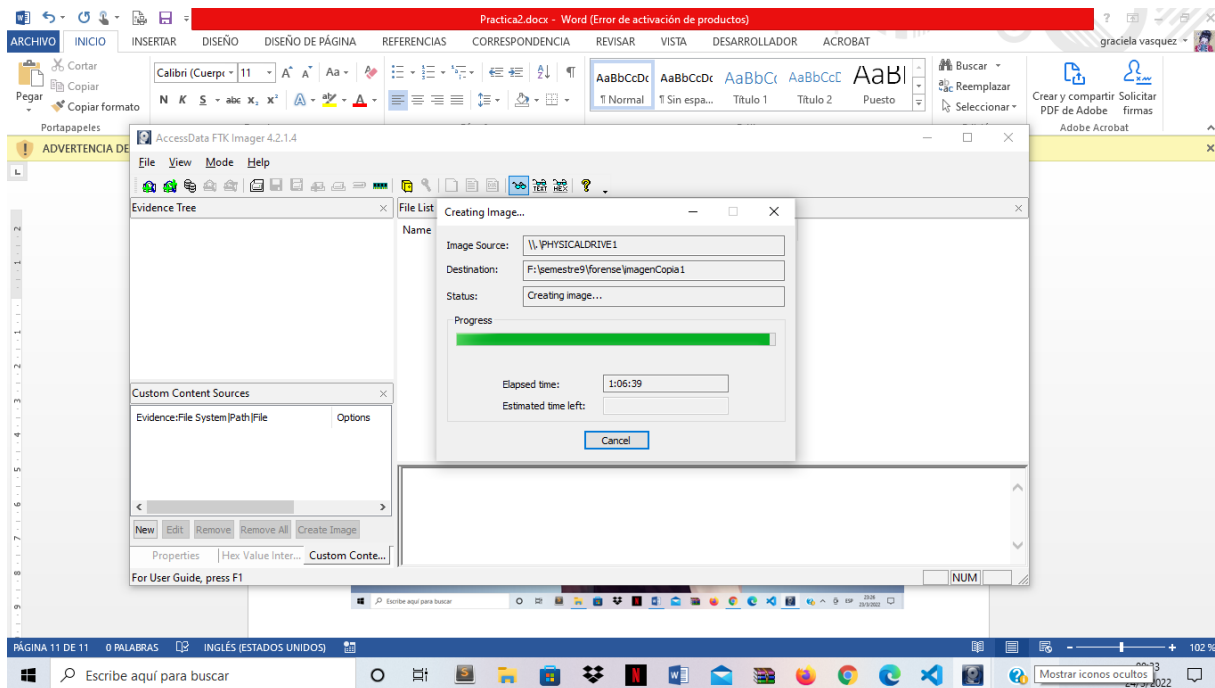
Field	Value
Image Destination Folder	F:\semestre9\forense
Image Filename (Excluding Extension)	imagenCopia1
Image Fragment Size (MB)	33000
Compression (0=None, 1=Fastest, ..., 9=Smallest)	0
Use AD Encryption	<input type="checkbox"/>

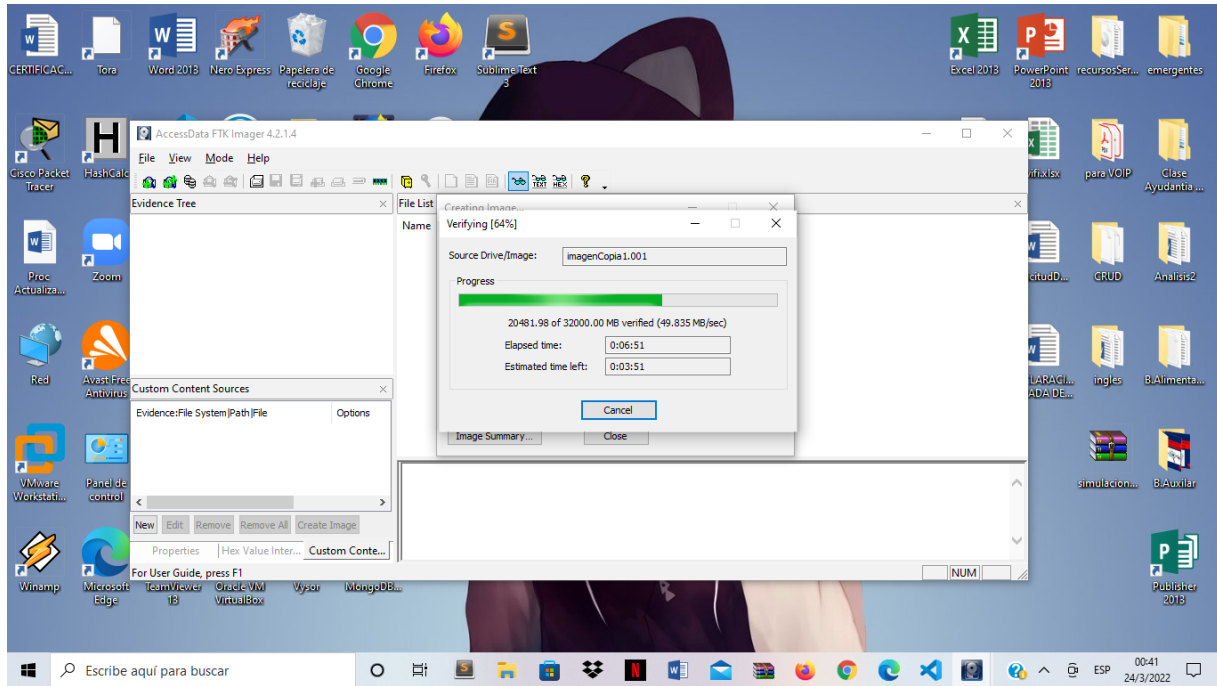
At the bottom, there are four buttons: '< Atrás', 'Finish', 'Cancel', and 'Help'. The 'Finish' button is highlighted with a blue border. A red circle highlights the 'Image Fragment Size (MB)' field with the value '33000'.

- Ahora se comenzara la copia, seleccionando “start”

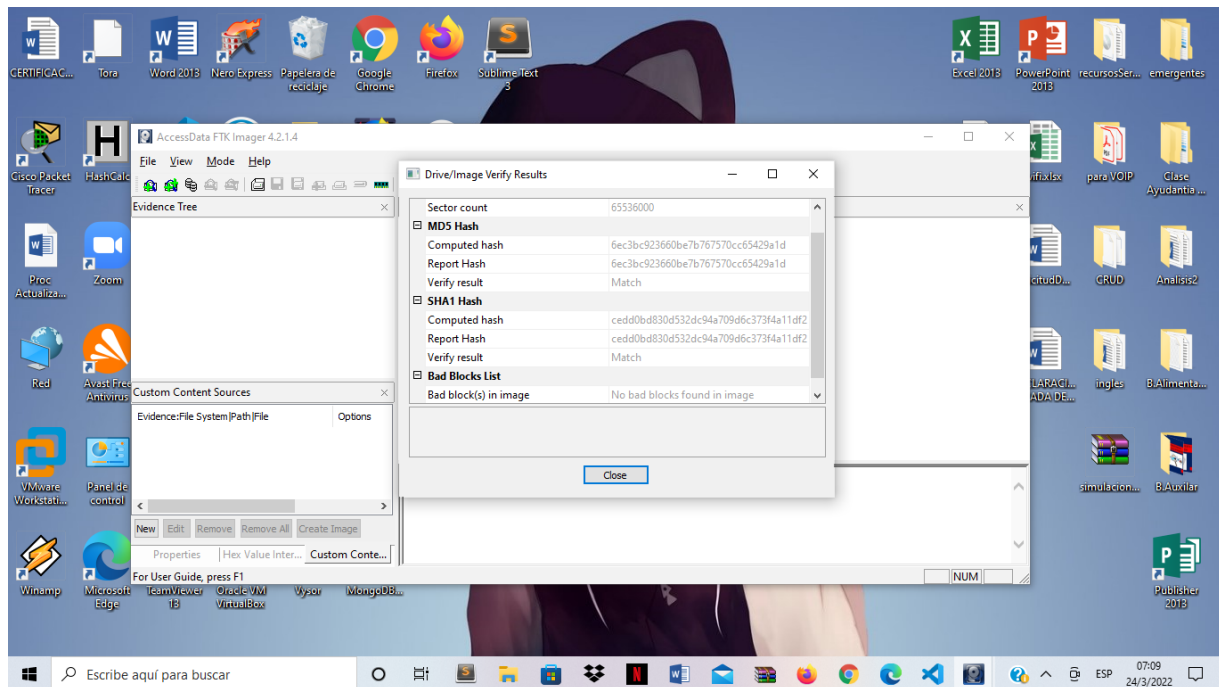


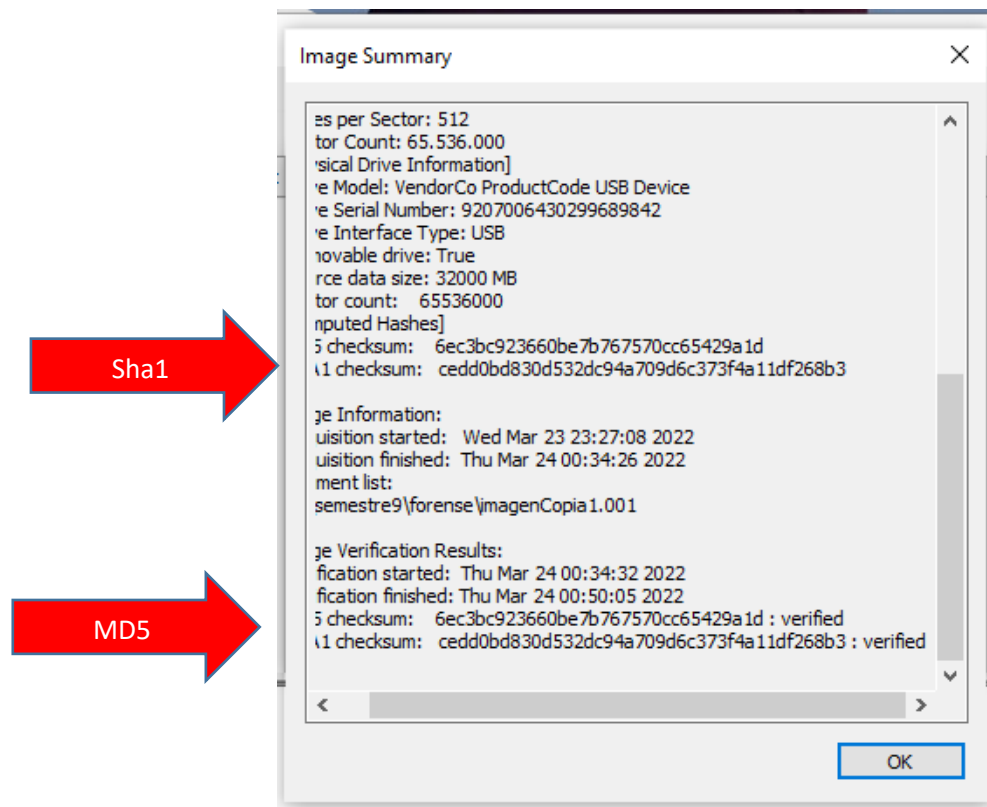
- Se observa que ya esta comenzando la copia.





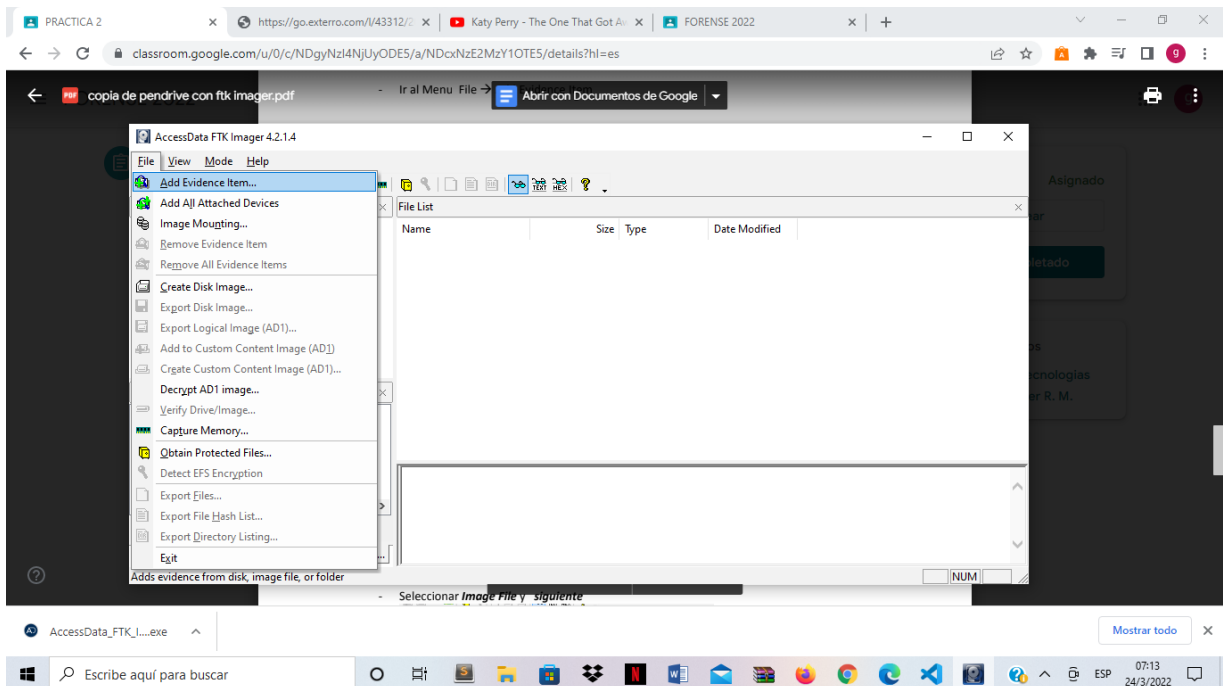
- Ya termino la copia del pendrive, generándonos un resumen de dicha imagen, como el código hash sha1 y md5 y otros datos que se debe considerar.



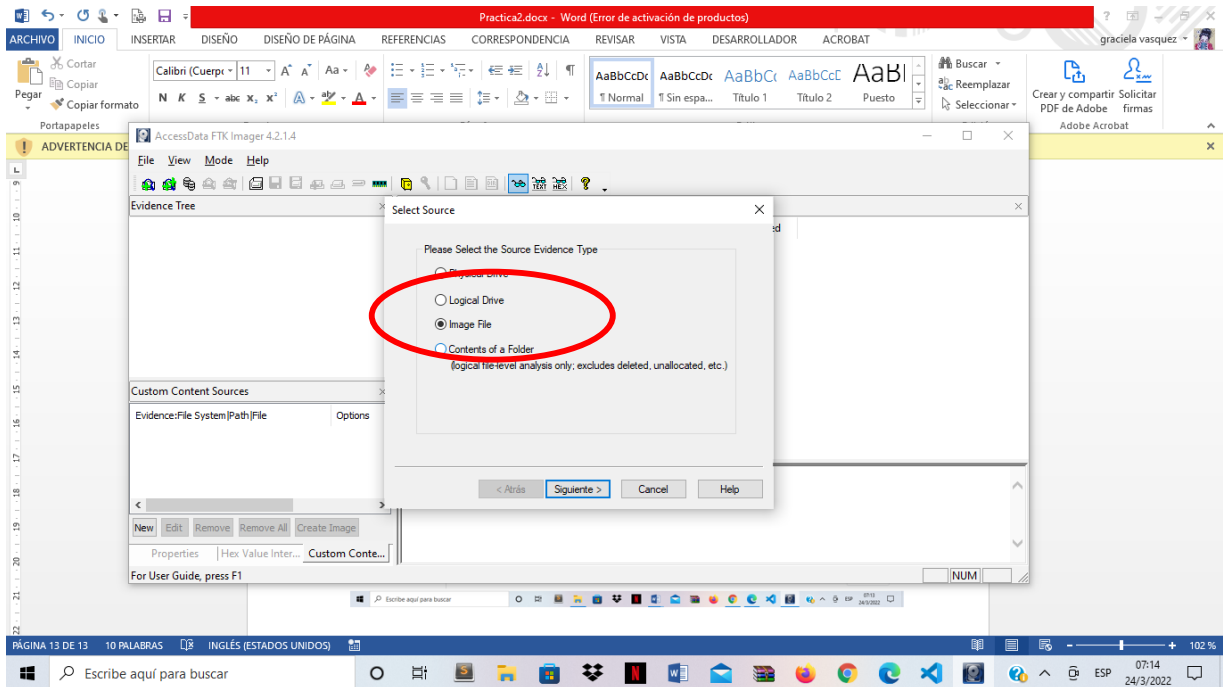


## 6) VIZUALIZAR LOS DATOS DE LA IMAGEN

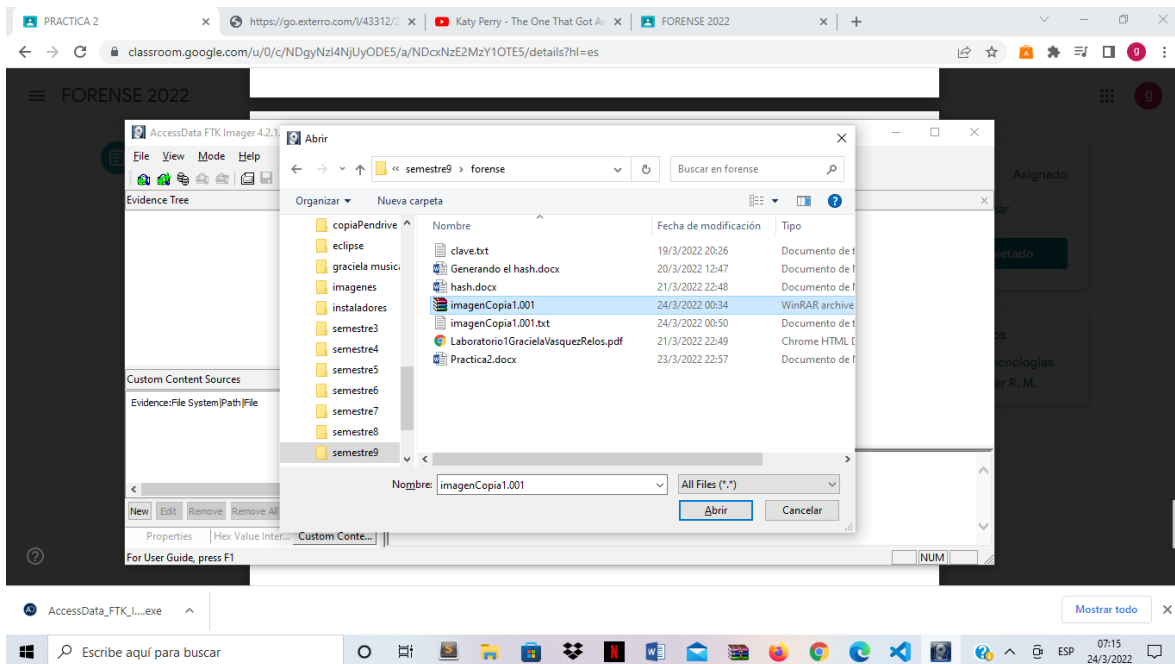
- Para la verificación de la imagen creada, se buscara “file” ->Add evidence Ram

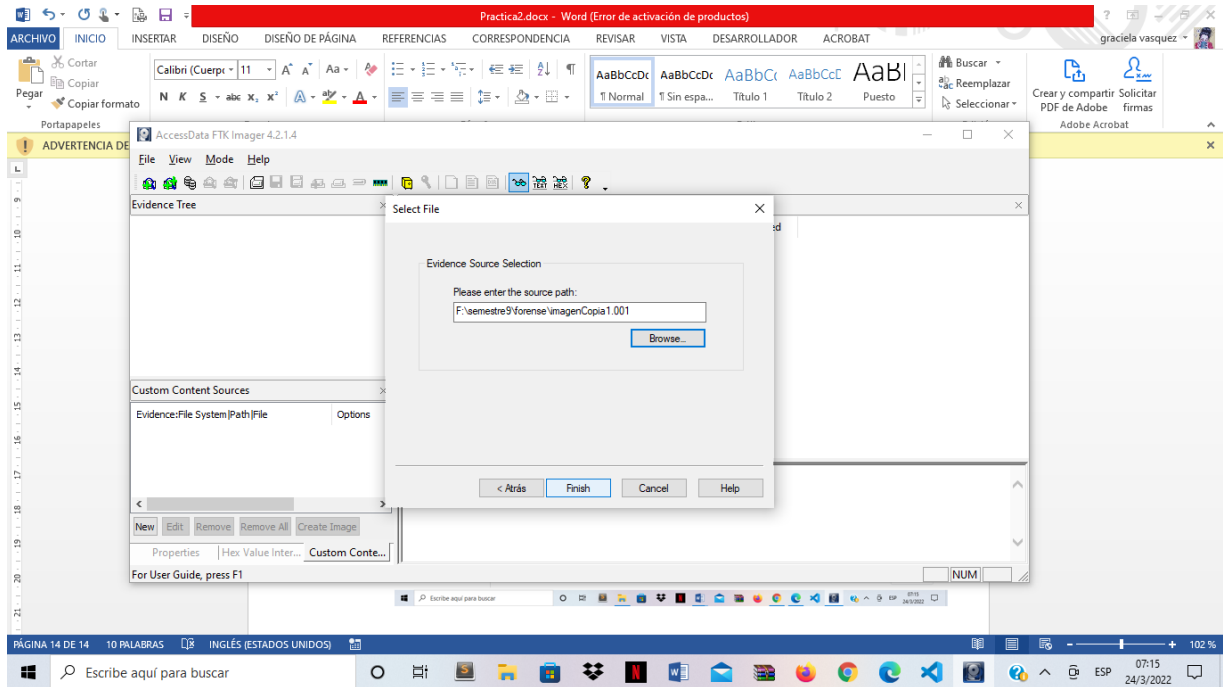


- Posteriormente seleccionamos “Image File”



- Al poner “siguiente”, mostrara una ventana para la búsqueda de la carpeta en donde se esta guardo la imagen.  
Seleccionamos el que dice “imagenCopia1.001”





- Finalmente se observa que realmente se hizo la copia de la imagen, y no solo eso sino que también de los archivos que se borraron en el pendrive.

