



DIGITAL FORENSIC FTK IMAGER

Tabla de contenidos

1	Abstracto	3
2	Introducción a las imágenes y al generador de imágenes FTK	5
3	Crear una imagen forense	7
4	Capturando memoria	14
5	Analizando el volcado de imágenes	17
6	Montaje de imagen para conducir	21
7	Imagen de contenido personalizado con cifrado AD	24
8	Descifrar imagen AD1	29
9	Obtener archivos protegidos	33
10	Detectar cifrado EFS	36
11	Exportar archivos	39
11	Acerca de nosotros	41

Abstracto

FTK Imager es un software de código abierto de AccessData que se utiliza para crear copias precisas de la evidencia original sin realizar ningún cambio. La imagen de la evidencia original sigue siendo la misma y nos permite copiar datos a un ritmo mucho más rápido, que pronto podrá conservarse y analizarse más a fondo.

El generador de imágenes FTK también le proporciona la función de verificación de integridad incorporada que genera un informe hash que ayuda a hacer coincidir el hash de la evidencia antes y después de crear la imagen de la evidencia original.

Introducción a las imágenes y al generador de imágenes FTK

La adquisición de datos de un Disco Duro se conoce como imagen, quizás imagen forense cuando se realiza en una investigación. La creación de una imagen forense es uno de los pasos más cruciales de la investigación forense digital.

Sin embargo, este disco con imagen debe aplicarse al disco duro para funcionar. No se puede restaurar un disco duro colocando los archivos de imagen del disco en él, ya que es necesario abrirlo e instalarlo en el disco mediante un programa de imágenes.

Un solo disco duro puede almacenar muchas imágenes de disco. Las imágenes de disco también se pueden almacenar en unidades flash de mayor capacidad.



¡Hecho de la diversión!

Puede crear una imagen forense desde una máquina en funcionamiento o inactiva. Es una instantánea literal en el tiempo que tiene verificación de integridad.



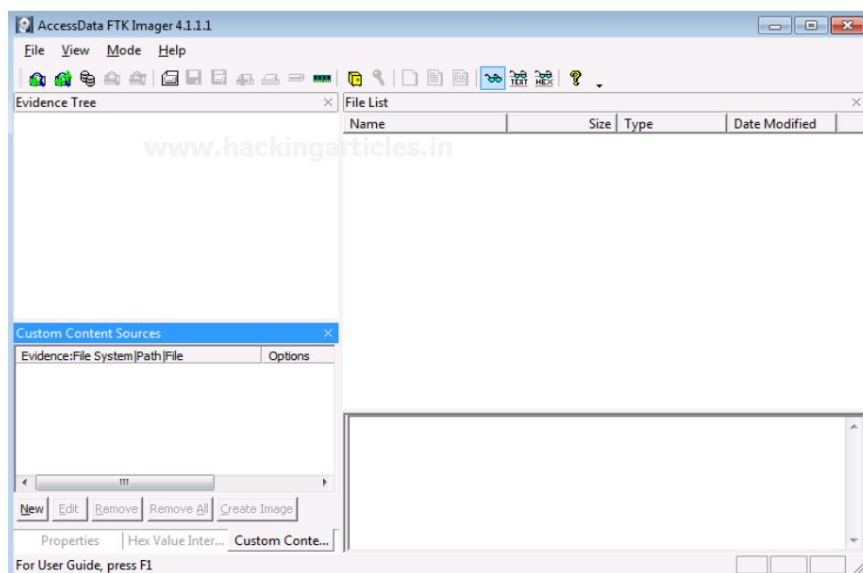
A menudo necesitamos verificar la integridad de la imagen forense, ya que nos proporciona un medio para mantener la integridad de la evidencia y garantizar que no sea manipulada.

Aunque el generador de imágenes FTK se utiliza generalmente como generador de imágenes y herramienta de vista previa, también tiene capacidades suficientes para ayudar a los investigadores forenses durante el examen de dispositivos digitales en otros asuntos.

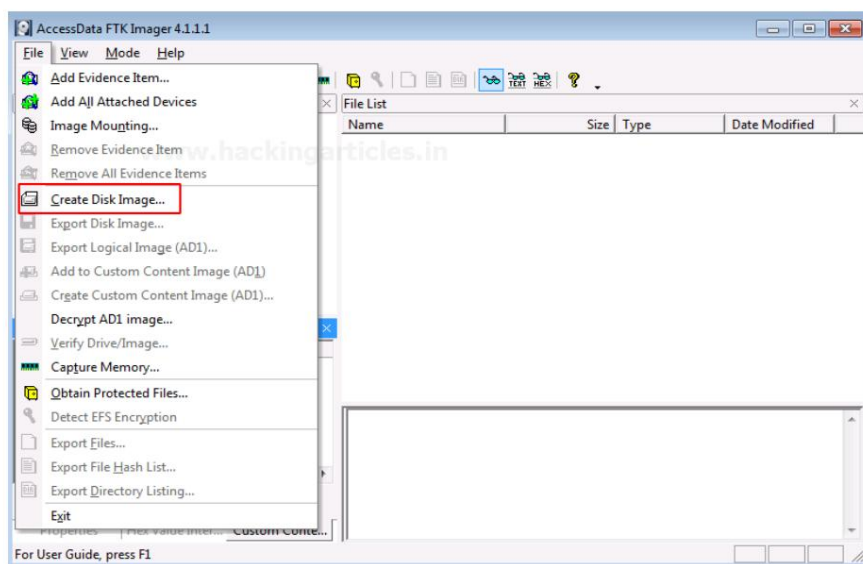
Así que comencemos, exploraremos las opciones que nos ofrece FTK imager en la pestaña Archivo .

Crear una imagen forense

Abra FTK Imager de AccessData después de instalarlo y verá la ventana emergente que es la primera página en la que se abre esta herramienta.

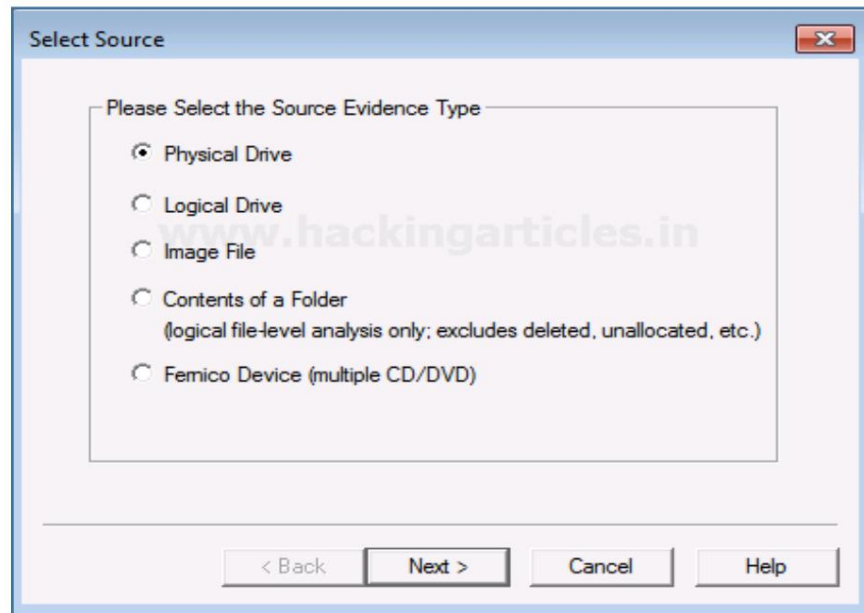


Ahora, para crear una imagen de disco. Haga clic en Archivo > Crear imagen de disco.

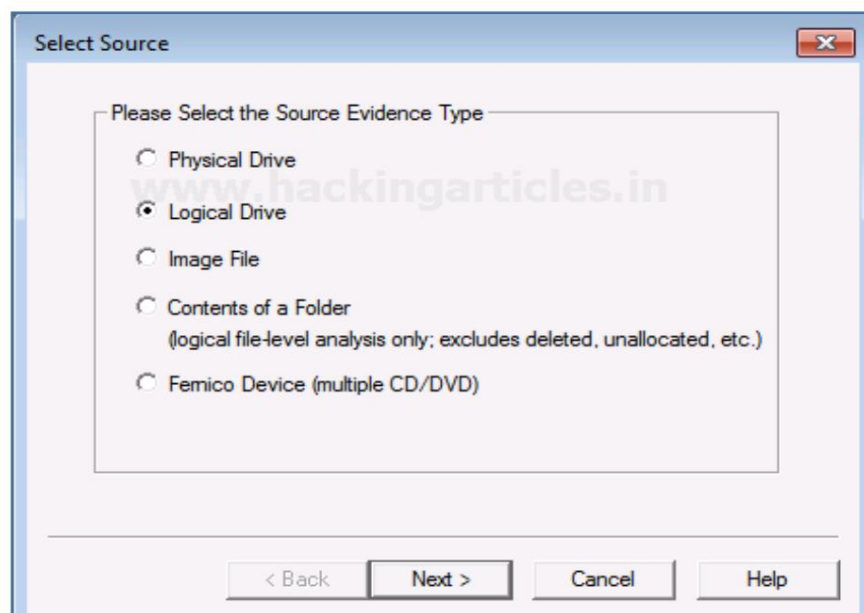


Ahora puedes elegir la fuente según la unidad que tengas. Puede ser una unidad física o lógica dependiendo de su evidencia.

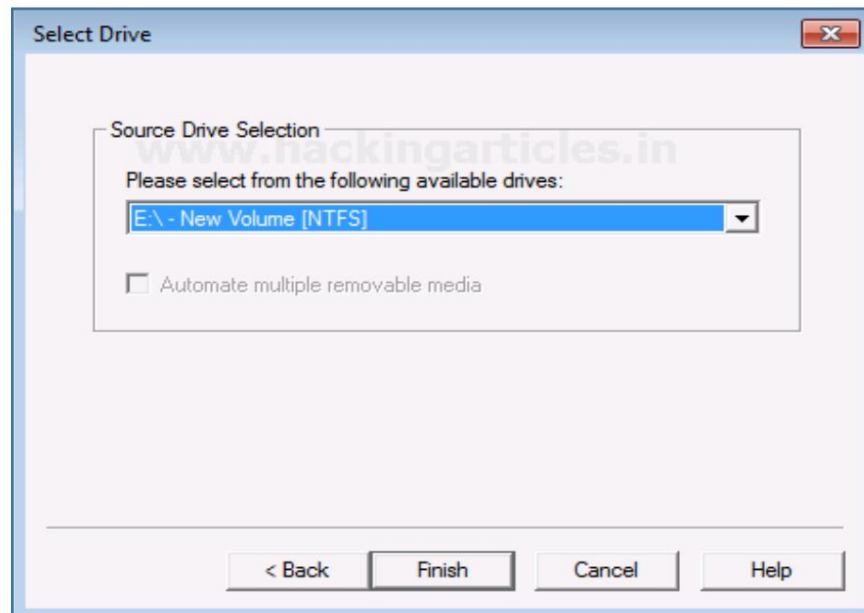
Una unidad física es el hardware de almacenamiento principal o el componente dentro de un dispositivo, que se utiliza para almacenar, recuperar y organizar datos.



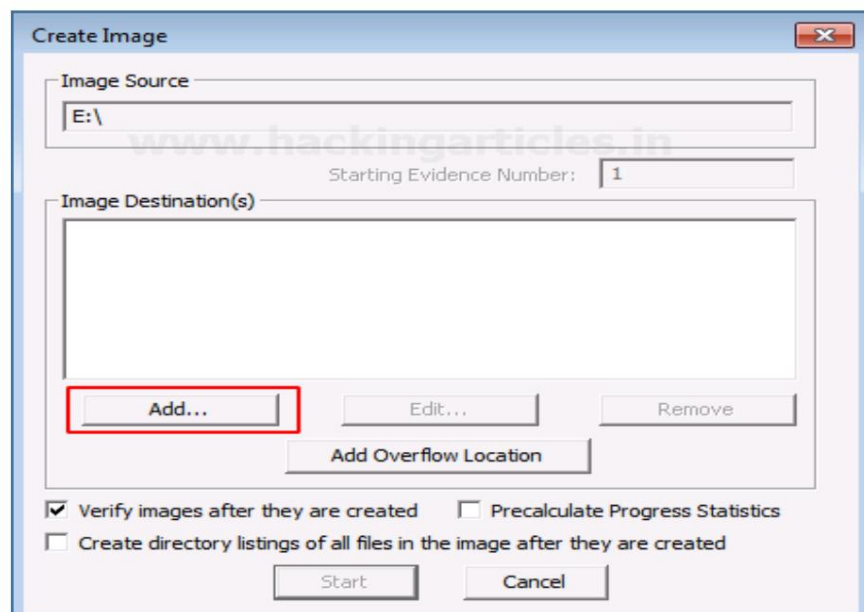
Una unidad lógica es generalmente un espacio en la unidad que se crea en un disco duro físico. Una unidad lógica tiene sus parámetros y funciones porque opera de forma independiente.



Ahora elija la fuente de su unidad de la que desea crear una copia de imagen.



Agregue la ruta de destino de la imagen que se va a crear. Desde la perspectiva forense, se debe copiar en un disco duro separado y se deben crear múltiples copias de la evidencia original para evitar la pérdida de evidencia.



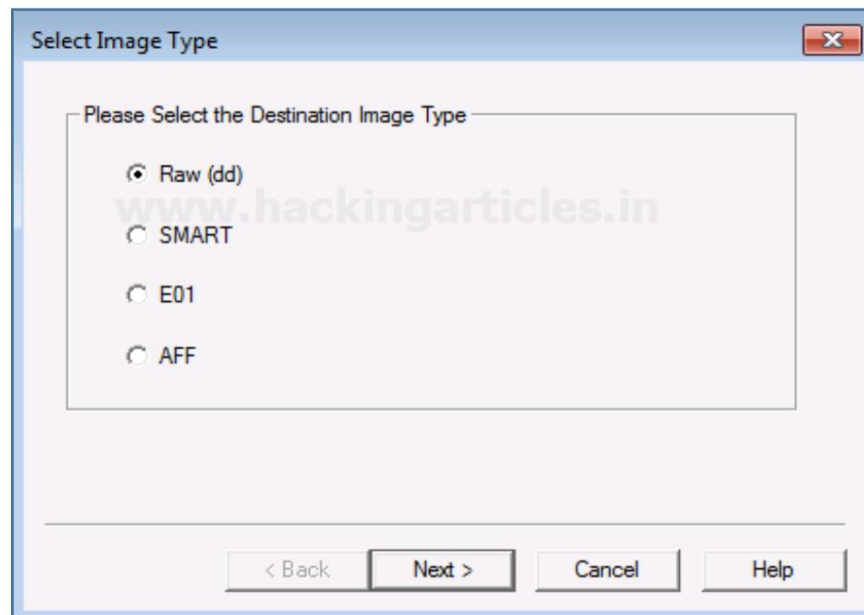
Seleccione el formato de la imagen que desea crear. Los diferentes formatos para crear la imagen son:

Sin procesar (dd): es una copia bit a bit de la evidencia original que se crea sin adiciones ni eliminaciones. No contienen ningún metadato.

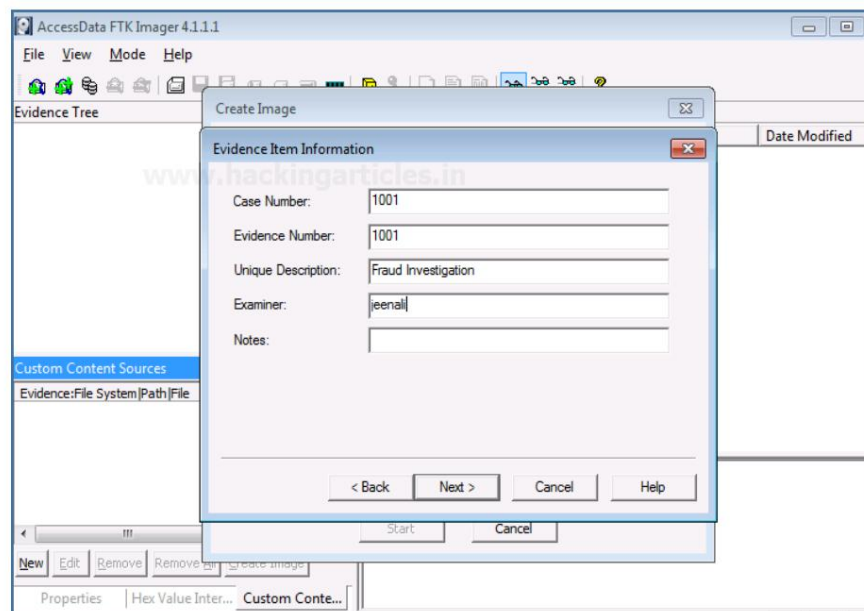
SMART: Es un formato de imagen que se usaba para Linux y que ya no se usa popularmente.

E01: Significa EnCase Evidence File, que es un formato comúnmente utilizado para imágenes y es similar a

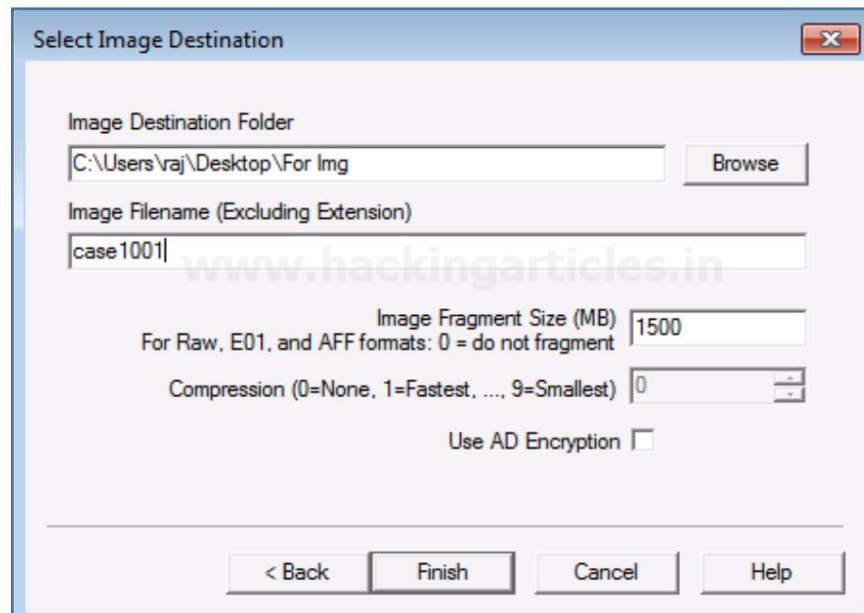
AFF: Significa formato forense avanzado, que es un tipo de formato de código abierto.



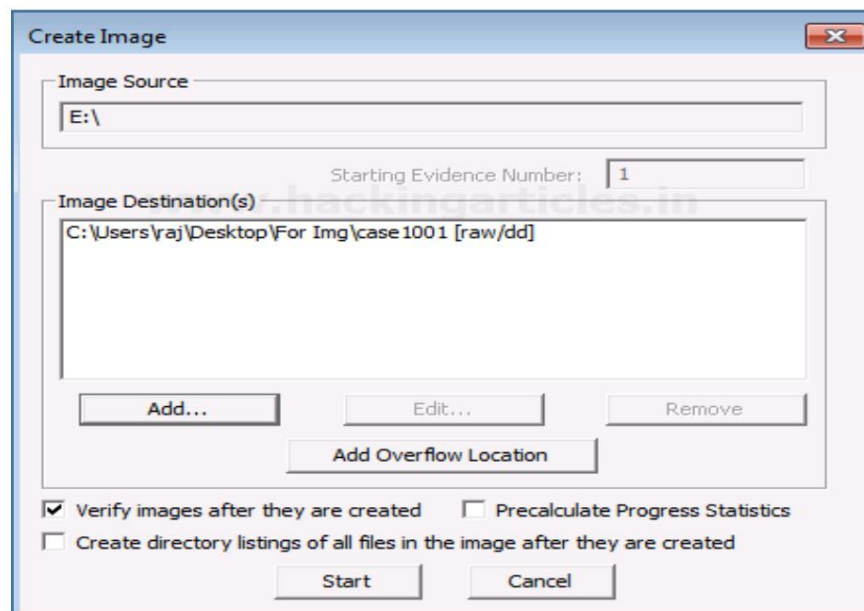
A Ahora, agregue los detalles de la imagen para continuar.



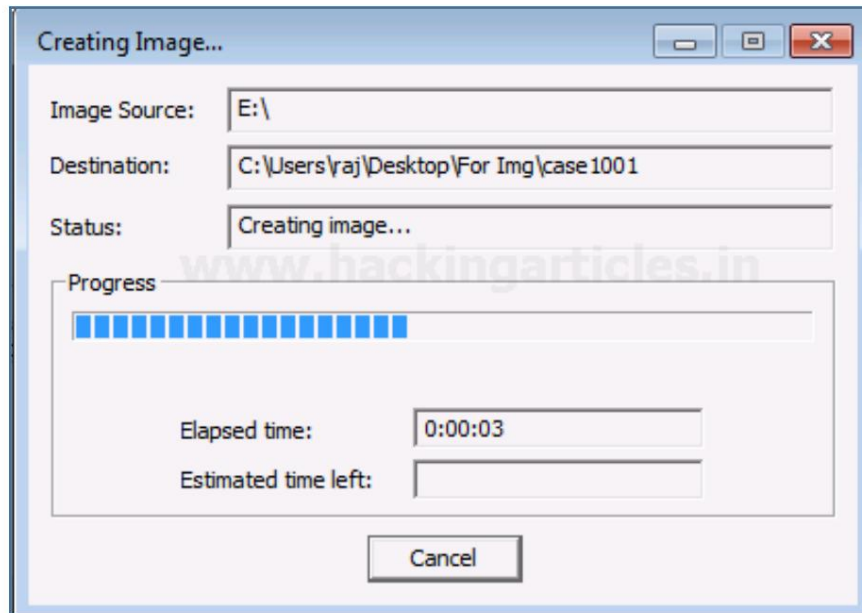
Ahora finalmente agregue el destino del archivo de imagen, asigne un nombre al archivo de imagen y luego haga clic en Finalizar.



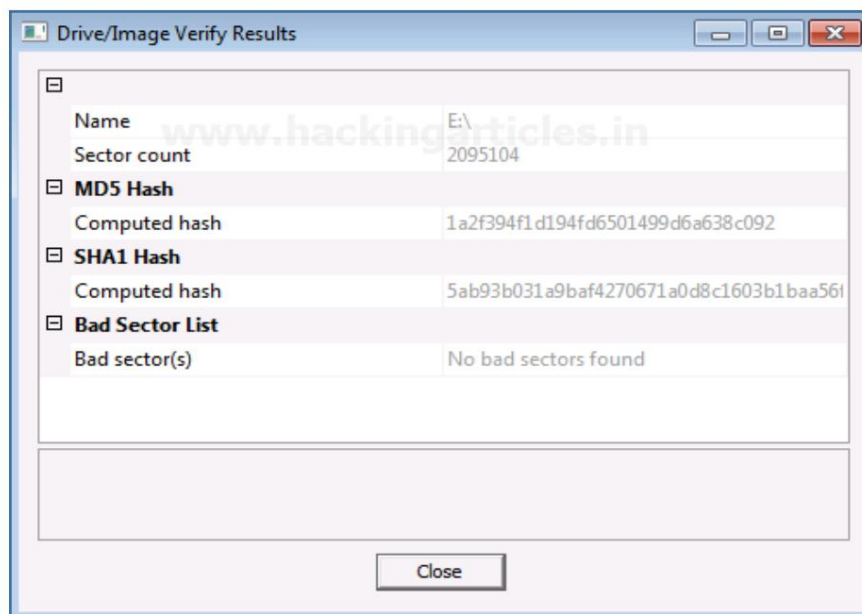
Una vez que haya agregado la ruta de destino, ahora puede comenzar con la imagen y también hacer clic en la opción de verificación para generar un hash.



Ahora esperemos unos minutos hasta que se cree la imagen.



Después de crear la imagen, se genera un resultado Hash que verifica el Hash MD5, el Hash SHA1 y la presencia de cualquier sector defectuoso.



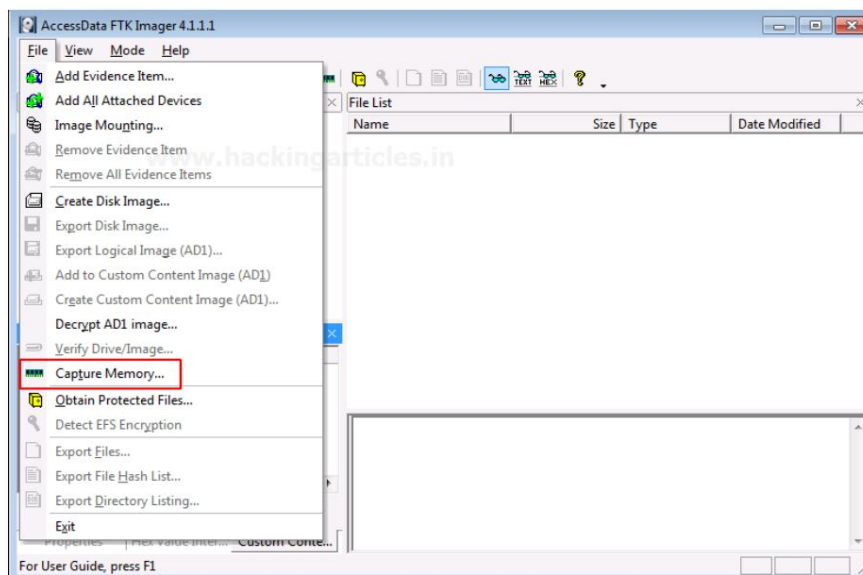
Capturando memoria

Es el método de capturar y volcar el contenido de un contenido volátil en un dispositivo de almacenamiento no volátil para preservarlo para una investigación adicional. Un análisis de RAM sólo se puede realizar con éxito cuando la adquisición se ha realizado con precisión sin corromper la imagen de la memoria volátil.

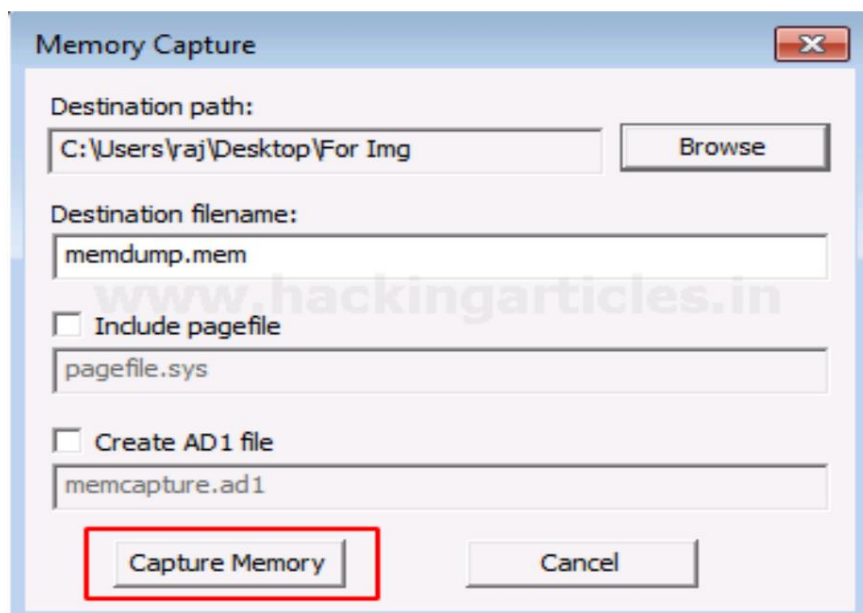
En esta fase, el investigador debe tener cuidado con sus decisiones de recopilar datos volátiles, ya que no existirán después de que el sistema se reinicie.

Ahora, comencemos por capturar el recuerdo.

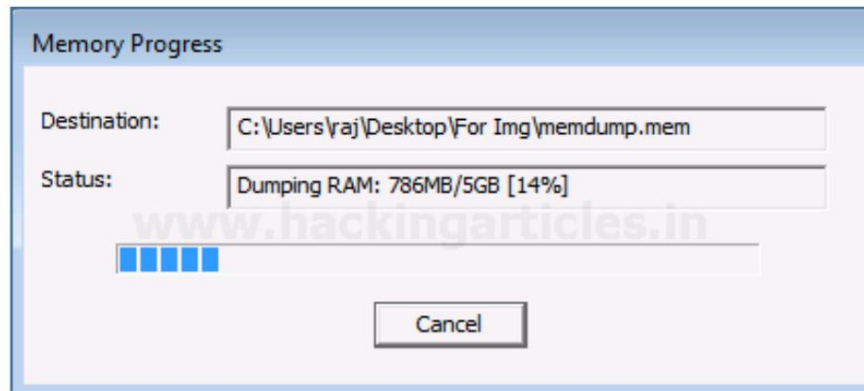
Para capturar la memoria, haga clic en Archivo > Capturar memoria.



Elija la ruta de destino y el nombre del archivo de destino, y haga clic en capturar memoria.



Ahora esperemos unos minutos hasta que capturen el carnero.



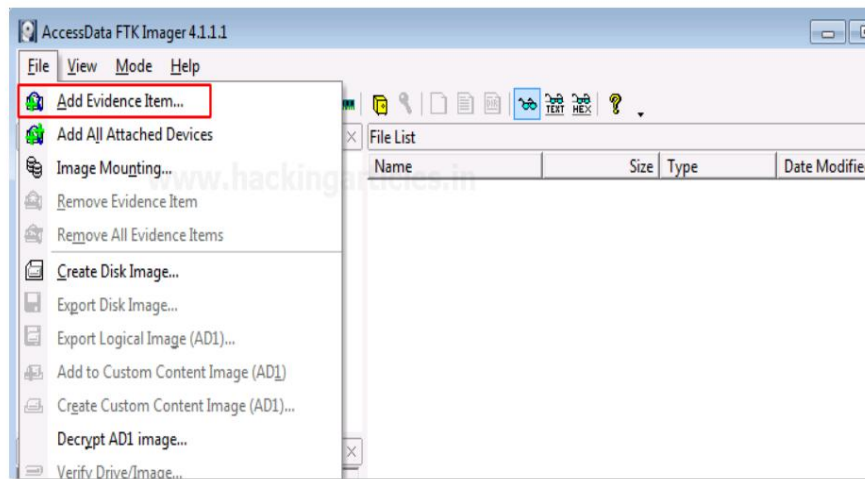
¡Hecho de la diversión!

Puedes tener suerte con las capturas de RAM en algún momento, ya que contienen:

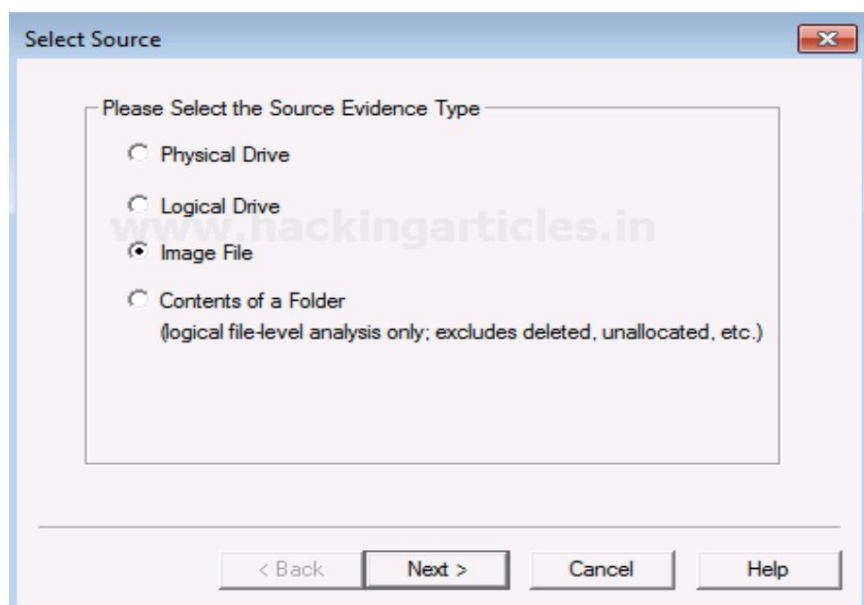
- Contraseñas
- Cartas credenciales
- Documentos no guardados

Analizando el volcado de imágenes

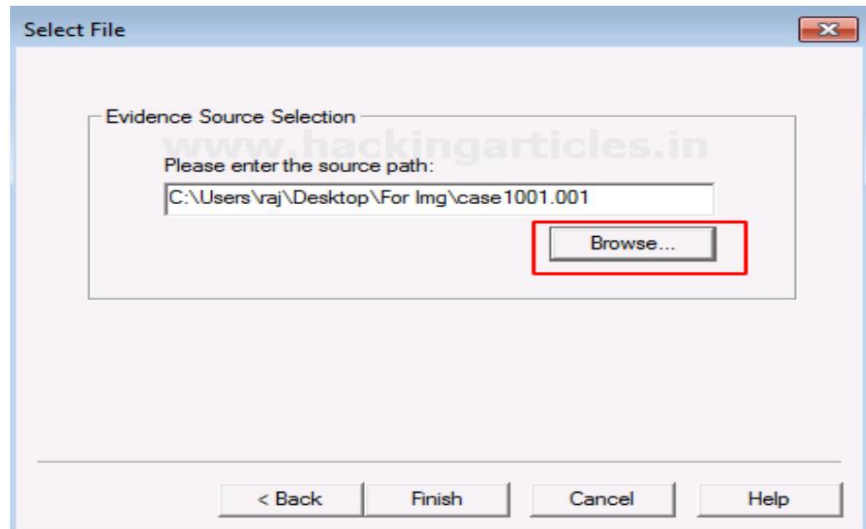
Ahora analicemos el volcado de imagen RAW una vez que se haya adquirido utilizando el generador de imágenes FTK. Para comenzar con el análisis, haga clic en Archivo> Agregar elemento de evidencia.



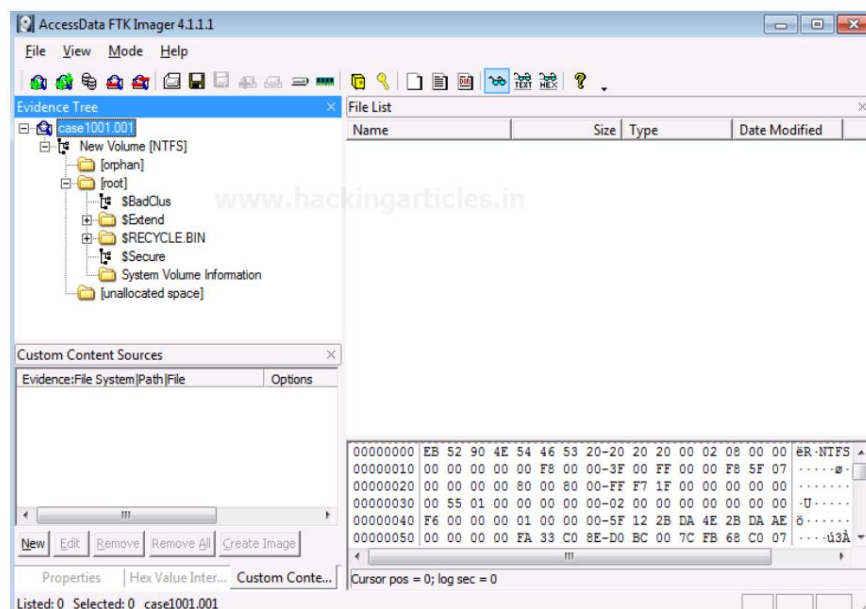
Ahora seleccione la fuente del archivo de volcado que ya ha creado, así que aquí debe seleccionar la opción de archivo de imagen y hacer clic en Siguiente.



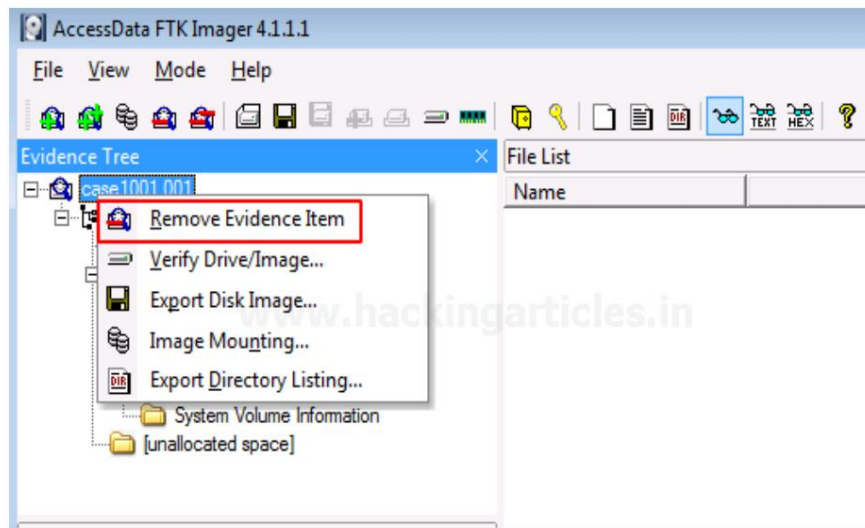
Elija la ruta del volcado de imágenes que ha capturado haciendo clic en Examinar.



Una vez que el volcado de imágenes esté adjunto a la parte de análisis, verá un árbol de evidencia que tiene el contenido de los archivos del volcado de imágenes. Esto podría haber eliminado y sobrescrito datos.

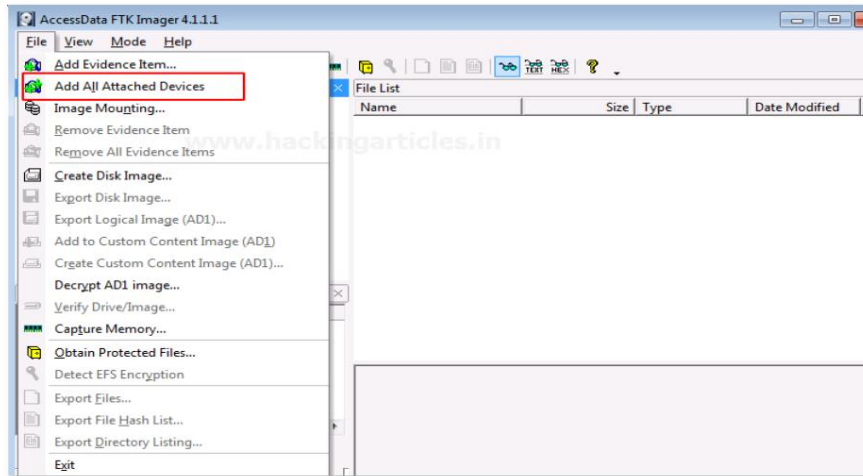


Para analizar otras cosas más a fondo, ahora eliminaremos este elemento de evidencia haciendo clic derecho en el caso y haciendo clic en Eliminar elemento de evidencia.

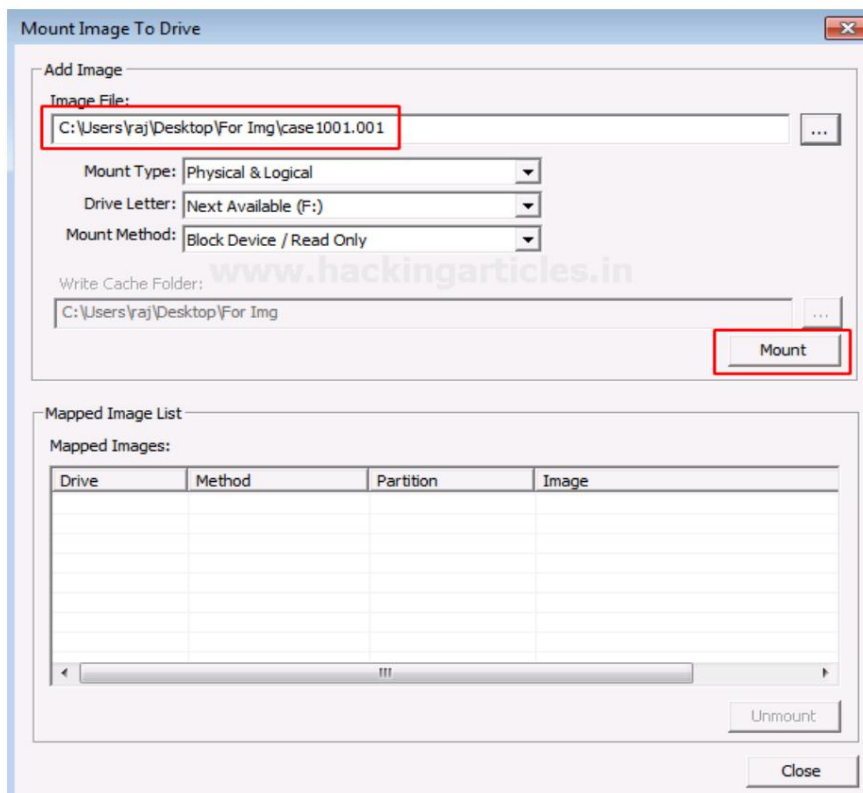


Montaje de imagen para conducir

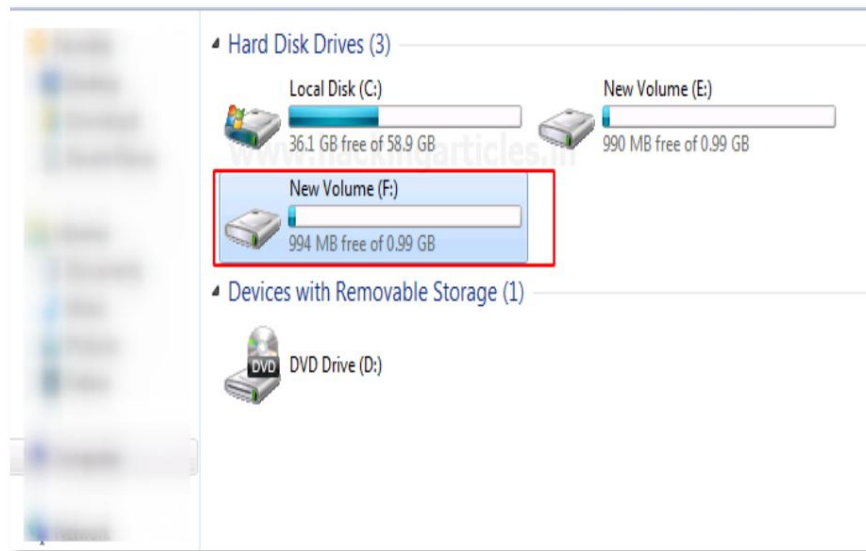
Para montar la imagen como una unidad en su sistema, haga clic en Archivo > Montaje de imagen



Una vez que aparezca la ventana Montar imagen en la unidad, puede agregar la ruta al archivo de imagen que desea montar y hacer clic en Montar.



Ahora puede ver que el archivo de imagen se ha montado como una unidad.



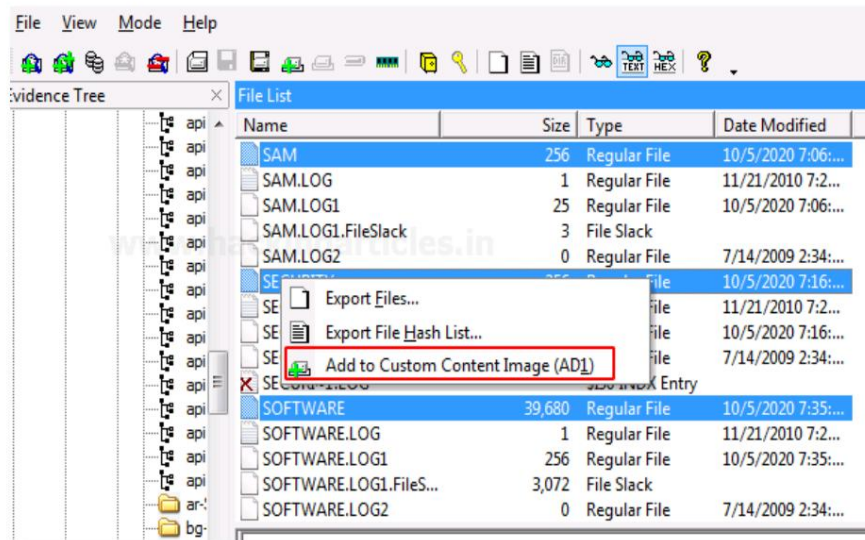
¡Hecho de la diversión!

Montar la imagen en una unidad le permite copiar archivos o directorios del archivo de imagen a discos duros existentes, lo que facilita mucho el flujo de trabajo.

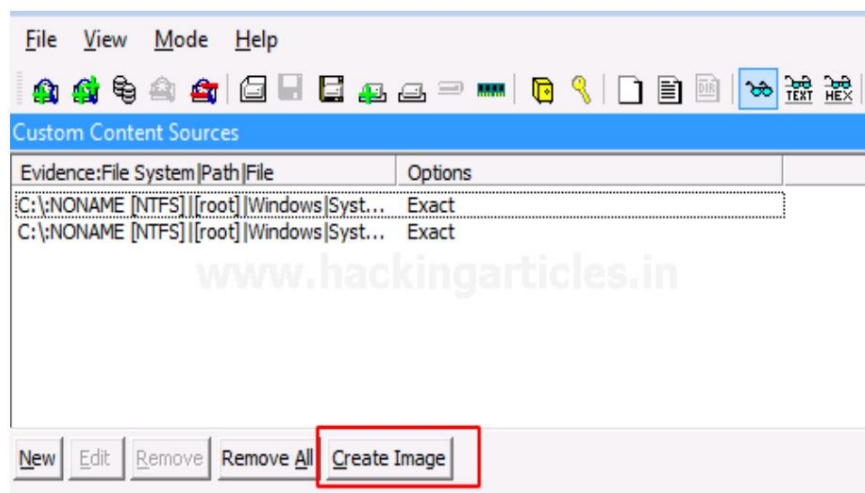
Sin embargo, aún no podrás eliminar ni agregar archivos.

Imagen de contenido personalizado con cifrado AD

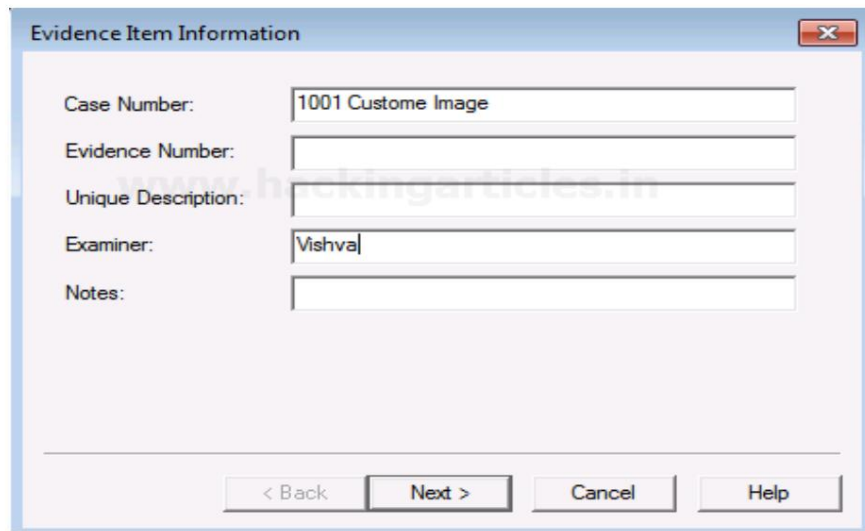
El generador de imágenes FTK tiene una función que le permite cifrar archivos de un tipo particular según los requisitos del examinador. Haga clic en los archivos que desea agregar a la imagen de contenido personalizado junto con el cifrado AD.



Todos los archivos seleccionados se mostrarán en una nueva ventana y luego haga clic en Crear imagen para continuar.

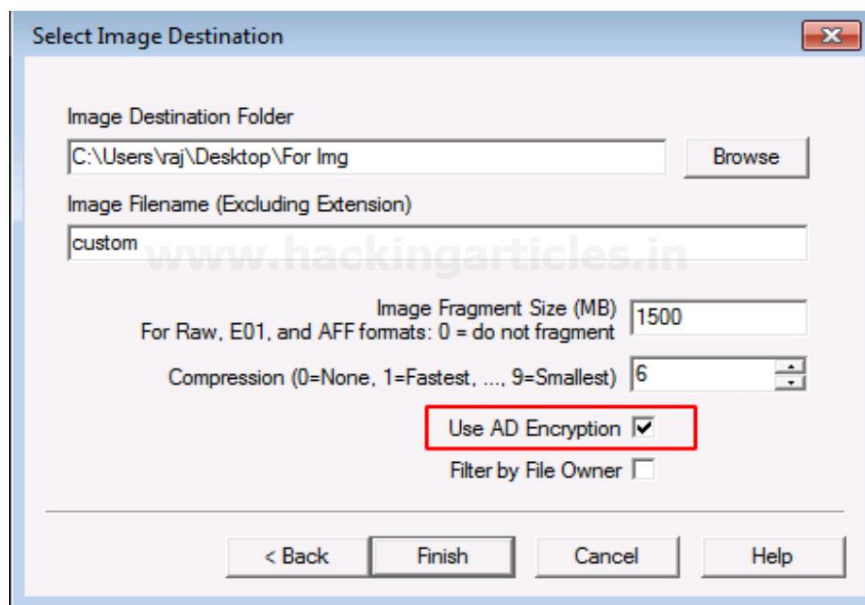


Complete los detalles requeridos para la evidencia que se creará.



A screenshot of a Windows-style dialog box titled "Evidence Item Information". It contains five text input fields: "Case Number:" with the value "1001 Custome Image", "Evidence Number:", "Unique Description:", "Examiner:" with the value "Vishva", and "Notes:". At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help". A watermark "www.hackingarticles.in" is visible across the center of the dialog.

Ahora agregue el destino del archivo de imagen que se va a crear, asigne un nombre al archivo de imagen y luego marque la casilla con cifrado AD, y luego haga clic en Finalizar.

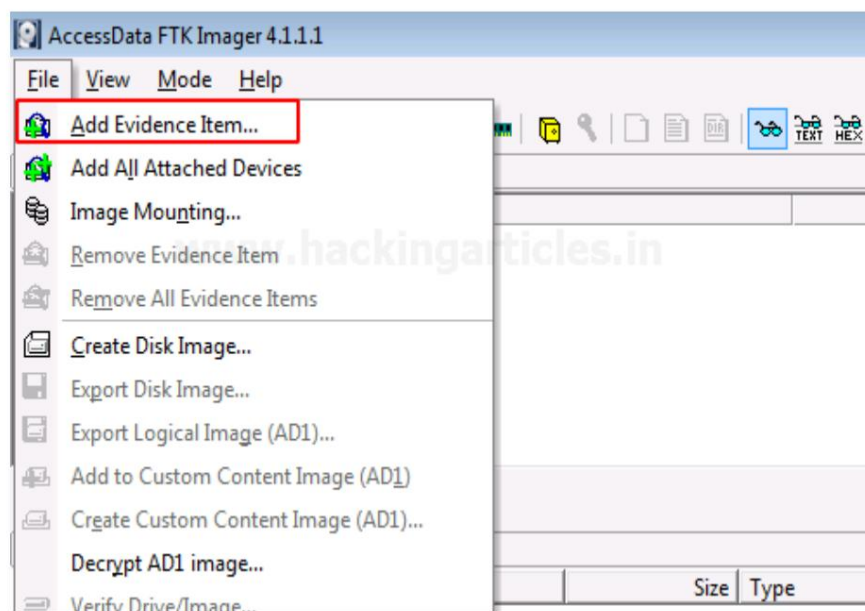


A screenshot of a Windows-style dialog box titled "Select Image Destination". It contains several fields and options: "Image Destination Folder" with the path "C:\Users\raj\Desktop\For Img" and a "Browse" button; "Image Filename (Excluding Extension)" with the value "custom"; "Image Fragment Size (MB)" with the value "1500" and a note "For Raw, E01, and AFF formats: 0 = do not fragment"; "Compression (0=None, 1=Fastest, ..., 9=Smallest)" with the value "6"; a checkbox "Use AD Encryption" which is checked and highlighted with a red rectangle; and a checkbox "Filter by File Owner" which is unchecked. At the bottom, there are four buttons: "< Back", "Finish", "Cancel", and "Help". A watermark "www.hackingarticles.in" is visible across the center of the dialog.

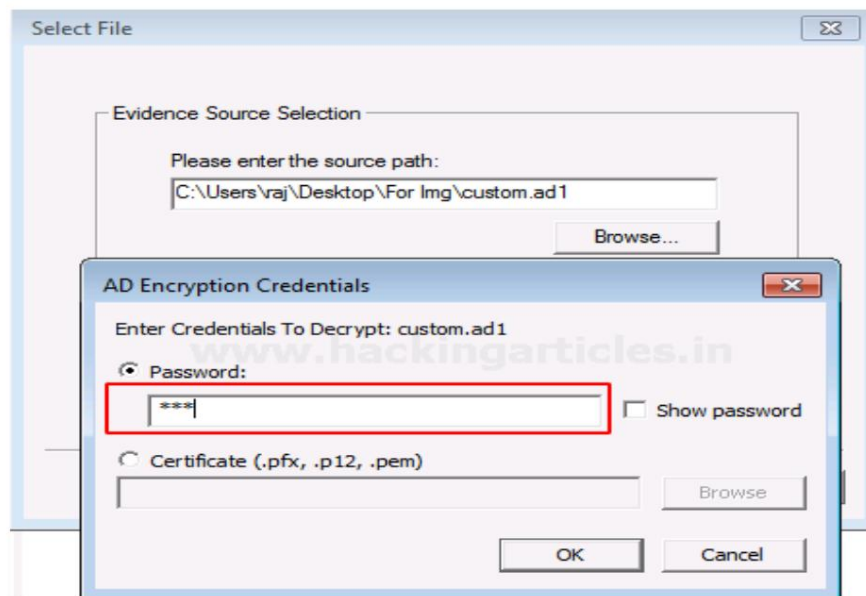
Aparecerá una nueva ventana para cifrar la imagen. Ahora alquila y vuelve a ingresar la contraseña que deseas agregar para tu imagen.



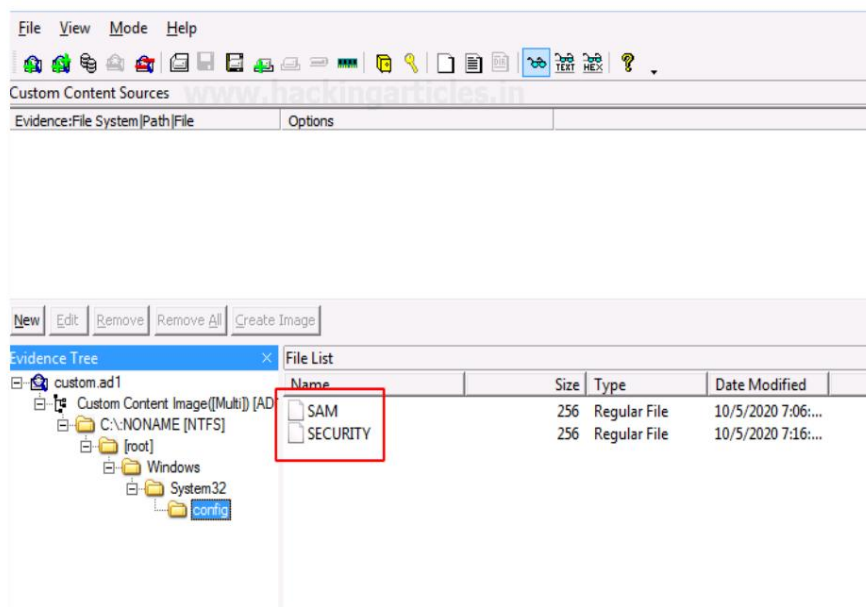
Ahora, para ver los archivos cifrados, haga clic en Archivo> Agregar elemento de evidencia...



La ventana para descifrar los archivos cifrados aparecerá una vez que agregue la fuente del archivo. Ingrese la contraseña y haga clic en Aceptar.

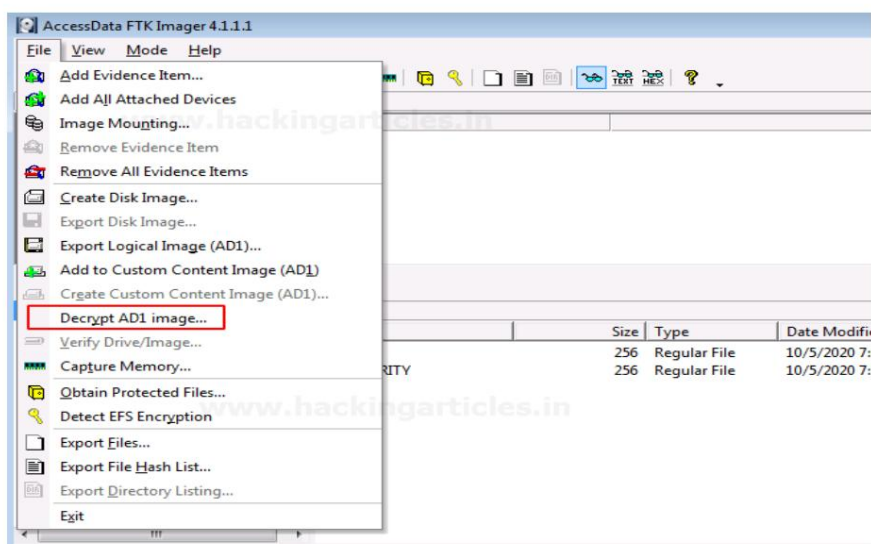


Ahora verá los dos archivos cifrados al ingresar las contraseñas válidas.

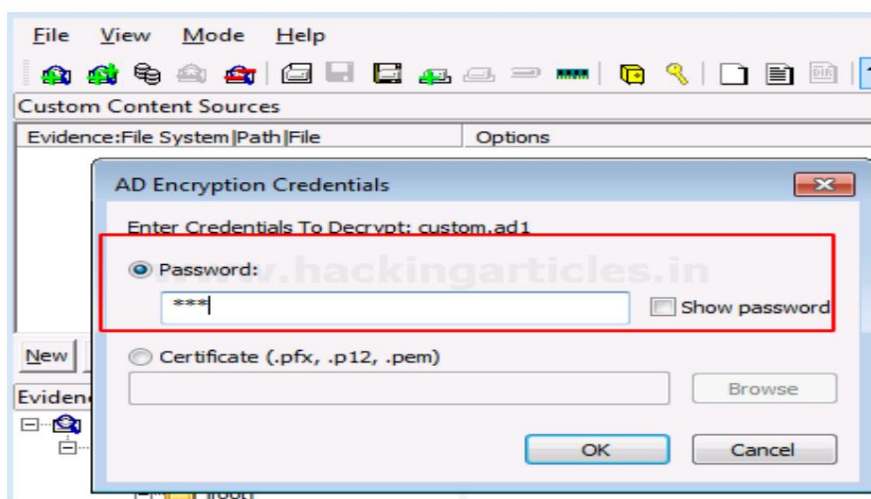


Descifrar imagen AD1

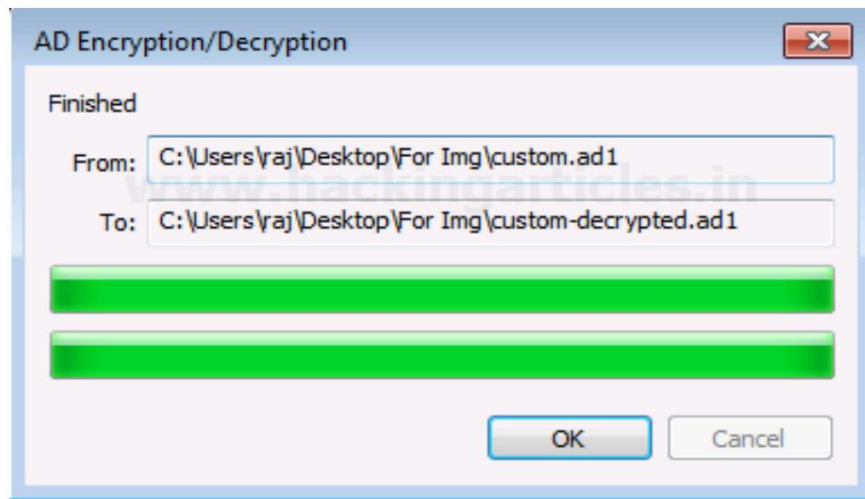
Para descifrar la imagen de contenido personalizado, haga clic en Archivo> Descifrar imagen AD1.



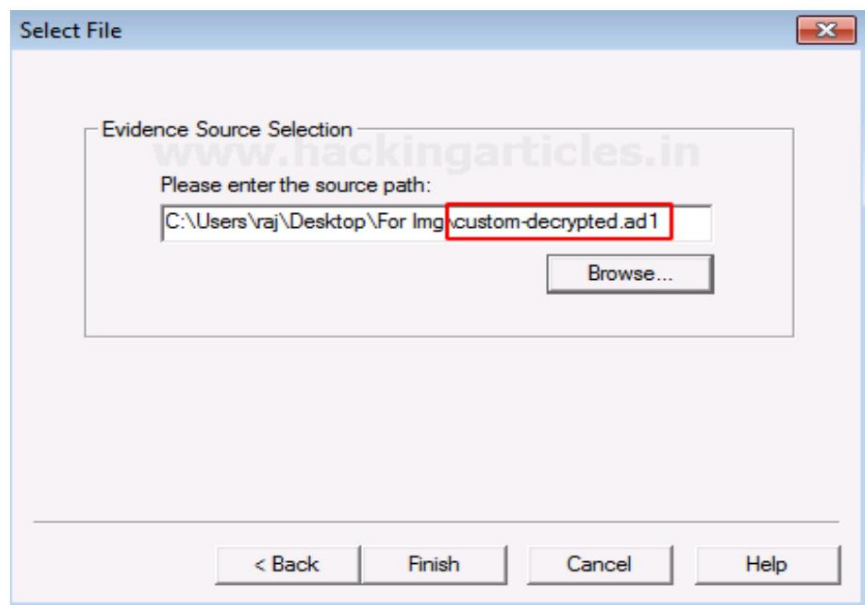
Ahora debe ingresar la contraseña del archivo de imagen que se cifró y hacer clic en Aceptar.



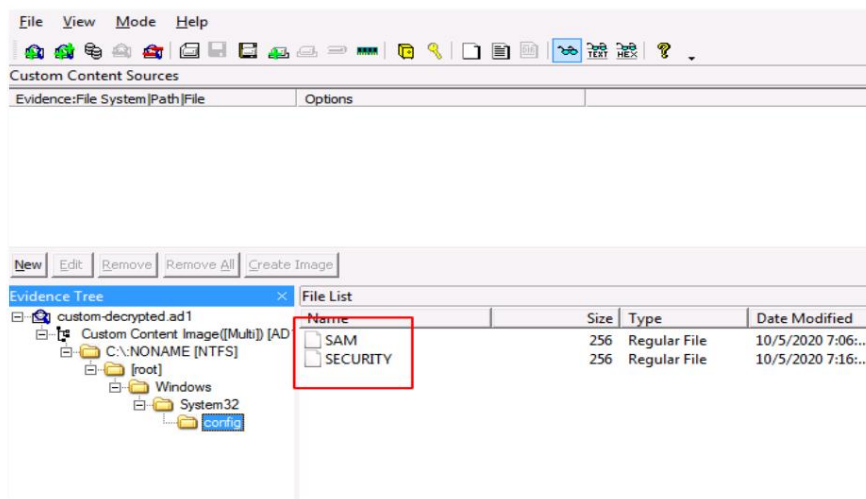
Ahora, espere unos minutos hasta que se cree la imagen descifrada.



Para ver la imagen de contenido personalizado descifrada, agregue la ruta del archivo descifrado y haga clic en Finalizar.

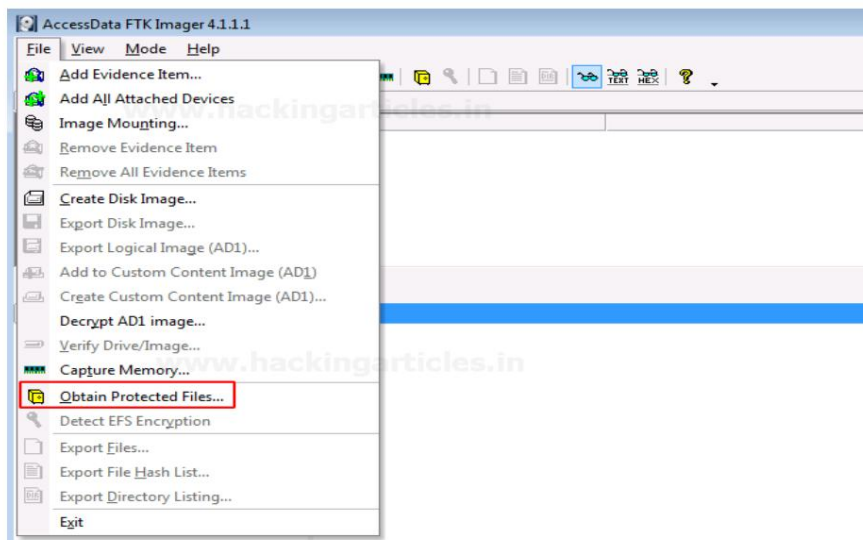


Ahora podrá ver los archivos cifrados utilizando la contraseña correcta para descifrarlos.

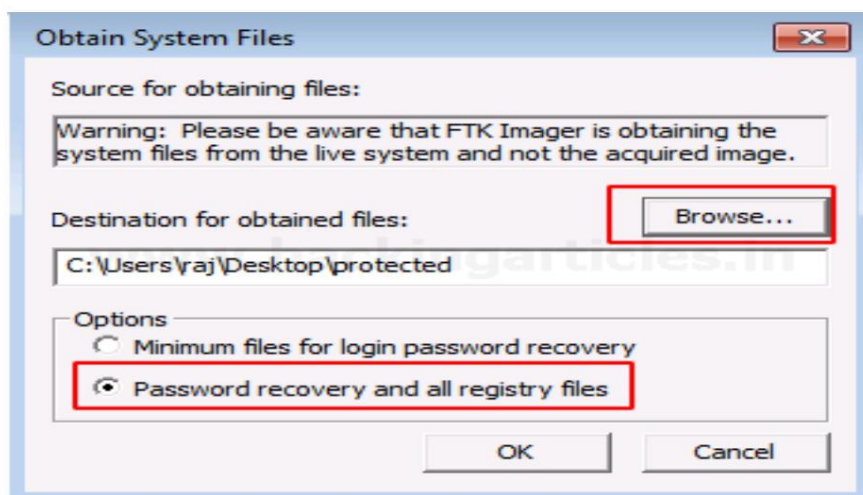


Obtener archivos protegidos

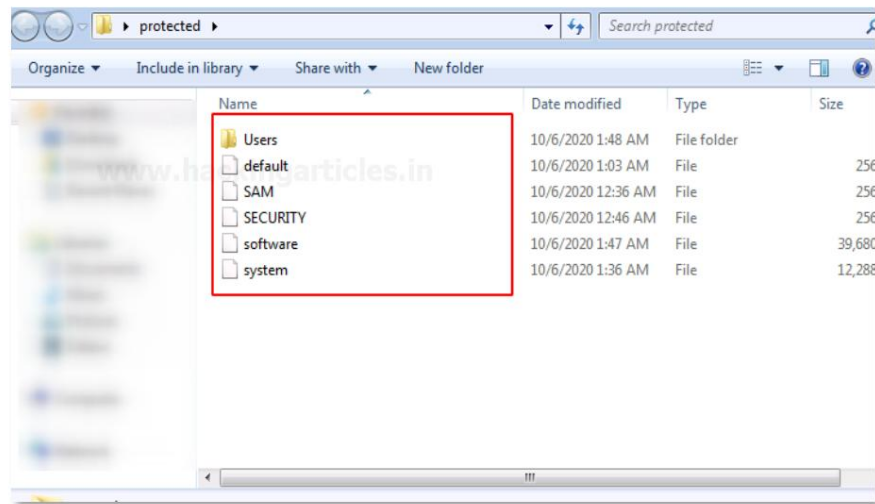
Ciertos archivos están protegidos durante la recuperación. Para obtener esos archivos, haga clic en Archivo> Obtener archivos protegidos.



Aparecerá una nueva ventana y haga clic en Examinar para agregar el destino del archivo que está protegido y haga clic en la opción que dice recuperación de contraseña y todos los archivos de registro y haga clic en Aceptar.

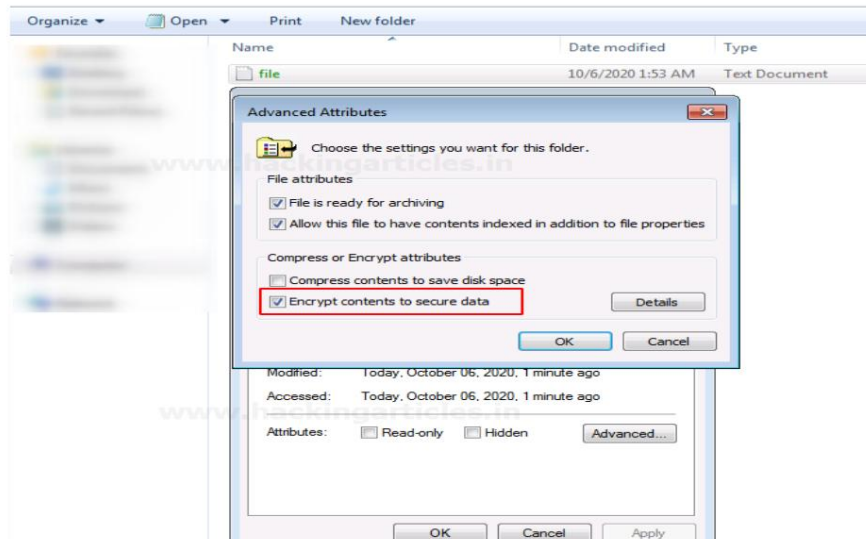


Ahora verás todos los archivos protegidos en un solo lugar

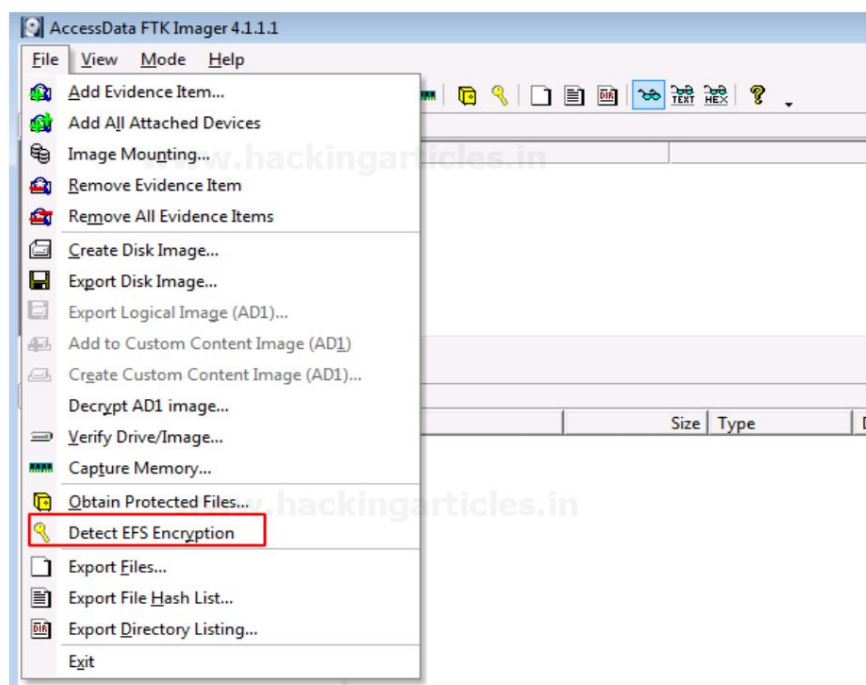


Detectar cifrado EFS

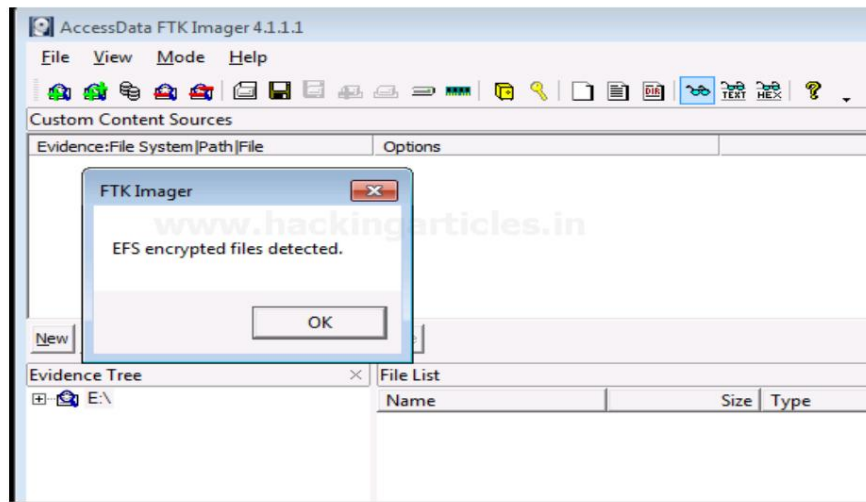
Cuando una carpeta o un archivo está cifrado, podemos detectarlo utilizando esta función de FTK Imager. Un archivo se cifra en una carpeta para proteger su contenido.



Para detectar el cifrado EFS, haga clic en Archivo > Detectar cifrado EFS

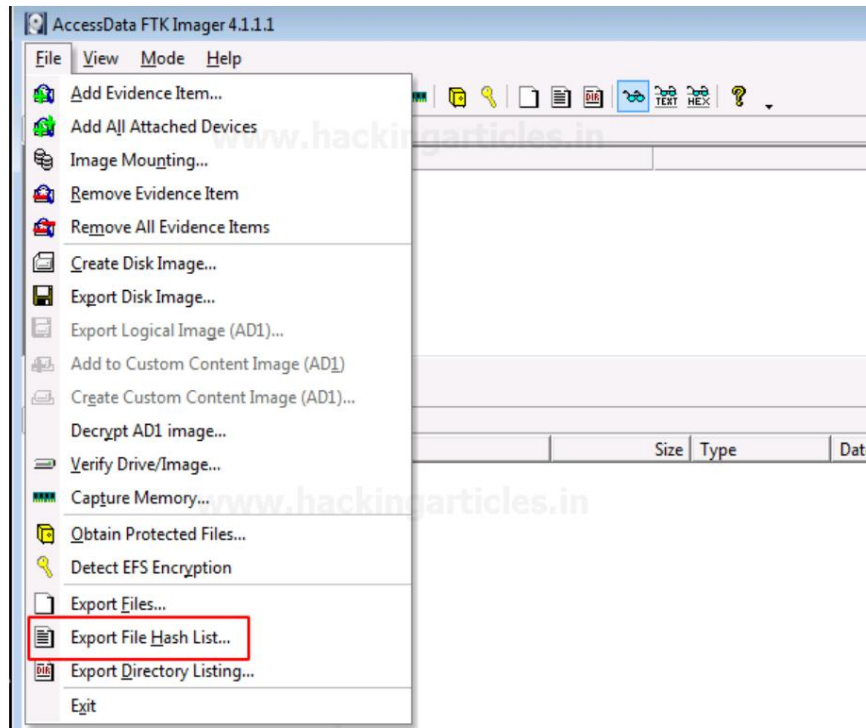


Puede ver que se detecta el cifrado.

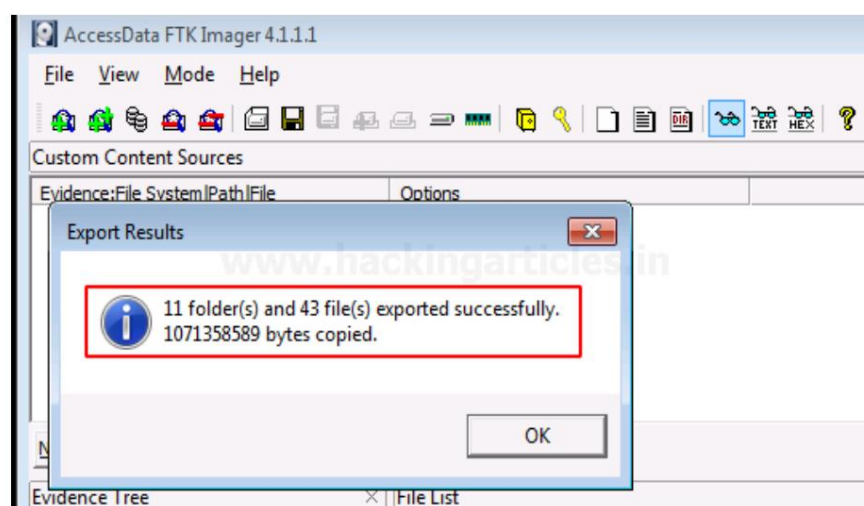


Exportar archivos

Para exportar los archivos y carpetas del archivo de imagen a su carpeta, puede hacer clic en Archivo > Exportar archivos.



Ahora puede ver los resultados de la exportación de la cantidad de archivos y carpetas que se han copiado al sistema.



ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

