# Creación de imágenes forenses

Laboratorio de Delitos Informáticos
Departamento de Justicia de los Estados Unidos
Sección de Delitos Informáticos y Propiedad Intelectual

# Orden de la presentación

- Qué es la creación de imágenes forenses
- El valor de la creación de imágenes forenses
- Bloqueadores de escritura
- Herramientas para crear imágenes
- Creación de imágenes con Bloqueador de Escritura

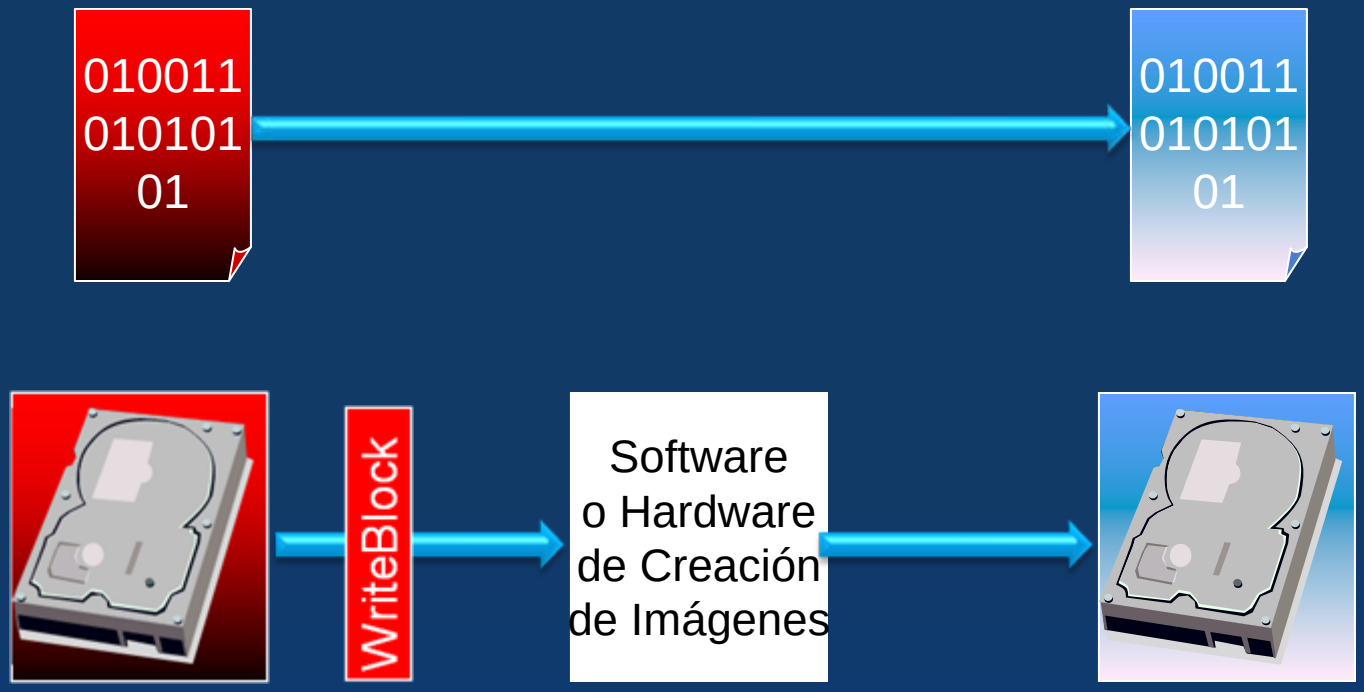
# Orden de la presentación

- Qué es la creación de imágenes forenses
- El valor de la creación de imágenes forenses
- Bloqueadores de escritura
- Herramientas para crear imágenes
- Creación de imágenes con Bloqueador de Escritura

# Qué es la creación de imágenes forenses

- Las imágenes se obtienen mediante un método que no altera, en ninguna manera, dato alguno del disco que está siendo duplicado.
- El duplicado debe contener una copia de cada bit, byte, y sector del disco original.
- El duplicado no contendrá ningún dato distinto a caracteres de relleno (para designar áreas dañadas del medio), además de los datos copiados del disco original.
- Preciso, verificable, reproducible.

# El proceso de creación de imágenes



# Orden de la presentación

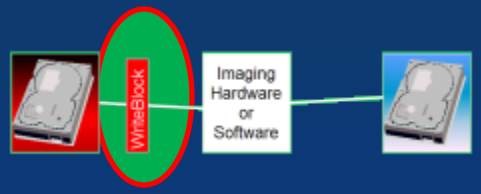
- Qué es la creación de imágenes forenses
- El valor de la creación de imágenes forenses
- Bloqueadores de escritura
- Herramientas para crear imágenes
- Creación de imágenes con Bloqueador de Escritura

# El valor de la creación de imágenes forenses

- La respuesta al incidente / creación de imágenes forenses es el paso MÁS IMPORTANTE en la investigación electrónica.
- El fracaso en este paso puede invalidar o hacer inadmisible toda la demás información recogida a partir de la prueba digital
  - O al menos les puede dar un dolor de cabeza a sus abogados

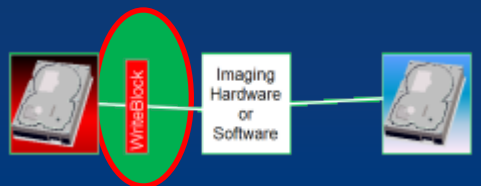
# Orden de la presentación

- Qué es la creación de imágenes forenses
- El valor de la creación de imágenes forenses
- Bloqueadores de escritura
- Herramientas para crear imágenes
- Creación de imágenes con Bloqueador de Escritura



# Bloqueadores físicos de escritura

- ¿Qué son?
  - Dispositivos físicos que impiden la escritura al disco analizado como prueba.
  - Constituyen el MEJOR método de creación de imágenes.




Imágenes de Firefly y Tableau

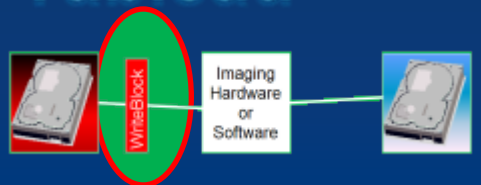
# Bloqueadores de escritura al disco duro



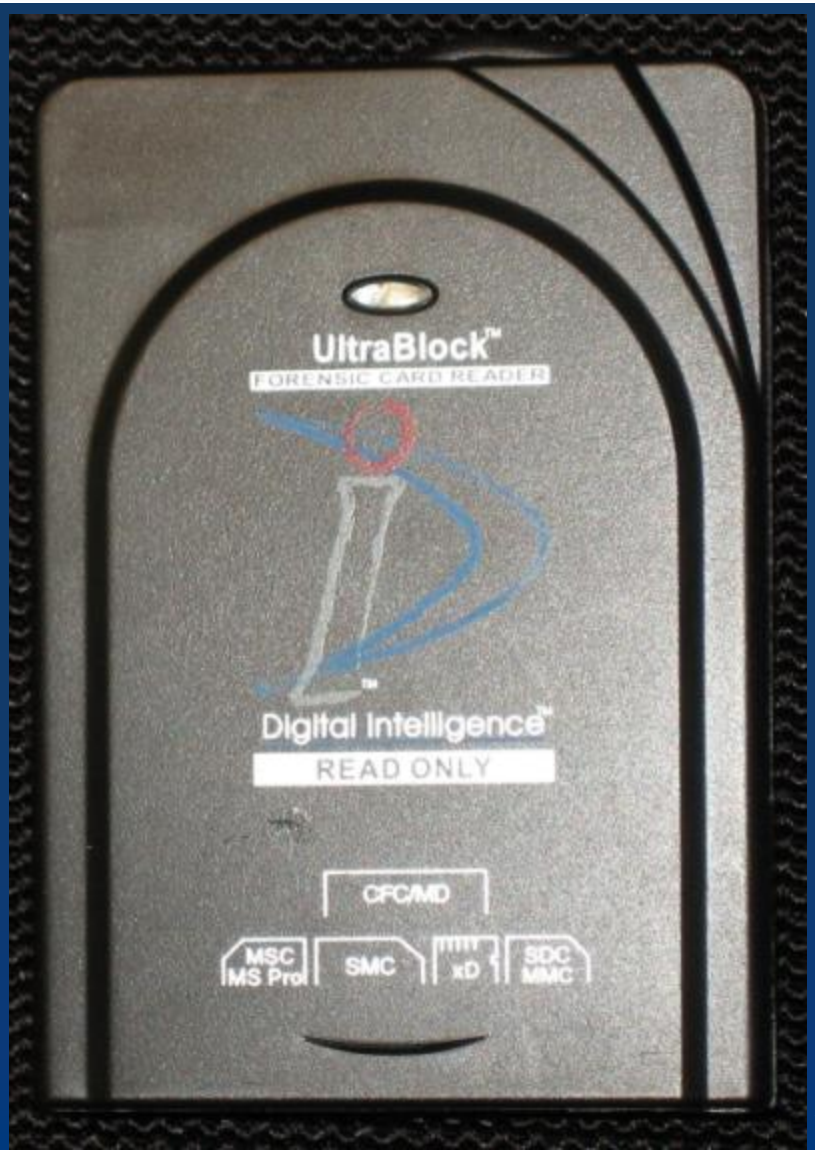
Bloqueador de Escritura Flash

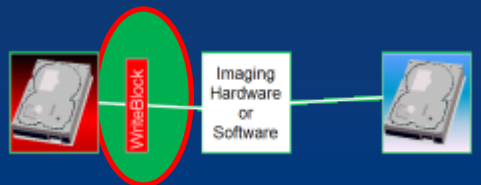
## FireFly – Digital Intelligence

## Tableau



# Otros medios de bloqueo



# Orden de la presentación

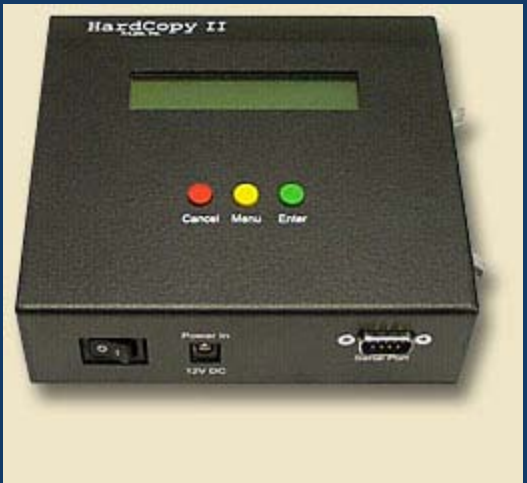
- Qué es la creación de imágenes forenses
- El valor de la creación de imágenes forenses
- Bloqueadores de escritura
- Herramientas para crear imágenes
  - Software
  - Hardware
- Creación de imágenes con Bloqueador de Escritura

# Creación de imágenes de software

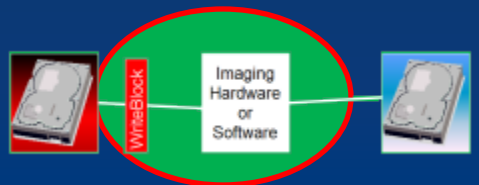
- Precaución con CD’s regrabables o discos floppy
  - Desconecte el cable de datos del disco del sospechoso
  - Reinicie el computador
  - Ingrese al BIO
    - Verifique la orden de iniciar
  - Inserte el disco de inicio
  - Conecte el disco de prueba
  - Reinicie
  - Si funciona, conecte el sospechoso y cree la imagen

# Hardware de creación de imágenes

- Hard Copy 2, fabricado por VoomTech
- LogiCube
- ImageMaster 3

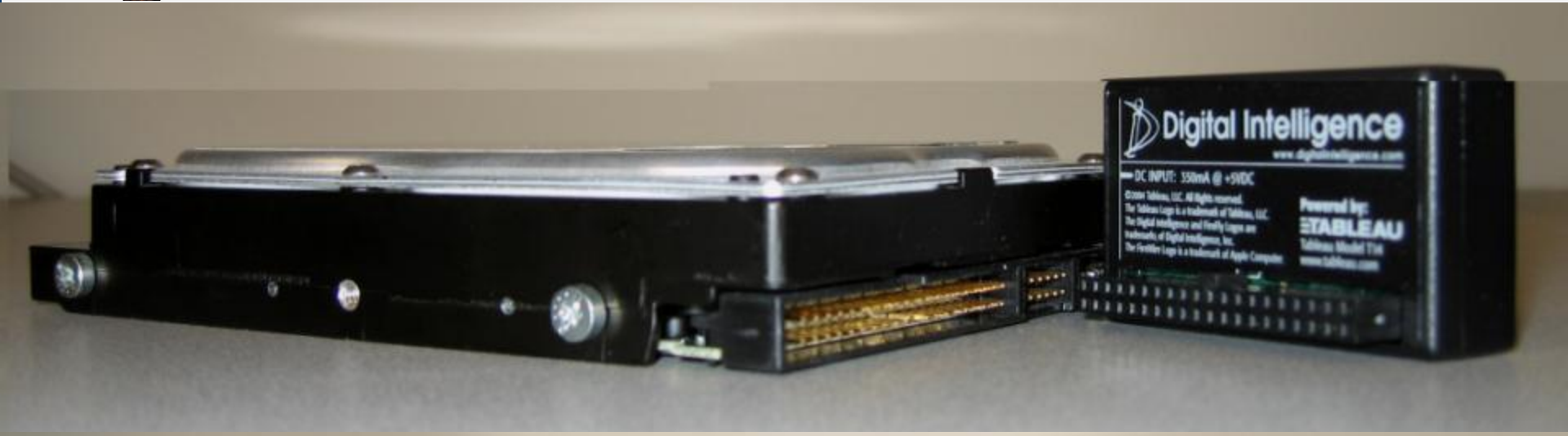





Incorporando un Firefly

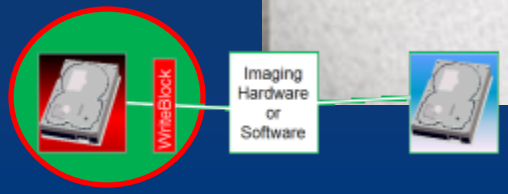
# Incorporando un bloqueador de escritura



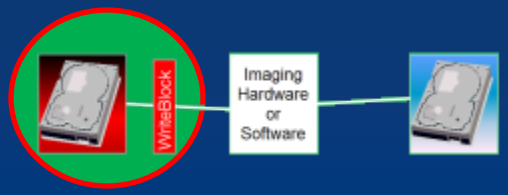


Otra perspectiva

# Incorporando un bloqueador de escritura

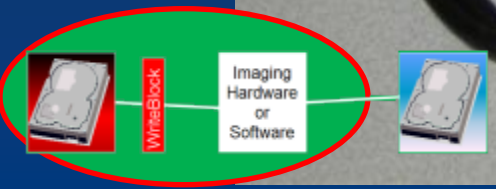



# Incorporando un bloqueador de escritura

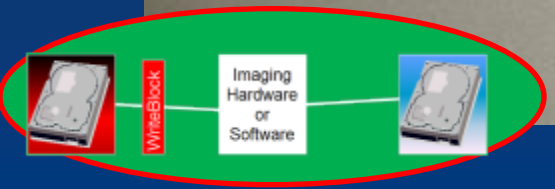

Conectar el dispositivo a la computadora

# Incorporando un bloqueador de escritura




Montaje completo

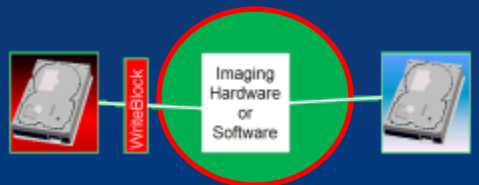
# Incorporando un bloqueador de escritura



# Herramientas de software para creación de imágenes

- Software
  - FTK Imager
  - EnCase
  - DD
  - Ghost
  - Otros


SafeBack 3.0
Evidence Grade Bitstream Backup Utility

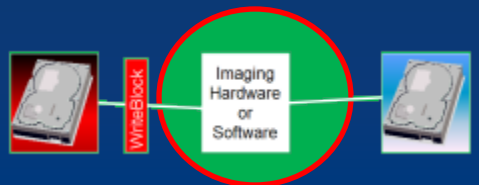
# Estructura Física vs. Lógica

- La estructura física de los datos se refiere a la organización real de los datos en un dispositivo de almacenamiento.

01001111 01110110 01101001 01100101

- La estructura lógica de los datos se refiere a la forma en la que la información se le presenta a un programa o al usuario.

Por ejemplo, un archivo de datos es una colección de información almacenada en un mismo sitio. Esta es su estructura lógica. Sin embargo, físicamente un archivo puede ser grabado dentro de un disco en varias piezas dispersas.




Pantalla inicial de FTK Imager

# Orden de la presentación

- Qué es la creación de imágenes forenses
- El valor de la creación de imágenes forenses
- Bloqueadores de escritura
- Herramientas para crear imágenes
- Creación de imágenes con Bloqueador de Escritura

# Creando imágenes con FTK Imager

FTK Imager

File View Mode Help

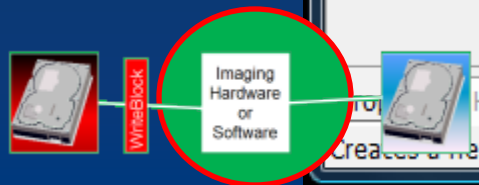
Add Evidence Item...
Remove Evidence Item
Create Disk Image...
Export Disk Image...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Verify Drive/Image...
Obtain Protected Files...
Export Files...
Export File Hash List...
Export Directory Listing...
Exit

Creates a new disk image

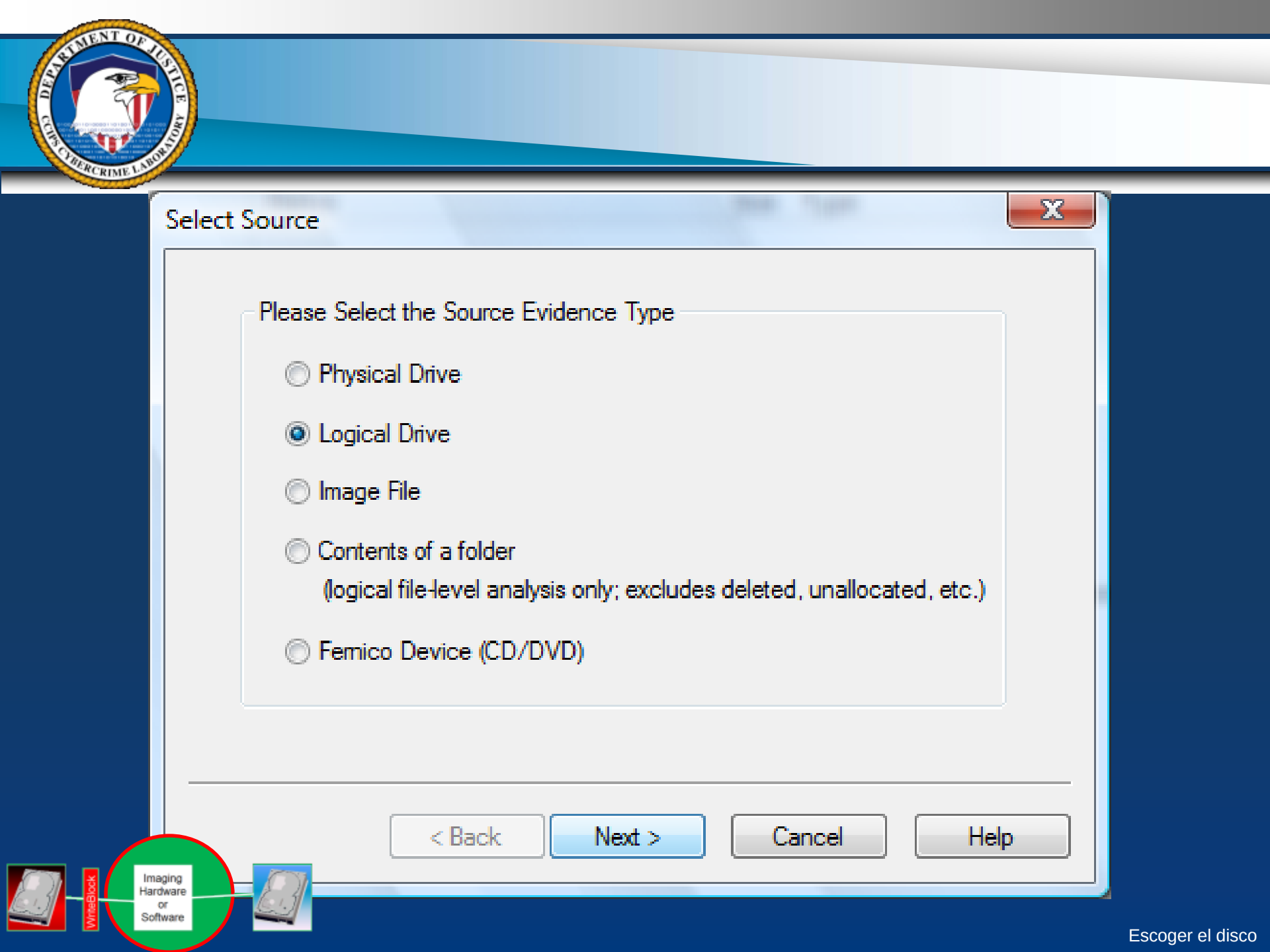
Name | Size | Type | Date

Hex Value Interpreter

Creates a new disk image

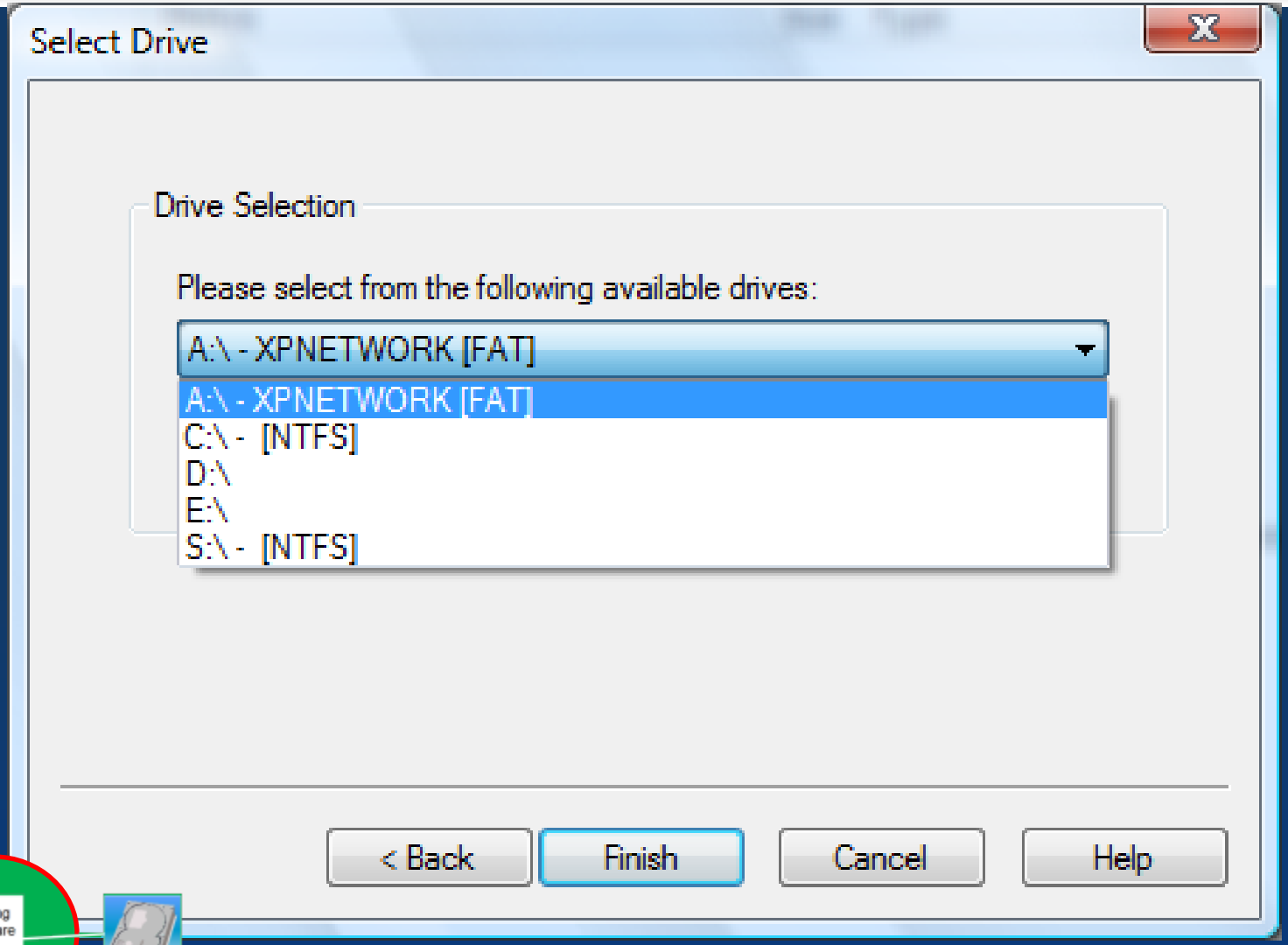


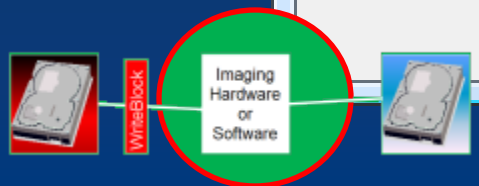

Escoger el disco físico



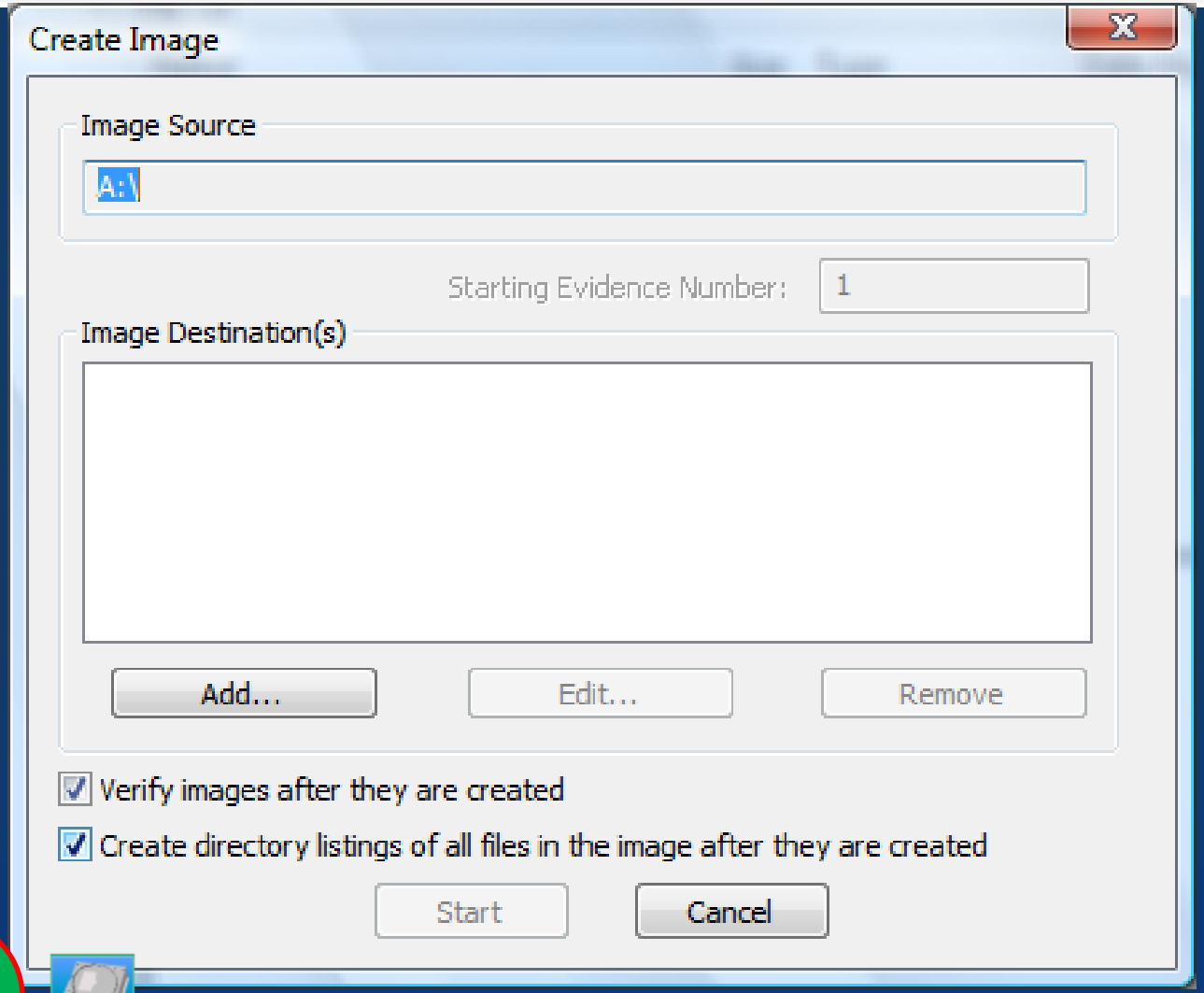

Escoger el disco

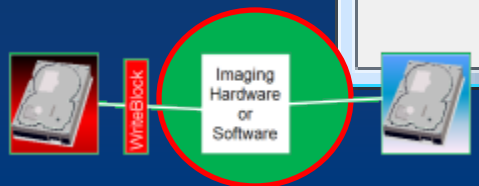
# Escoger el disco para crear la imagen

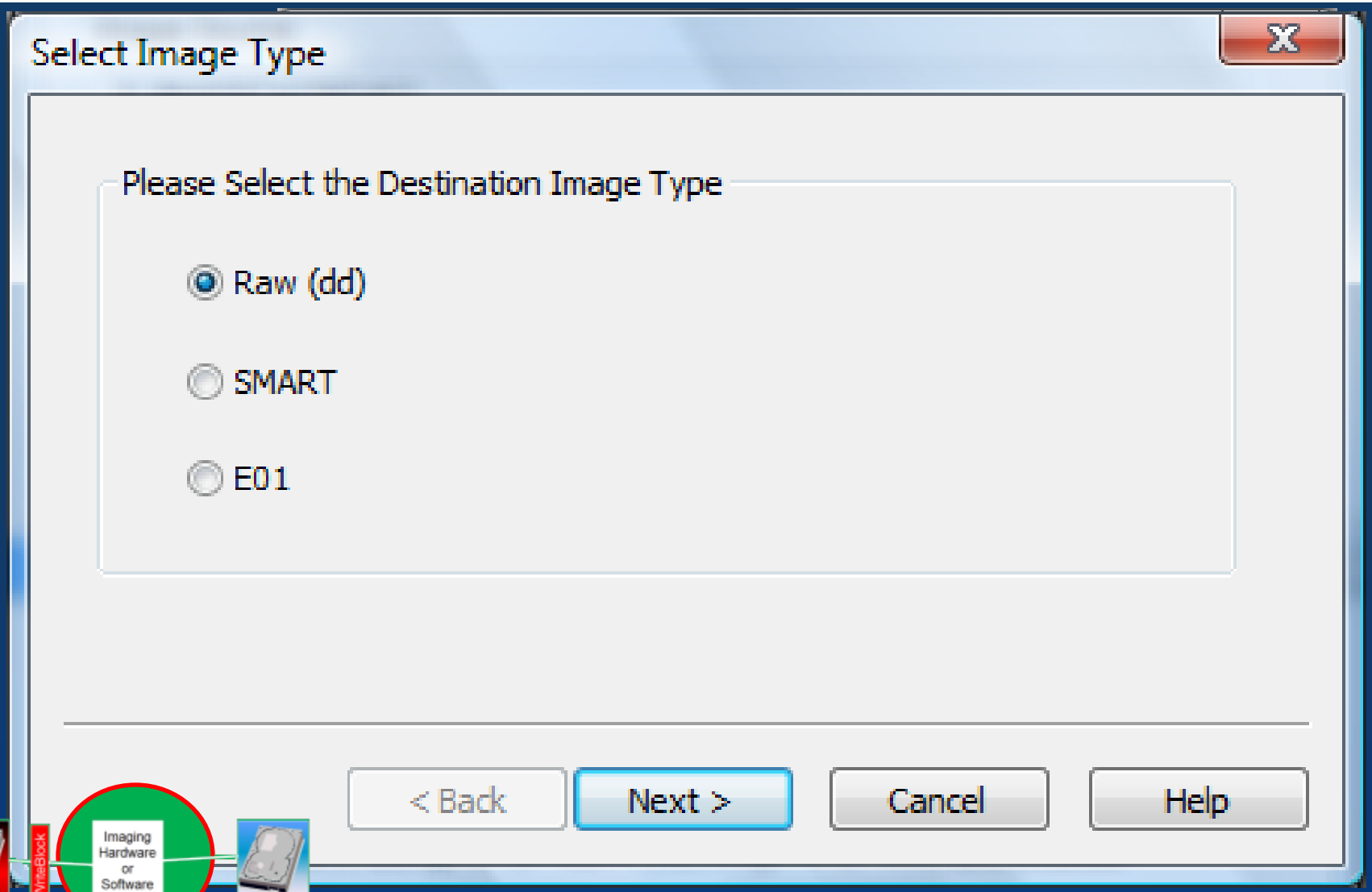


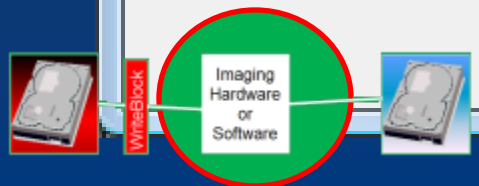




Una manera de identificar los discos


Create Image
Image Source
A:\
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Verify images after they are created
Create directory listings of all files in the image after they are created
Start
Cancel


WriteBlock
Imaging
Hardware
or
Software




Rellenar la información sobre el caso

## Select Image Destination

Image destination folder

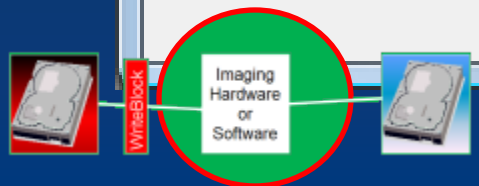
Browse

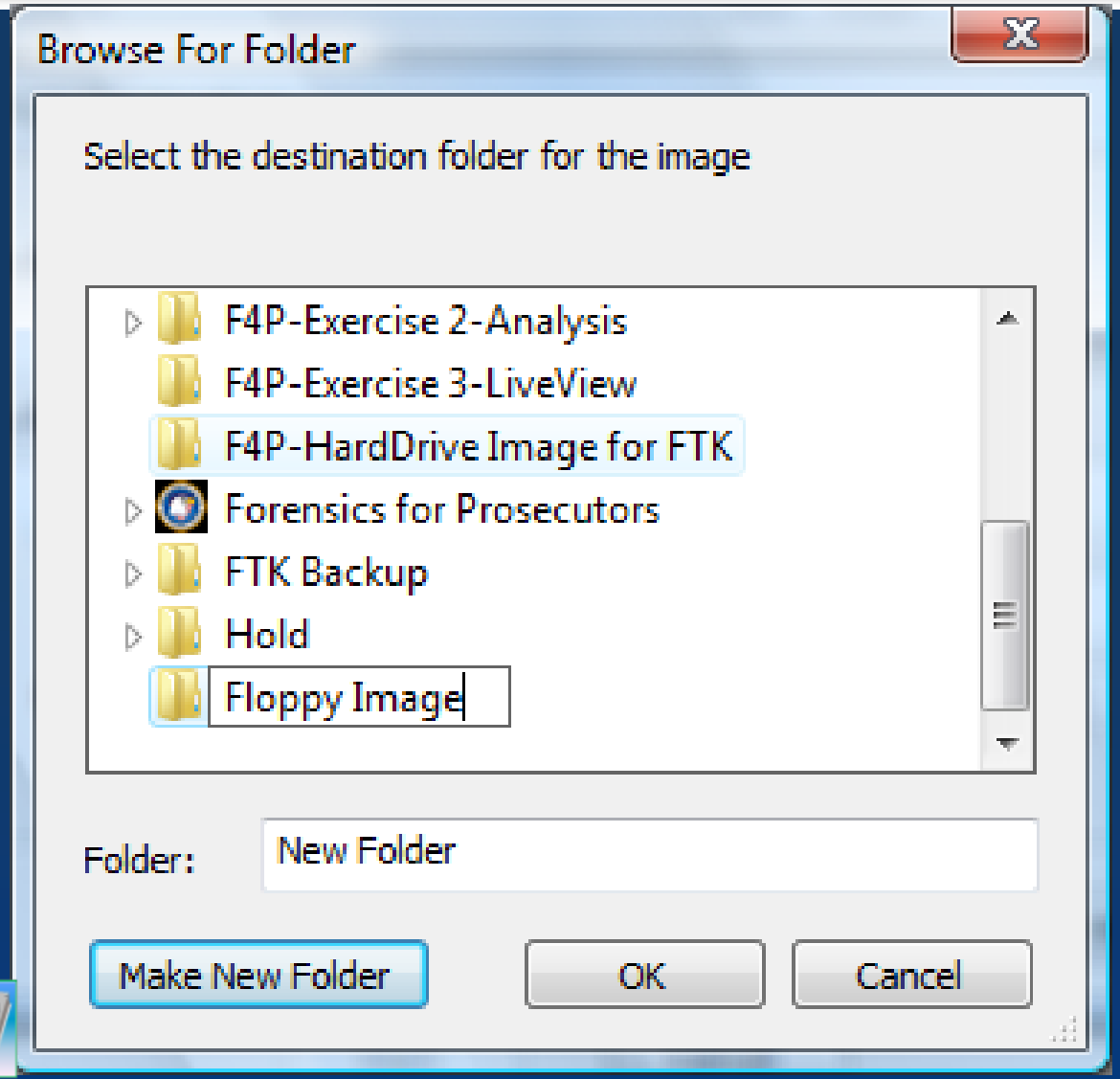
Image filename (excluding extension)

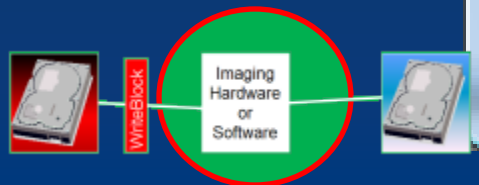
Image fragment size (MB) 650

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

< Back | Finish | Cancel | Help




Browse For Folder
Select the destination folder for the image
F4P-Exercise 2-Analysis
F4P-Exercise 3-LiveView
F4P-HardDrive Image for FTK
Forensics for Prosecutors
FTK Backup
Hold
Floppy Image
Folder:
New Folder
Make New Folder
OK
Cancel


WriteBlock
Imaging
Hardware
or
Software

## Select Image Destination

Image destination folder

C:\Users\CCIPS\Desktop\Floppy Image

Browse

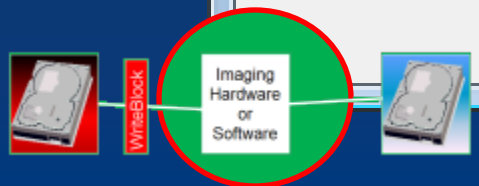
Image filename (excluding extension)

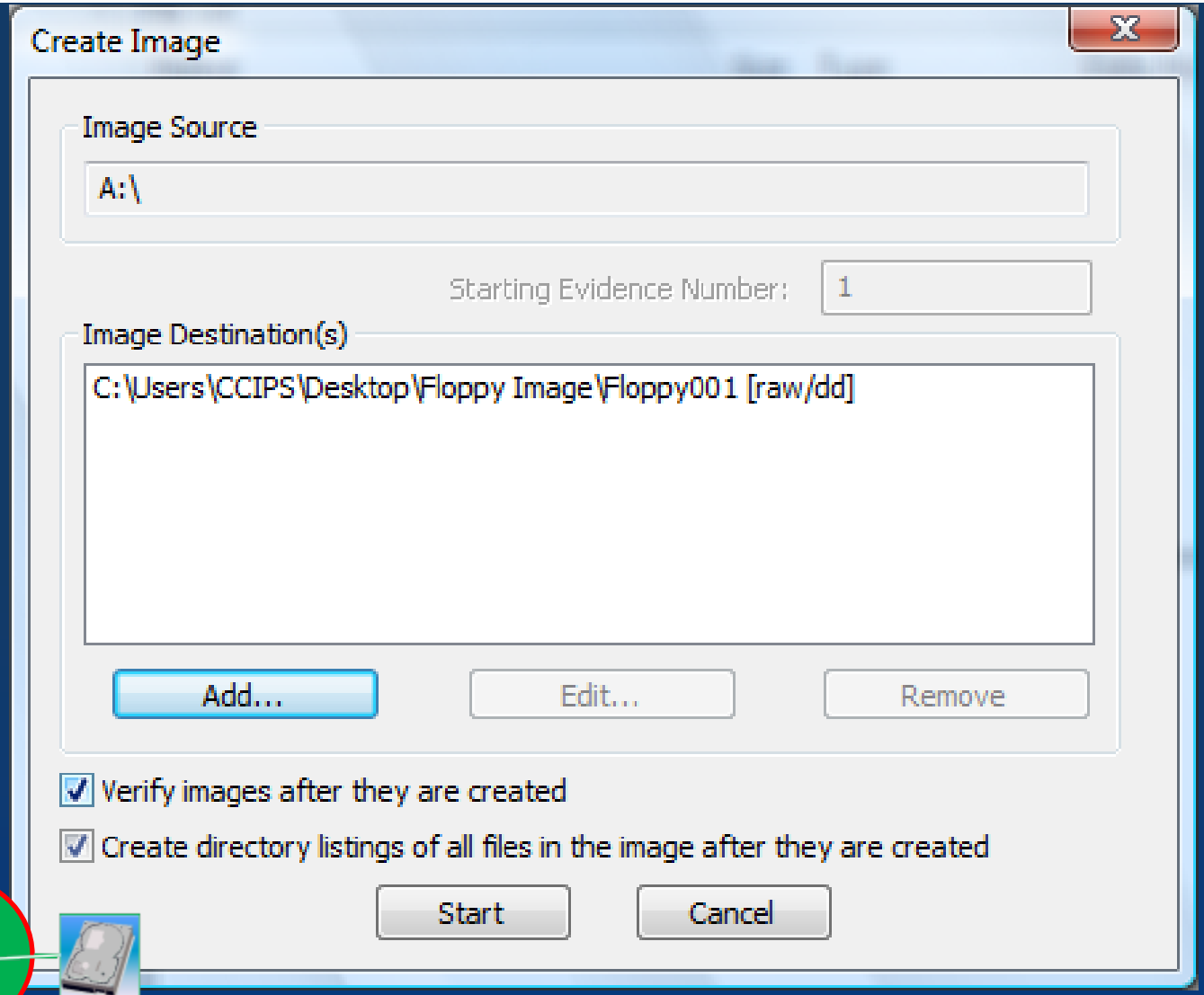
Floppy001

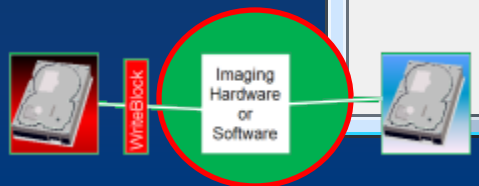
Image fragment size (MB) 650

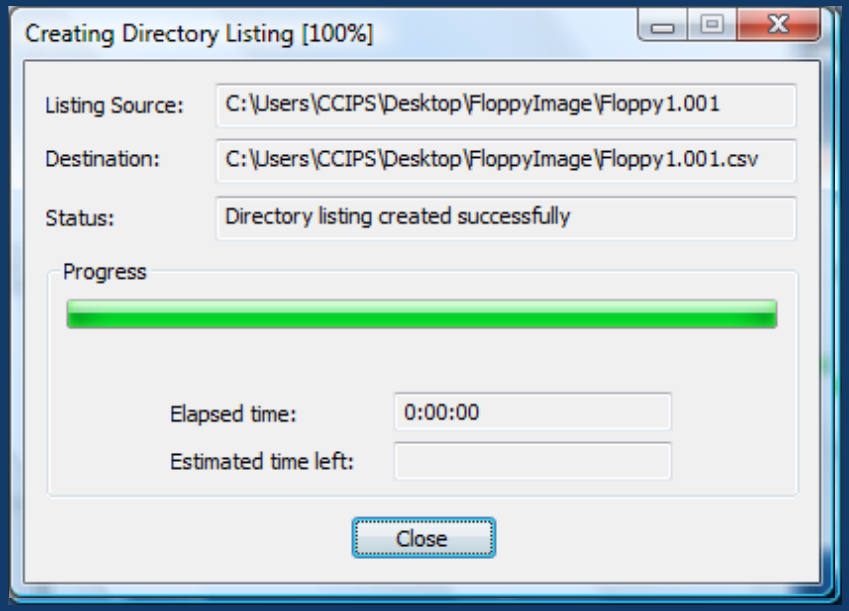
Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

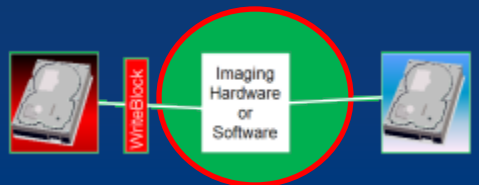
< Back | Finish | Cancel | Help




Create Image
Image Source
A:\
Starting Evidence Number:
1
Image Destination(s)
C:\Users\CCIPS\Desktop\Floppy Image\Floppy001 [raw/dd]
Add...
Edit...
Remove
Verify images after they are created
Create directory listings of all files in the image after they are created
Start
Cancel


WriteBlock
Imaging
Hardware
or
Software



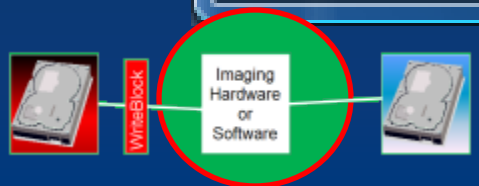




Da un valor hash

Drive/Image Verify Results

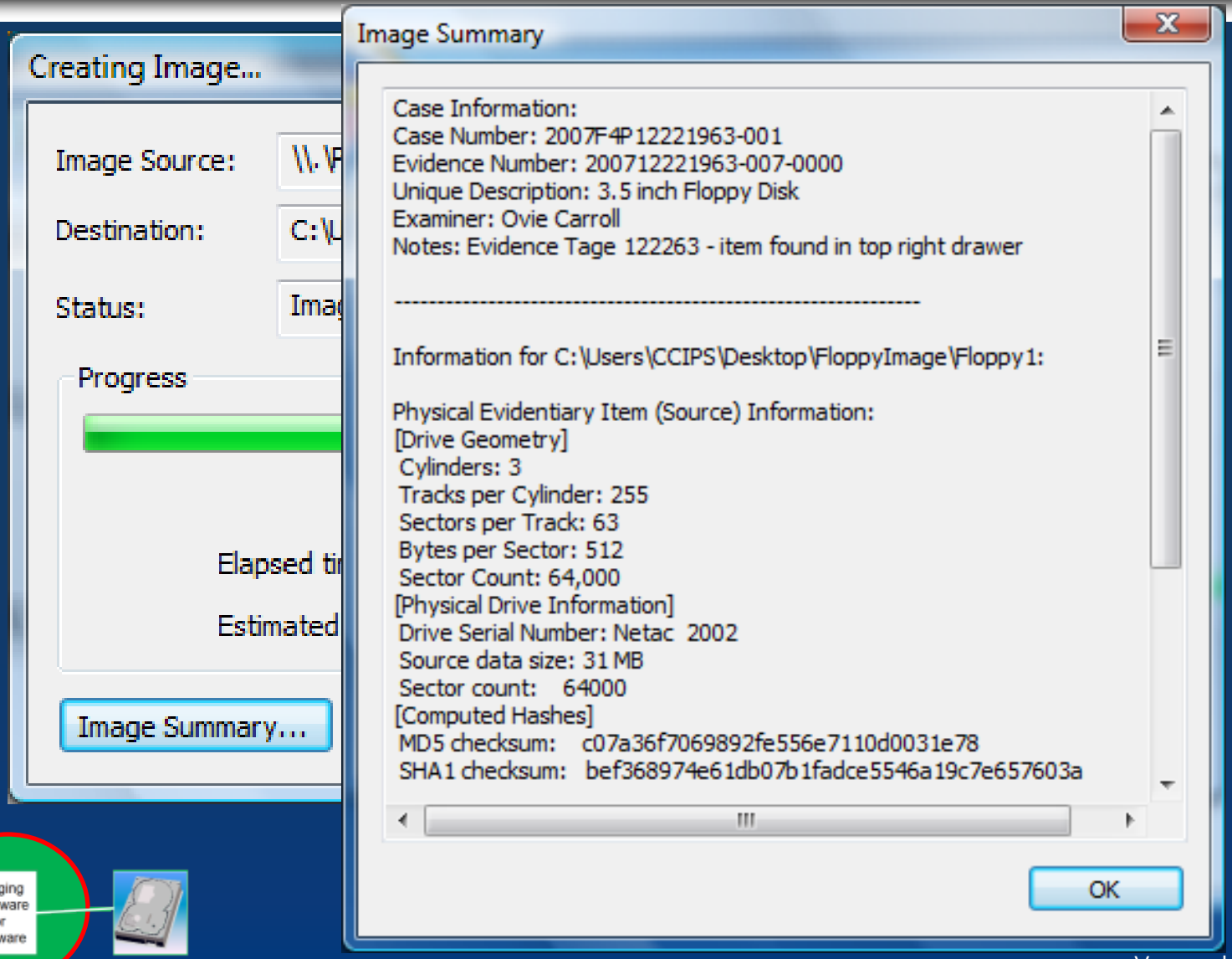
| | |
|---|---|
| **General** | |
| Name | Floppy1.001 |
| Sector count | 64000 |
| **MD5 Hash** | |
| Computed hash | c07a36f7069892fe556e7110d0031e78 |
| Report Hash | c07a36f7069892fe556e7110d0031e78 |
| Verify result | Match |
| **SHA1 Hash** | |

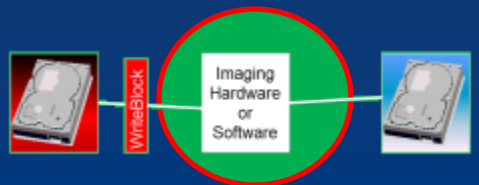
Close




Hacer click en Image Summary

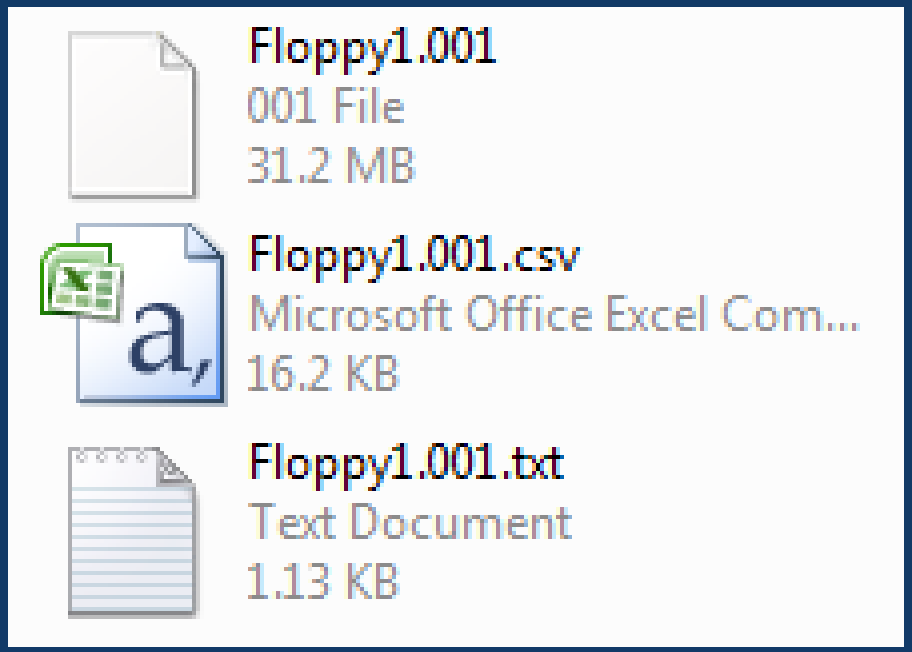
# Resumen de la imagen




Veamos los resultados

- Floppy1.001
  - Imagen DD
- CSV
  - Excel con listado de archivos
- TXT



| | A | B | C | D | E | F | |
|---|---|---|---|---|---|---|---|
| 1 | Filename | Full Path | Size | Created | Modified | Accessed | Is D |
| 2 | [root] | 32 MEG [FAT16]\[root]\ | 16384 | | | | no |
| 3 | unallocated space | 32 MEG [FAT16]\unallocated space\ | 0 | | | | no |
| 4 | Dobsons Email forward mechanism new.ppt | 32 MEG [FAT16]\[root]\Dobsons Email forward mechanism ne | 146944 | 2006-Oct-27 09:10:06.680000 | 2006-Oct-26 18:50:40 | 2006-Oct-27 00:00:00 | yes |
| 5 | Ads for October 29, 2006.ppt | 32 MEG [FAT16]\[root]\Ads for October 29, 2006.ppt | 0 | 2006-Oct-29 07:43:29.910000 | 2006-Oct-29 07:43:30 | 2006-Oct-29 00:00:00 | yes |
| 6 | Ads for October 29, 2006.ppt | 32 MEG [FAT16]\[root]\Ads for October 29, 2006.ppt | 6308352 | 2006-Oct-29 07:42:00 | 2006-Oct-29 07:42:00 | 2006-Nov-16 00:00:00 | yes |
| 7 | October 29, 2006.ppt | 32 MEG [FAT16]\[root]\October 29, 2006.ppt | 0 | 2006-Oct-29 07:43:49.120000 | 2006-Oct-29 07:43:50 | 2006-Oct-29 00:00:00 | yes |
| 8 | October 29, 2006.ppt | 32 MEG [FAT16]\[root]\October 29, 2006.ppt | 425984 | 2006-Oct-29 07:42:00 | 2006-Oct-29 07:42:00 | 2006-Oct-29 00:00:00 | yes |
| 9 | October 29, 2006 Evening.ppt | 32 MEG [FAT16]\[root]\October 29, 2006 Evening.ppt | 0 | 2006-Oct-29 07:43:55.260000 | 2006-Oct-29 07:43:56 | 2006-Oct-29 00:00:00 | yes |
| 10 | October 29, 2006 Evening.ppt | 32 MEG [FAT16]\[root]\October 29, 2006 Evening.ppt | 489984 | 2006-Oct-29 07:42:00 | 2006-Oct-29 07:42:00 | 2006-Nov-16 00:00:00 | yes |
| 11 | !pt4.tmp | 32 MEG [FAT16]\[root]\!pt4.tmp | 0 | 2006-Nov-16 10:34:14.980000 | 2006-Nov-16 10:34:16 | 2006-Nov-16 00:00:00 | yes |
| 12 | !pt4.tmp | 32 MEG [FAT16]\[root]\!pt4.tmp | 94208 | 2006-Oct-29 07:42:00 | 2006-Nov-16 10:34:18 | 2006-Nov-16 00:00:00 | yes |
| 13 | October 29, 2006 Evening.ppt~RF8e3c5a.TMP | 32 MEG [FAT16]\[root]\October 29, 2006 Evening.ppt~RF8e3c5 | 0 | 2006-Nov-16 10:34:17.820000 | 2006-Nov-16 10:34:18 | 2006-Nov-16 00:00:00 | yes |
| 14 | October 29, 2006 Evening.ppt~RF8e3c5a.TMP | 32 MEG [FAT16]\[root]\October 29, 2006 Evening.ppt~RF8e3c5 | 489984 | 2006-Oct-29 07:42:00 | 2006-Oct-29 07:42:00 | 2006-Nov-16 00:00:00 | yes |
| 15 | October 29, 2006 Evening.ppt | 32 MEG [FAT16]\[root]\October 29, 2006 Evening.ppt | 94208 | 2006-Oct-29 07:42:00 | 2006-Nov-16 10:34:18 | 2006-Nov-16 00:00:00 | yes |
| 16 | My Secret Presentation.ppt | 32 MEG [FAT16]\[root]\My Secret Presentation.ppt | 0 | 2006-Nov-16 10:36:40.420000 | 2006-Nov-16 10:36:42 | 2006-Nov-16 00:00:00 | yes |
| 17 | My Secret Presentation.ppt | 32 MEG [FAT16]\[root]\My Secret Presentation.ppt | 294912 | 2006-Nov-16 10:36:40.420000 | 2006-Nov-16 10:36:46 | 2006-Nov-16 00:00:00 | yes |
| 18 | My SecreT.ppt | 32 MEG [FAT16]\[root]\My SecreT.ppt | 294912 | 2006-Nov-16 10:36:40.420000 | 2006-Nov-16 10:36:46 | 2006-Nov-16 00:00:00 | yes |
| 19 | sPECIAL TEST.txt | 32 MEG [FAT16]\[root]\sPECIAL TEST.txt | 0 | 2006-Nov-16 11:18:28.400000 | 2006-Nov-16 11:18:30 | 2006-Nov-16 00:00:00 | yes |
| 20 | sPECIAL TEST.txt | 32 MEG [FAT16]\[root]\sPECIAL TEST.txt | 13 | 2006-Nov-16 11:18:28.400000 | 2006-Nov-16 11:18:30 | 2006-Nov-16 00:00:00 | yes |
| 21 | ZoomIt.exe | 32 MEG [FAT16]\[root]\ZoomIt.exe | 77824 | 2006-Nov-16 11:34:39.210000 | 2006-Jul-10 12:02:26 | 2006-Nov-24 00:00:00 | yes |
| 22 | cximage.dll | 32 MEG [FAT16]\[root]\cximage.dll | 946176 | 2006-Nov-24 13:38:54.160000 | 2004-Mar-15 10:05:00 | 2007-Feb-05 00:00:00 | no |
| 23 | FTK Imager.exe | 32 MEG [FAT16]\[root]\FTK Imager.exe | 3600384 | 2006-Nov-24 13:38:56.080000 | 2006-Jul-27 11:54:00 | 2007-Mar-14 00:00:00 | no |
| 24 | IsoBuster.dll | 32 MEG [FAT16]\[root]\IsoBuster.dll | 1466368 | 2006-Nov-24 13:39:03 | 2005-Feb-02 18:05:00 | 2007-Mar-11 00:00:00 | no |

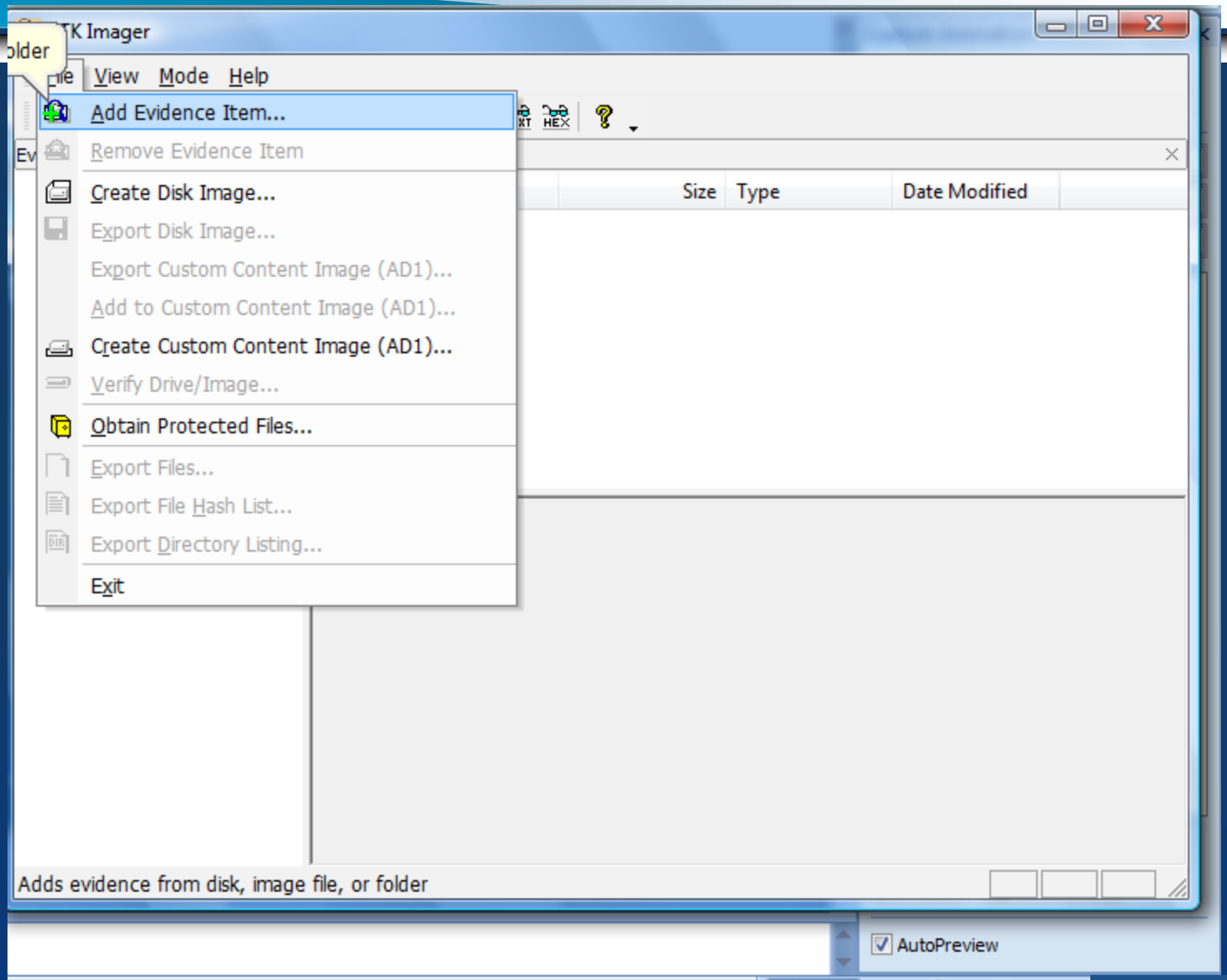
Floppy1.001

Ready

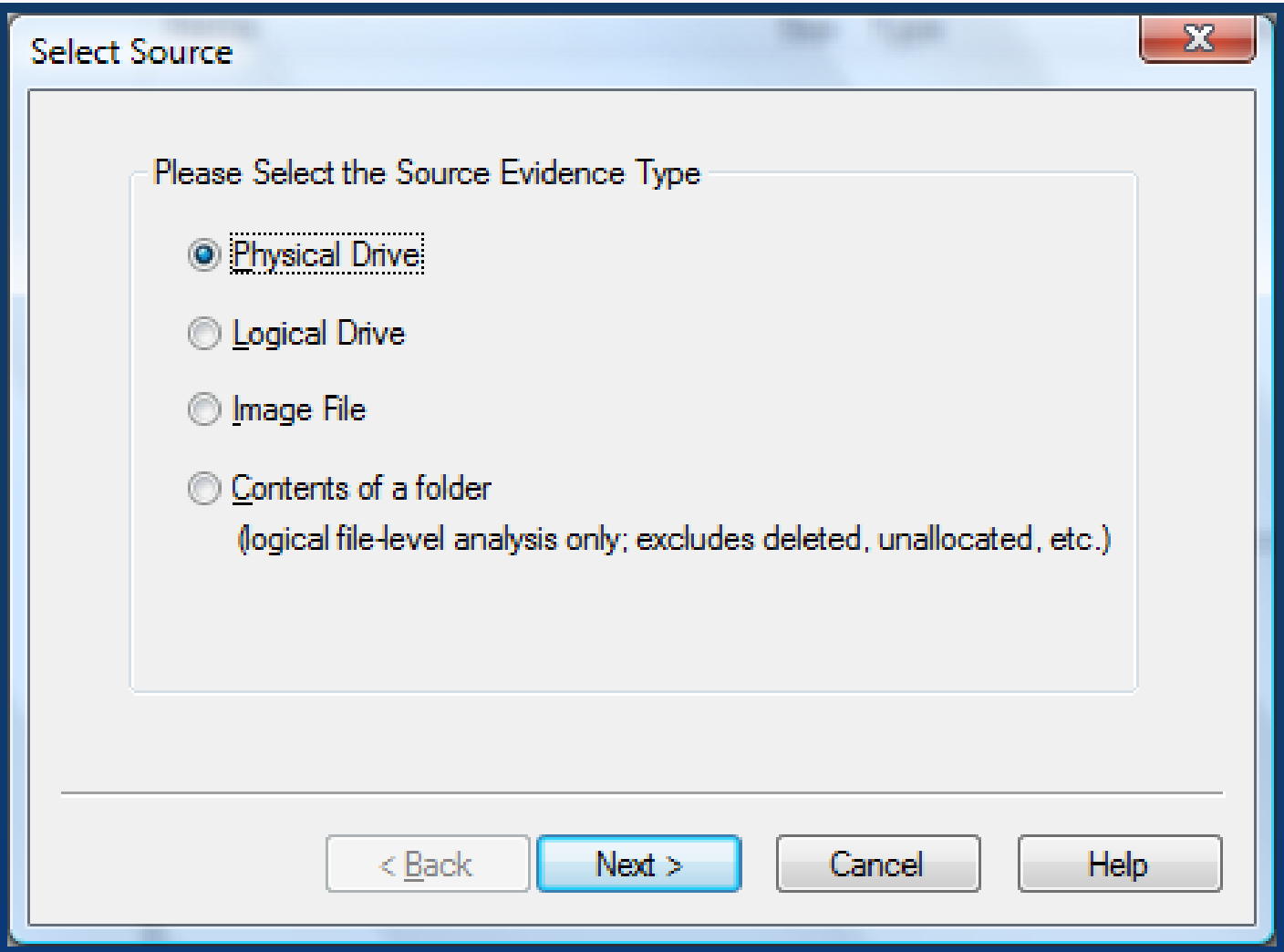
También puede ser usado como un programa de recuperación de baja intensidad

# Instalar FTK Image

- FTK Imager también puede ser usado como un programa de recuperación de baja intensidad.

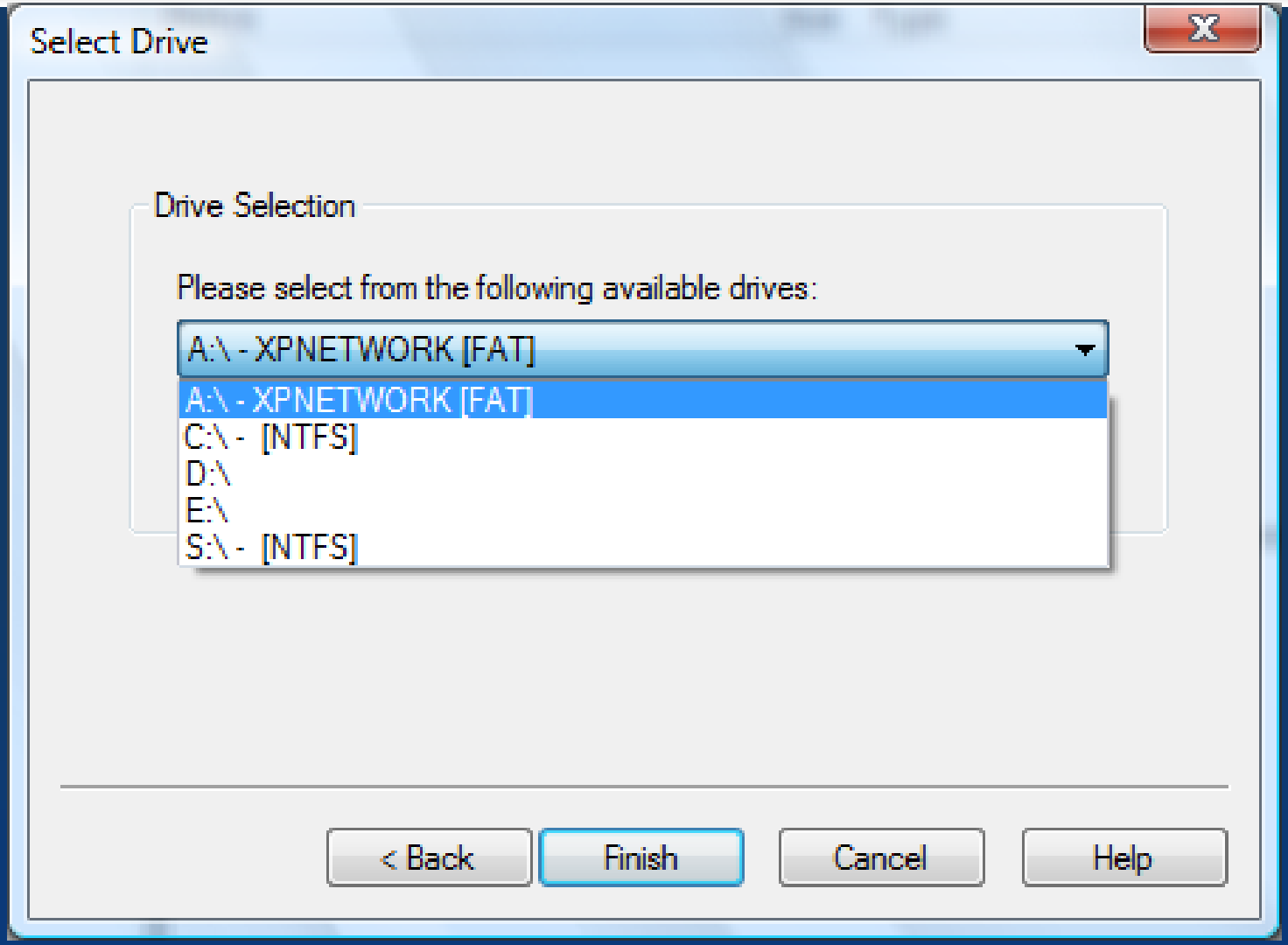



El disco físico de nuevo

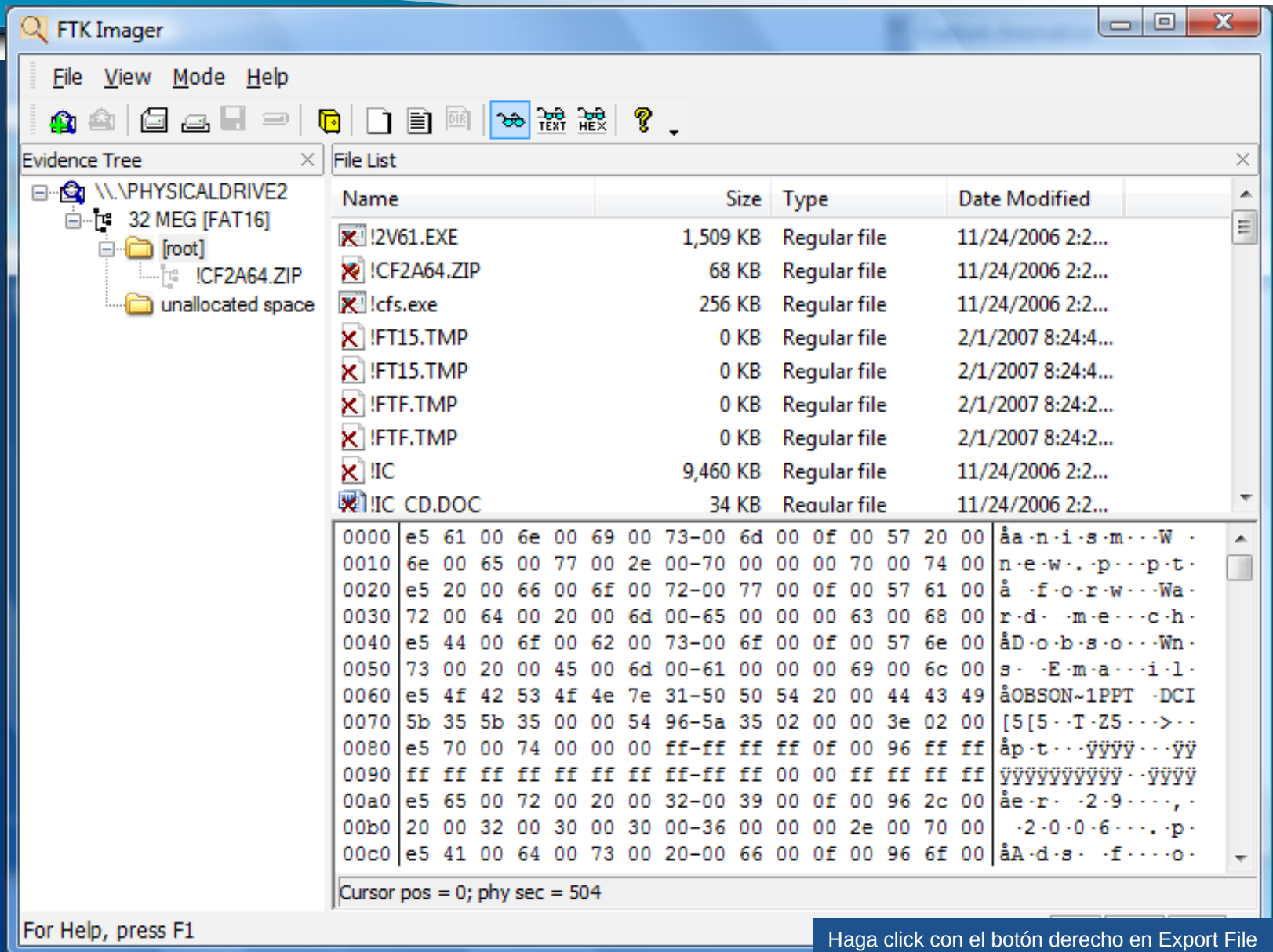



Escoger el disco

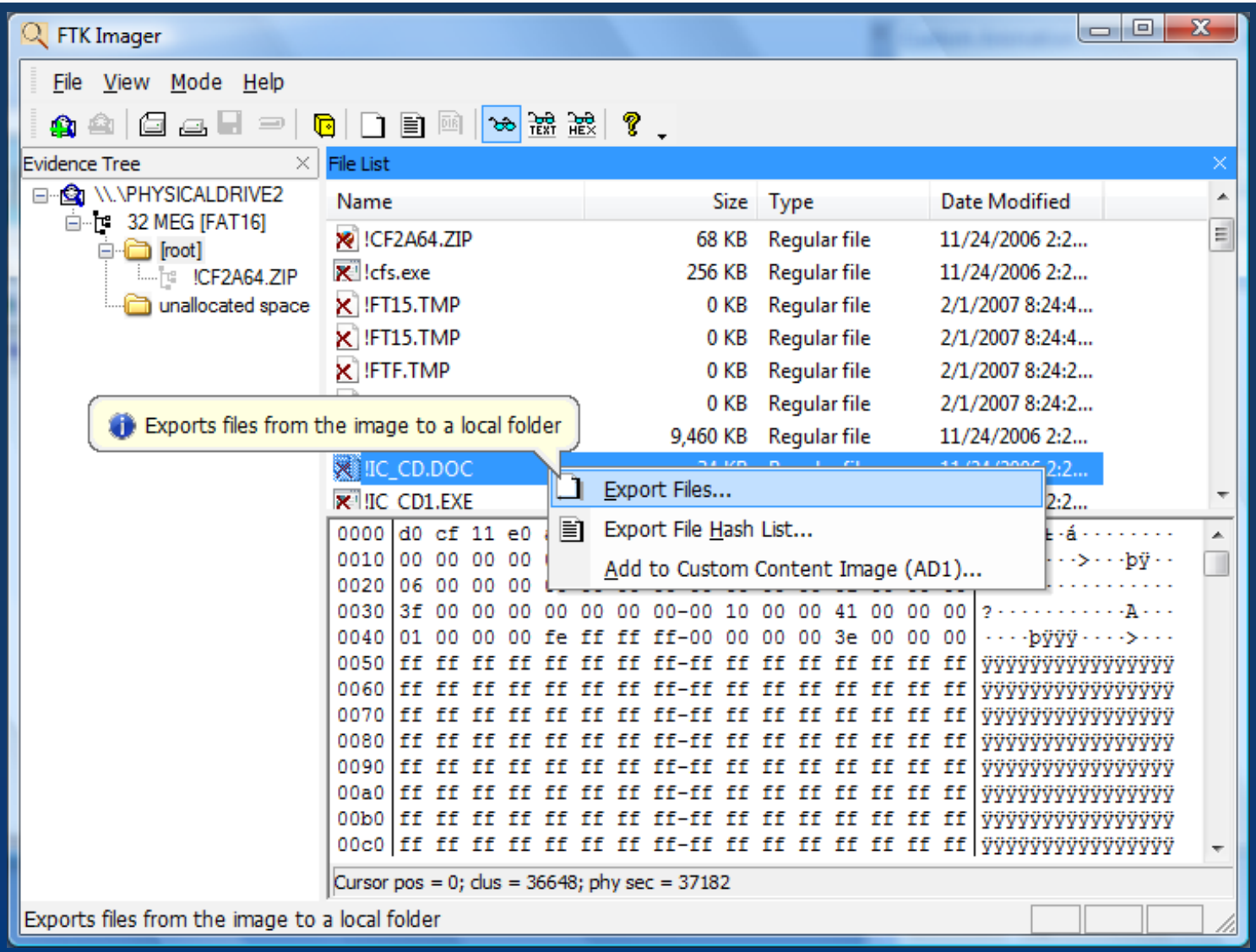
# Escoger el disco




Expandir +




Haga click con el botón derecho en Export File


FTK Imager
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE2
32 MEG [FAT16]
[root]
!CF2A64.ZIP
unallocated space
File List
Name Size Type Date Modified
!CF2A64.ZIP 68 KB Regular file 11/24/2006 2:2...
!cfs.exe 256 KB Regular file 11/24/2006 2:2...
!FT15.TMP 0 KB Regular file 2/1/2007 8:24:4...
!FT15.TMP 0 KB Regular file 2/1/2007 8:24:4...
!FTF.TMP 0 KB Regular file 2/1/2007 8:24:2...
0 KB Regular file 2/1/2007 8:24:2...
9,460 KB Regular file 11/24/2006 2:2...
!IC_CD.DOC
!IC_CD1.EXE
Exports files from the image to a local folder
Export Files...
Export File Hash List...
Add to Custom Content Image (AD1)...
Cursor pos = 0; clus = 36648; phy sec = 37182
Exports files from the image to a local folder

Preguntas

# Contacto

Laboratorio de Delitos Informáticos
Sección de Delitos Informáticos
y Propiedad Intelectual
Departamento de Justicia de los Estados Unidos

- Teléfono: 202-514-1026
- Internet: www.cybercrime.gov