FORENSE DIGITAL BASICO

Jerry W. Hoover, CISSP
Chairman, Digital Evidence Committee

Verificación y Autenticaión de Evidencia

Hash Cryptographico

- Verifica un archivo con MD5
- Como funciona MD5 and SHA hashes
- Usa hash con fotografia forense

Regla de mejor Evidencia

Para comprobar el contenido de un escritura, grabación, o fotografia, el original escritura, grabación, of fotografia es requerido, otra que como proveido por estas reglas o acto del congreso.

Federal Rules of Evidence, rule 1002

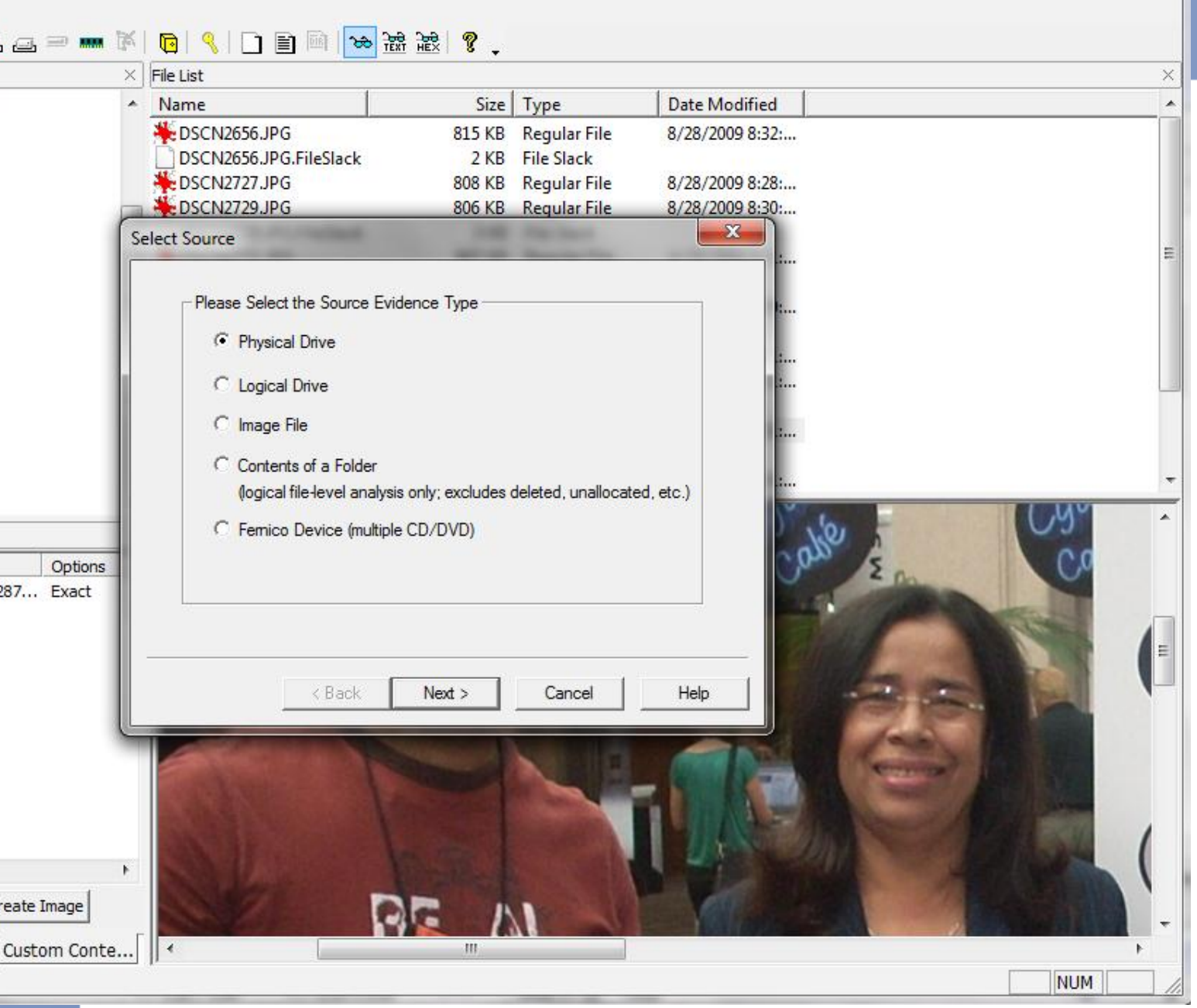
Sin embargo, en practica federal, una copia exacta del original lleva la mismo peso que el original otra que su autenticidad esta en questión.

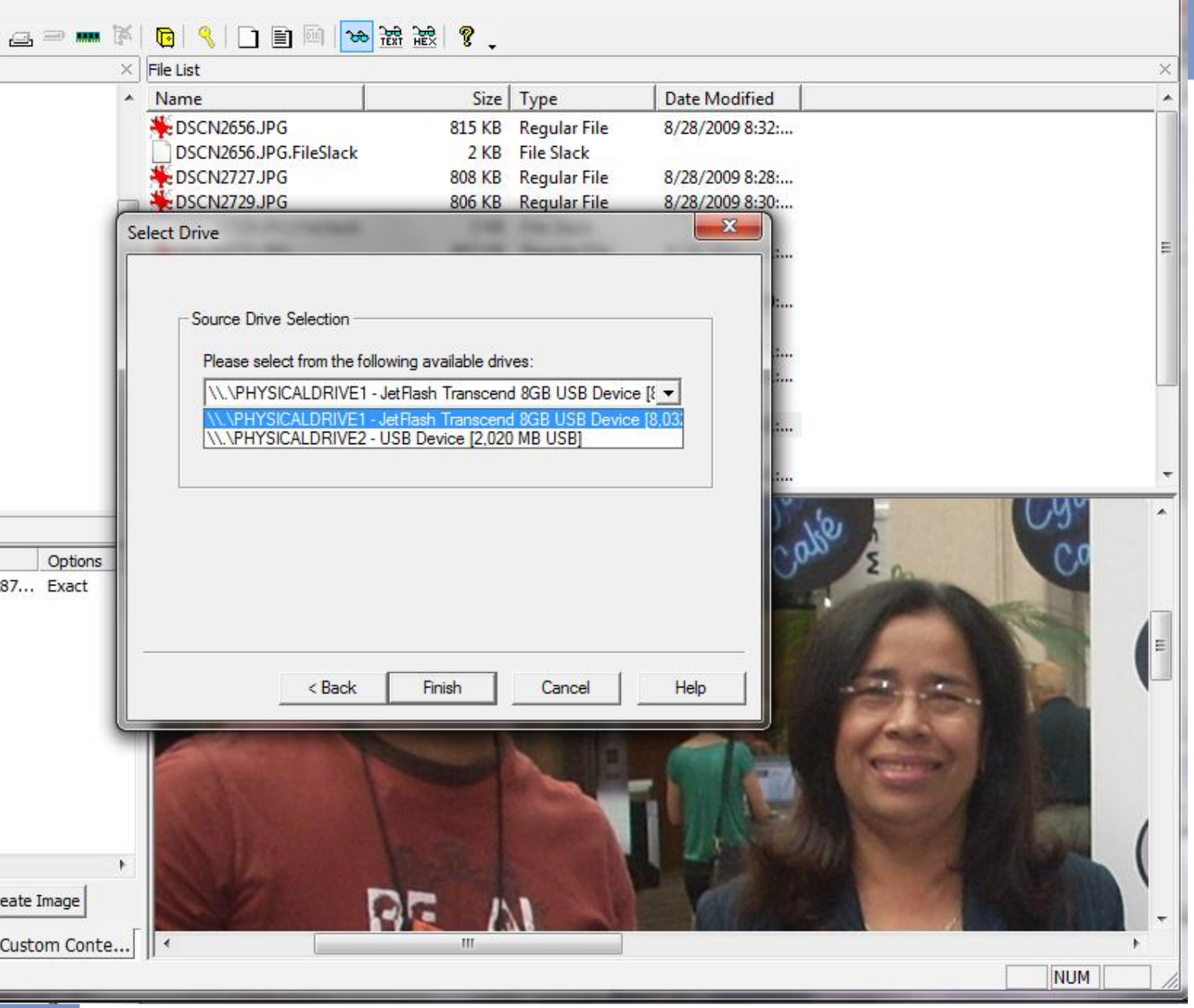
http://en.wikipedia.org/wiki/Best_evidence_rule

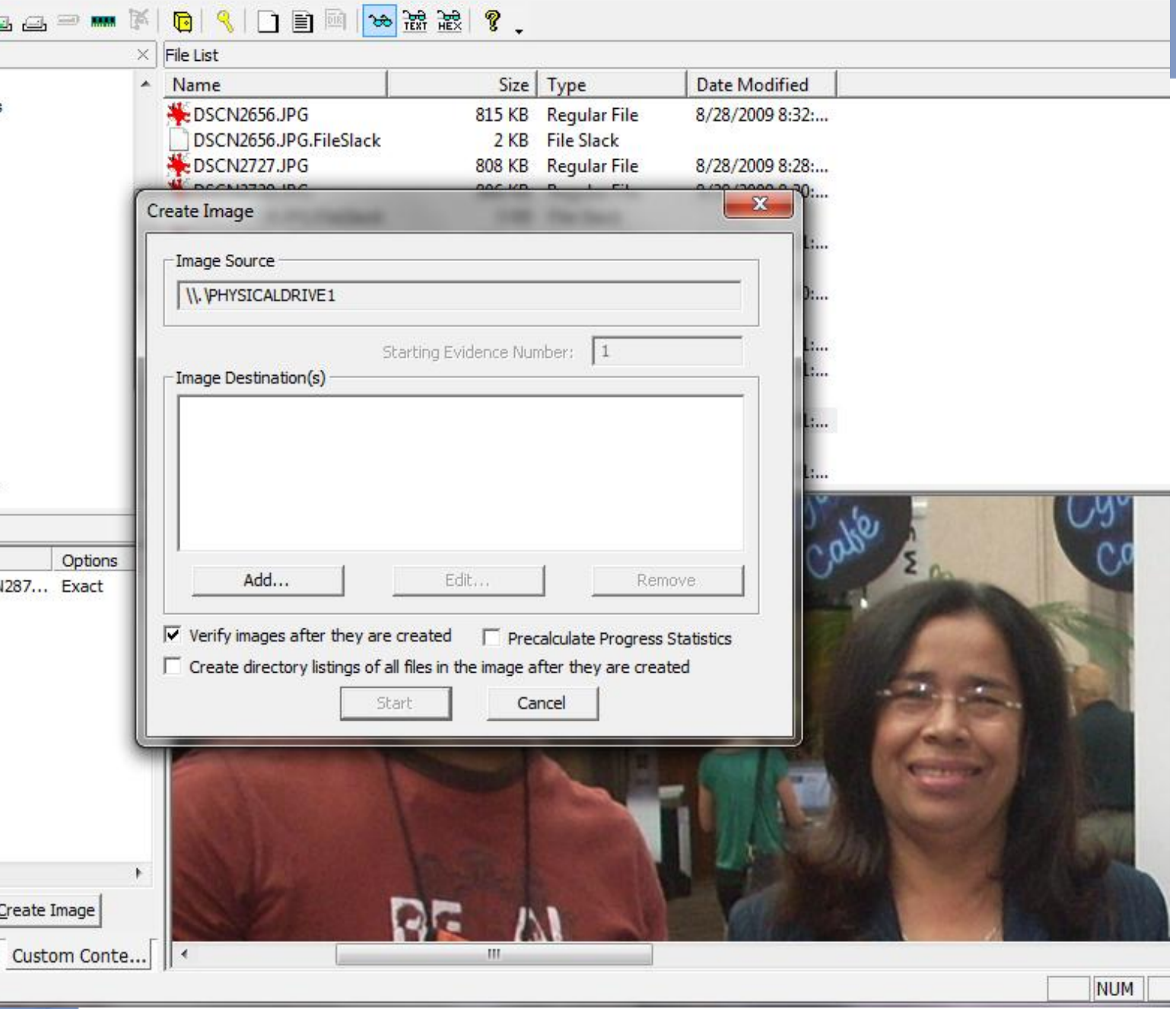
- El original es el mejor evidencia.
  - Disco Duro Original, 35mm pelicula
  - Hay limite (No puede llevar el cadaver al corte.)
- Como comprobar la copia es exacta
  - El ojo humano. (No muy bueno.)
  - Calculos Hash
    - MD5

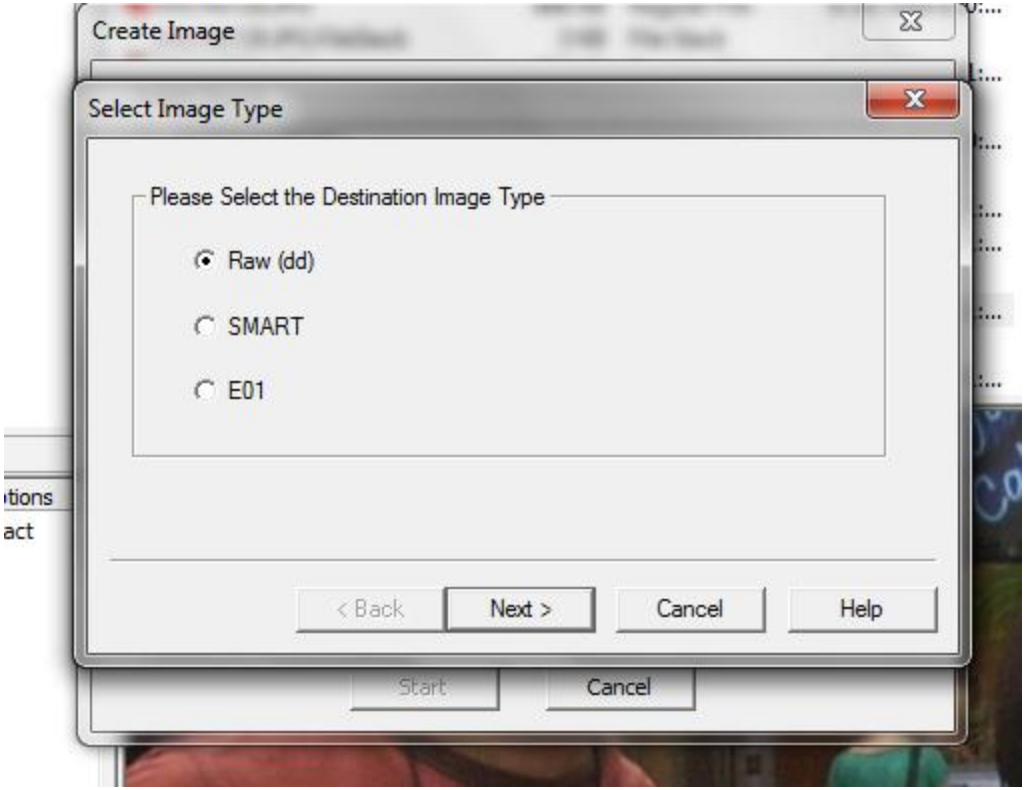
Utilidades Forenses

- MD5Calc- Verifica que una copia es exacta
- FTKImager- Herramienta par examinación forense
- ProDiscover Basic 6.11-
- Irfanview 4.00- Editador de imagenes.


File List
Name
Size
Type
Date Modified
DSCN2656.JPG
815 KB
Regular File
8/28/2009 8:32:...
DSCN2656.JPG.FileSlack
2 KB
File Slack
DSCN2727.JPG
808 KB
Regular File
8/28/2009 8:28:...
DSCN2729.JPG
806 KB
Regular File
8/28/2009 8:30:...
Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help
Options
Exact
Custom Conte...
NUM


File List
Name
Size
Type
Date Modified
DSCN2656.JPG
815 KB
Regular File
8/28/2009 8:32:...
DSCN2656.JPG.FileSlack
2 KB
File Slack
DSCN2727.JPG
808 KB
Regular File
8/28/2009 8:28:...
DSCN2729.JPG
806 KB
Regular File
8/28/2009 8:30:...
Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE1 - JetFlash Transcend 8GB USB Device [8
\\.\PHYSICALDRIVE1 - JetFlash Transcend 8GB USB Device [8,03
\\.\PHYSICALDRIVE2 - USB Device [2,020 MB USB]
< Back
Finish
Cancel
Help
Options
Exact
eate Image
Custom Conte...
NUM


File List
Name
Size
Type
Date Modified
DSCN2656.JPG
815 KB
Regular File
8/28/2009 8:32:...
DSCN2656.JPG.FileSlack
2 KB
File Slack
DSCN2727.JPG
808 KB
Regular File
8/28/2009 8:28:...
Create Image
Image Source
\\.\PHYSICALDRIVE1
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel
Options
Exact
Create Image
Custom Conte...
NUM


Create Image
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
< Back
Next >
Cancel
Help
Start
Cancel

AccessData FTK Imager 2.6.1.62

File View Mode Help

Evidence Tree

- My Documents
- Outlook Express
- Outlook
- Transcend
- Personal Data
- VLC
- Palm
- HSA
- Security
- IRS
- DIACAP Toolset
- ICITAP ES
- Pics
- Forensics
- downloads
- PDBas65011
- Deleted files
- FreeOTFE_Explorer

File List

Name	Size	Type	Date Modified
DSCN2656.JPG	815 KB	Regular File	8/28/2009 8:32:...
DSCN2656.JPG.FileSlack	2 KB	File Slack	
DSCN2727.JPG	808 KB	Regular File	8/28/2009 8:28:...
DSCN2729.JPG	806 KB	Regular File	8/28/2009 8:30:...
DSCN2729.JPG.FileSlack	3 KB	File Slack	
DSCN2771.JPG	807 KB	Regular File	8/28/2009 8:31:...
DSCN2771.JPG.FileSlack	2 KB	File Slack	
DSCN2773.JPG	810 KB	Regular File	8/28/2009 8:30:...
DSCN2773.JPG.FileSlack	3 KB	File Slack	
DSCN2776.JPG	820 KB	Regular File	8/28/2009 8:31:...
DSCN2822.JPG	809 KB	Regular File	8/28/2009 8:31:...
DSCN2822.JPG.FileSlack	4 KB	File Slack	
DSCN2878.JPG	810 KB	Regular File	8/28/2009 8:31:...
DSCN2878.JPG.FileSlack	3 KB	File Slack	
DSCN2881.JPG	814 KB	Regular File	8/28/2009 8:31:...

Custom Content Sources

Evidence:File System|Path|File	Options
F:\:NONAME [FAT32]|[root]|Pics|DSCN287...	Exact

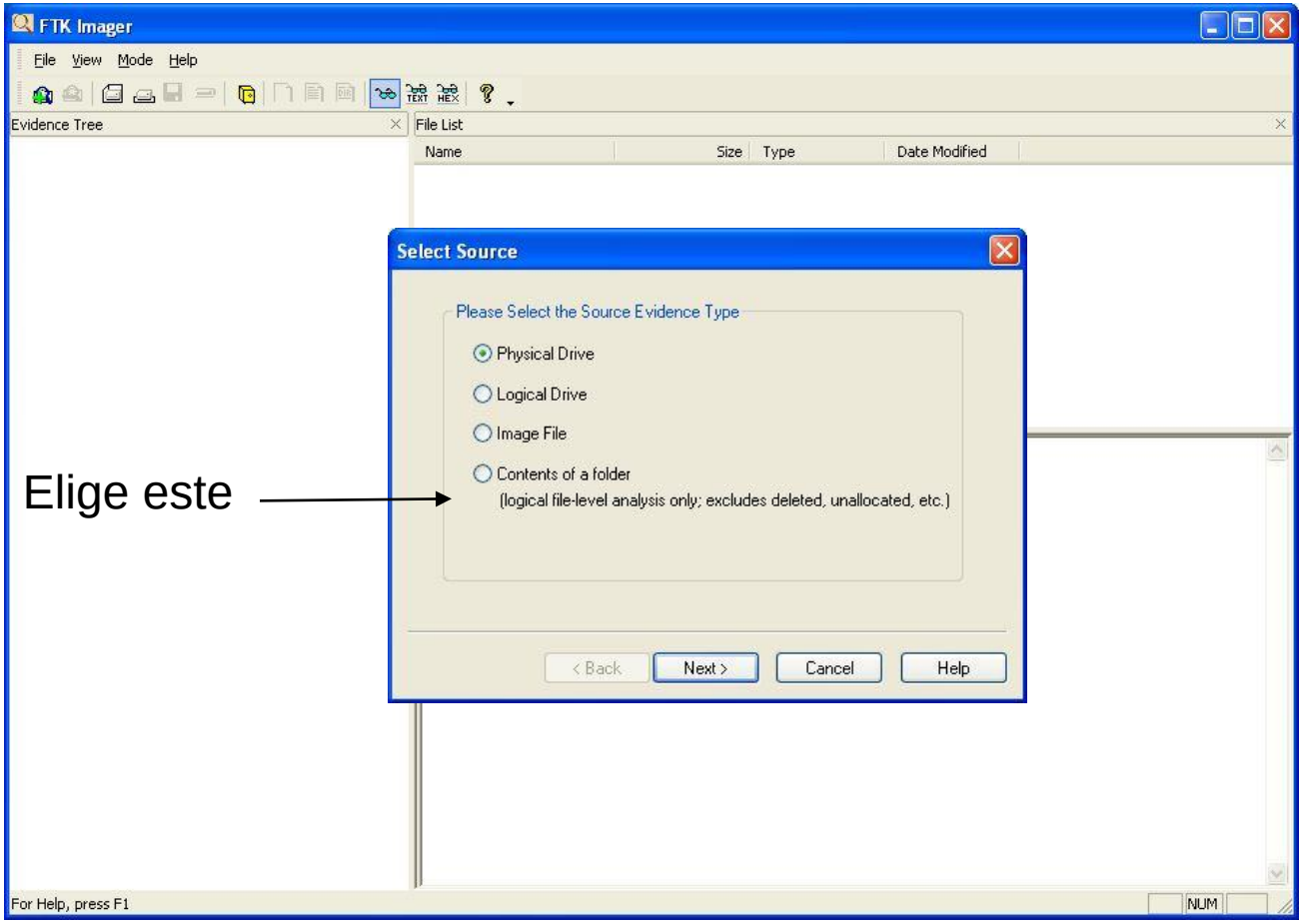
New Edit Remove Remove All Create Image

Properties Hex Value Int... Custom Conte...

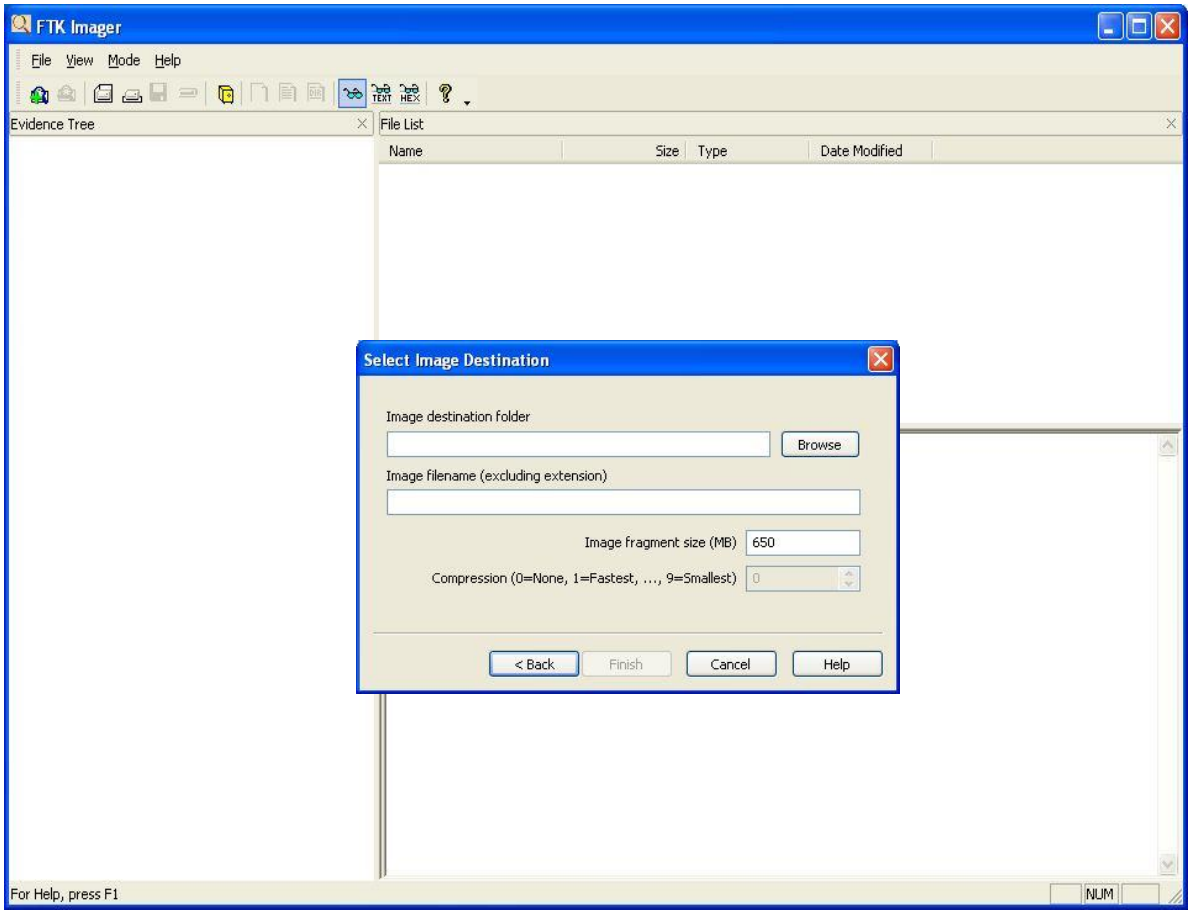
For Help, press F1

NUM

FTK Imager
Carga archivo de imagenes



Select Folder

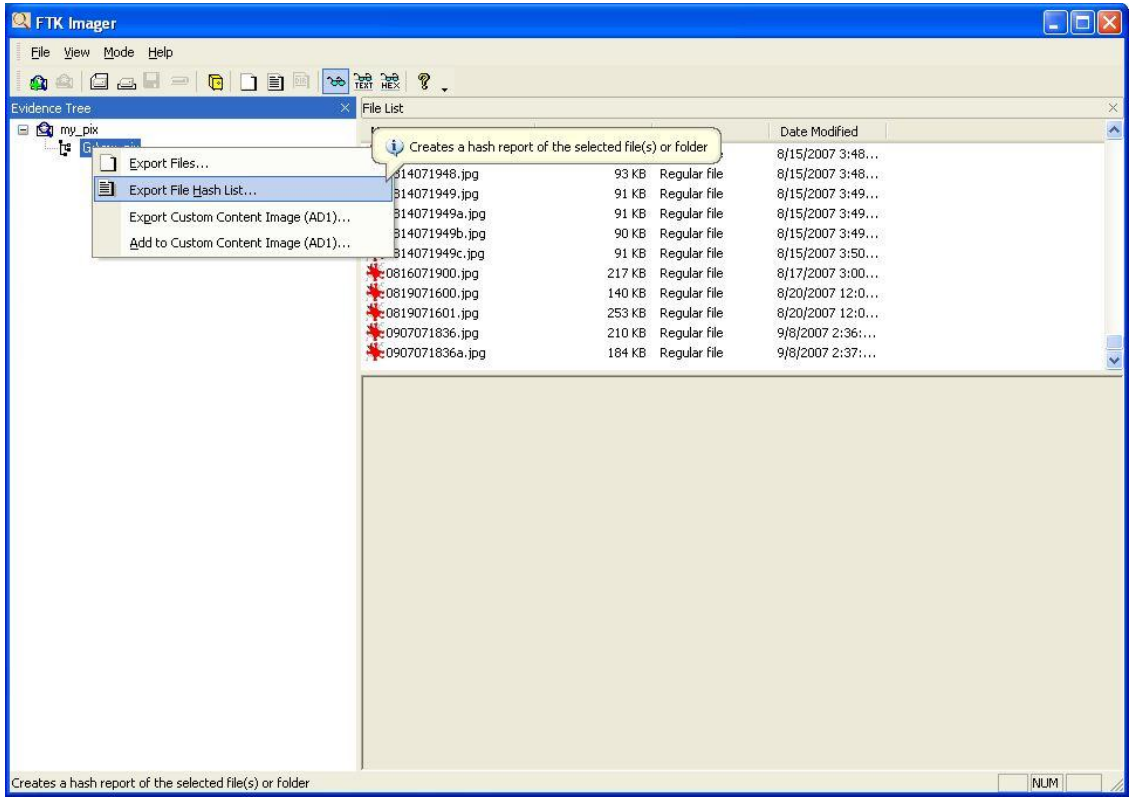


- Click Browse and navigate to Desktop\CFE\8-jpeg-search.

Find 8-jpeg-search.dd

- Selecciona el archivo y Finish.

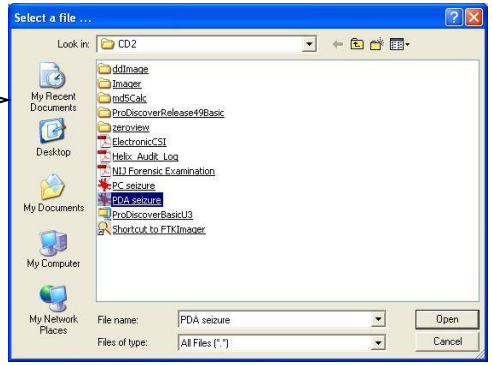
Hash Archivos deEvidencia . (Como verificar fotos digitales)



Sample Hash List

MD5 Utility

CD photo hash.

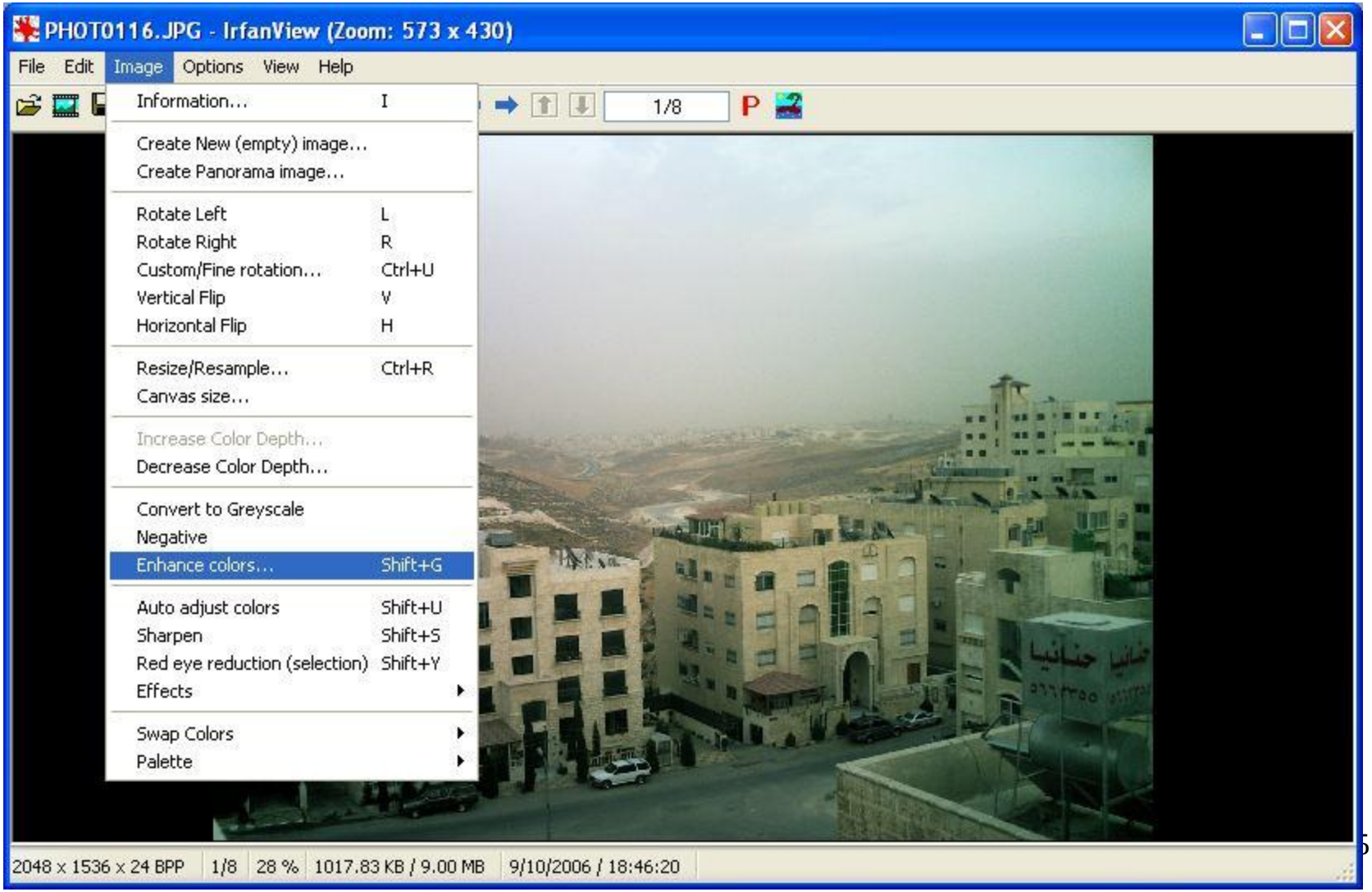


Open file dialogue.

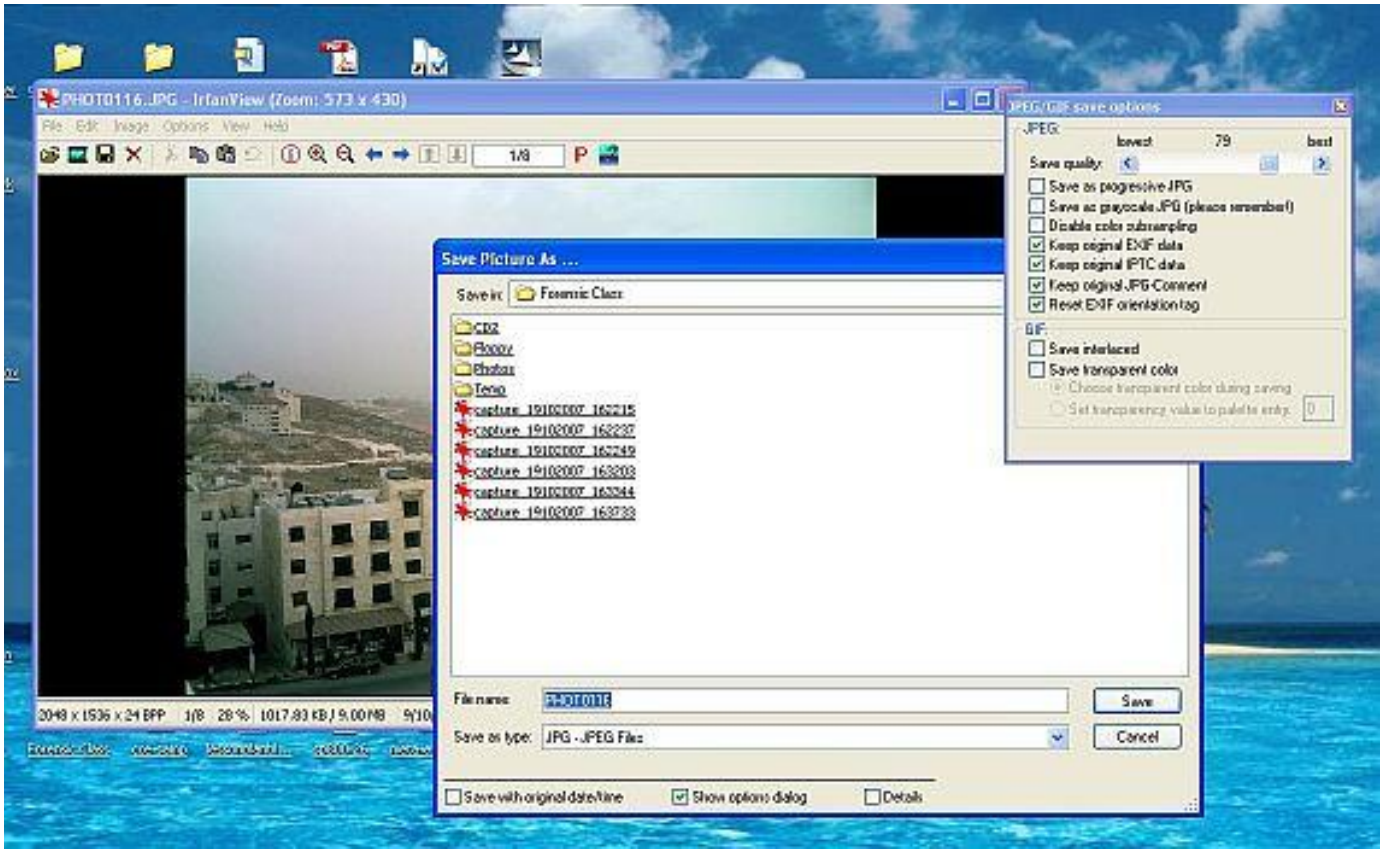
Same photo on desktop.

Hash text. (Cute but useless.)

IRFANVIEW

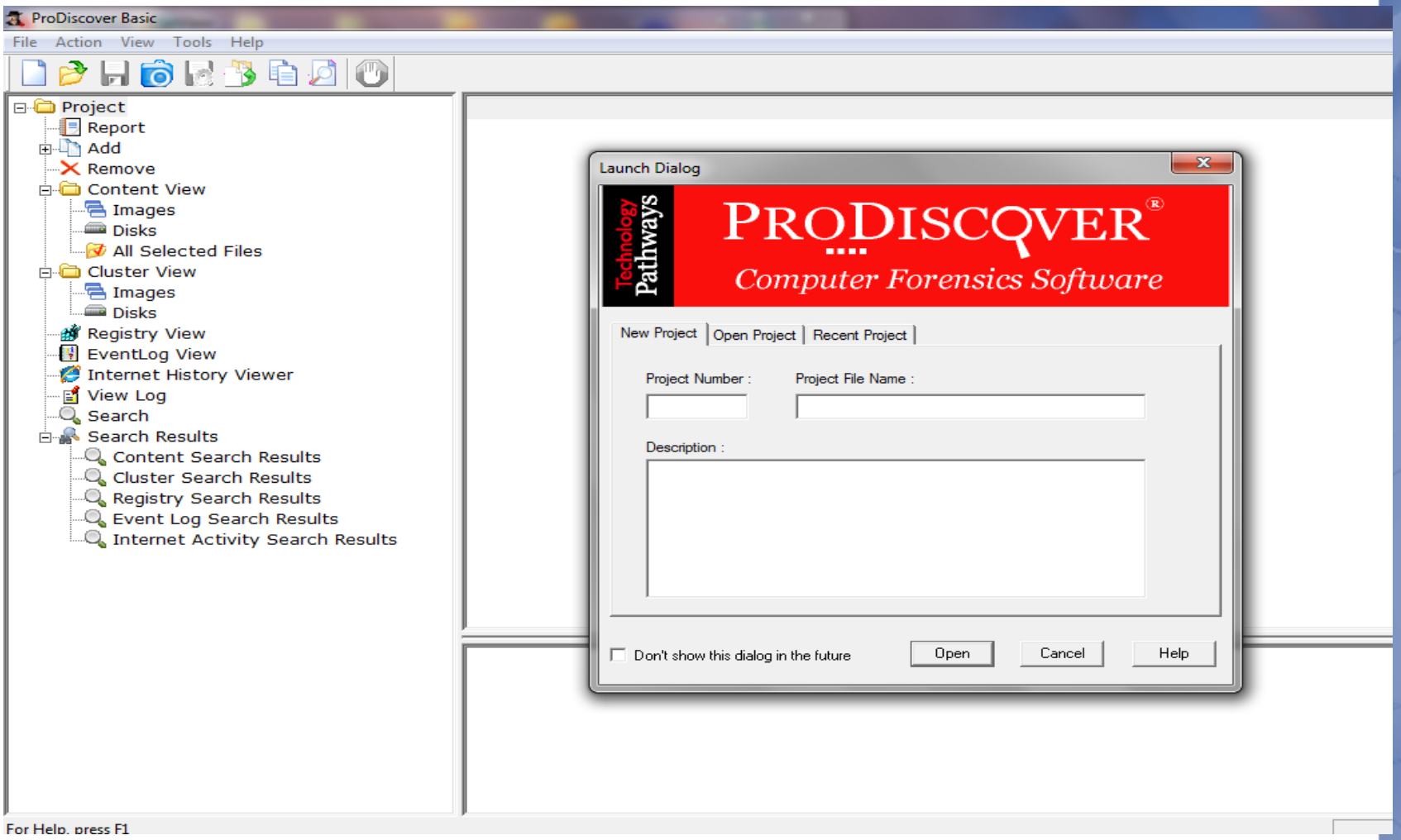

PHOT0116.JPG - IrfanView (Zoom: 573 x 430)
File Edit Image Options View Help
1/8
Information... I
Create New (empty) image...
Create Panorama image...
Rotate Left L
Rotate Right R
Custom/Fine rotation... Ctrl+U
Vertical Flip V
Horizontal Flip H
Resize/Resample... Ctrl+R
Canvas size...
Increase Color Depth...
Decrease Color Depth...
Convert to Greyscale
Negative
Enhance colors... Shift+G
Auto adjust colors Shift+U
Sharpen Shift+S
Red eye reduction (selection) Shift+Y
Effects
Swap Colors
Palette
2048 x 1536 x 24 BPP
1/8
28 %
1017.83 KB / 9.00 MB
9/10/2006 / 18:46:20

Guardar un Mejoramiento

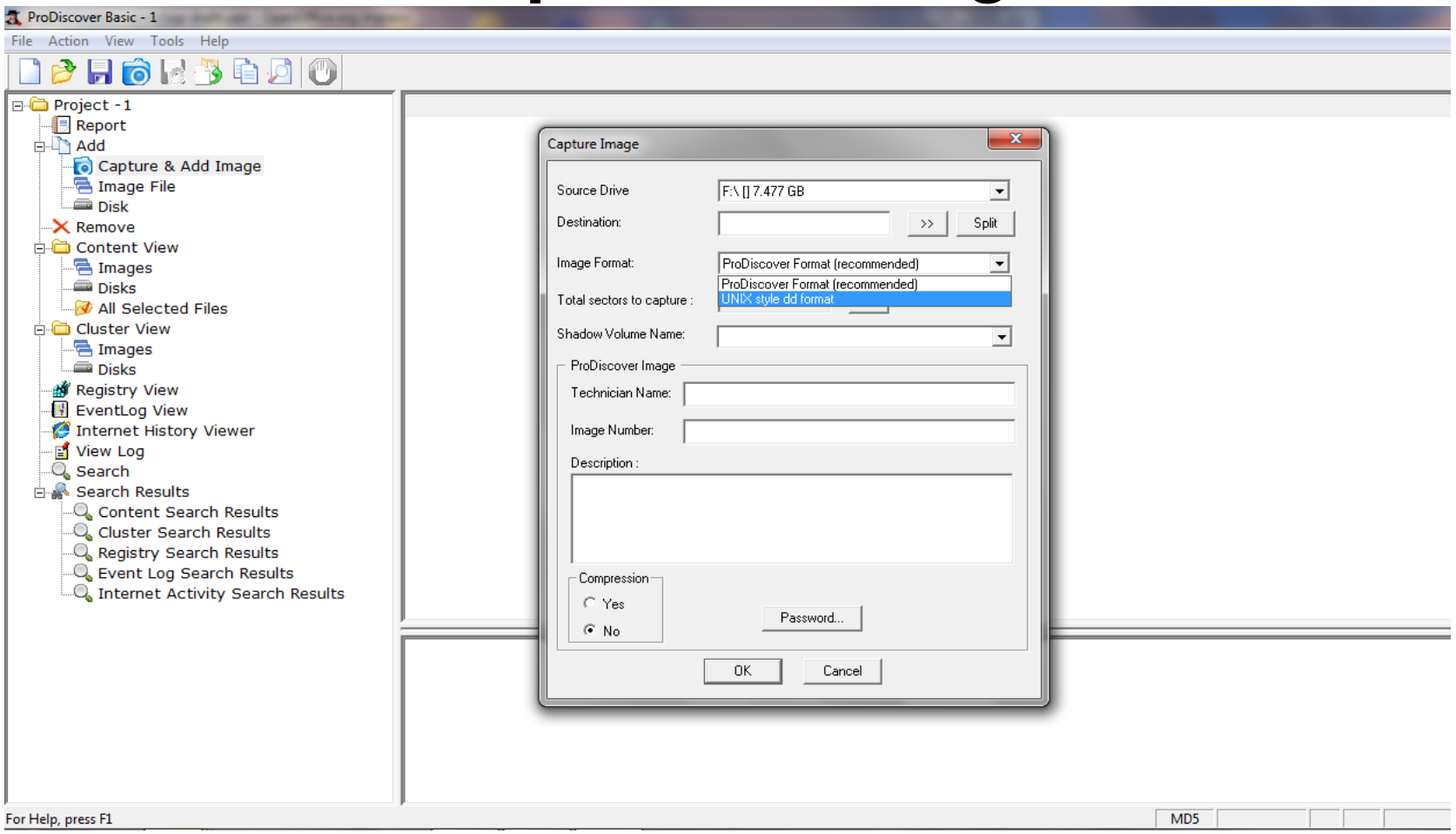


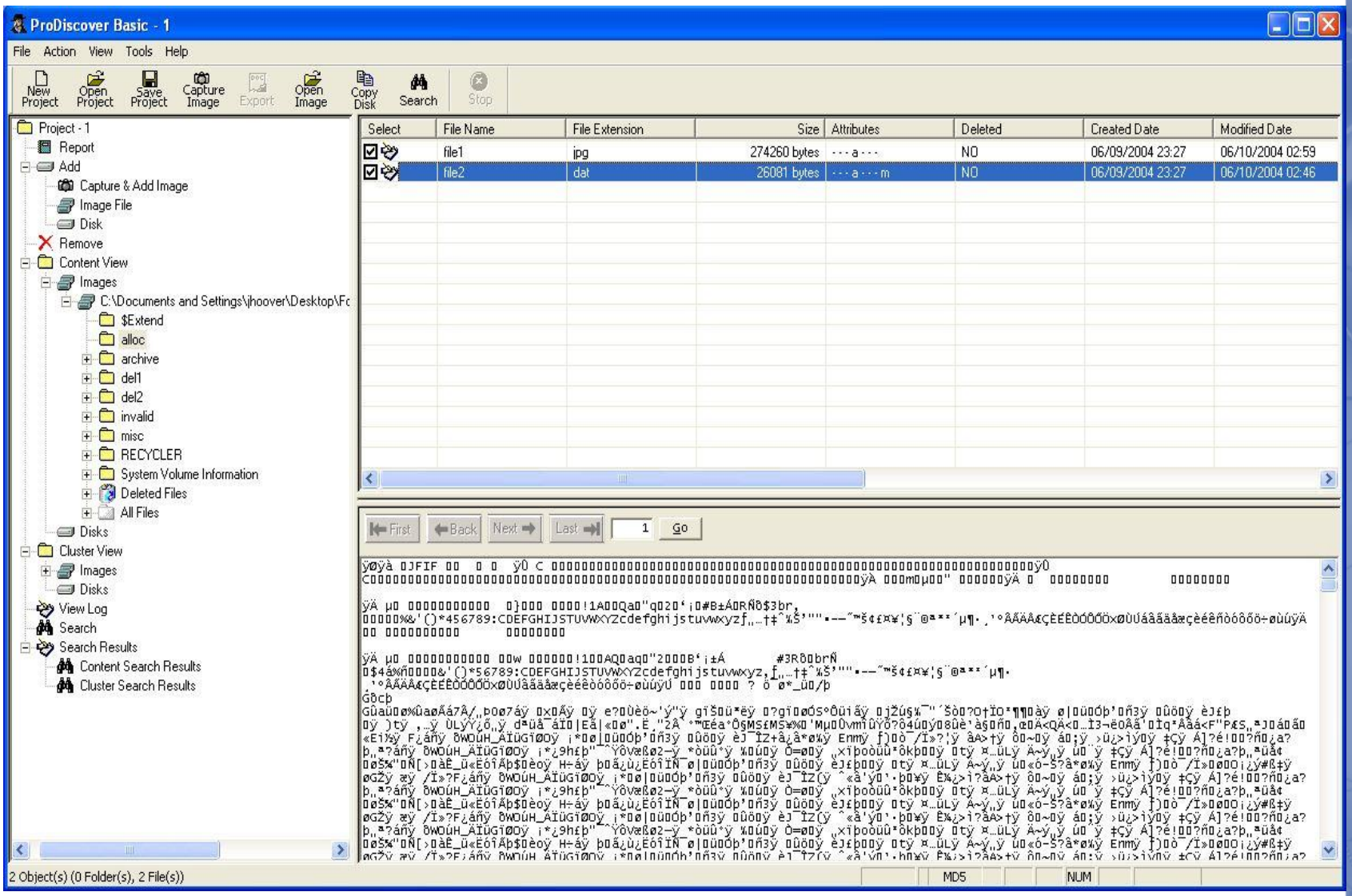
Irfanview siempre pregunta por nombre para prevenir sobreescribiendo

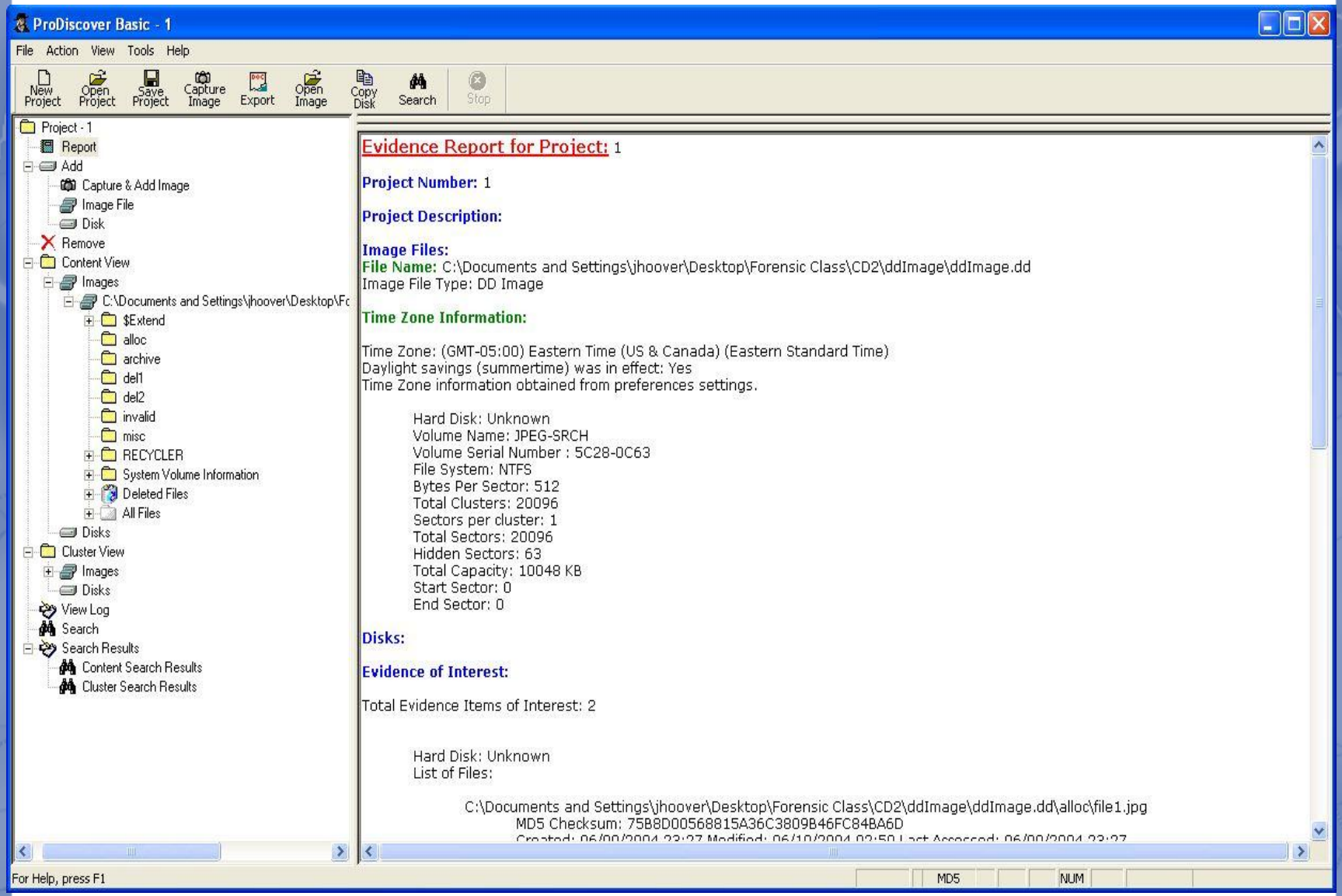
ProDiscover Basic



Capture an Image




ProDiscover Basic - 1
File Action View Tools Help
New Project
Open Project
Save Project
Capture Image
Export
Open Image
Copy Disk
Search
Stop
Project - 1
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
C:\Documents and Settings\jhoover\Desktop\Fc
$Extend
alloc
archive
del1
del2
invalid
misc
RECYCLER
System Volume Information
Deleted Files
All Files
Disks
Cluster View
Images
Disks
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Select
File Name
File Extension
Size
Attributes
Deleted
Created Date
Modified Date
file1
jpg
274260 bytes
---a---
NO
06/09/2004 23:27
06/10/2004 02:59
file2
dat
26081 bytes
---a---m
NO
06/09/2004 23:27
06/10/2004 02:46
First
Back
Next
Last
1
Go
2 Object(s) (0 Folder(s), 2 File(s))
MD5
NUM


ProDiscover Basic - 1
File Action View Tools Help
New Project
Open Project
Save Project
Capture Image
Export
Open Image
Copy Disk
Search
Stop
Project - 1
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
C:\Documents and Settings\jhoover\Desktop\Fc
$Extend
alloc
archive
del1
del2
invalid
misc
RECYCLER
System Volume Information
Deleted Files
All Files
Disks
Cluster View
Images
Disks
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Evidence Report for Project: 1
Project Number: 1
Project Description:
Image Files:
File Name: C:\Documents and Settings\jhoover\Desktop\Forensic Class\CD2\ddImage\ddImage.dd
Image File Type: DD Image
Time Zone Information:
Time Zone: (GMT-05:00) Eastern Time (US & Canada) (Eastern Standard Time)
Daylight savings (summertime) was in effect: Yes
Time Zone information obtained from preferences settings.
Hard Disk: Unknown
Volume Name: JPEG-SRCH
Volume Serial Number : 5C28-0C63
File System: NTFS
Bytes Per Sector: 512
Total Clusters: 20096
Sectors per cluster: 1
Total Sectors: 20096
Hidden Sectors: 63
Total Capacity: 10048 KB
Start Sector: 0
End Sector: 0
Disks:
Evidence of Interest:
Total Evidence Items of Interest: 2
Hard Disk: Unknown
List of Files:
C:\Documents and Settings\jhoover\Desktop\Forensic Class\CD2\ddImage\ddImage.dd\alloc\file1.jpg
MD5 Checksum: 75B8D00568815A36C3809B46FC84BA6D
For Help, press F1
MD5
NUM

Habilidades del Laboratorio

- Busqueda
  - Espacio “Slack”
  - Espacio Libre
- Producción de Evidencia
- Testigo Experto

RECURSOS

WWW.THEIAI.ORG

Digital Evidence Committee

FAQ)Preguntas Frequentes

The following is a non-inclusive list covering a wide range of forensic document issues and related subjects:

- International Association for Identification (IAI): www.theiai.org
- FBI Computer Analysis Response Team (CART): www.fbi.gov/hq/lab/cart.htm
- White Collar Crime Center (NW3C): www.nw3c.org
- National Center for Forensic Science (NCFS): www.ncfs.ucf.edu/digital_evid.html
- Scientific Working Group on Digital Evidence (SWGDE): www.ncfs.org/swgde
- Scientific Working Group on Imaging Technologies (SWGIT): www.theiai.org/guidelines/swgit
- American Academy of Forensic Sciences (AAFS): www.aafs.org
- International Organization on Computer Evidence: www.ioce.org
- Defense Computer Forensics Laboratory: www.dcfl.gov/dc3/home.htm
- American Society of Crime Laboratory Directors: www.ascld.org
- American Society of Crime Laboratory Directors-Laboratory Accreditation Board: www.ascld-lab.org
- International Association of Computer Investigative Specialists: www.cops.org
- American Academy of Forensic Sciences: www.aafs.org
- High Technology Crime Investigation Association: www.htcia.org
- Law Enforcement & Emergency Services Video Association (LEVA): www.leva.org

8. What are current guidelines available to support law enforcement in the area of digital evidence?

There are new drafts of documents being worked continuously, but here are a few sites and documents:

- NIJ, "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition" http://www.ncjrs.gov/pdffiles1/nij/219941.pdf
- NIJ, "Electronic Crime Scene Investigation: An On-the Scene Reference for First Responders" http://www.ncjrs.gov/pdffiles1/nij/227050.pdf
- NIJ, "Digital Evidence in the Courtroom: A Guide For Law Enforcement and Prosecutors" http://www.ncjrs.gov/pdffiles1/nij/211314.pdf
- NIJ, "Forensic Examination of Digital Evidence: A Guide For Law Enforcement" http://www.ncjrs.gov/pdffiles1/nij/199408.pdf
- IOCE: "Draft Best Practices on the Examination of Digital Evidence"
- SWGDE/SWGIT [www.theiai.org/guidelines/swgit]:
  - "Minimum Best Practices for Documenting Image Enhancement"
  - "Recommended Guidelines for Developing Standard Operating Procedures"
  - "Guidelines and Recommendations for Training in Digital & Multimedia Evidence"

Conclusión

Recuerda

- Probar las herramientas
- Documentar el trabajo.
- Siempre trabaja con copia. Nunca con el original.
- Conoce sus limites.

Gracias

Ing. Jerry Hoover, MSCIS, CISSP

Perito Digital

IBM,

Rocket Center, WV

jwh45@yahoo.com