Análisis forense informático

Búsquedas por palabra clave, expresión regular, y búsquedas de archivos de gráficos

ITS/FE Laura K. Heldwein, FBI

Herramientas forenses para realizar búsquedas

- AccessData Corporation – Forensic Tool Kit (FTK), herramienta de análisis forense primaria del FBI
- Software de Apoyo — EnCase, herramienta de análisis forense
- Grep/Find – Unix, Linux, Mac OSX

Expresiones regulares

- Una expresión regular es un conjunto de caracteres que especifica o describe un patrón.
- Las expresiones regulares se usan cuando se quiere buscar líneas específicas de texto que contienen un patrón particular.
- Es posible buscar palabras de un tamaño específico. Es posible buscar palabras con cuatro o más vocales que terminan con la letra “s.” Los números, los símbolos de puntuación: lo que se le ocurra, una expresión regular lo puede encontrar. Lo que sucede una vez el programa que esté usando lo encuentre, eso es otro asunto. Algunos sólo buscan el patrón. Otros imprimen la línea que contiene el patrón.

Ejemplos de expresiones regulares

- Use este patrón con grep para imprimir cada dirección en la bandeja de entrada de su correo electrónico:
  - grep '^From: ' /usr/spool/mail/$USER
- El patrón que encontrará cualquier línea de texto que contenga exactamente un número es
  - ^[0-9]$
- Este patrón encontrará un carácter único, que sea una letra, un número, o el guión bajo:
  - [A-Za-z0-9_]
- Encontrar la palabra “the” en el inicio, en el medio, o en el final de una frase, o al final de una línea, se puede hacer con la expresión regular extendida
  - (^|)the([^a-z]|$)
- Con las expresiones regulares, es posible buscar cualquier cosa: ¡el único límite es su imaginación!

Búsqueda de palabras clave

- La búsqueda de palabras clave – es una técnica poderosa usada en el transcurso de una investigación forense. La búsqueda de palabras clave permite definir una búsqueda que persiga una palabra o una combinación de palabras en la prueba digital.

Tipos básicos de búsqueda

- La búsqueda por **frases** encuentra frases como: *debido proceso*.
- Operadores **booleanos** como and/or/not pueden unir palabras y frases: *debido proceso* and not (*protección igual* or *derechos civiles*)
- La búsqueda por **proximidad** busca una palabra o frase ubicada a “n” palabras de otra palabra o frase: *pie de manzana* w/38 *torta de melocotón*.
- La búsqueda por **proximidad dirigida** encuentra una palabra o frase ubicada “n” palabras antes de otra palabra o frase: *pie de manzana* pre/38 *torta de melocotón*.
- Búsqueda **fónica** busca palabras que suenan parecido, como *Smythe* al buscar *Smith*.
- Búsqueda por **raíces** encuentra variaciones en las terminaciones de las palabras, como *aplica*, *aplicado*, *aplicando* al buscar *aplicar*.
- Búsqueda por **rango numérico** encuentra cualquier número entre dos números, tal como entre *6* y *36*.
- Las capacidades **macro** hacen que sea fácil incluir elementos frecuentemente utilizados en una solicitud de búsqueda.
- Apoyo de **comodín** permite que ? denote el lugar de una letra, y que * denote el lugar de múltiples letras: *apple** and not *appl?sauce*.

Búsqueda por palabras clave

- Existen dos formas de buscar por palabras clave usando el programa FTK:

  - Búsqueda por índice: Permite realizar búsquedas rápidas basadas en palabras clave. FTK automáticamente prepara un índice de las pruebas mientras se procesa el caso.

  - Búsqueda en vivo: Este es un proceso demorado que involucra una comparación elemento por elemento con el término de la búsqueda. **La ventaja principal de una búsqueda en vivo es que permite hacer búsquedas de "expresiones regulares" y de "términos foráneos." "Usted querrá explicar la expresión regular un poco en este momento."**

Búsqueda por índices usando FTK

- Indexación – El fin de guardar un índice es optimizar la velocidad y la ejecución en el momento de encontrar documentos pertinentes durante una búsqueda. Sin un índice, el motor de búsqueda examinaría cada documento en el conjunto, lo que tomaría un tiempo considerable y una capacidad significativa de la computadora.
- En FTK, una búsqueda por índices usa el archivo del índice para encontrar un término de búsqueda.
- El archivo de índice se genera durante la creación del caso.
- El archivo de índice contiene todas las palabras discretas o cadenas de números encontradas tanto en el espacio asignado (*allocated*) como en el espacio no asignado en las pruebas del caso. El archivo no captura espacios o símbolos, incluyendo los siguientes:

  . , : ; “ ‘ ~ ! @ # $ % ^ & * = +
- FTK usa el motor de búsqueda dtSearch, para realizar todas las búsquedas por índices.

Búsqueda por índices

File Edit View Tools Help

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Indexed Search | Live Search

Search Term: | Add | Import | Options

Indexed Words	Co...

Search Items	Hits	Files
Greg Stocksdales'	2	1
CART	111	41
North Texas Regional Computer Forensic	5	1
----------	----	----
Cumulative Results (using AND)	0	0

Edit Item | Remove Item | Remove All | View Item Results »

Cumulative operator: AND | OR | View Cumulative Results »

7 Hits in 1 File - QUERY: (Hot Mail and Yahoo)
2 Hits in 1 File - QUERY: (Greg Stocksdales')
2 Hits - C:\1test\FTKissues.pst>>Personal Folders>>Top of Personal Folders>>ftk Issues:
according to my notes: 1. <<Greg>> Stocksdales' case where FTK would crash in Da
ding to my notes: 1. Greg <<Stocksdales'>> case where FTK would crash in Data Ca
5 Hits in 1 File - QUERY: (North Texas Regional Computer Forensic)
5 Hits - C:\1test\FTKissues.pst>>Personal Folders>>Top of Personal Folders>>ftk Issues:
nvestigation Dallas Division <<North>> Texas Regional Computer Forensic Laboratory
gation Dallas Division North <<Texas>> Regional Computer Forensic Laboratory 301 N
Dallas Division North Texas <<Regional>> Computer Forensic Laboratory 301 North M
ivision North Texas Regional <<Computer>> Forensic Laboratory 301 North Market St
orth Texas Regional Computer <<Forensic>> Laboratory 301 North Market Street, Sui

Rod Gregg
Information Technology Specialist - Forensic Examiner
Federal Bureau of Investigation
Dallas Division
North Texas Regional Computer Forensic Laboratory
301 North Market Street, Suite 500, Dallas, Texas 75202
Office: 972-559-5808
Fax: 972-559-5880
Cell: 214-929-5016
rod.gregg@ic.fbi.gov <mailto:rod.gregg@ic.fbi.gov>
WWW.NTRCFL.ORG

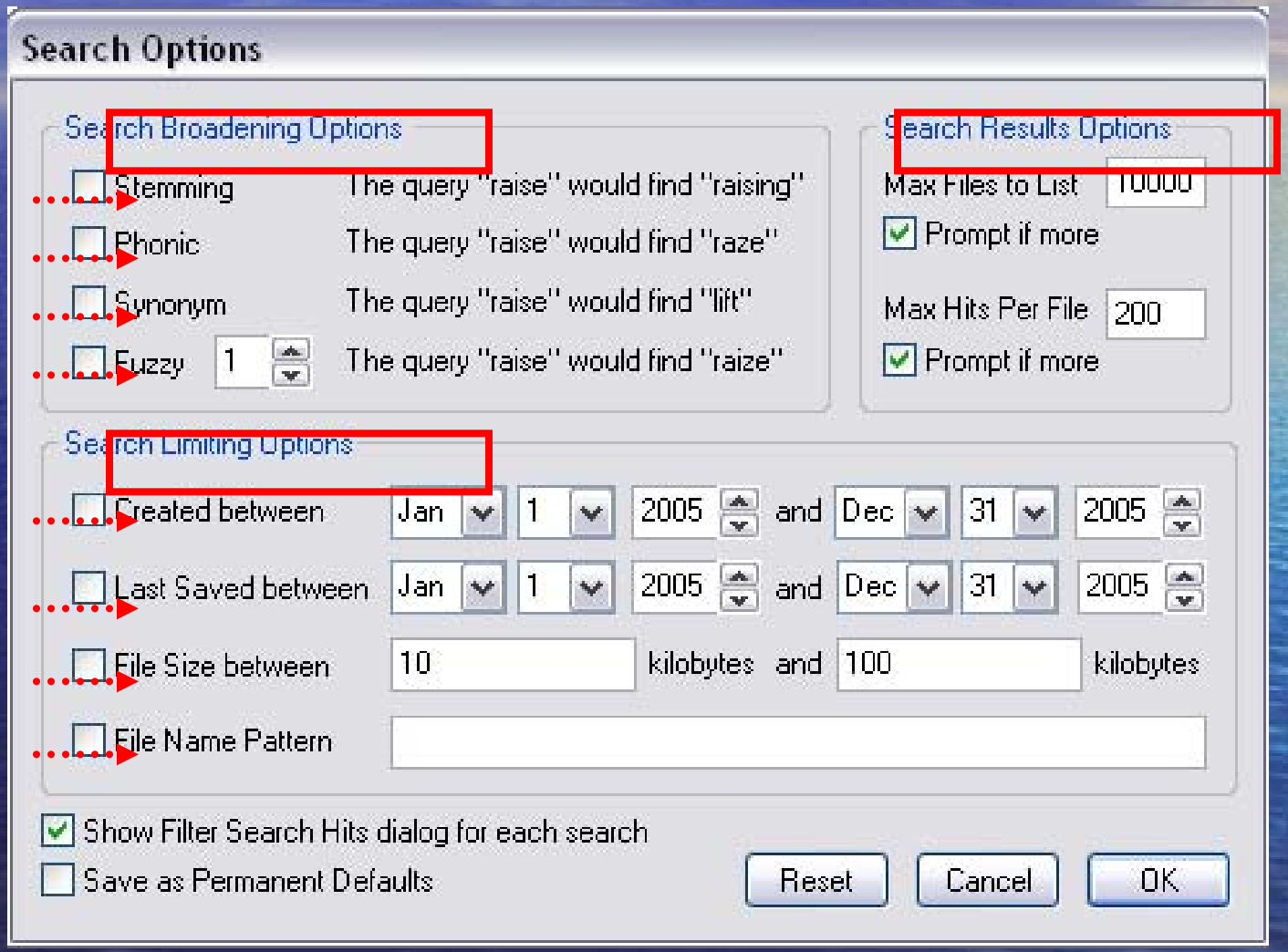
From: Jessica Parry [mailto:jessica@accessdata.com]

OFF Unfiltered | tom's email

File Name	Email Date	Subject	From	To	CC	Atta...
Message0083	4/1/2005 1:...	"RE: FTK 1.51a"	Gregg, Rod	Jessica Parry	to...	0

1 Listed | 1 Checked Total | C:\1test\FTKissues.pst>>Personal Folders>>Top of Personal Folders>>ftk Issues>>Message0083

Opciones de la búsqueda por índices



Búsquedas en vivo y las expresiones regulares usando FTK

- Usted puede realizar una búsqueda en vivo para encontrar patrones de caracteres. (Recuerde que esto es un proceso demorado.)
- La búsqueda en vivo permite trabajar con expresiones regulares, que son patrones de datos tales como un número de tarjeta de crédito o un número de identificación (o de seguridad social).
- FTK trae las siguientes expresiones regulares predefinidas:
  - Número de teléfono en los Estados Unidos
  - Número de teléfono en Gran Bretaña
  - Número de tarjeta de crédito
  - Número de identificación (o de seguridad social)
  - Dirección IP
- De ser necesario, es posible editar las expresiones o aún crear expresiones nuevas usando un editor de texto.

Búsqueda en vivo usando expresiones regulares

File Edit View Tools Help

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Indexed Search | Live Search

Search Term: Add

Search Items | Type

Item Type:
- Text
- ASCII
- Unicode
- Case Sensitive
- Regular Expression
- Hexadecimal

Max Hits Per File: 200

Edit Item | Delete Item | Reset | Search

Search Performed 8/30/2005 6:29:34 PM -- 13 Hits in 2 Checked Files
- Query: "<<US Phone Number>>" <ASCII/Unicode, Case Insensitive, Regular Expression> -- 13
  - 9 Hits -- ADC FLOPPY\EVIDENCE-FAT12\Recycler\S-1-5-21-1929781967-2543695198-660823
  - 4 Hits -- ADC FLOPPY\EVIDENCE-FAT12\PHONE TEST.txt
    - Offset 0131 (305) -- aaaaaaaaa <<222-8899>> aaaaaaaaaaaaaaaaaaaaa..aaaaaaaaa
    - Offset 0251 (593) -- aaaaaaaaa <<555 1212>> ddddddddddddddddddddddddddddddd
    - Offset 0453 (1107) -- aaaaaaaaa <<888.777.9999>> oooooooooooooooooooooo..aaa
    - Offset 0000 (1738) -- aaaaaaa.. <<1-222-333-4444>> aaaaaaaaaaaaaaaaaaaaaaaa

- US Phone Number
- UK Phone Number
- Credit Card Number
- Social Security Number
- IP Address
- Edit expressions...

```
000006a0 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000006b0 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000006c0 61 61 61 61 61 61 61 0d-0a 20 31 2d 32 32 32 2d  aaaaaaa·· 1-222-
000006d0 33 33 33 2d 34 34 34 34-20 61 61 61 61 61 61 61  333-4444 aaaaaaa
000006e0 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
000006f0 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000700 61 61 61 61 61 61 61 61-61 61 61 61 0d 0a 61 61  aaaaaaaaaaaa··aa
00000710 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000720 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000730 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000740 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000750 0d 0a 61 61 61 61 61 61-61 61 61 61 61 61 61 61  ··aaaaaaaaaaaaaa
00000760 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000770 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000780 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 61  aaaaaaaaaaaaaaaa
00000790 61 61 0d 0a 61 61 61 61-61 61 61 61 61 61 61 61  aa··aaaaaaaaaaaa
```

Pre-Built Regular Expressions are available. For more advanced expressions see your local CART/RCFL examiner

Selection start = 1738, length = 14; cluster = 1856; physical sector = 1887

OFF Unfiltered | tom's email

File Name	Full Path	Recycl...	E..	File Type	Category	Subject	Cr Date	Mod Date
PHONE TEST.txt	ADC FLOPPY\EVIDENCE-FAT12\PHONE TES...		txt	Plain Text D...	Document		10/1/2003 10:32:36 ...	10/1/2003 9:30

2 Listed | 134 Checked Total | ADC FLOPPY\EVIDENCE-FAT12\PHONE TEST.txt

Búsqueda por palabras clave y copia de archivos - Unix

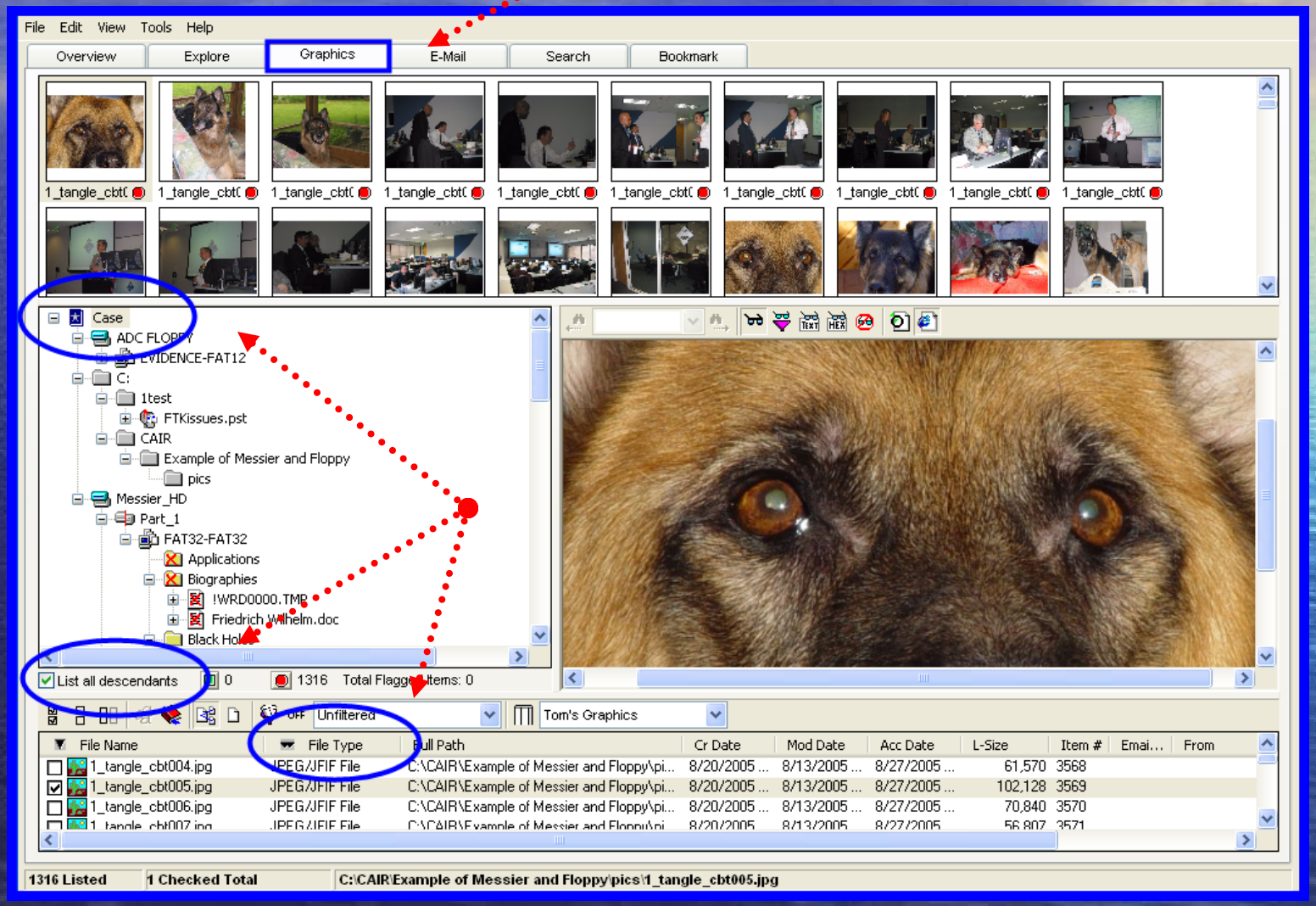
- **find -type f -exec grep -iq "My_String_or_RE" '{}' \; -print | tee output-log.txt | xargs -i cp -a --parents "{}" /My_Copy_Dir**
  - **Este comando busca la cadena de caracteres entre “ ” y copia los archivos al directorio /My_Copy_dir**

Buscando archivos de gráficos

- Los archivos de gráficos o de “imágenes” son archivos designados específicamente para representar imágenes gráficas.

- Los archivos de gráficos vienen en diferentes formatos; los siguientes son formatos comunes de archivos de gráficos:
  - BMP, Windows bitmap file format
  - JPEG, Joint Photo graphics Experts Group
  - PNG, Portable Network Graphic
  - TIFF, Tagged Image File Format

Ver gráficos usando FTK



Pestaña de gráficos

File Edit View Tools Help

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Case
ADC FLOPPY
EVIDENCE-FAT12
C:
1test
FTKissues.pst
CAIR
Example of Messier and Floppy
pics
Messier_HD
Part_1
FAT32-FAT32
Applications
Biographies
!WRD0000.TMP
Friedrich Wilhelm.doc
Black Holes

List all descendants | 0 | 1316 | Total Flagged Items: 0

Unfiltered | Tom's Graphics

File Name	File Type	Full Path	Cr Date	Mod Date	Acc Date	L-Size	Item #	Emai...	From
1_tangle_cbt004.jpg	JPEG/JFIF File	C:\CAIR\Example of Messier and Floppy\pi...	8/20/2005 ...	8/13/2005 ...	8/27/2005 ...	61,570	3568		
1_tangle_cbt005.jpg	JPEG/JFIF File	C:\CAIR\Example of Messier and Floppy\pi...	8/20/2005 ...	8/13/2005 ...	8/27/2005 ...	102,128	3569		
1_tangle_cbt006.jpg	JPEG/JFIF File	C:\CAIR\Example of Messier and Floppy\pi...	8/20/2005 ...	8/13/2005 ...	8/27/2005 ...	70,840	3570		
1_tangle_cbt007.jpg	JPEG/JFIF File	C:\CAIR\Example of Messier and Floppy\pi...	8/20/2005 ...	8/13/2005 ...	8/27/2005 ...	56,807	3571		

1316 Listed | 1 Checked Total | C:\CAIR\Example of Messier and Floppy\pics\1_tangle_cbt005.jpg

Programas para ver gráficos

- Image Scan – Gratuito (Comuníquese con el contacto local del FBI para obtener entrenamiento y el programa)
- Irfanview – Gratuito www.irfanview.com
- Picasa – Gratuito www.picasa.google.com
- Acdsee – Bajo costo www.acdsee.com

Gráficos y thumbs.db ?

- El archivo thumbs.db es un archivo oculto generado por el sistema operativo Windows. Es una imagen reducida de un gráfico o documento.

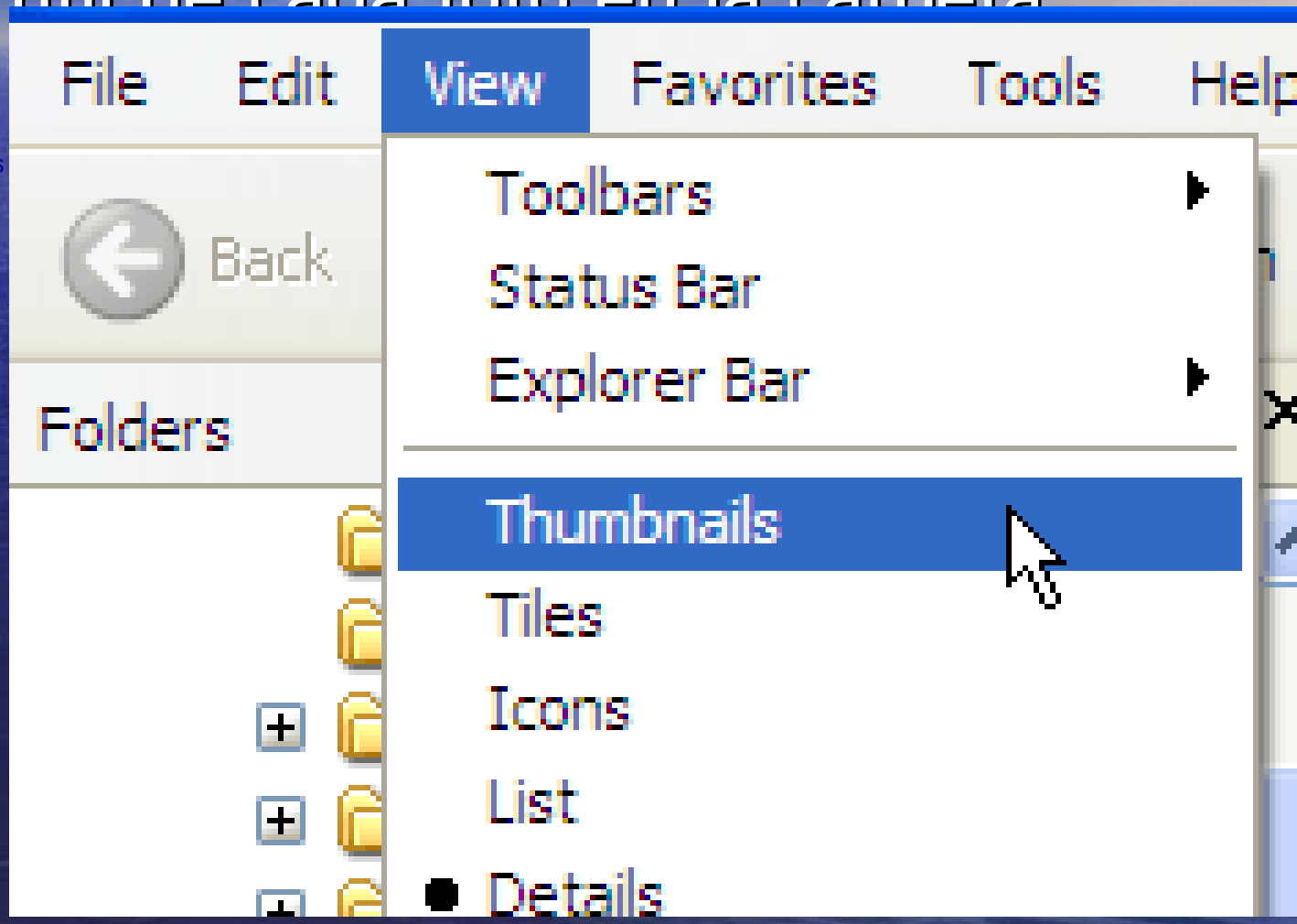
- El Explorador de Windows “amablemente” crea el archivo “thumbs.db” para acelerar la visión de miniaturas en ocasiones posteriores.

- Las miniaturas (*thumbnails*) son usadas por programas de edición de fotos y de gráficos para explorar rápidamente varias páginas de archivos de imágenes gráficas.

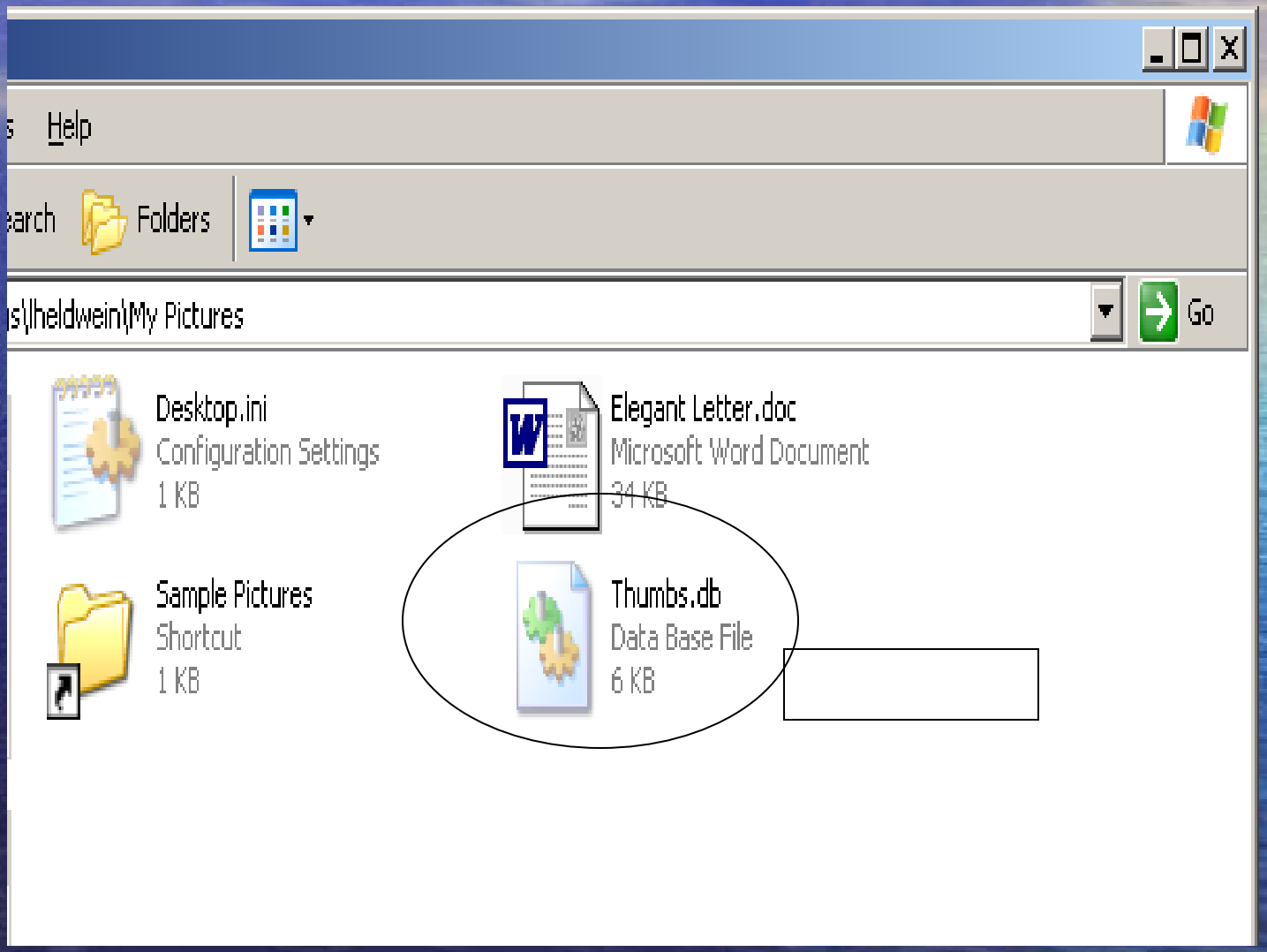
- Este caché se guarda para que Windows no tenga que generar de nuevo estas miniaturas cada vez que alguien consulte la carpeta.

- Desde el Explorador de Windows o Mi PC, haga click en el menú **Ver [View]**, **Miniaturas [Thumbnails]**, y obtendrá una miniatura pequeña y útil de cada foto en la carpeta

Desde el Explorador de Windows



Archivo Thumbs.db



Vista de FTK Forensic de Thumbs.db

Thumbs.db

Full path: Thumbs database\Part_1\Thumbs Database-NTFS\Good Pictures evidence\Thumbs.db

File type: Shell Thumbnail Cache

Shell Thumbnail Cache

Database version: 7 (Windows 2003)

Original Filename	Last Modified
Picture 029.jpg	1/23/2005 4:59:32 PM
Picture 022.jpg	1/23/2005 4:59:20 PM
Picture 018.jpg	1/23/2005 4:59:14 PM
Picture 019.jpg	1/23/2005 4:59:16 PM
Picture 020.jpg	1/23/2005 4:59:18 PM
Picture 021.jpg	1/23/2005 4:59:20 PM
Picture 023.jpg	1/23/2005 4:59:22 PM
Picture 024.jpg	1/23/2005 4:59:24 PM
Picture 025.jpg	1/23/2005 4:59:26 PM
Picture 026.jpg	1/23/2005 4:59:28 PM
Picture 027.jpg	1/23/2005 4:59:28 PM
Picture 028.jpg	1/23/2005 4:59:30 PM

Otros programas para ver Thumbs.db

- Polyview – bajo costo
  - www.polybytes.com
- DHThumbs – bajo costo
  - www.dmthumbs.com

Adaptado para Linux

Inicia con CD-ROM / Disco Floppy

Sistema de Visión Previa de Imágenes Gráficas

Versión 2.1

La historia de Image Scan

- Creado y probado por la oficina central del CART (el Equipo de Análisis y Respuesta Informático) del FBI– Programa Unix
- Específicamente para investigaciones sobre la explotación de niños
- Una herramienta de software para que los investigadores puedan usarla en el campo, sin alterar pruebas originales, para ver archivos de imágenes gráficas.

Objetivos de Image Scan

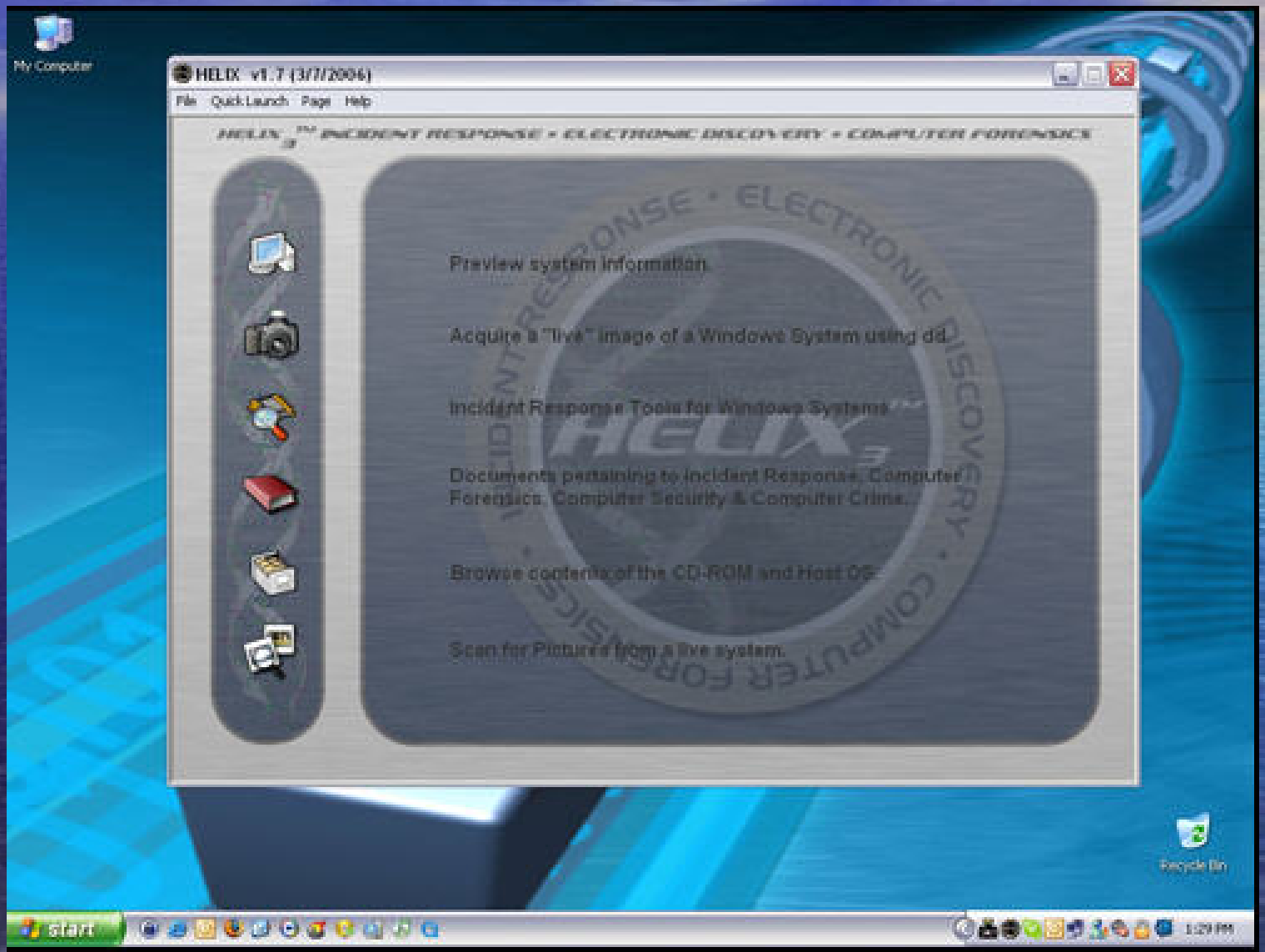
- Primero – Tomar un sistema técnicamente complejo y presentarlo de tal manera que resultara entendible, preciso y útil.

- Segundo – Entregar un recurso técnico que pueda ayudar de manera dramática a los investigadores en el campo, sin la necesidad de contar con la presencia de expertos en informática.

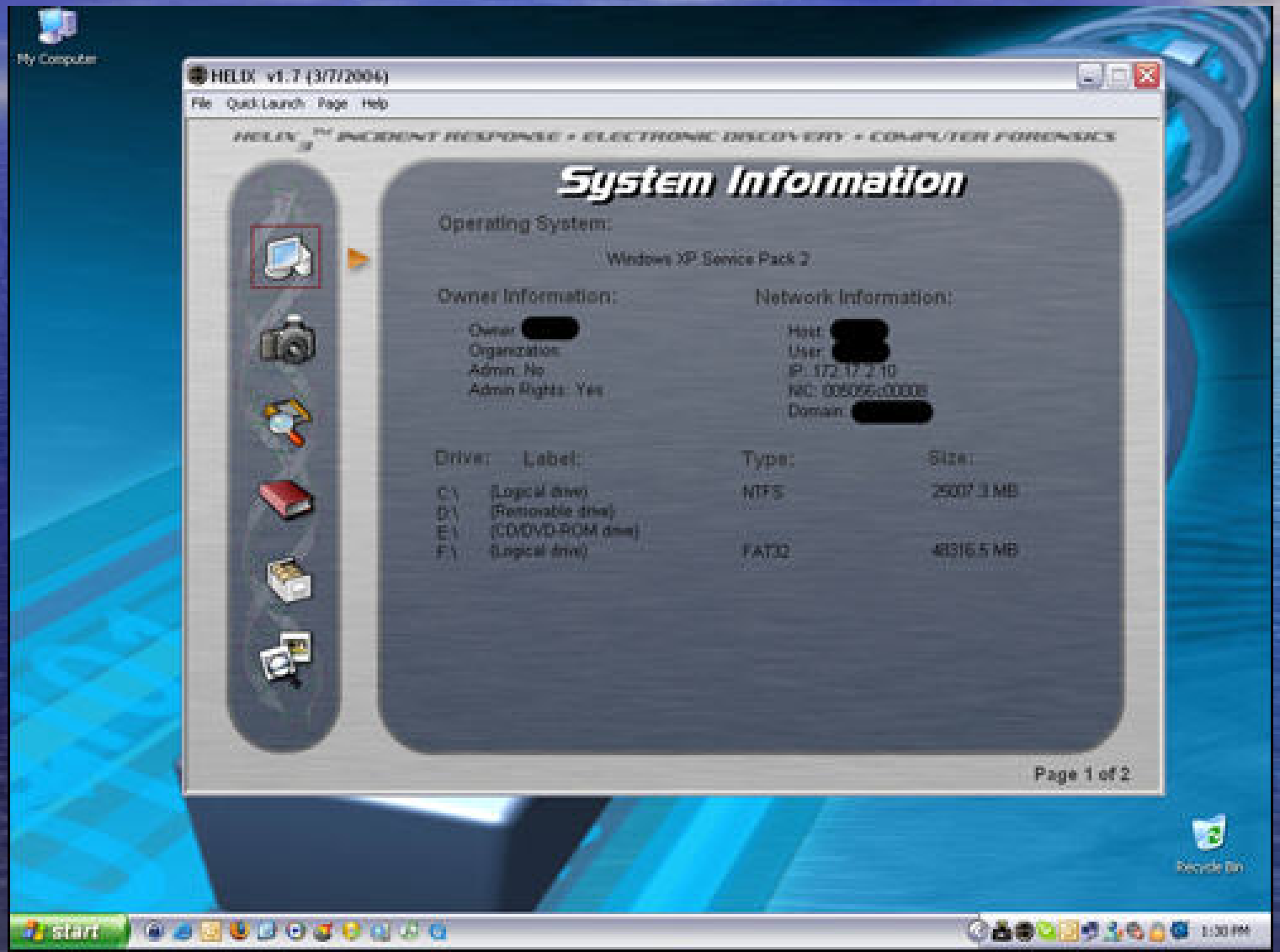
Helix – Una herramienta gratuita de imágenes y respuesta a incidentes

- Carga un IGU (Interfaz Gráfico del Usuario) Linux al RAM del CPU del sujeto
- No monta discos
- Puede DD a otro dispositivo
- Puede revisar imágenes gráficas sin cambiar las fechas y los tiempos, y mucho más
- Disponible en:
  - www.e-fense.com/helix

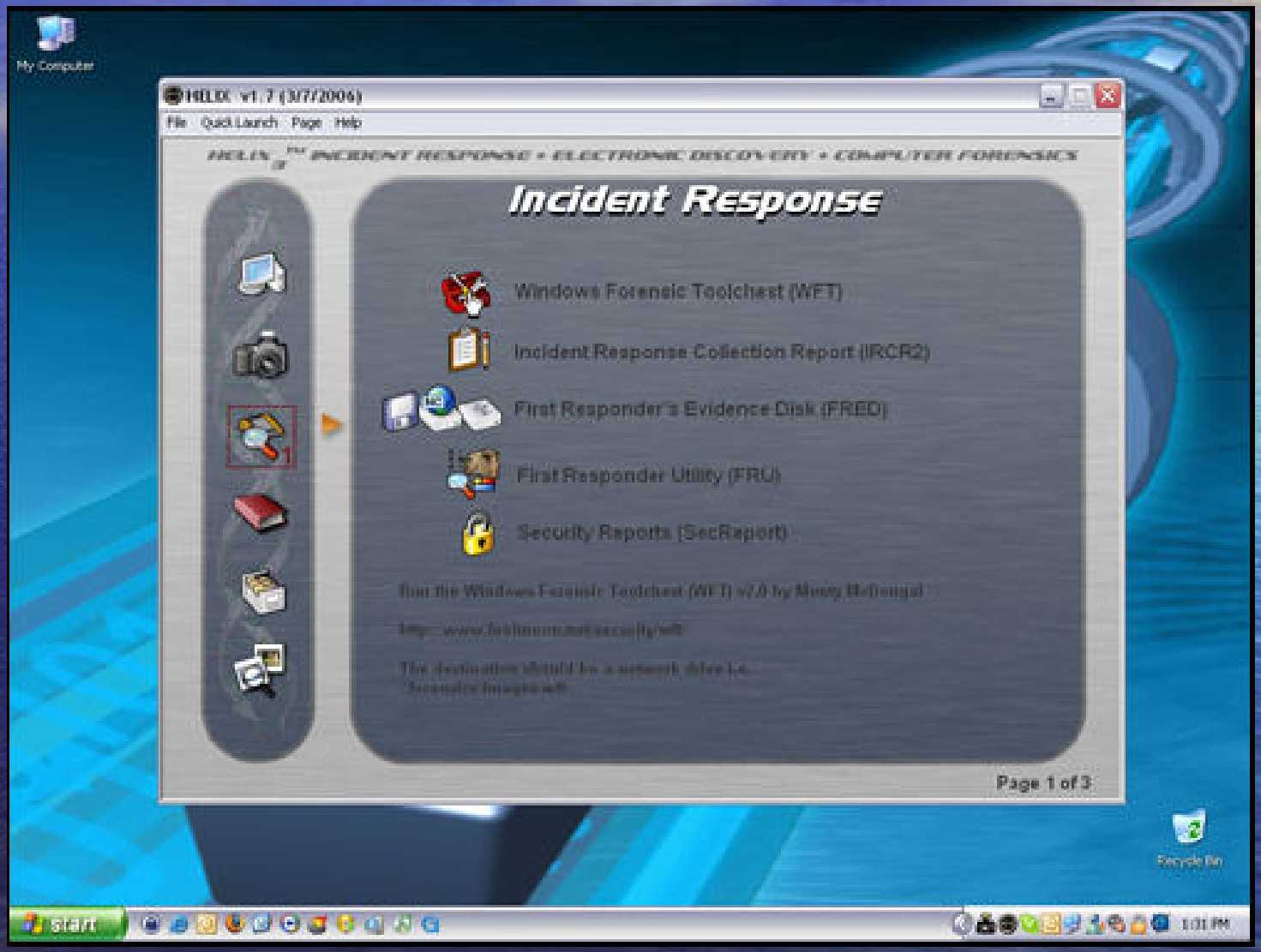
Helix – Imágenes de la pantalla



Helix – Imágenes de la pantalla



Helix - Imágenes



Helix – Imágenes

Preguntas

ITS/FE Laura K. Heldwein, FBI

lheldwein@adelphia.net