Computer Forensic Analysis

Keyword searches,

regular expression and

searches of graphic files

Detective/FE Reggy Chapman, Federal Bureau of Investigation

Forensic Tools for Searching

- AccessData Corporation – Forensic Tool Kit (FTK), FBI primary forensic examination tool
- Guidance Software – EnCase, forensic examination tool
- Grep/Find – Unix, Linux, Mac OSX

Regular Expressions

- A regular expression is a set of characters that specify a pattern.
- Regular expressions are used when you want to search for specify lines of text containing a particular pattern.

Regular Expressions

- You can search for words of a certain size. You can search for a word with four or more vowels that end with an "s." Numbers, punctuation characters, you name it, a regular expression can find it. What happens once the program you are using find it is another matter. Some just search for the pattern. Others print out the line containing the pattern.

Regular Expression Examples

- Use this pattern with grep to print every address in your incoming mail box:
  - grep '^From: ' /usr/spool/mail/$USER
- The pattern that will match any line of text that contains exactly one number is
  - ^[0-9]$

Regular Expression Examples

- This pattern will match a single character that is a letter, number, or underscore:
  - [A-Za-z0-9_]
- Matching the word "the" in the beginning, middle, end of a sentence, or end of a line can be done with the extended regular expression:
  - (^|)the([^a-z]|$)
- With Regular expressions, you can search for anything…Only limited to your imagination!

Keyword Searches

- Keyword searching - is a powerful technique used during a forensic investigation. Keyword searching allows you to construct a search by looking for a word or combination of words in digital evidence.

Basic Search Types

- **Phrase** searching finds phrases like:
  - *due process of law*.
- **Boolean** operators like and/or/not can join words and phrases:
  - *due process of law and not (equal protection or civil rights).*
- **Proximity** searching finds a word or phrase within "n" words of another word or phrase:
  - *apple pie w/38 peach cobbler.*
- **Directed Proximity** searching finds a word or phrase "n" words before another word or phrase:
  - *apple pie pre/38 peach cobbler*.

Basic Search Types

- **Phonic** searching finds words that sound alike, like:
  - *Smythe* in a search for *Smith*.
- **Stemming** finds variations on endings, like:
  - *applies*, *applied*, *applying* in a search for *apply*.
- **Numeric** range searching finds any number between two numbers, such as between *6* and *36*.
- **Macro** capabilities make it easy to include frequently used items in a search request.
- **Wildcard** support allows ? to hold a single letter place, and * to hold multiple letter places:
  - *apple* and not appl?sauce*.

Keyword Searching

- There are two ways of keyword search using the software program FTK:

  - Indexed Search: Allows for fast searching based on keywords. FTK automatically indexes your evidence while the case is being processed.

  - Live Search: This is a time consuming process involving an item-by-item comparison with the search term. **The main advantages of a live search is that it allows for "Regular Expressions" and "Foreign Term" searches. "you may want to explain regular expression a little here"**

Indexed Searching using FTK

- **Indexing** – The goal of storing an index is to optimize the speed and performance of finding relevant documents during a search query. Without an index, the search engine would scan every document in the corpus, which would take a considerable amount of time and computing power.

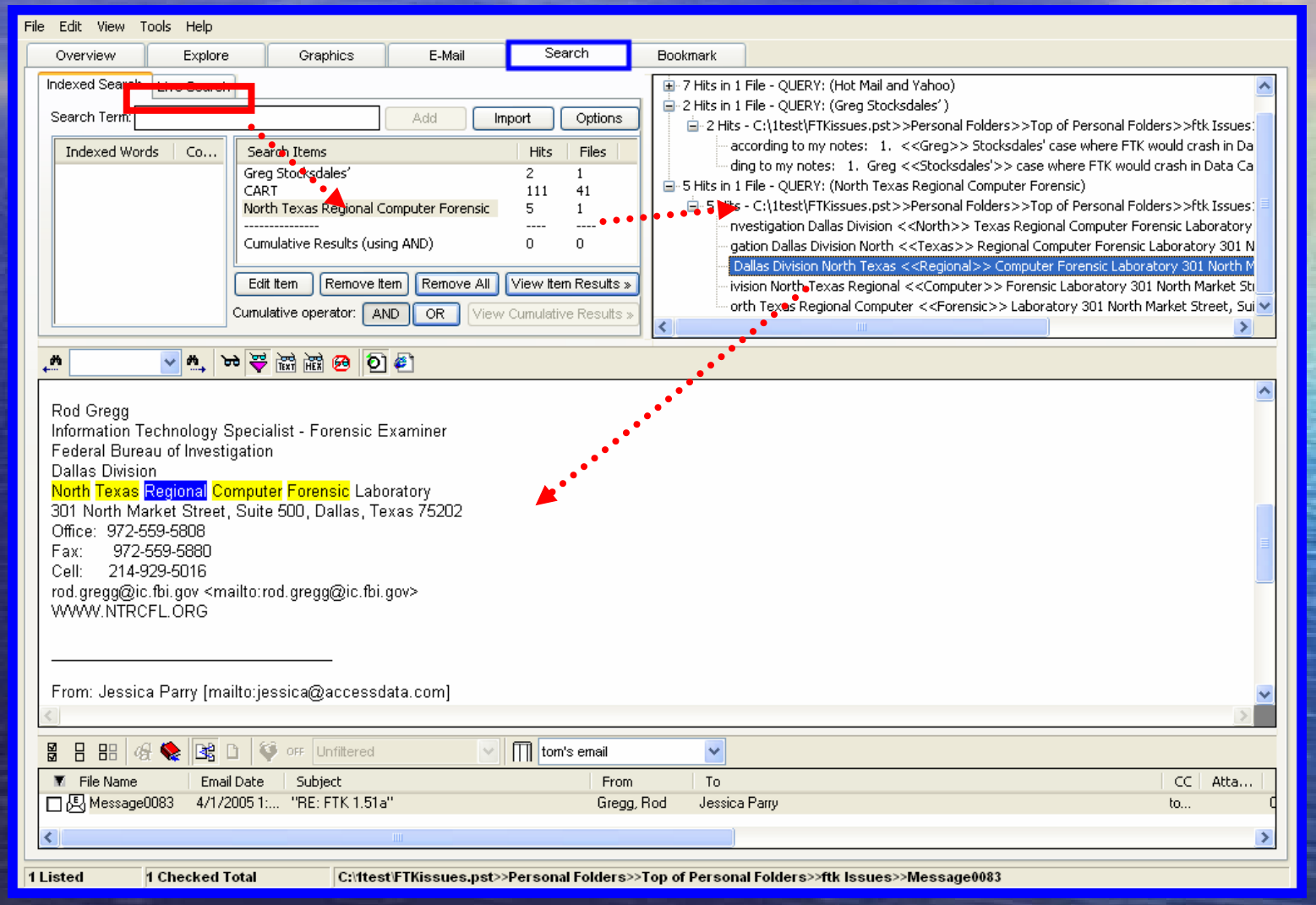
Indexed Searching using FTK

- In FTK an indexed search uses the index file to find a search term.
- The index file is generated during the creation of a case.
- The index file contains all discrete words or number strings found in both the allocated and unallocated space in the case evidence. It does not capture spaces or symbols, including the following:

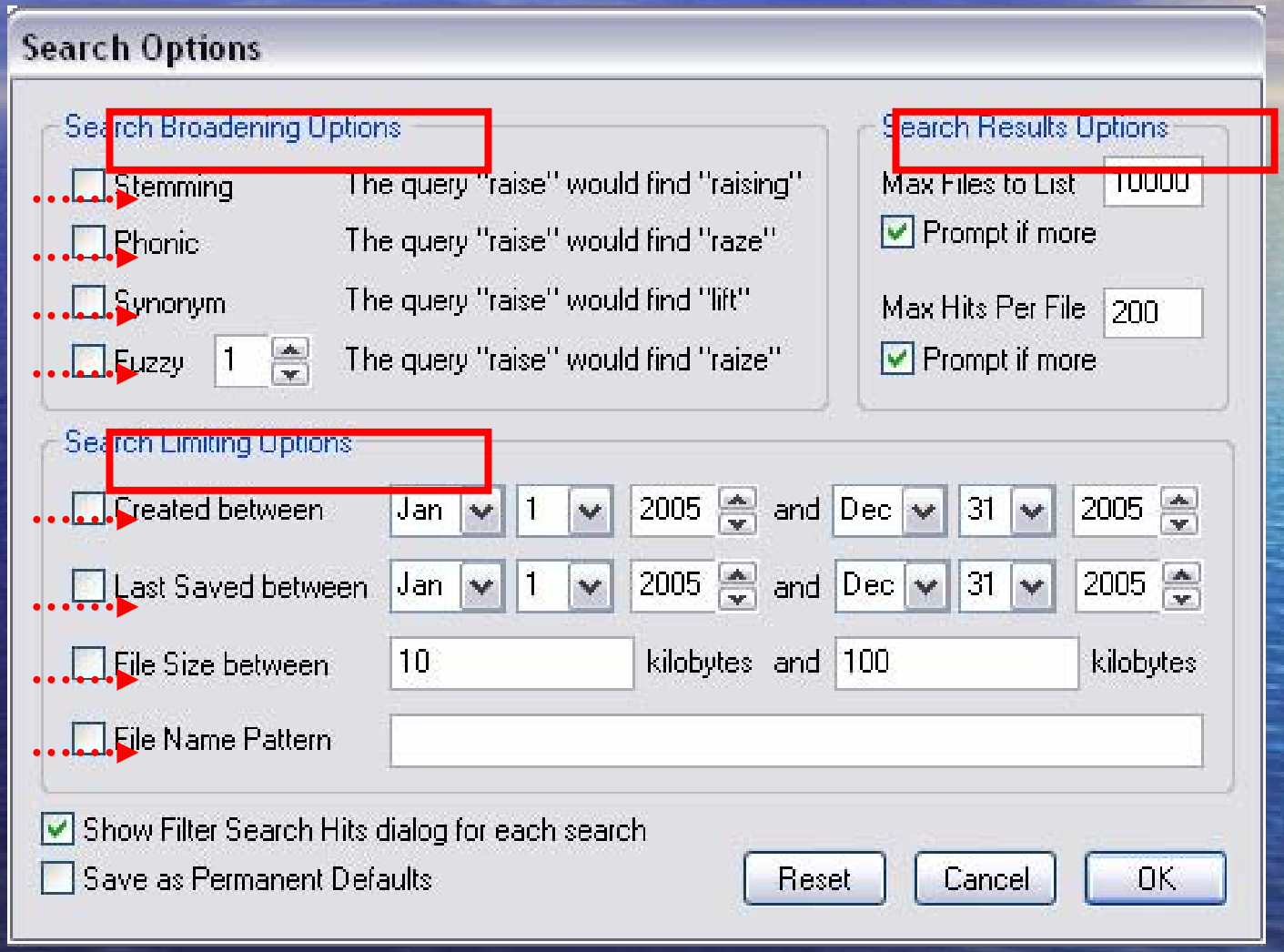
  . , : ; “ ‘ ~ ! @ # $ % ^ & * = +

- FTK uses the search engine, dtSearch, to perform all indexed searches.

Indexed Search



Index Search Options



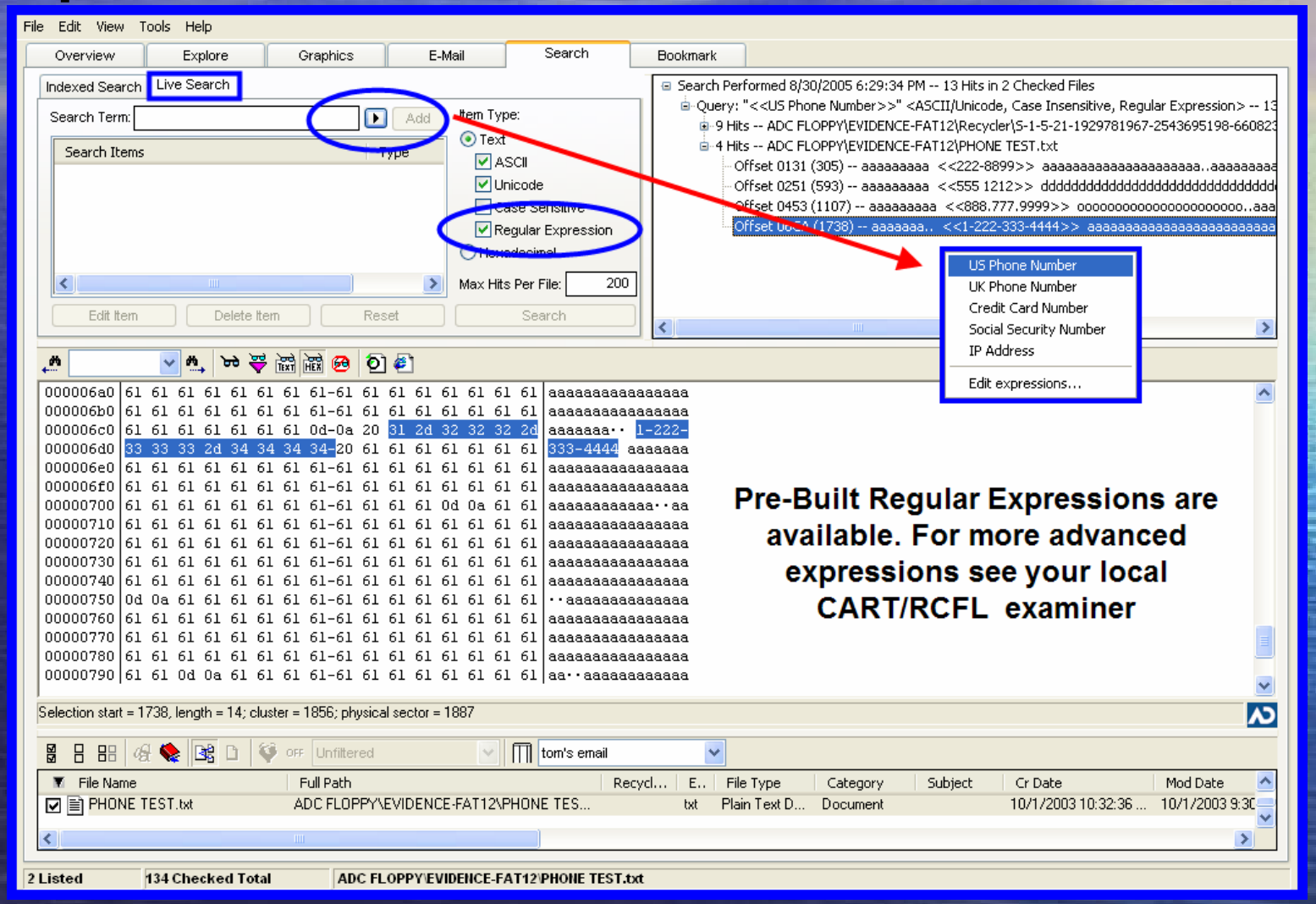
Live Searching and Regular Expressions using FTK

- You can conduct a live search to find patterns of characters. (Remember this is a time consuming process)
- Live searching allows for regular expressions, which are patterns of data such as a Credit Card number or Social Security number.

Live Searching and Regular Expressions using FTK

- FTK comes with the following predefined regular expressions:
  - US Phone Number
  - UK Phone Number
  - Credit Card Number
  - Social Security Number
  - IP Address
- If needed, you can edit the expressions or even create new ones using a text editor.

Live Search using Regular Expressions



Key Word Search and File Copy - Unix

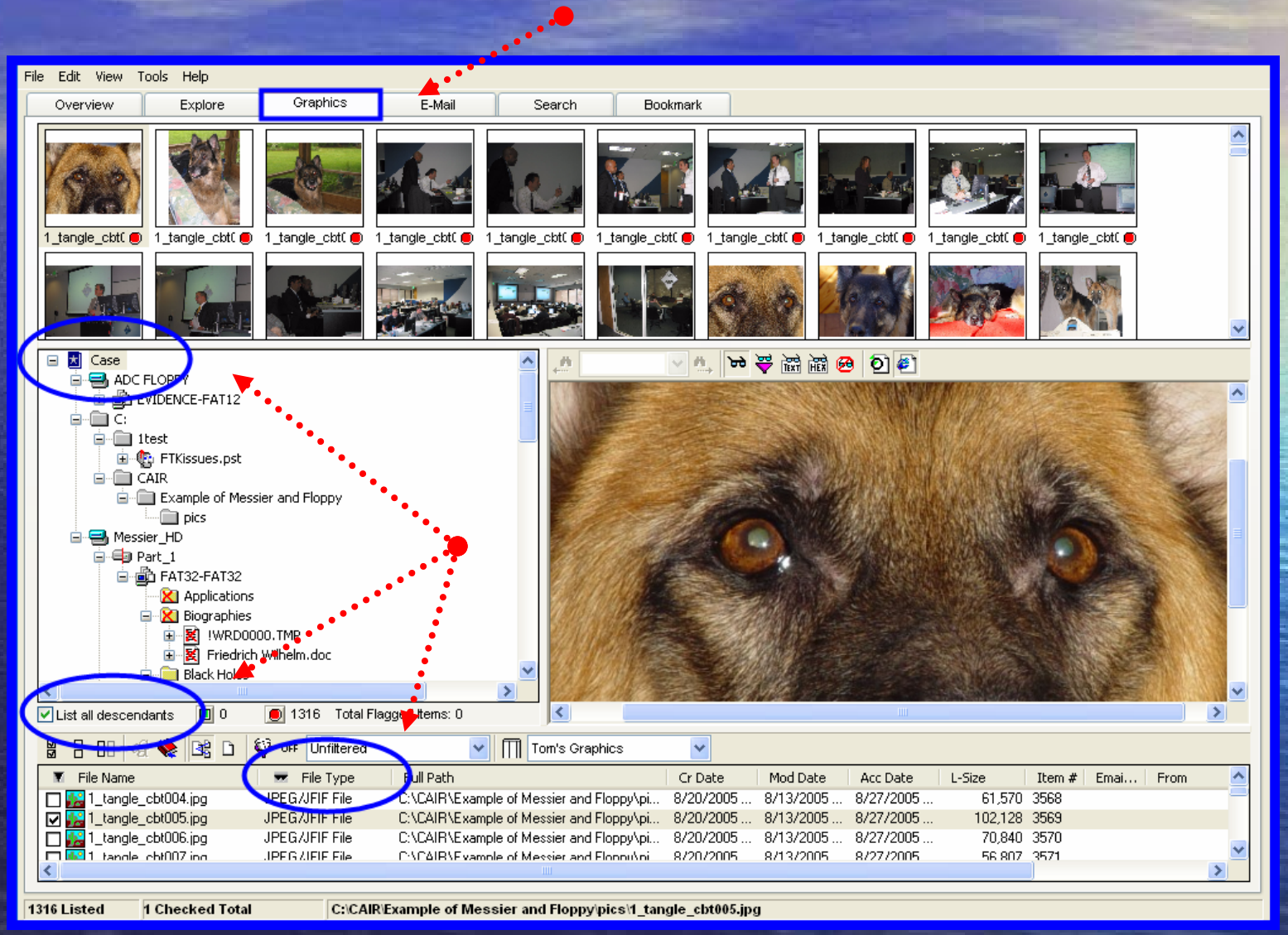
- **find -type f -exec grep -iq "My_String_or_RE" '{}' \; -print | tee output-log.txt | xargs -i cp -a --parents "{}" /My_Copy_Dir**
  - This command searches for any string of characters between “ ” and copies the files to the directory /My_Copy_dir

Searching Graphic Files

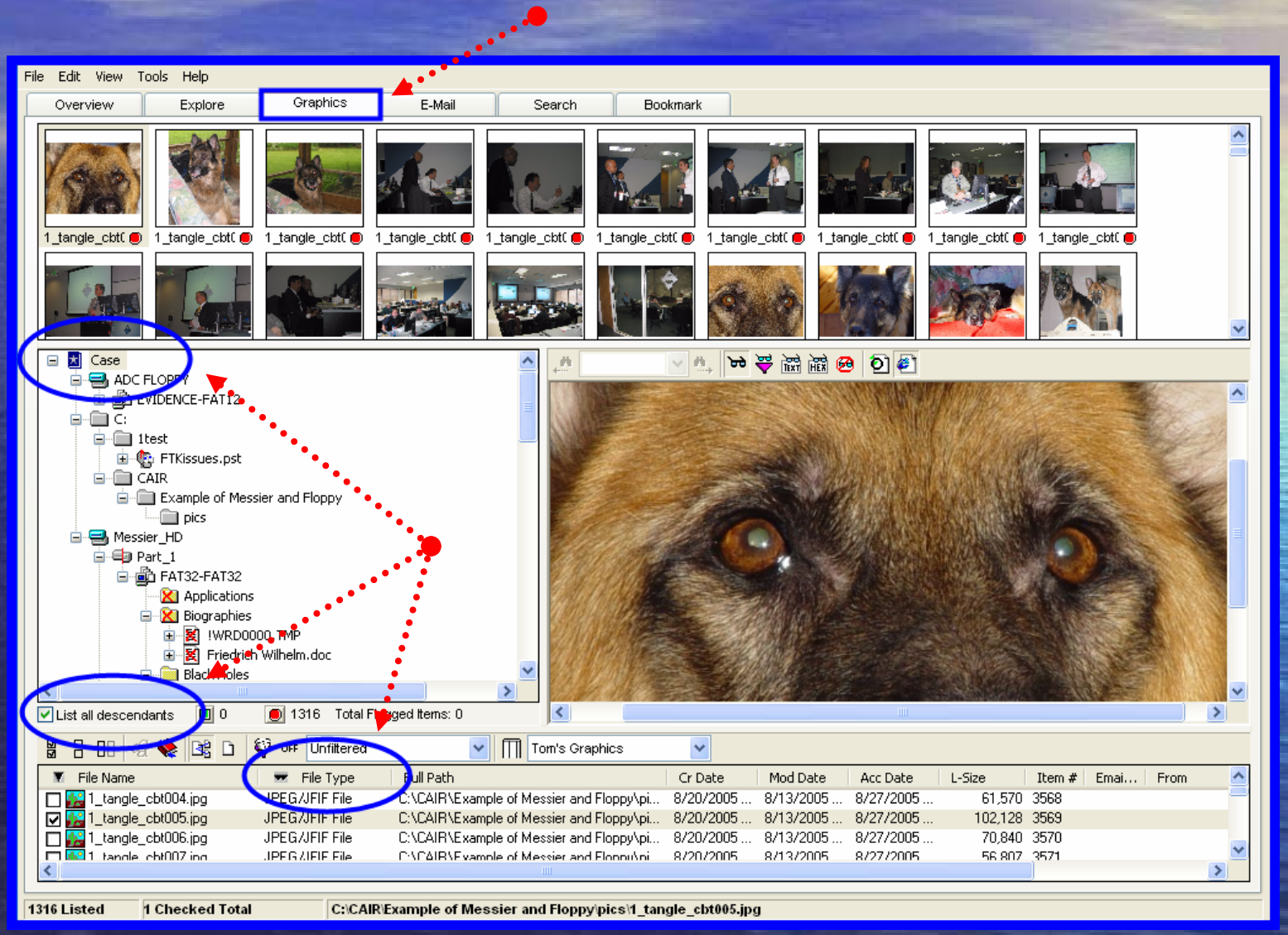
- Graphic or “picture” files are files designed specifically for representing graphical images.

- Graphic files come in different formats, the following are some common graphic formats:
  - BMP, Windows bitmap file format
  - JPEG, Joint Photo graphics Experts Group
  - PNG, Portable Network Graphic
  - TIFF, Tagged Image File Format

Graphics Viewing using FTK



Graphics Tab



Graphic Viewing Programs

- Image Scan – Free (Contact Local FBI Legat for obtaining Training and Software)
- Irfanview – Free www.irfanview.com
- Picasa – Free www.picasa.google.com
- Acdsee – Low cost www.acdsee.com

Graphics and Thumbs.db ?

- The thumbs.db file is a hidden file generated by the Windows operating system. A reduced image of a graphic or document.

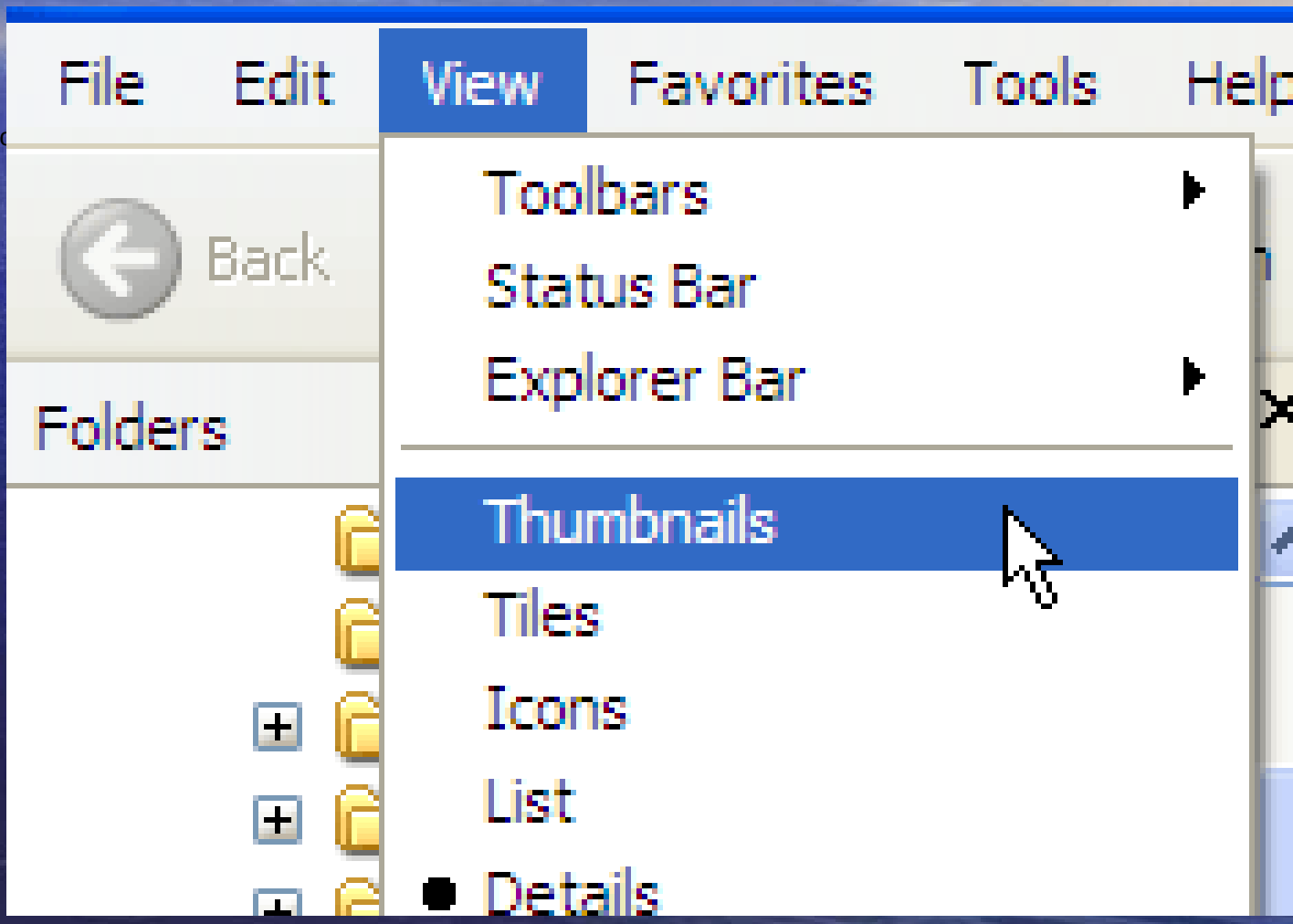
- Windows Explorer "helpfully" creates the “thumbs.db” to speed up the viewing of thumbnails on subsequent occasions.

Graphics and Thumbs.db ?

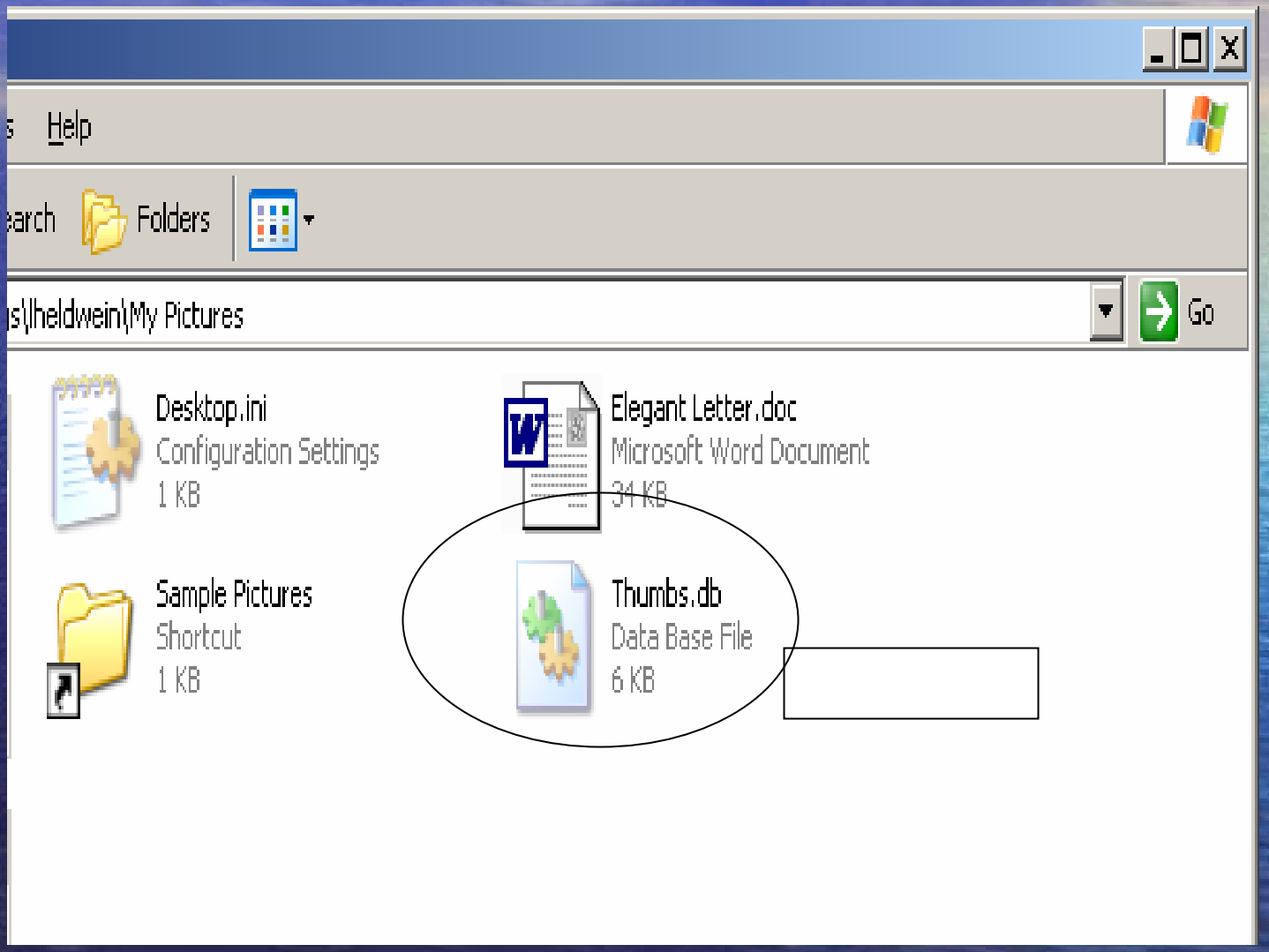
- Thumbnails are used by photo editing and graphics programs to quickly browse multiple pages of graphic picture files.
- This cache is saved so windows does not have to regenerate these thumbnail files every time somebody views the folder.

- From Windows Explorer or My Computer, click the **View** menu, **Thumbnails**, and you'll get a handy little thumbnail of each picture in the folder.

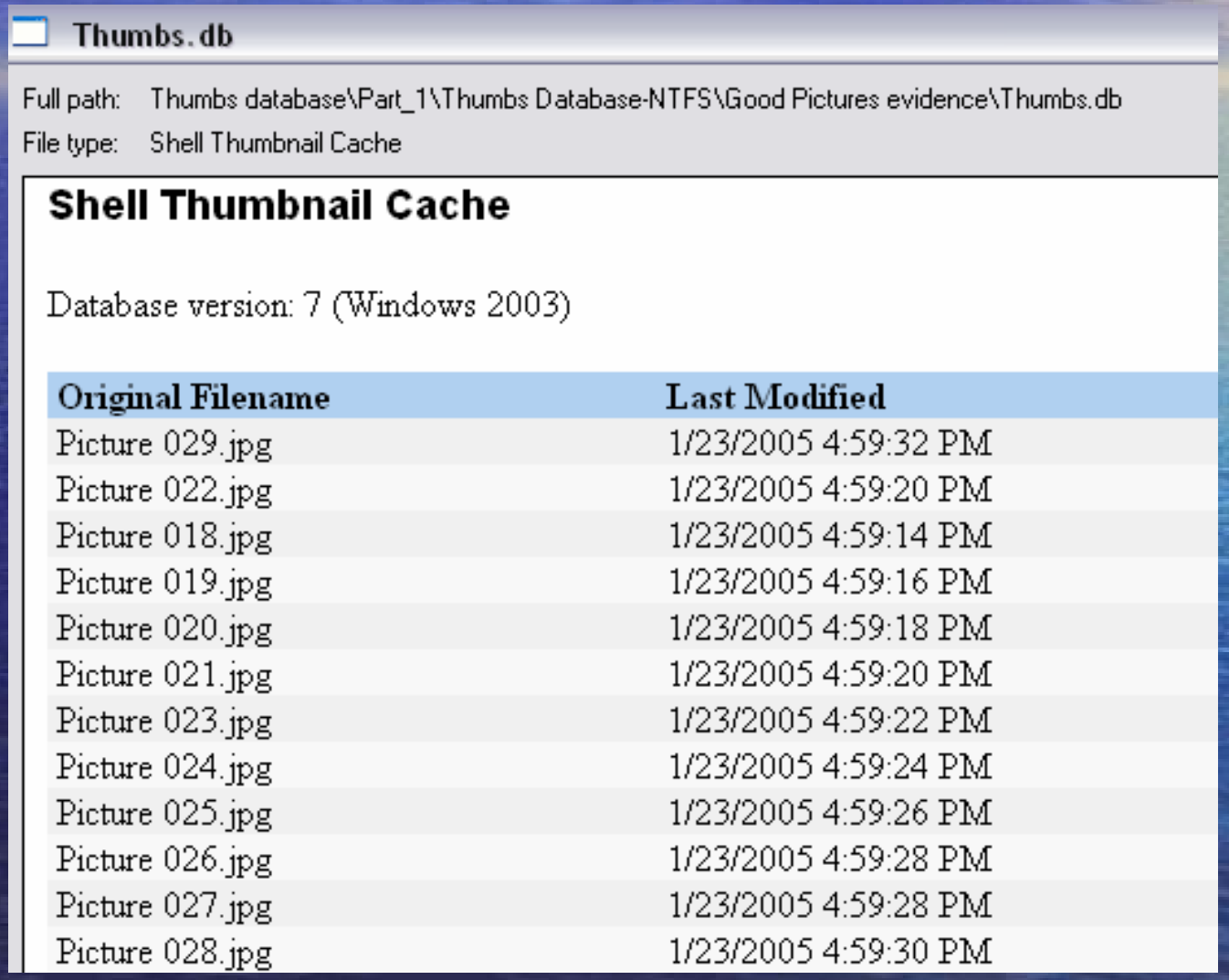
From Windows Explorer or My Co



Thumbs.db File



FTK Forensic View of 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

Other Thumbs.db Viewers

- Polyview – low cost
  - www.polybytes.com
- DHThumbs – low Cost
  - www.dmthumbs.com

Customized Linux

Boot CD-ROM / Floppy Disk

Graphic Image Preview System

Version 2.1

The History of Image Scan

- Created and Tested by FBI CART Headquarters – Unix Program
- Specifically for Child Exploitation Investigations
- A software tool for Investigators to use in the field without altering original evidence to view graphic image files.

Image Scan Objectives

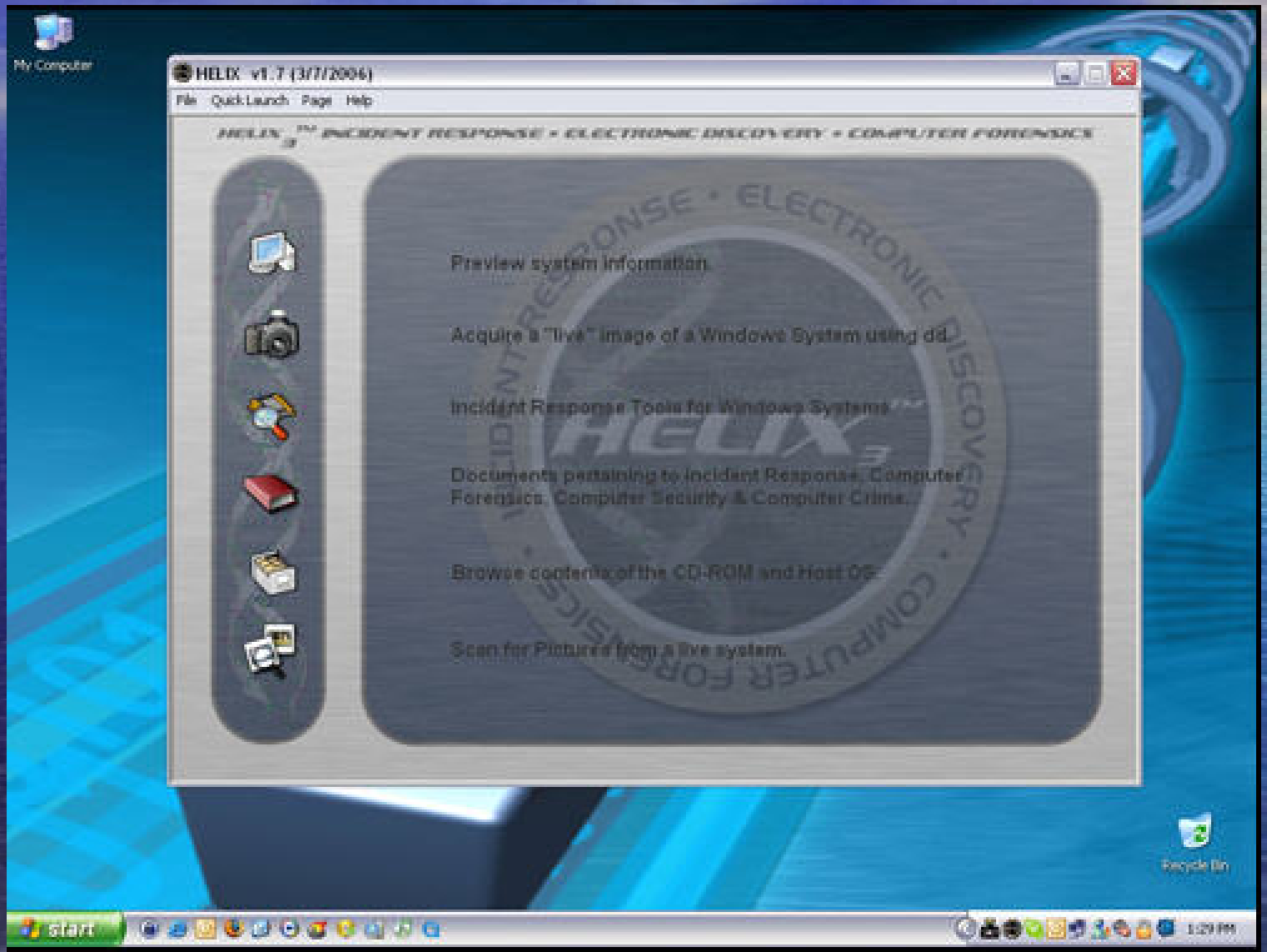
- First - To take a technically complicated system and present it in such a way that it is understandable, accurate and useful.

- Secondly - To deliver a technical resource that will dramatically assist Investigators in the field without the need for computer experts to be on scene.

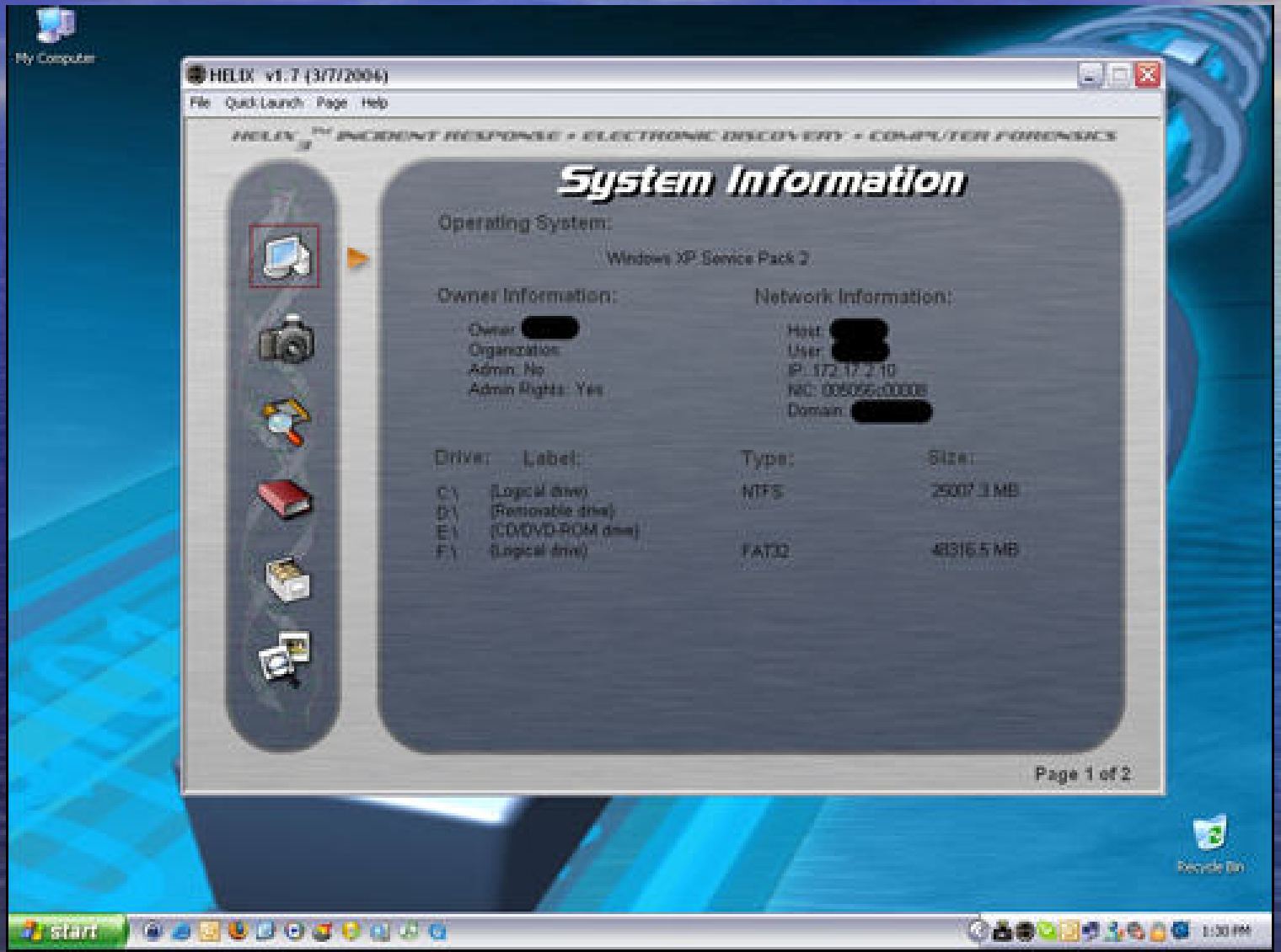
Helix – A free imaging and incident response tool

- Loads a Linux GUI into ram of subject CPU
- Does not mount drives
- Can DD to another device
- Can Review graphic files without changing dates and times, and much more
- Available from:
  - www.e-fense.com/helix

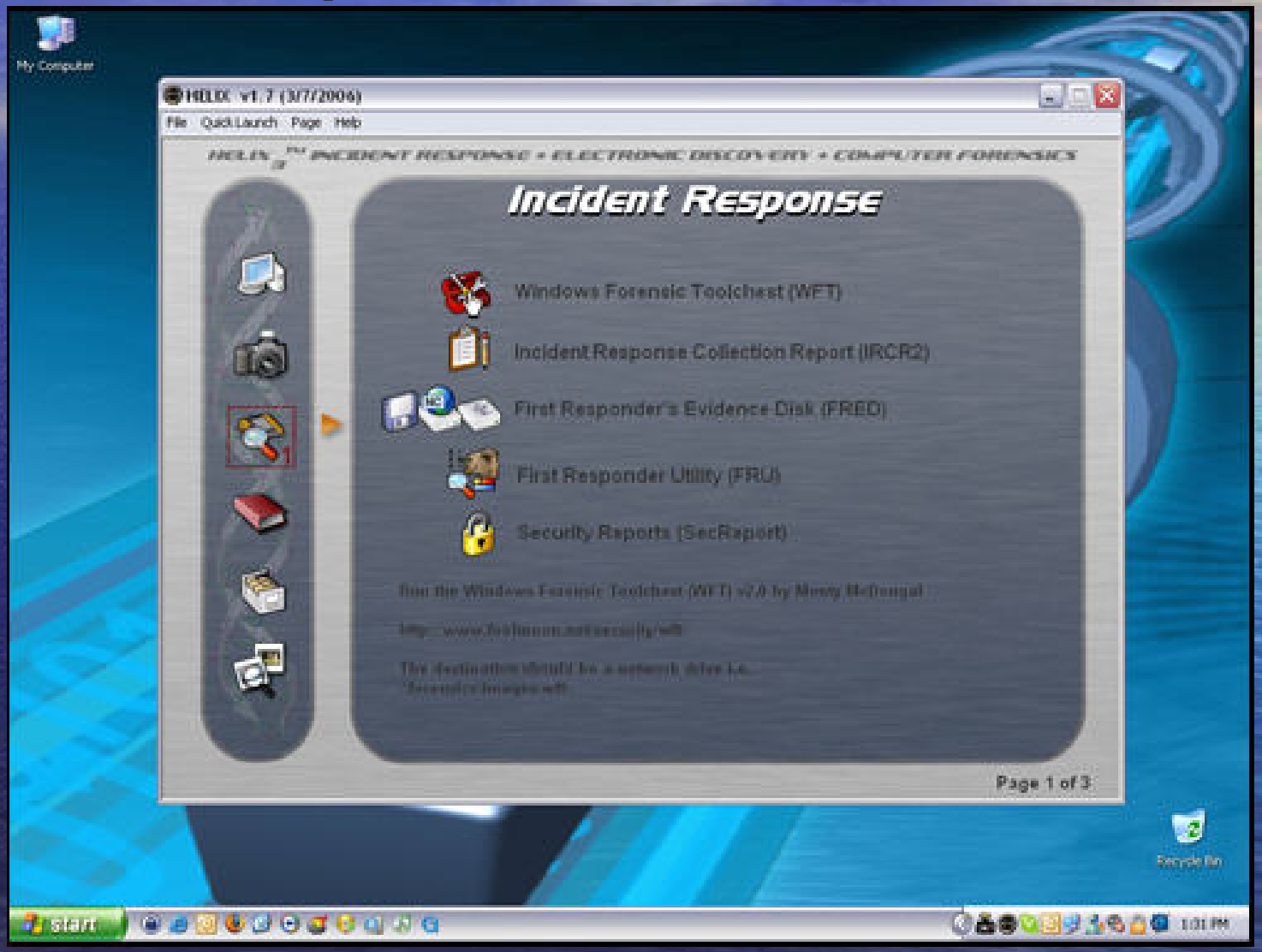
Helix - Screenshots



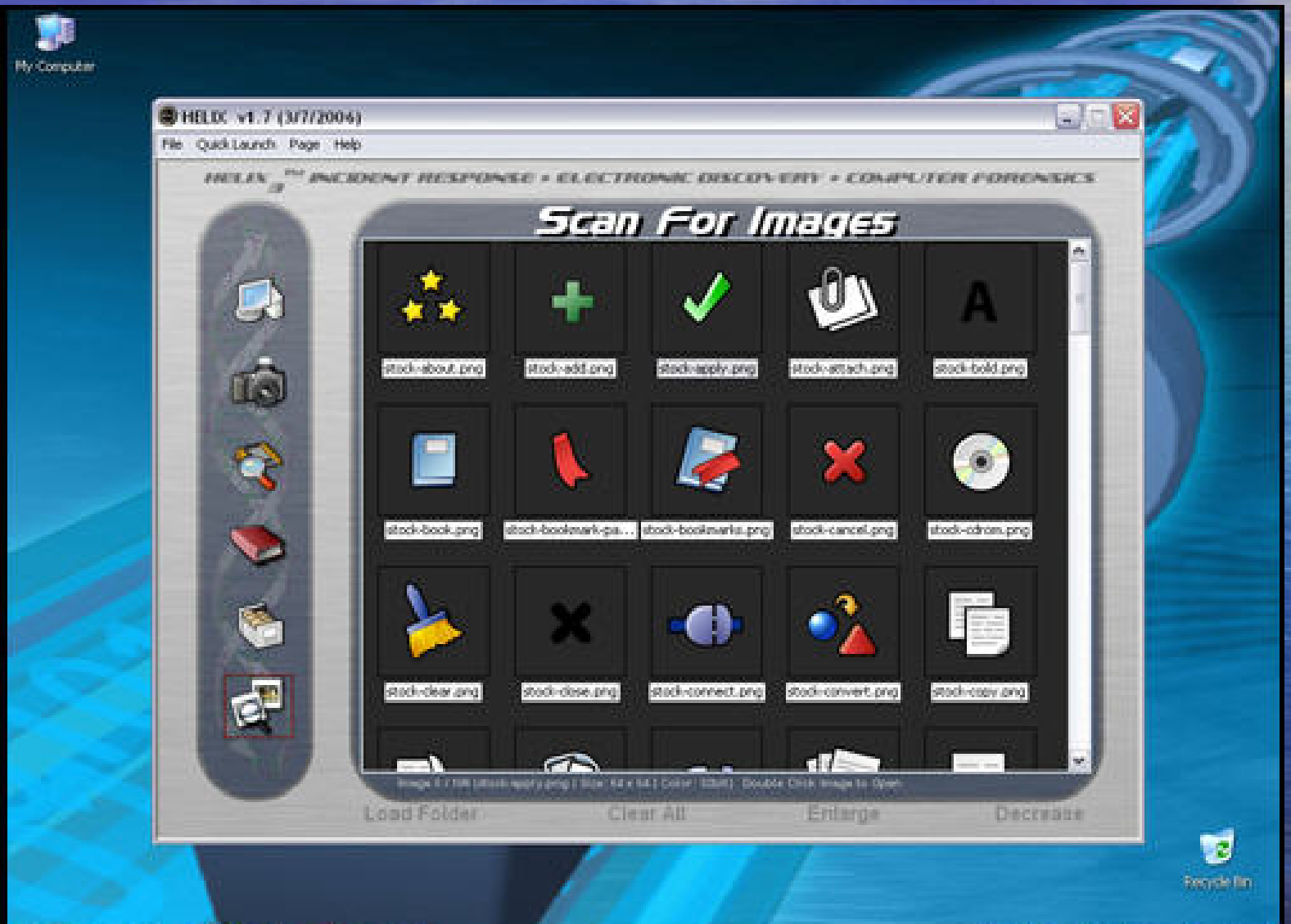
Helix Screen Shots



Helix Snapshots



Helix Snapshots



Questions

Detective/FE Reggy Chapman, FBI

Regianld.chapman@ic.fbi.gov