

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

The screenshot shows an email client interface with a search window open. The search window has a search term field containing "North Texas Regional Computer Forensic". Below this is a table of search results:

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

Below the table are buttons for "Edit Item", "Remove Item", "Remove All", and "View Item Results". The cumulative operator is set to "AND".

The search results pane on the right shows a tree view of the search results. A red dotted arrow points from the search term "North Texas Regional Computer Forensic" to the search results table, and another red dotted arrow points from the table to the search results pane.

The main email view shows the following text:

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]

The email header shows the file name "Message0083", the date "4/1/2005 1:...", and the subject "RE: FTK 1.51a". The sender is "Gregg, Rod" and the recipient is "Jessica Parry".

The status bar at the bottom shows "1 Listed", "1 Checked Total", and the current path: "C:\test\FTKIssues.pst>>Personal Folders>>Top of Personal Folders>>ftk Issues>>Message0083".

Index Search Options

Search Options

Search Broadening Options

- Stemming The query "raise" would find "raising"
- Phonic The query "raise" would find "raze"
- Synonym The query "raise" would find "lift"
- Fuzzy 1 The query "raise" would find "raize"

Search Results Options

- Max Files to List 10000
- Prompt if more
- Max Hits Per File 200
- Prompt if more

Search Limiting Options

- Created between Jan 1 2005 and Dec 31 2005
- Last Saved between Jan 1 2005 and Dec 31 2005
- File Size between 10 kilobytes and 100 kilobytes
- File Name Pattern

Show Filter Search Hits dialog for each search

Save as Permanent Defaults

Reset Cancel OK

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

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Indexed Search **Live Search**

Search Term: Add

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\5-1-5-21-1929781967-2543695198-660823
- 4 Hits -- ADC FLOPPY\EVIDENCE-FAT12\PHONE TEST.txt

Offset 0131 (305) -- aaaaaaaaa <<222-8899>> aaaaaaaaaaaaaaaaaaaaaa..aaaaaaaa

Offset 0251 (593) -- aaaaaaaaa <<555 1212>> ddddddddddddddddddddddddddd

Offset 0453 (1107) -- aaaaaaaaa <<888.777.9999>> oooooooooooooooooooooo..aaa

Offset 0655 (1738) -- aaaaaaa., <<1-222-333-4444>> aaaaaaaaaaaaaaaaaaaaaa

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 aaaaaaaaaaaaaaaaaa

000006b0 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 aaaaaaaaaaaaaaaaaa

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 aaaaaa

000006e0 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 aaaaaaaaaaaaaaaaaa

000006f0 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 aaaaaaaaaaaaaaaaaa

00000700 61 61 61 61 61 61 61 61-61 61 61 61 0d 0a 61 61 aaaaaaaaaaa..aa

00000710 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 aaaaaaaaaaaaaaaaaa

00000720 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 aaaaaaaaaaaaaaaaaa

00000730 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 aaaaaaaaaaaaaaaaaa

00000740 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 aaaaaaaaaaaaaaaaaa

00000750 0d 0a 61 61 61 61 61 61 61-61 61 61 61 61 61 61 ..aaaaaaaaaaaaaaaa

00000760 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 aaaaaaaaaaaaaaaaaa

00000770 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 aaaaaaaaaaaaaaaaaa

00000780 61 61 61 61 61 61 61 61-61 61 61 61 61 61 61 aaaaaaaaaaaaaaaaaa

00000790 61 61 0d 0a 61 61 61 61-61 61 61 61 61 61 61 aa..aaaaaaaaaaaa

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

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

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

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

The screenshot displays the FTK (Forensic Toolkit) interface. The 'Graphics' tab is selected, showing a grid of image thumbnails. A red dotted line points from the title bar to the 'Graphics' tab and then to a specific image in the grid. Below the grid, a file explorer pane shows a directory structure with 'List all descendants' checked. A second red dotted line points from the file explorer to the 'Unfiltered' view button. The main preview area shows a large, detailed image of a dog's face. At the bottom, a table lists the files in the current view.

File Name	File Type	Full Path	Cr Date	Mod Date	Acc Date	L-Size	Item #	Email...	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

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 ?

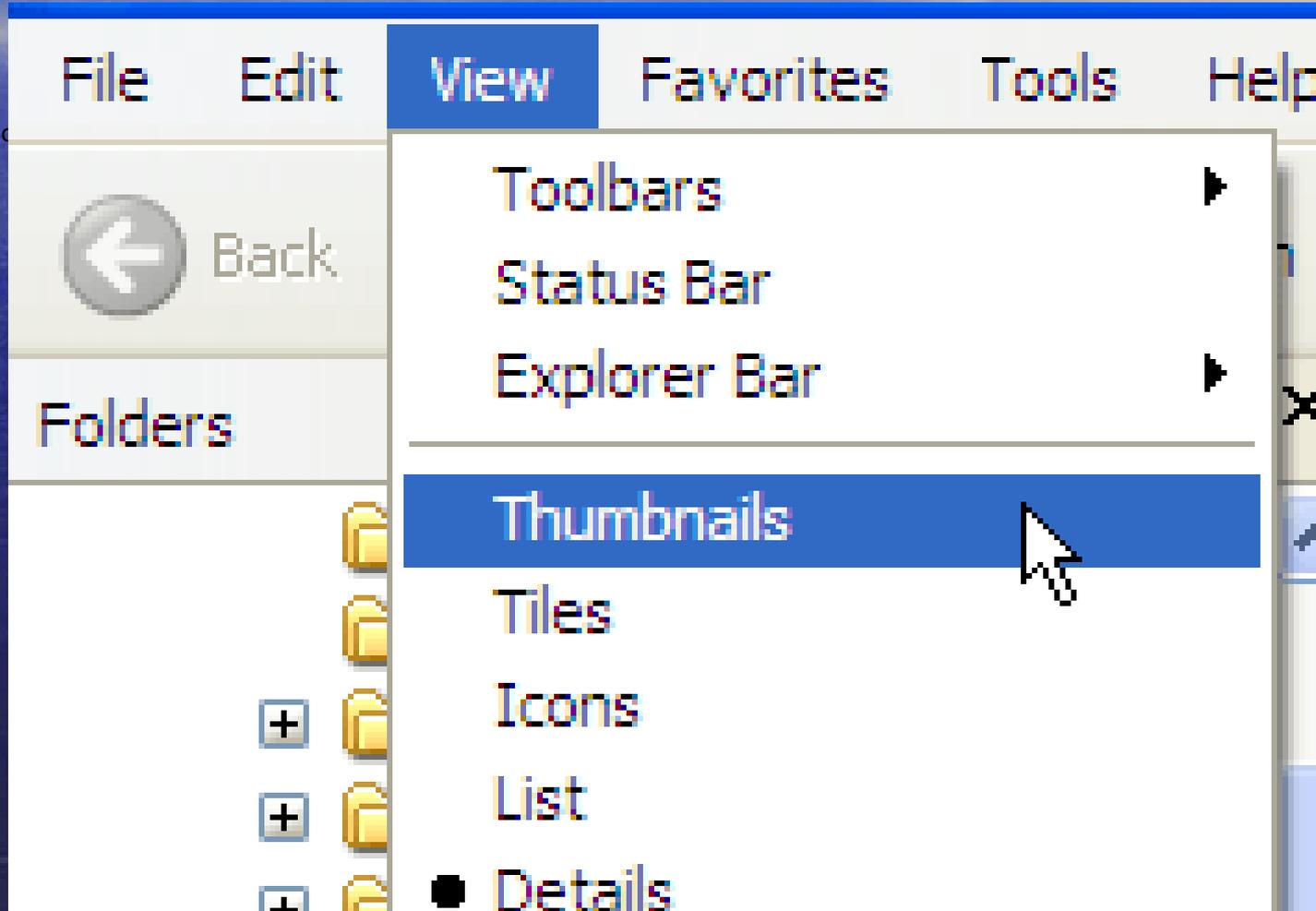
- The thumbs.db file is a hidden file generated by the Windows operating system. A reduced image of a graphic or document.
- Windows Explorer "helpfully" creates the "thumbs.db" to speed up the viewing of thumbnails on subsequent occasions.

Graphics and Thumbs.db ?

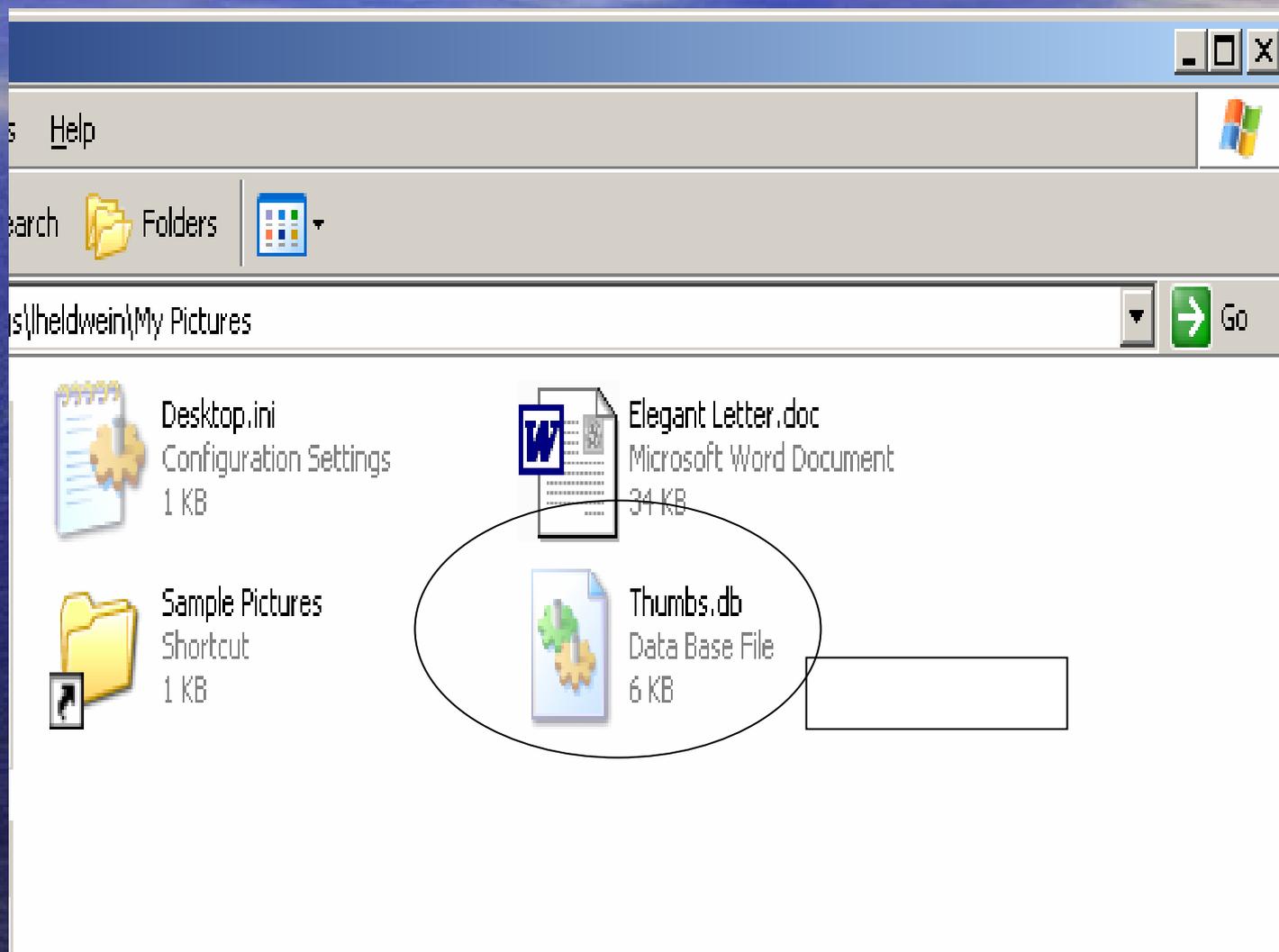
- Thumbnails are used by photo editing and graphics programs to quickly browse multiple pages of graphic picture files.
- This cache is saved so windows does not have to regenerate these thumbnail files every time somebody views the folder.

- 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 Computer



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

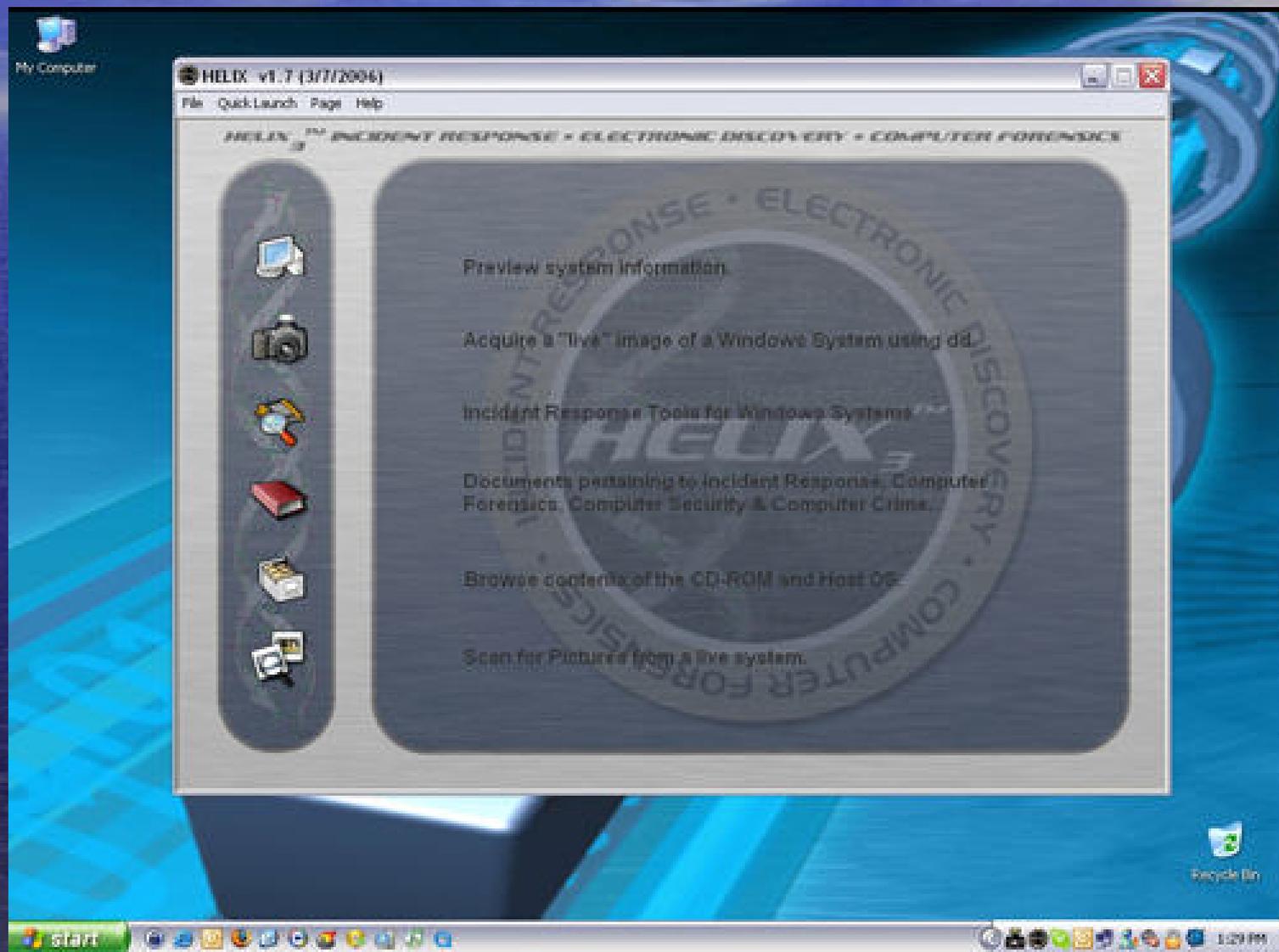
- First - To take a technically complicated system and present it in such a way that it is understandable, accurate and useful.
- Secondly - To deliver a technical resource that will dramatically assist Investigators in the field without the need for computer experts to be on scene.

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

The screenshot shows a Windows XP desktop with a blue and green abstract background. A window titled "HELIX v1.7 (3/7/2004)" is open, displaying a "System Information" report. The window has a menu bar with "File", "Quit/Launch", "Page", and "Help". The report content is as follows:

HELIX™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS

System Information

Operating System:
Windows XP Service Pack 2

Owner Information:
Owner: [REDACTED]
Organization:
Admin. No:
Admin Rights: Yes

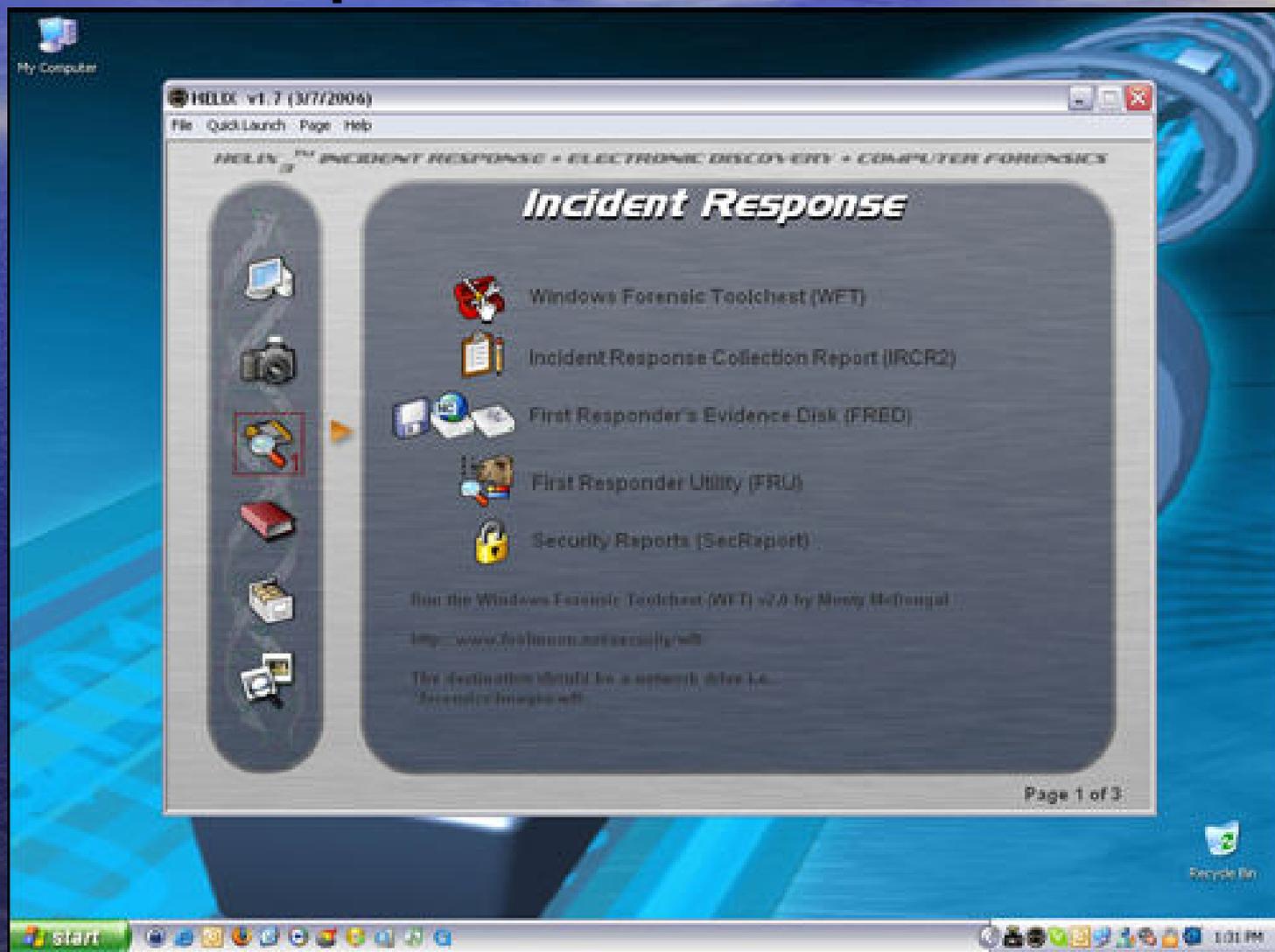
Network Information:
Host: [REDACTED]
User: [REDACTED]
IP: 172.17.2.10
MAC: 005056:00008
Domain: [REDACTED]

Drive:	Label:	Type:	Size:
C:\	Logical drive	NFS	25007.3 MB
D:\	(Removable drive)		
E:\	(CD/DVD-ROM drive)		
F:\	Logical drive	FAT32	48316.5 MB

Page 1 of 2

The desktop includes a "My Computer" icon in the top-left corner and a "Recycle Bin" icon in the bottom-right corner. The taskbar at the bottom shows the Start button, several application icons, and the system tray with the time "1:30 PM".

Helix Snapshots



Helix Snapshots



Questions

Detective/FE Reggy Chapman, FBI

RegianId.chapman@ic.fbi.gov