

File Hound

A Law Enforcement First Response Tool

Wm. Blair Gillam & Marc Rogers
DFRWS 2005

Objectives

- Background
- Program Goals
- Program Design & Features
- Results
- Future Roadmap

Background

- Most “First Responder” software relates to Incident Response.
- First Responder Software
 - Designed for Law Enforcement First Responders
 - Fulfills a small set of functions
- Encase and FTK
 - Case Management

Background (cont.)

- NIJ Study (March 2001)
 - Electronic Crime Needs Assessment for State and Local Law Enforcement
- Most law enforcement agencies do not have the resources (people & money)
- Software was needed for the summer NW3C Conference @ Purdue

What is File Hound?

- “Field Analysis Software”
 - Custom software developed at Purdue
 - Designed for Law Enforcement First Responders
 - VB.NET (due to time and client requirements)
- Free and supported for law enforcement
 - 18+ agencies use it
 - 14+ CP cases & 1 tax fraud

FH Goals

- Create an affordable (i.e. free) package that...
 - Search hard drive for images
 - Identify images relevant to investigation
 - Generate a report of the results
 - Minimal training for user
 - Work with hardware write blockers

FH Design

- Modular Program Structure
 - Search
 - Identification
 - Reporting

Search

Identify

Report

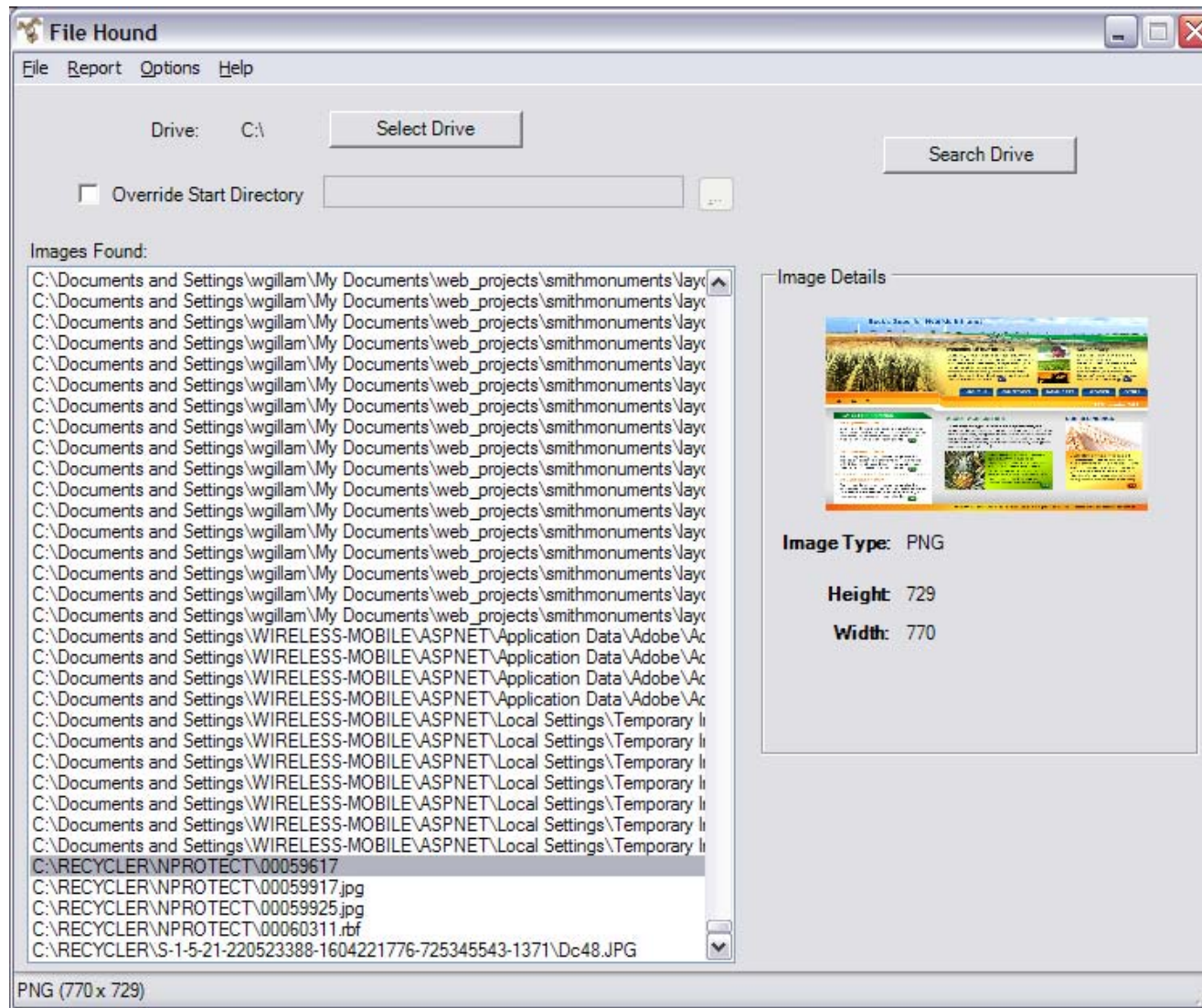
Search

- Recursive directory search
- Search for images based on header information
 - Examples: PNG, GIF, JPG, TIF, WMF, BMP
- Search filenames for a pattern
 - Examples: *.xls (Excel Documents)
 *.doc (Word Documents)

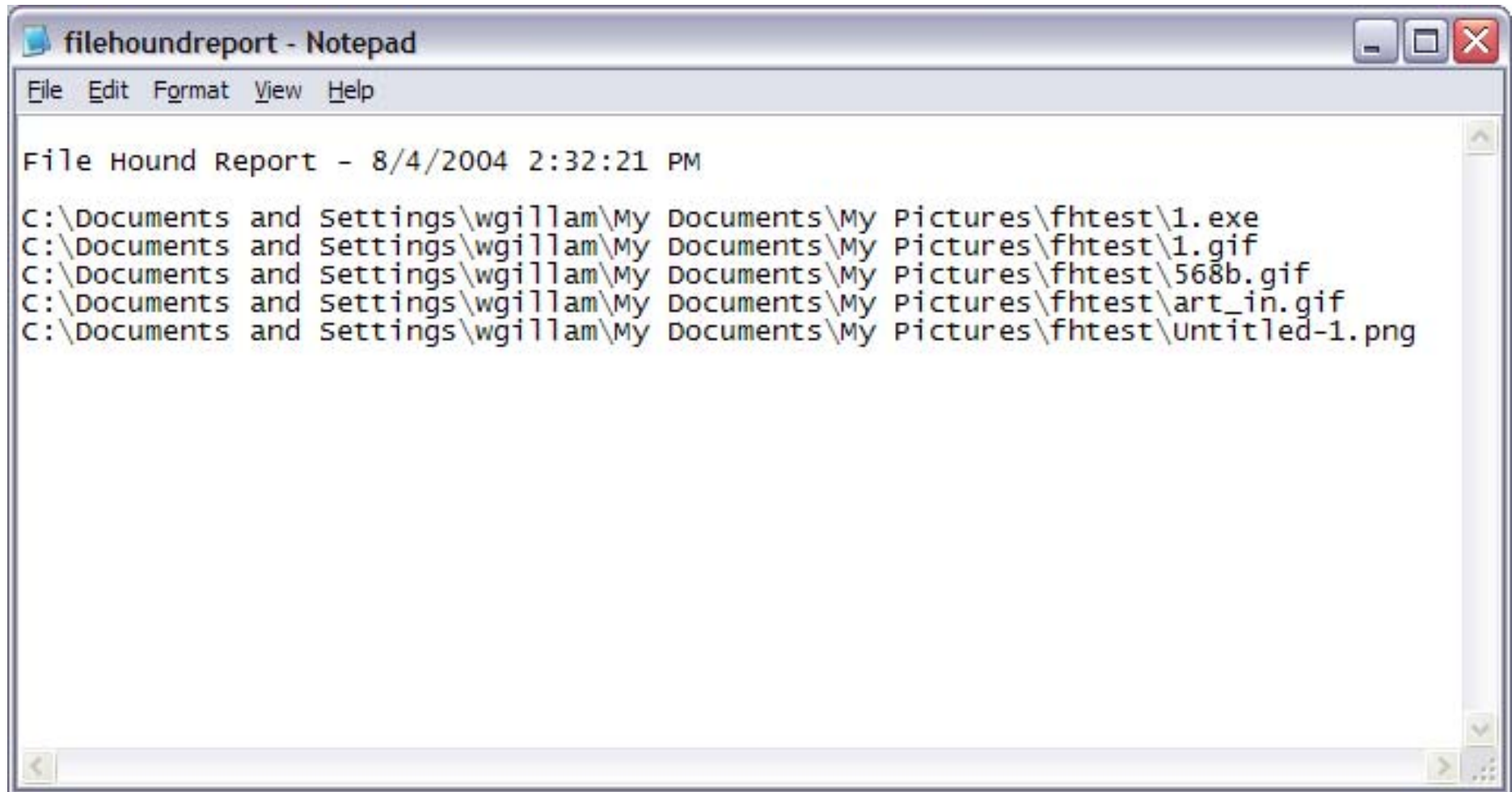
Identify & Report

- View image thumbnails
- Select images for further investigation
- Report should include:
 - Logical path
 - Thumbnail image*
 - Modified, Accessed, & Created times*
 - MD-5/SHA-X hash*

File Hound v1



File Hound v1 - Report



```
filehoundreport - Notepad
File Edit Format View Help

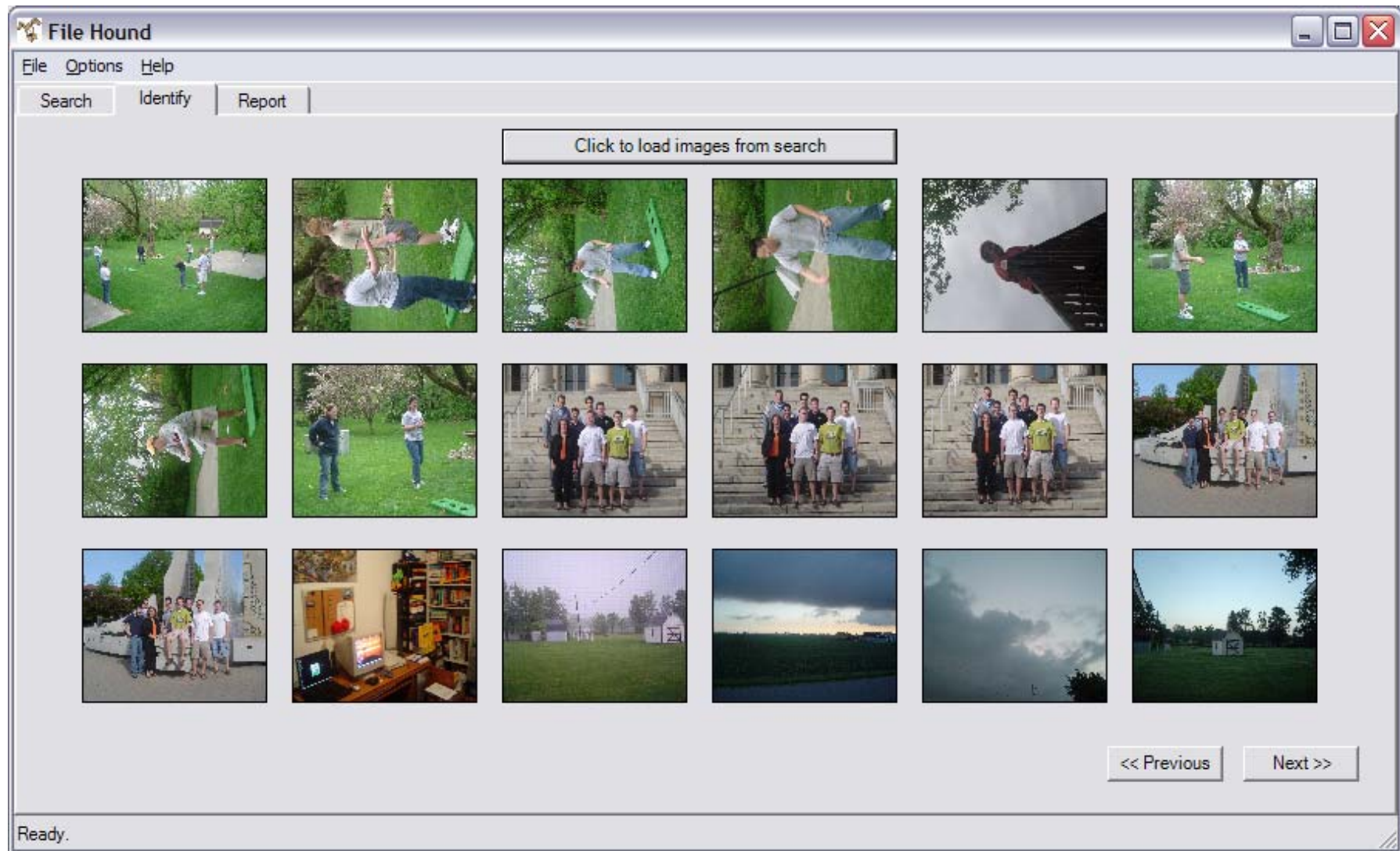
File Hound Report - 8/4/2004 2:32:21 PM

C:\Documents and Settings\wgillam\My Documents\My Pictures\fhtest\1.exe
C:\Documents and Settings\wgillam\My Documents\My Pictures\fhtest\1.gif
C:\Documents and Settings\wgillam\My Documents\My Pictures\fhtest\568b.gif
C:\Documents and Settings\wgillam\My Documents\My Pictures\fhtest\art_in.gif
C:\Documents and Settings\wgillam\My Documents\My Pictures\fhtest\Untitled-1.png
```

FH v1 Results

- Released at the NW3C Training Conference at Purdue (August 2004)
- Heard from the people requesting the program
- 13 feature requests
 - Cancel if you have seen enough
 - View 8+ thumbnails at once
 - Report
 - MAC Times
 - MD-5/SHA-X hash
 - Print thumbnail on report

File Hound v2 - Prototype



File Hound v3 - Search

File Hound
File Options Help

Search Identify Report

Search type:
☒ Image Search
☐ Filename Search

All or part of the file name:

Look In:

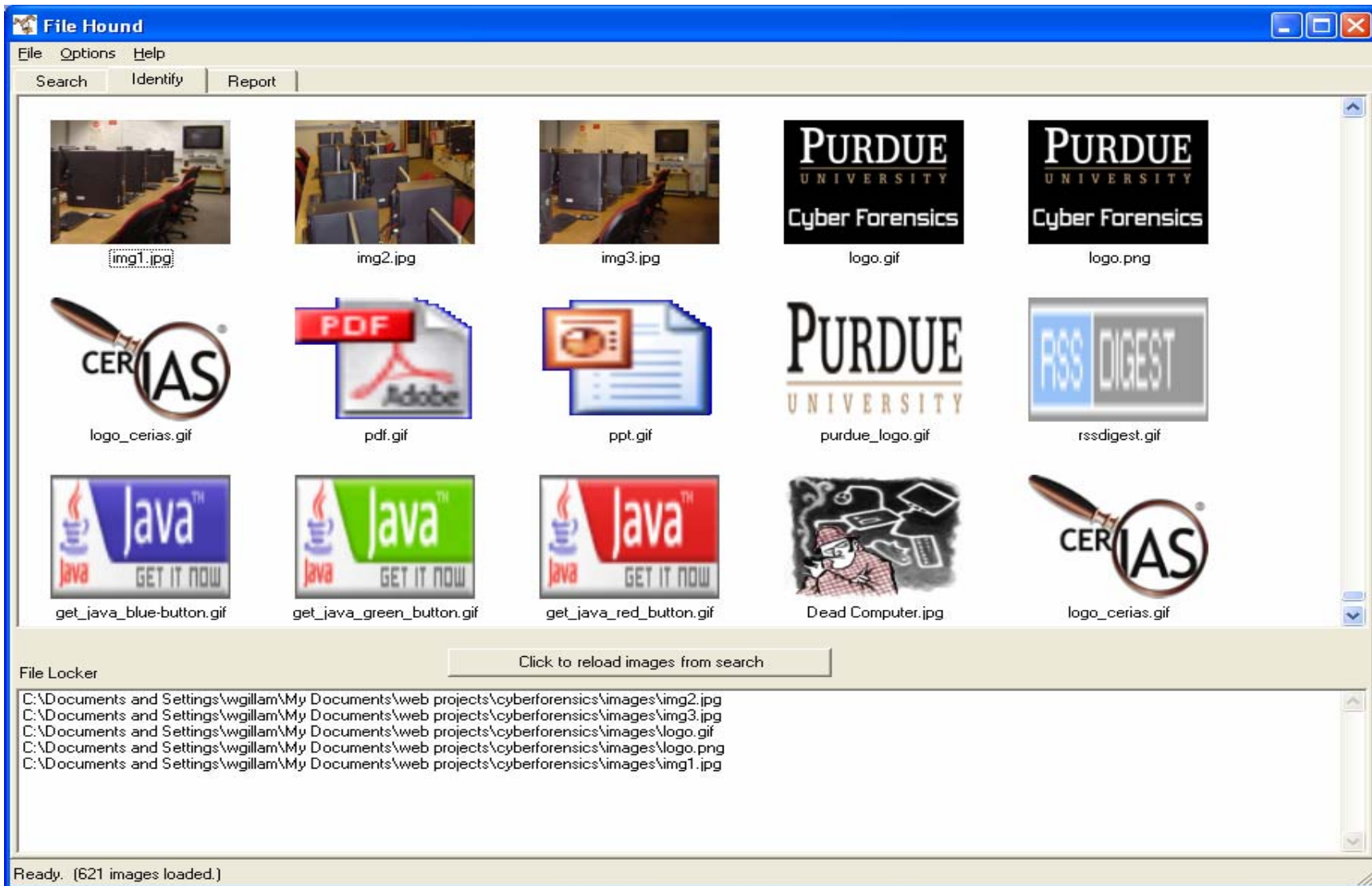
Search

621 images found.

Name	In Folder	Size	Date Modified
links_32.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	868	9/21/2003 2:30:00 PM
LowPriority_16.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	544	9/20/2003 7:10:00 PM
LowPriority_32.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	781	9/20/2003 7:09:00 PM
Messenger_16.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	651	9/20/2003 6:27:00 PM
Messenger_32.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	1243	9/20/2003 6:26:00 PM
NormalPriority_16.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	651	9/20/2003 7:18:00 PM
NormalPriority_16_ver2.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	550	9/20/2003 7:18:00 PM
NormalPriority_32.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	1059	9/20/2003 7:17:00 PM
NormalPriority_32_ver2.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	805	9/20/2003 7:18:00 PM
OtherType_16.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	653	9/20/2003 6:37:00 PM
OtherType_32.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	1024	9/20/2003 6:37:00 PM
tools_16.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	378	9/21/2003 2:36:00 PM
tools_32.gif	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\Tracker\Tracker	784	9/21/2003 2:36:00 PM
App.ico	C:\Documents and Settings\wgillam\My Documents\Visual Studio Projects\WindowsAp...	1078	6/25/2004 12:44:00 PM
design1.png	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	132539	12/27/2004 9:46:48 PM
design1_r1_c1.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	2565	12/27/2004 9:46:47 PM
design1_r2_c1.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	888	12/27/2004 9:46:47 PM
design1_r2_c3.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	1211	12/27/2004 9:46:47 PM
design1_r3_c1.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	507	12/27/2004 9:46:47 PM
design1_r3_c2.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	9378	12/27/2004 9:46:47 PM
design1_r4_c1.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	472	12/27/2004 9:46:48 PM
design1_r5_c2.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	273	12/27/2004 9:49:23 PM
design1_r5_c4.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	191	12/27/2004 9:46:48 PM
design1_r6_c1.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	688	12/27/2004 9:46:48 PM
design1_r7_c2.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	737	12/27/2004 9:46:48 PM
design1_r8_c1.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	408	12/27/2004 9:46:48 PM
design1_r9_c1.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	4389	12/27/2004 9:46:48 PM
spacer.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\desig...	43	12/27/2004 9:46:47 PM
gov.jpg	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\home...	109214	2/23/2005 10:05:46 AM
bkgrd1.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	92	1/5/2005 10:21:38 PM
bkgrd2.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	92	1/5/2005 10:22:02 PM
img1.jpg	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	9824	1/5/2005 10:31:19 PM
img2.jpg	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	11150	1/5/2005 10:31:41 PM
img3.jpg	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	9169	1/5/2005 10:32:05 PM
logo.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	3934	1/6/2005 8:14:10 PM
logo.png	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	44349	1/6/2005 8:21:39 PM
logo_ceris.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	3334	12/22/2004 10:08:35 PM
pdf.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	1106	1/6/2005 7:51:37 PM
ppt.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	1034	1/6/2005 7:52:37 PM
purdue_logo.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	2961	12/22/2004 10:08:34 PM
rssdigest.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	207	1/12/2005 9:13:46 PM
get_java_blue-button.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	3144	6/3/2003 1:58:08 PM
get_java_green-button.gif	C:\Documents and Settings\wgillam\My Documents\web projects\cyberforensics\image...	3208	6/3/2003 1:58:08 PM

Ready. [621 images loaded.]

File Hound v3 - Identify



File Hound v3 - Report

File Hound

File Options Help

Search Identify Report

Report Options

Report Title:
File Hound Report

Examiner's Name:
Blair Gillam

Case # (optional):
2005-TEST-12345

Other Options

☒ Show thumbnail (if exists)
☐ Show file hash
☐ Show Exif Info (if exists)


Preview 1st Page

Print Preview


Examiner: Blair Gillam

File Hound Report


Case #: 2005-TEST-12345




C:\Documents and Settings\William\My Documents\web projects\cyberforensics\images\img2.jpg




C:\Documents and Settings\William\My Documents\web projects\cyberforensics\images\img3.jpg



C:\Documents and Settings\William\My Documents\web projects\cyberforensics\images\logo.gif



C:\Documents and Settings\William\My Documents\web projects\cyberforensics\images\logo.png



C:\Documents and Settings\William\My Documents\web projects\cyberforensics\images\img1.jpg

3/5/2005 12:53:00 PM

Page 1

Ready. (621 images loaded.)

First Responder Equipment

- Suspect's Hard Drive
- Hardware Write Blocker
- Examiner's Laptop
- File Hound Software



File Hound Roadmap

- Platform independent
- Timeline Viewer
- Hash comparisons
- Skin Color Analysis Algorithm
 - Michael Hoeschele

Future Research

- Skin Color Analysis Algorithm (SCAA)
 - Detect flesh tones
 - Sort based on temporal data
 - Issues
 - Ethnic Diversity
 - Limiting scope?

Questions?

Contact Information

Wm. Blair Gillam

wgillam@purdue.edu

Marc Rogers

mkr@cerias.purdue.edu