iRecover V1.0

File Recovery Tool

Prepared By:

ANDREW BELL. HASSAN ALSAFFAR . LEONARDO RUBIO

WHAT ?

- **iRecover** – provides a GUI interface using the Perl/Tk programming library for forensics examiners to use when retrieving deleted files from an image/ file partition under forensic investigation.

- Investigators can use this tool to selectively retrieve only certain kinds of files (text, images, video, audio, documents, etc.)

- iRecover offers support for images with FAT, NTFS, and EXT2/3 file systems.

W H Y ?

- **More Information in a VERY Short Time.**
  - retrieved information includes filename, location, and certain metadata attributes such as file size and time of last modification.

- **Efficient and Effective Recovery Process.**
  - The user can also choose to retrieve only a subset of the discovered items for a given filetype. Rather than retrieving all of them which could waste some space on disk especially if some of the uninteresting files are excessively large in terms of file size.

HOW ?

- **The standard procedure for operating our tool is to:**

1. Select an image to process determine what like to retrieve a specific catego ry of files (only 1 category as of# version 1.0) holding certain file types or all of the files on the image.
2. After clicking the "find" button, the tool will go into the image and using a wide variety of sleuth kit tools (***mmls, sorter, fls, istat***) gather information a nd metadata on all the files that match the desired file type being searched for.
3. Explore the findings (It is possible to sort, resize, and# move around these columns by clicking on the column headers and borders between each column).
4. For recovering the files, simply click on the files of interest (default is ALL fil es are selected) and then hit the "Recover" button. Recovery is done via a sleuth kit command, ***icat***.

D E M O


iRecover - File Recovery Tool
iRECOVER
File Recovery Tool V.1.0
File Type
All
Image to Search
Open
"/root/Desktop/toolProject/fat12.dd"
Clear
Find
File(s) Found
File Name | File Size (in KB) | File Path | Last Modified Time | Description
ile1.doc | 0 | /root | Tue, 16 Dec 2003 @ 21:02:28 | no read permission
older1/_ile11.txt | 25 | /root | Tue, 16 Dec 2003 @ 21:03:52 | ASCII text, with no line terminators
older1/Copy of file2.txt | 25 | /root | Tue, 16 Dec 2003 @ 21:03:52 | ASCII text, with no line terminators
older1/Copy of Copy of | 25 | /root | Tue, 16 Dec 2003 @ 21:03:52 | ASCII text, with no line terminators
older1/Copy (2) of file2. | 25 | /root | Tue, 16 Dec 2003 @ 21:03:52 | ASCII text, with no line terminators
older1/RIT-logo.gif | 2053 | /root | Tue, 16 Dec 2003 @ 21:09:36 | GIF image data, version 89a, 282 x 88
MALLP~1.JPG | 4066 | /root/$OrphanFiles/ | Tue, 16 Dec 2003 @ 21:09:46 | JPEG image data, JFIF standard 1.02
ile8.txt | 25 | /root/$OrphanFiles/ | Tue, 16 Dec 2003 @ 21:03:52 | ASCII text, with no line terminators
ile9.txt | 25 | /root/$OrphanFiles/ | Tue, 16 Dec 2003 @ 21:03:52 | ASCII text, with no line terminators
ile10.txt | 25 | /root/$OrphanFiles/ | Tue, 16 Dec 2003 @ 21:03:52 | ASCII text, with no line terminators
♣ | 2053 | /root | Tue, 16 Dec 2003 @ 21:09:36 | GIF image data, version 89a, 282 x 88
♣ | 4066 | /root | Tue, 16 Dec 2003 @ 21:09:46 | JPEG image data, JFIF standard 1.02
Clear Results
Recover

Any Questions