



CyberScience Laboratory Functional Analysis
of

DataLifter v 2.0

(Build 189)

CyberScience Laboratory

November 2004

**Prepared By:
CyberScience Laboratory
Rome, New York 13441-4114
315.838.7000**

www.cybersciencelab.com

DISCLAIMER

This report was prepared for the United States Government by the CyberScience Laboratory (CSL).

With respect to information provided in this document, neither the United States Government, nor any of its employees, nor the CSL, nor any of its employees makes any warranty, expressed or implied, including, but not limited to, the warranties of merchantability and fitness for a particular purpose. Further, neither the United States Government, nor any of its employees, nor the CSL, nor any of its employees, assumes any legal liability for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the CSL. The information and statements contained in this document shall not be used for the purpose of advertising, or to imply the endorsement or recommendation of the United States Government or the CSL.

Acknowledgment:

This study was sponsored by the National Institute of Justice. The National Institute of Justice is a component of the Office of Justice Programs. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice.



TABLE OF CONTENTS

| | | |
|----------|---|----|
| 1 | OVERVIEW | 1 |
| 2 | METHODOLOGY..... | 2 |
| 2.1 | File Systems Tested | 2 |
| 2.2 | Functional Analysis..... | 2 |
| 2.3 | Hardware Used..... | 2 |
| 2.4 | Software Used | 2 |
| 2.5 | Using DataLifter..... | 3 |
| 3 | TESTING RESULTS..... | 12 |
| 3.1 | Active Reports..... | 12 |
| 3.2 | Recycle Bin History | 12 |
| 3.3 | Internet History | 14 |
| 3.4 | Disk2File | 16 |
| 3.5 | Image Linker | 18 |
| 3.6 | File Signature Generator | 19 |
| 3.7 | File Extractor..... | 20 |
| 3.8 | Email Retriever | 22 |
| 3.9 | Ping/Trace Route/Whois | 23 |
| 4 | CONCLUSION | 26 |
| 5 | APPENDIX A – SAMPLE ACTIVE REPORTS OUTPUT | 27 |



FIGURES

| | |
|------------------|----|
| Figure 1-1 | 1 |
| Figure 2-1 | 3 |
| Figure 2-2 | 4 |
| Figure 2-3 | 5 |
| Figure 2-4 | 6 |
| Figure 2-5 | 7 |
| Figure 2-6 | 8 |
| Figure 2-7 | 9 |
| Figure 2-8 | 10 |
| Figure 2-9 | 11 |
| Figure 3-1 | 17 |

TABLES

| | |
|------------------|----|
| Table 3-1 | 13 |
| Table 3-2 | 15 |
| Table 3-3 | 15 |
| Table 3-4 | 17 |
| Table 3-5 | 18 |
| Table 3-6 | 19 |
| Table 3-7 | 20 |
| Table 3-8 | 21 |
| Table 3-9 | 23 |
| Table 3-10 | 24 |
| Table 3-11 | 24 |
| Table 3-12 | 24 |



1 OVERVIEW

In the world of computer forensics, there is a vast array of computer forensic software suites that provide investigators with tools to make their job easier. Such is the aim with the software suite known as DataLifter. DataLifter v2.0 includes 10 tools that are designed to assist with computer forensics, information auditing, information security and data recovery. These tools include a recycle bin viewer, an Internet history viewer, a screen capture tool, a file extractor, a directory viewer, an image extractor, a file signature generator, an email retriever, and a network tool. Along with those tools, DataLifter comes with the ability to monitor the program usage with a tool called Active Reports.

The DataLifter forensic tool suite was created by Data Lifter and is available for \$140.00 from <http://www.datalifter.com>.

Figure 1-1 presents a screenshot of the main operating window of DataLifter.

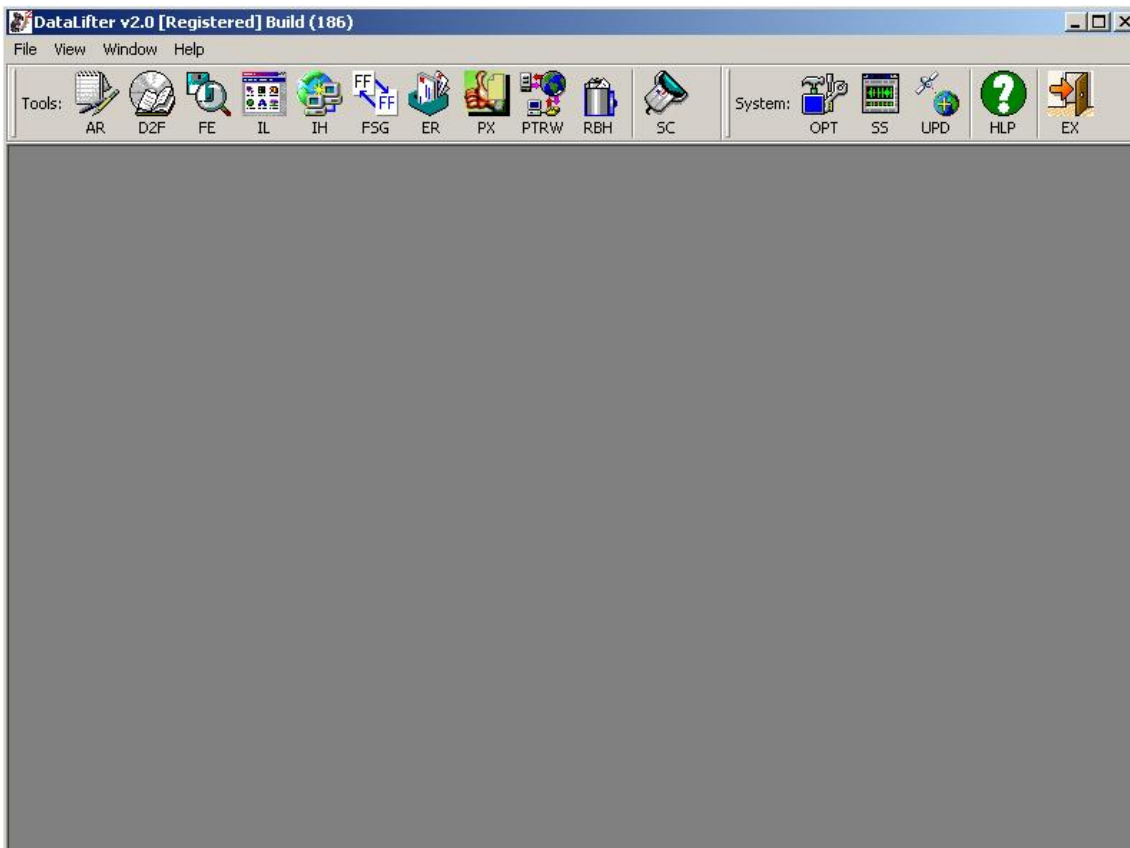


Figure 1-1

2 METHODOLOGY

2.1 File Systems Tested

- NTFS Version 3.0
- FAT 32

2.2 Functional Analysis

This functional analysis will assess DataLifter's ability to:

- Explore the recycle bin INFO2 file on a suspect drive.
- Retrieve email saved on a suspect drive.
- View the Internet activity on a suspect drive.
- Use ping, trace route, and WHOIS to query IP addresses and websites.
- Generate file signatures.
- Generate a list of files and file information on the entire suspect drive. File information includes
- Extract files from file slack space and unallocated space.
- Create an HTML listing of image thumbnails.

2.3 Hardware Used

- Forensic Recovery of Evidence Device (FRED) Sr. Workstation
 - Windows 2000 Build 5.00.2195 with Service Pack 4
 - AMD Athlon XP 2200+
 - 1GB RAM
 - Western Digital Caviar WD1200 120GB Hard Drive
 - Western Digital Caviar 31600 3 GB Hard Drive

2.4 Software Used

- Windows 2000 Build 5.00.2195 with Service Pack 4
- Internet Explorer 6.0 Build 2800.1106 with Service Pack 1
- DataLifter V2.0 Build 189
- FTK Imager V2.0b
- Eudora V6.1



- Pegasus Mail V4.0
- Netscape V7.2
- Microsoft Outlook Express 6.0
- Microsoft Outlook 2000 Base Install
- MS DOS Version 5.00.2195

2.5 Using DataLifter

2.5.1 Using Active Reports

After clicking on the Active Reports button from within DataLifter's main operating screen, the user sees the report generated by Active Reports, along with several options presented to them. Figure 2-1 shows the main Active Reports operating screen.

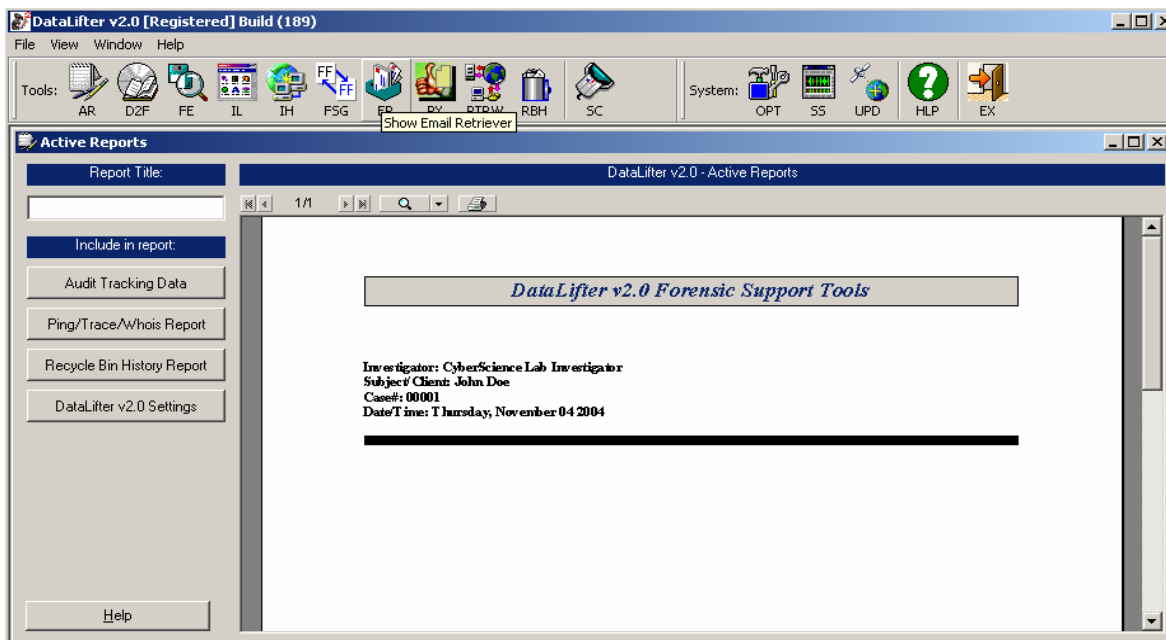


Figure 2-1

From within this screen, the user has the options of what to include in the Active Report's summary. Along with that, the user has the options to include the Ping/Trace Route/WhoIs queries, the Recycle Bin History, a report title, and the current DataLifter v2.0 settings in the summary report. Active Reports gives the user the ability to Audit the entire forensic investigation.

2.5.2 Using Recycle Bin History

Once the Recycle Bin History program is initiated from within DataLifter's main operating screen, the user is presented with the Recycle Bin History operating screen, as shown in Figure 2-2.

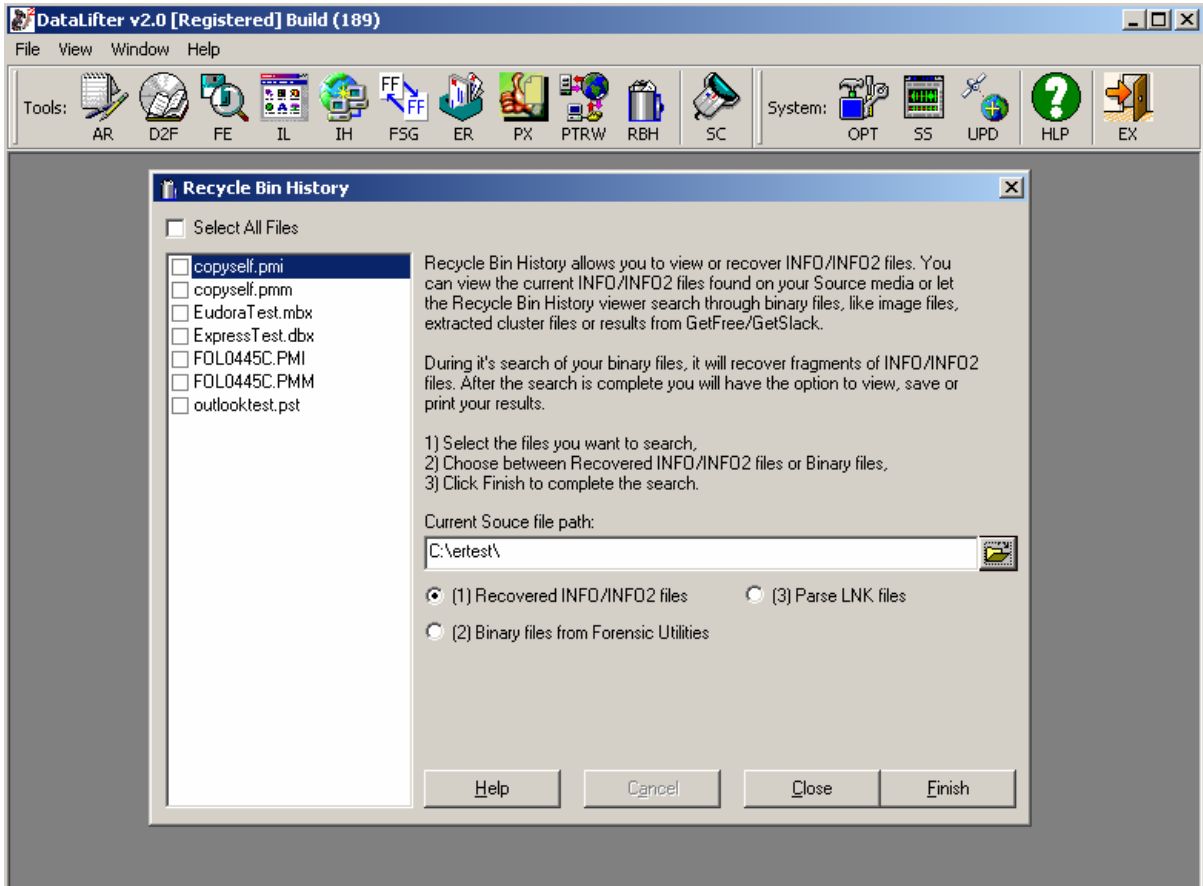


Figure 2-2

Within this screen, the user is presented with several options. First, the user must choose the file path where the copied INFO2 files were placed. Once that path is selected, the user chooses the correct file from the list on the left side of the window. Then the user must select the file type from Recovered INFO/INFO2 files, Binary (FTK Imager) files, or Parse LNK files. Once satisfied with the settings, the user just needs to press "Finish." The resulting screen allows for the user to add the results to the Active Reports summary or to save the results in a text file. Once the user has completed using Recycle Bin History, clicking on the "Close" button will close the window.

2.5.3 Using Internet History Viewer

Once the Internet History component is activated from within DataLifter's main operating screen, the user is presented with the screen shown in Figure 2-3.

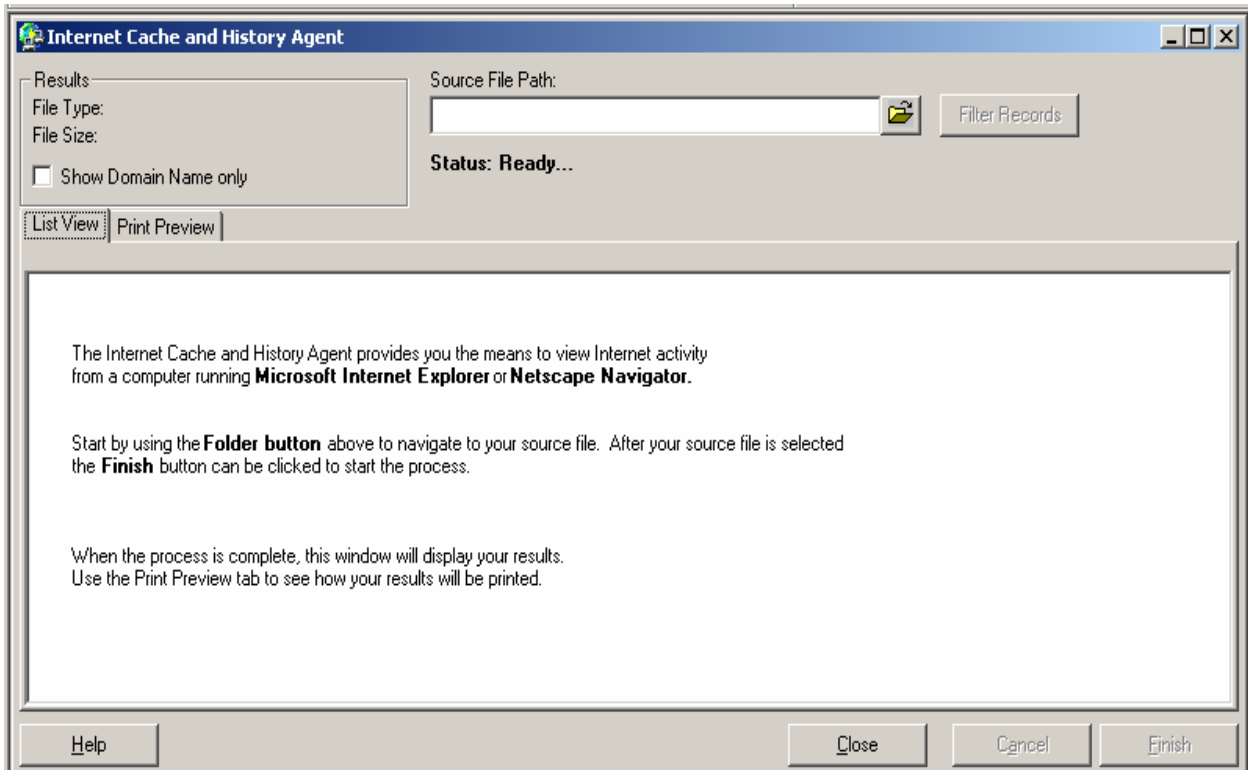


Figure 2-3

In order to operate the program, the user only needs to click on the folder icon on the right side of the "source file path" window. Then the user selects the file they copied for analysis. From within the main screen, the user clicks on the "Finish" button, and the results will appear in the main window.

2.5.4 Using Disk2File

Once the user has initialized the Disk2File component of DataLifter from within the main operating screen, they are presented with the screen shown in Figure 2-4. All the user needs to do in order to operate Disk2File is select the target drive or folder, and select the target filename as a text file. Once both parameters are met, the user clicks on finish, and the resulting text file is placed in the desired path.

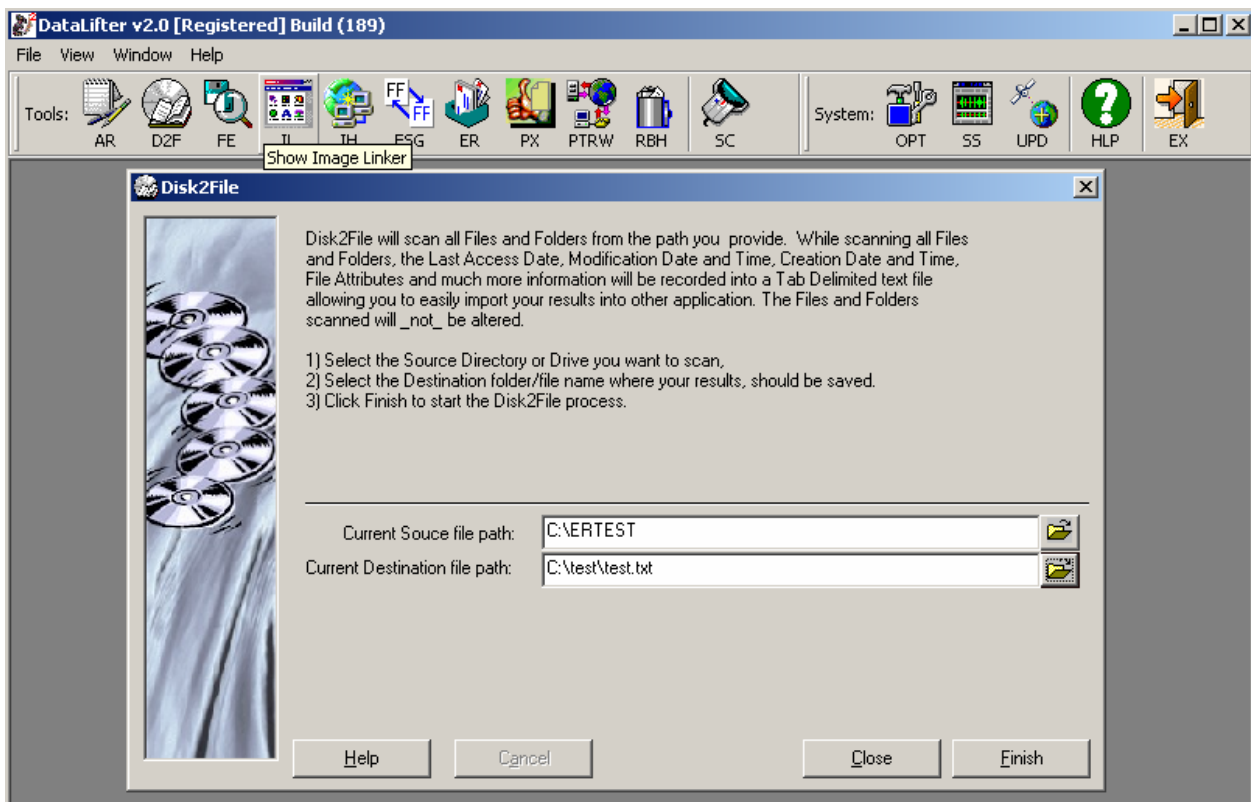


Figure 2-4

2.5.5 Using Image Linker

After initializing the Image Linker component from within the main window of DataLifter, the user is presented with the Image Linker main screen. First, the user needs to designate a source and a destination. The source is either a drive or a folder that contains the images the user wants to link in the HTML page. The destination is where the program places the resulting HTML file.

The user is also provided with several options. First, the user has the option of linking only ART image files. The user can also choose to launch the default HTML browser after completion of the Image Linker scan. Also, the program provides for an option to strip the file path from the image in order to allow for placement onto a CD for distribution. The user can choose whether or not to include subdirectories of the source path. The final option the user has is to designate the number of images to place within each HTML file created. Figure 2-5 shows the Image Linker operating screen.

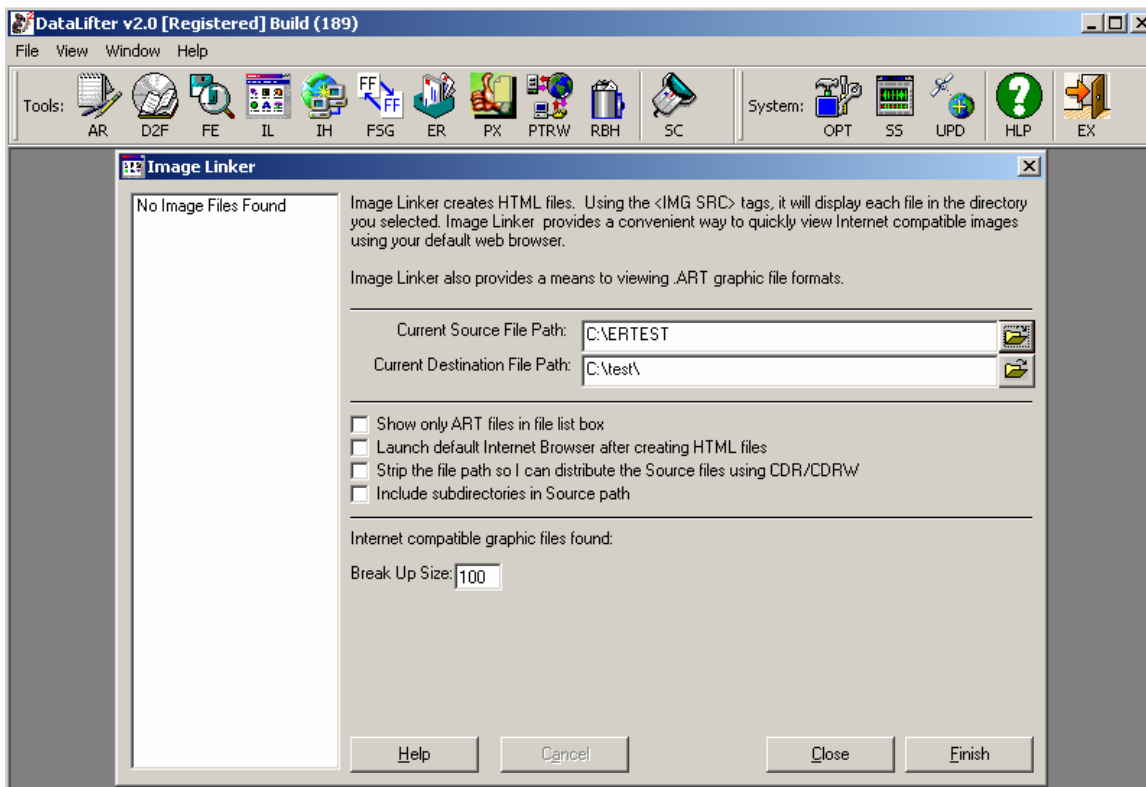


Figure 2-5

2.5.6 Using File Signature Generator

The File Signature Generator component is initialized from within the main operating screen of DataLifter. When the File Signature screen appears, the user selects the two files they wish to compare by clicking on the folder icons provided. Once the two files are selected, the user clicks on the “Create Signature” button. If DataLifter finds a valid signature common between the two files, it then provides a window that allows for the filling in of the file signature properties. These details include file extension, file size, and file header. Figure 2-6 shows the comparison window of File Signature Generator.

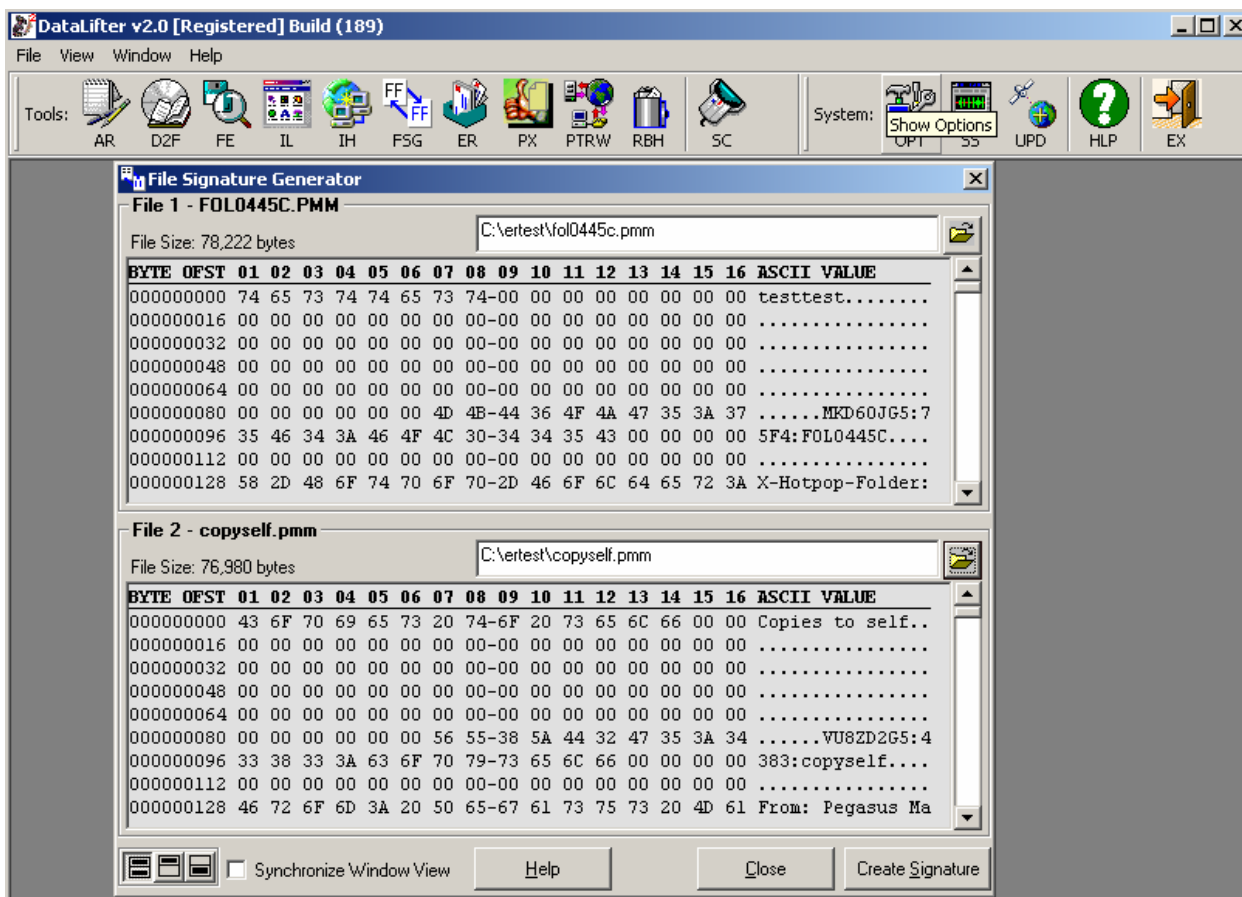


Figure 2-6

2.5.7 Using File Extractor

For DataLifter’s File Extractor component to work, the user must first have a raw image of the evidence they want to scan. File Extractor scans the image file of unallocated space for files based upon two different lists; the “ds2_hdr.txt” and “ds2_advhdr.txt” lists which come standard with every DataLifter install.

Once the user has created raw data images of the evidence in question, the user can activate File Extractor from the main operating screen in DataLifter by clicking on the button labeled “FE.” From the main screen of File Extractor (shown in Figure 2-7), the user has a couple parameters to define before running a file extractor scan.

First, the user must select a source path by using the folder icon and navigating to the folder that holds the raw image files the user wants to scan. From there, the user selects a destination file path. This is where DataLifter places all of the recovered files, along with summary files detailing what files were recovered.

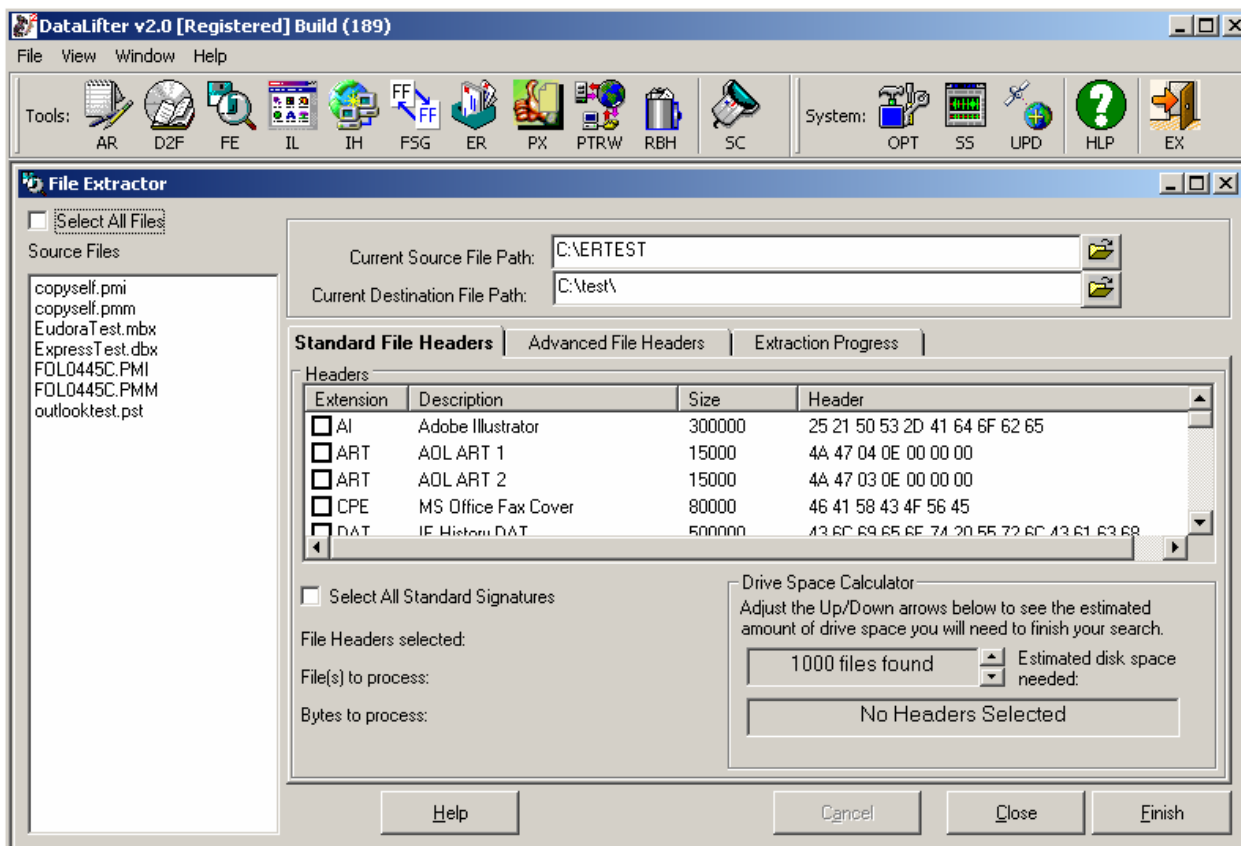


Figure 2-7

Once these two options are filled in, the user selects the options desired to customize the scan. First, the user chooses what image file they want File Extractor to scan. They can choose one image, or check the box “Select All Files” and DataLifter will scan all files in that source directory. Then the user must choose what file types they want to search for. This is done by checking off the file signatures in both the “Standard File Headers” tab and the “Advanced File Headers” tab. The user has the option to “Select All Standard Signatures” and to “Select All Advanced Signatures” or they can choose just one file signature to base the scan on. Once the user fills in these options, they click Finish, and the results of the scan are placed into a folder in the user defined destination path. DataLifter by default places a maximum 2000 files per folder. If more than 2000 files are extracted, the program creates a new folder. The folders created are labeled 1 – 2000, 2001 – 4000, etc. Within the options screen, the user can designate how many files they want placed in each folder.

2.5.8 Using Email Retriever

DataLifter’s Email Retriever works in a slightly different way than the other components of DataLifter. In order to obtain the files needed for examination, the user must navigate to the File menu in the upper left hand corner of the screen and click on “Import Email Files”. Once this is done, the user must select the folder where the email databases are located.

After the folder is selected, DataLifter attempts to import every single file in that folder. When doing this, DataLifter shows a status window of successful and failed file imports.

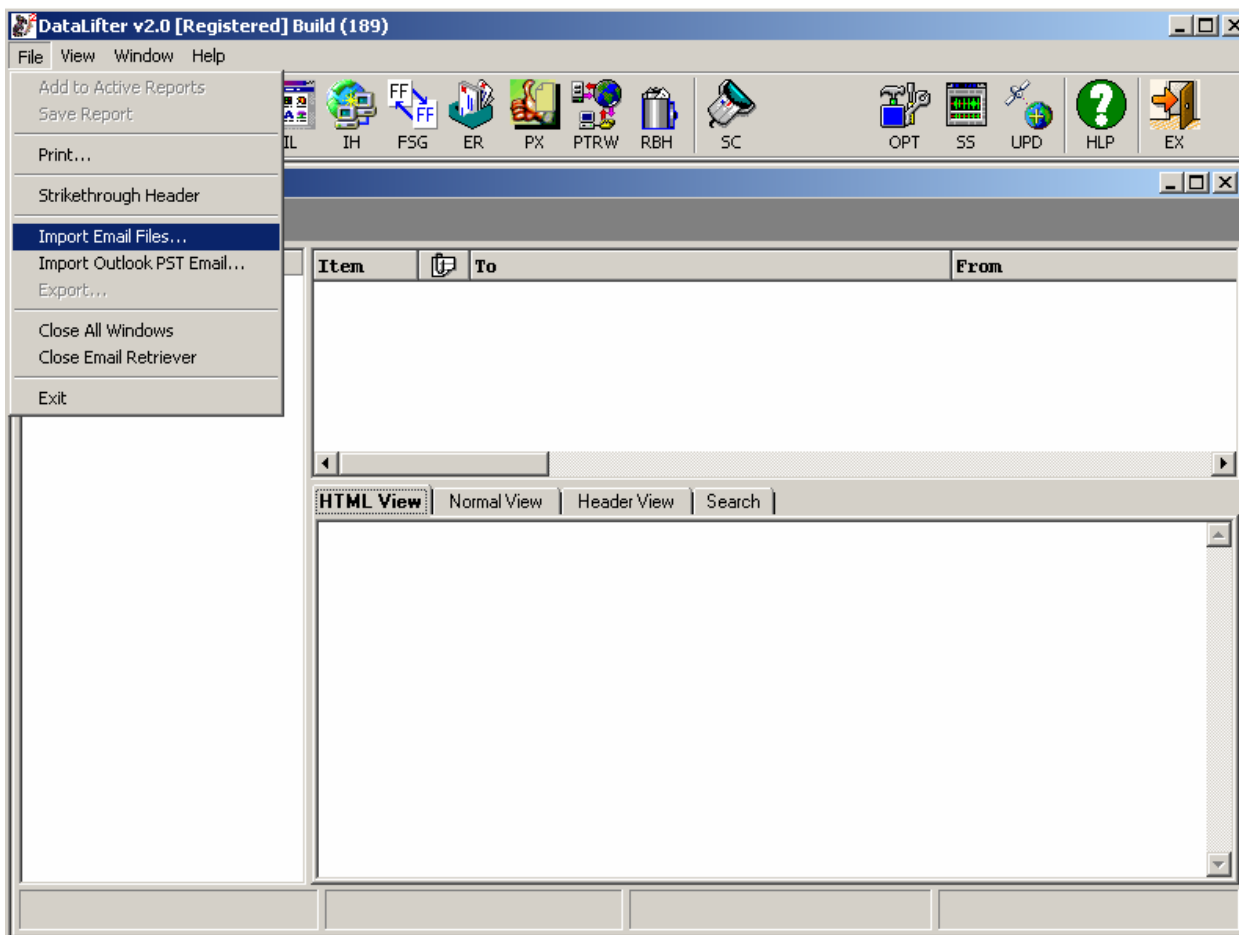


Figure 2-8

Once the files have been imported, the user may select the email database they want to examine. DataLifter tries to determine what type of email is sent, HTML or text-based in order to display it in the correct format. If not determined, Email Retriever, by default, displays it in the text format. The user can also use the search tab to search the email for keyword text strings.

2.5.9 Using Ping/Trace Route/WhoIs

DataLifter's Ping/Trace Route/WhoIs query tool is activated from the main operating screen of DataLifter by selecting the button labeled "PTRW." Figure 2-9 represents the Ping/Trace Route/WhoIs operating screen.

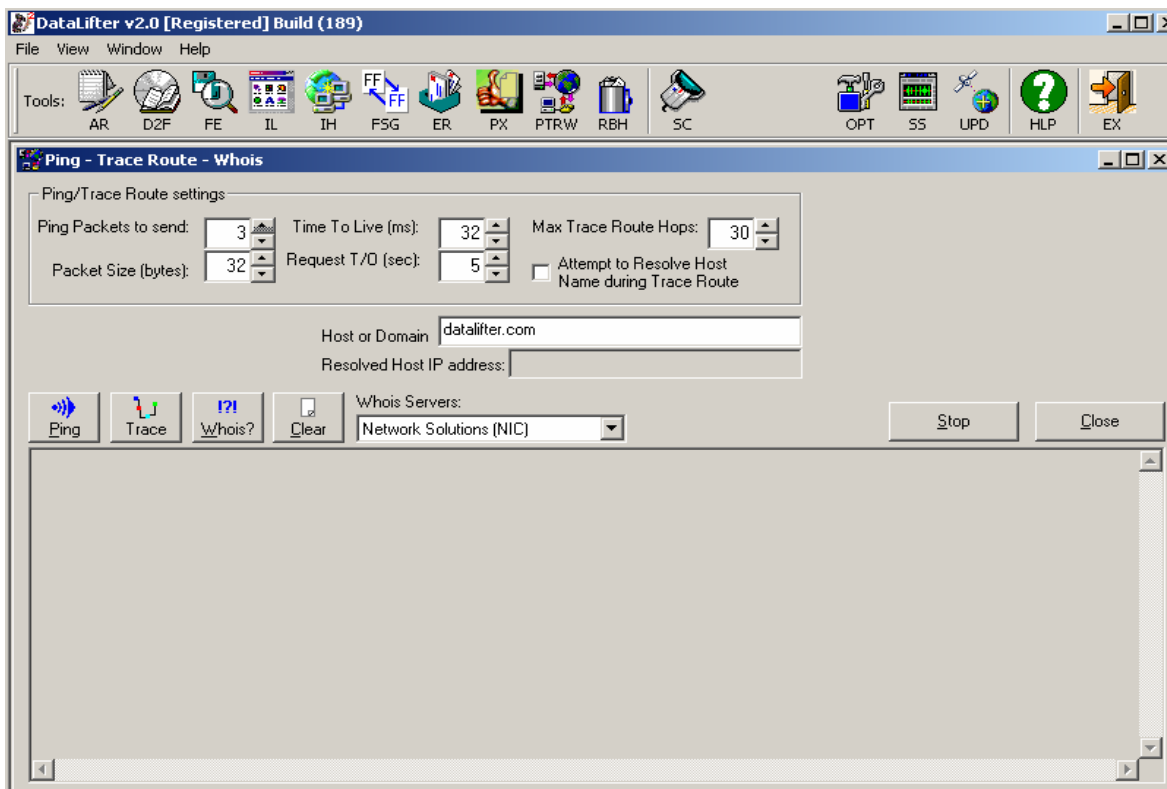


Figure 2-9

In order to use Ping/Trace Route/WhoIs, the user first inputs the “Host or Domain” they wish to examine. Once this is done, the user clicks on the desired operation button – “Ping”, “Trace”, “Whois”. The results are displayed in the window at the bottom of the screen. When using WhoIs, the user has the option to select which WhoIs search database they want to use. Anytime the user wants the screen to be cleared for easier reading, they may click on the “Clear” button.

When using Ping, the user can choose how many packets to ping with and the size in bytes of those packets. Three packets at thirty two bytes per packet is the default setting. Also, the user can designate “Time to Live” in milliseconds, and “Request Time Out” in seconds. When using the Trace Route function, the user can designate a maximum number of hops to record. Thirty is the default value.

3 TESTING RESULTS

3.1 Active Reports

3.1.1 Analysis of Active Reports

Active Reports is DataLifter's built in audit tracking report manager. For the analysis, Active Reports was run side by side with each of the tests. The tool claims to be able to monitor all activities within DataLifter and include them in a report style format to allow for easy viewing and printing.

DataLifter's Active Reports logged every test that was performed. After each test, the Active Reports summary was inspected to see if it correctly documented all the activity occurring within DataLifter.

3.1.2 Analysis Results

DataLifter's Active Reports performed exactly as the vendor stated it would. It correctly documented tests from the Recycle Bin History, Internet History, Disk2File, Image Linker, File Signature Generator, File Extractor, Email Retriever, and Ping/Trace Route/Whois queries. The logged system time was correct, as was all the recorded summary information about the usage of each tool.

3.2 Recycle Bin History

3.2.1 Analysis of Recycle Bin History

During this analysis, DataLifter was executed six times against the INFO2 file within both the NTFS file system and the FAT 32 file system creating a total of twelve test scenarios. The INFO2 file is the file that Windows uses to store information about the Recycle Bin and its usage.

For testing purposes:

- 5 .JPG graphic files, 5 MS Word .DOC files, 5 Adobe .PDF files, 5 MS Excel .XLS files, 5 .HTML files, 5 .GIF graphic files, 5 .BMP graphic files, and 5 executable .EXE files, for a total of 40 files, were placed onto the hard drive.
- The 40 files were then deleted (sent to the Recycle Bin), then DataLifter's Recycle Bin History was executed against a copy of the INFO2 file.
- 20 of the 40 files were then restored to their original location, and Recycle Bin History was executed against a new copy of the INFO2 file.
- The other 20 files were then restored back to their original location and Recycle Bin History was executed a third time against a new copy of the INFO2 file.



- The 40 files were then sent back to the Recycle Bin. 20 files were then selected and deleted from within the Recycle Bin explorer. Recycle Bin History was then executed against a new copy of the INFO2 file.
- The rest of the files were then deleted from the Recycle Bin in the same manner. Recycle Bin History viewer was then executed on a new copy of the INFO2 file.
- All 40 files were then sent back to the Recycle Bin a third time and the “Empty the Recycle Bin” option was executed. The INFO2 file was then copied, and Recycle Bin History was executed against it.

After each operation, the results from DataLifter’s scan of the copied INFO2 file were saved into a tab-delimited format text file. That file was then imported into an Excel spreadsheet for analysis.

The Recycle Bin History tool also has the ability to scan unallocated space file dumps for deleted INFO2 files. To do this, FTK¹ Imager was utilized in Windows 98 DOS. A total of three 640MB file dumps were created. Recycle Bin History was then executed and each 640MB cluster of unallocated space was examined.

3.2.2 Analysis Results

DataLifter’s Recycle Bin History was executed against a series of INFO2 files. If file history is found in the INFO2 file, Recycle Bin History returns information about it. This information includes the byte offset (location of the file), the file name, the file path, the date the file was deleted, and whether or not that file was purged from the recycle bin.

Table 3-1 below shows the results of each scan of an INFO2 file after an action was taken.

| | Results on FAT32 Drive | Results on NTFS Drive |
|--|---------------------------|---------------------------|
| Recycle Bin Full | Expected Results Achieved | Expected Results Achieved |
| Half of Recycle Bin Restored | Expected Results Achieved | Expected Results Achieved |
| Rest of Recycle Bin Restored | Expected Results Achieved | Expected Results Achieved |
| Half of Recycle Bin Deleted (from within Recycle Bin) | Expected Results Achieved | Expected Results Achieved |
| Rest of Recycle Bin Deleted (from within Recycle Bin) | Expected Results Achieved | Expected Results Achieved |
| Empty Recycle Bin command | Expected Results Achieved | Expected Results Achieved |
| Unallocated Space Scan | Expected Results Achieved | Expected Results Achieved |

Table 3-1

Results

All the tests run with the Recycle Bin History viewer achieved the expected results. When the recycle bin was full, the INFO2 file scan returned information about all 40 files that

¹ FTK refers to the tool suite known as Forensic Tool Kit created by Access Data. More information can be found at <http://www.accessdata.com>.



were placed into the recycle bin. After restoring half of the recycle bin contents back to their original location, the INFO2 file returned all 40 files, along with a “Purged” marking next to those files that were restored. After all the files were restored to their original location, Recycle Bin History returned all 40 files with the purged value set to yes. The same results were returned when files were deleted from within the recycle bin as were achieved when restoring the files back to their original location. When emptying the recycle bin with the “Empty Recycle Bin” command, the INFO2 file information is wiped clean, and no information or history is returned. Also, when scanning the raw data, Recycle Bin History was able to recover the INFO2 files and display the information contained within.

3.3 Internet History

3.3.1 Analysis of Internet History

During the analysis, DataLifter’s Internet History Viewer was executed four times on three different index.dat files. This procedure was conducted on both the NTFS drive and the FAT 32 drive. Using Internet Explorer (IE), 30 websites were visited in order to log information into Internet Explorer’s index.dat files. One of these files stored cookies, one file stored Internet history and one contained temporary Internet files. These index.dat files can be found in the following locations.

Windows 95/98/ME:

- C:\Windows\Temporary Internet Files\Content.IE5\
- C:\Windows\Cookies\
- C:\Windows\History\History.IE5\

Windows 2000/XP:

- C:\Documents and Settings\\Cookies\
- C:\Documents and Settings\\Local Settings\History\History.IE5\
- C:\Documents and Settings\\Local Settings\Temporary Internet Files\Content.IE5\

Additionally, the number of index.dat files present on a Windows 2000 or Windows XP system will depend on the number of individual users of that machine. A folder containing Internet history information is present for each user of the machine and typically for a default or administrator account.

Internet History Viewer was executed to collect the information initially present in the index.dat files. The Internet history trail was then cleared, temporary Internet files were deleted, and the cookies gathered by Internet Explorer were erased. Each of these functions was performed from within Internet Explorer’s “Internet Options” screen. After each of these three actions, Internet History Viewer was executed again and the results were exported for further analysis.



3.3.2 Analysis Results

Internet Explorer was used to visit 30 websites. A handwritten log of the websites visited was maintained to compare the results to. After all the websites were visited, copies of the three index.dat files were made. The cookies were then cleared, the history was erased, and the temporary Internet files were deleted, all from within the Internet Options menu in Internet Explorer. After each of these actions, copies of the three index.dat files were made. Table 3-2 represents the results of the Internet History scan on the Windows 98 SE index.dat files. Table 3-3 represents the results of the Internet History scan on the Windows 2000 index.dat files.

| Windows 98 SE | Index.dat (Cookies) | Index.dat (History) | Index.dat (Temporary Internet Files) |
|---|----------------------------|----------------------------|---|
| 30 Websites Visited | 45 URLs Found | 33 URLs Found | 1 URL Found |
| Cookies Deleted | 45 URLs Found | 33 URLs Found | 1 URL Found |
| History Erased | 0 URLs Found | 1 URL Found | 1 URL Found |
| Temporary Internet Files Deleted | 0 URLs Found | 1 URL Found | 0 URLs Found |

Table 3-2

| Windows 2000 Pro | Index.dat (Cookies) | Index.dat (History) | Index.dat (Temporary Internet Files) |
|---|----------------------------|----------------------------|---|
| 30 Websites Visited | 45 URLs Found | 33 URLs Found | 1 URL Found |
| Cookies Deleted | 45 URLs Found | 33 URLs Found | 1 URL Found |
| History Erased | 0 URLs Found | 1 URL Found | 1 URL Found |
| Temporary Internet Files Deleted | 0 URLs Found | 1 URL Found | 0 URLs Found |

Table 3-3

Results

All expected results were achieved. Internet History scans the index.dat files for URL files. Although the Temporary Internet Files index.dat file contained many more items within, only one item contained a URL. This one item was a Macromedia Flash SWF file, with a URL in its file name. If an item does not contain a URL, Internet History will not report it. Also, when deleting the Cookies, the Internet History and Temporary Internet files were not affected. When deleting the History files, Cookies and Temporary Internet Files were not affected. Temporary Internet Files activity did not affect the Cookies or Internet History. When attempting to scan the Netscape history.dat file, DataLifter was



unable to find any URL records. In using Notepad to look at the file, URL records are included in the file; therefore Internet History has a problem reading the history.dat file.

3.4 Disk2File

3.4.1 Analysis of Disk2File

DataLifter's Disk2File component was created to give the investigator a quick and easy way to document all of the files that exist on a suspect hard drive. During this analysis, Disk2File was executed two times on the NTFS file system and two times on the FAT 32 file system. A compilation of files and folders approximately totaling 300MB was placed onto the test drive. A MD5 hash of the hard drive was then recorded. Disk2File was then executed against the hard drive. A MD5 hash was then recorded again. This was done to determine whether Disk2File alters the contents of the hard drive in any way.

Approximately half of the files were then deleted from the hard drive. Disk2File was executed again to see how deleted files affect the scan. The resulting text files for each scan were then imported into Microsoft Excel in order to examine the data. The data was then reviewed to determine if the proper data was recorded. This data includes:

- Parent folder
- DOS 8.3 filename
- Long File Name (LFN)
- Filename extension
- Last access date and time
- Creation date & time
- Modification date & time
- Logical file size
- File attributes

3.4.2 Analysis Results

A compilation of approximately 300MB of files and folders were collected and placed onto the evidence drive. DataLifter's Disk2File component was then executed against the evidence drive. The table below indicates the results of the scan on both the FAT32 drive and the NTFS drive. Table 3-4 represents the results of the analysis performed on Disk2File.



| | FAT32 File System | NTFS File System |
|--------------------------|-------------------|------------------|
| Parent folder | Yes | Yes |
| DOS 8.3 filename | Yes | Yes |
| Long File Name (LFN) | Yes | Yes |
| Filename extension | Yes | Yes |
| Last access date | Yes | Yes |
| Creation date & time | Yes | Yes |
| Modification date & time | Yes | Yes |
| Logical file size | Yes | Yes |
| File attributes | Yes | Yes |
| All Files Found | Yes | Yes |

Table 3-4

Results

Upon completion of the Disk2File scan, the resulting text file was imported into a Microsoft Excel spreadsheet. The original software did not perform properly, as it left out folders that started with a “.” as shown in Figure 3-1. DataLifter was contacted concerning this problem, and responded quickly with a new version to fix the problem. After the new build was installed, all files were correctly documented for both the FAT32 and NTFS file systems. Along with that, DataLifter also shows hidden system folders in the results of the Disk2File scan. As expected, deleted files did not get documented through the Disk2File scan. Disk2File maintains forensic integrity of the evidence source. The hash value of the drive did not change after the Disk2File scan was performed. Build 190 was only used to test Disk2File. According to the Vendor, build 190 was created only to fix the Disk2File component, and would have no effect on the other component’s analysis.

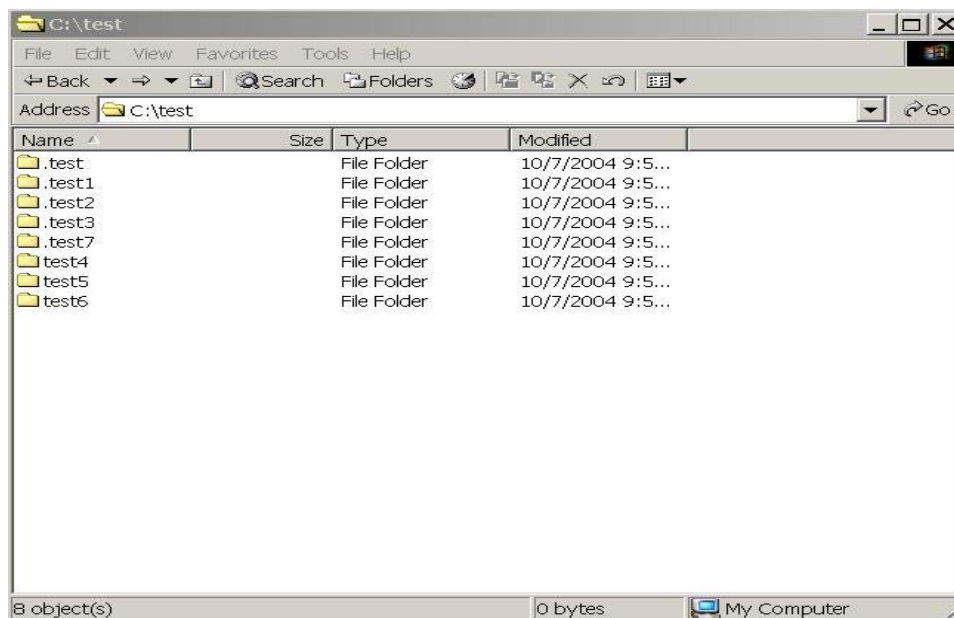


Figure 3-1

3.5 Image Linker

3.5.1 Analysis of Image Linker

The Image Linker component included in DataLifter's forensic suite is a tool designed to scan the evidence directory in question, and place the image into an HTML file along with the file path of that image's location. During this Analysis, DataLifter's Image Linker component was executed two times on both the FAT32 file system and NTFS file system.

The Image Linker component of DataLifter was tested to see if it could accurately scan the designated directory and place those images into a web page with links to that actual image location. Image Linker was specifically designed to be able to read ART image files, but also states the ability to read JPEG and GIF images as well.

A total of 100 image files were collected and placed onto the hard drive. These files consisted of 30 AOL graphic image files (.ART files), 25 .JPEG graphic files, 25 .GIF graphic files, and 20 miscellaneous image file types (.PSD, .TIF .BMP, .PNG). A test was also performed to determine if DataLifter could strip the file path from the image and make it ready for CD distribution. It does this by removing the drive letter from the file path. When the files are placed onto a CD with the Image Linker HTML file, the HTML file links direct the user to the file located on the CD.

3.5.2 Analysis Results

A total of 100 image files were compiled and placed onto the evidence hard drive. This was done on both the NTFS file system and the FAT 32 file system. DataLifter's Image Linker component was then executed, and the results were placed into an HTML file. The following table designates whether or not DataLifter could link the image type into the web page. Table 3-5 shows the results of the Image Linker analysis performed on both the NTFS file system and the FAT 32 file system.

| | FAT32 File System | NTFS File System |
|--|-------------------|------------------|
| .ART file (AOL graphic image file) | Yes | Yes |
| .JPG file (Joint Photographic Experts Group graphic image file) | Yes | Yes |
| .GIF file (Graphic Interchange Format) | Yes | Yes |
| .PNG file (Portable Network Graphic) | Yes | Yes |
| .PSD file (Adobe Photoshop Image) | No | No |
| .TIF file (Tagged Image Format File) | No | No |
| .BMP file (Windows Bitmap Format) | No | No |

Table 3-5

Results



Image Linker was specifically designed to scan the system for web-compatible graphics, and link those images into an HTML file with the path name. Web compatible graphics are images with the extensions of .art, .jpeg, .gif and .png. The Image Linker scan effectively displayed these image types, and correctly linked them to their original location. Image Linker, as expected, was unable to link the PSD, TIF, and BMP graphic image files. Image Linker was also capable of making the results of the scan CD-ready. Once the file path had been stripped, the HTML Image Linker file along with the images were placed onto a CD. The HTML file displayed all the images and the links did lead back to the file location.

3.6 File Signature Generator

3.6.1 Analysis of File Signature Generator

DataLifter’s File Signature Generator module is designed to both create file signatures and also add those signatures to the “ds2_hdr.txt” file that the File Extractor component uses to search the unallocated space data for files. File Signature Generator takes two files of the same file type, and compares the first fourteen bytes of the file headers for consistency. If consistency between the two files of two or more bytes is found, then DataLifter allows the user to add that file signature to the “ds2_hdr.txt” file.

Per this analysis, DataLifter’s File Signature Generator was tested on ten file types: five that are listed in the “ds2_hdr.txt” file and five that are not. Each test was executed once on both the NTFS file system and the FAT32 file system. After the test, File Extractor was executed with the new file signatures included to determine if the File Signature Generator correctly added the file signatures to the “ds2_hdr.txt” list. The new files added include .TIF graphic image files, Adobe Photoshop files (.PSD), .RAR compressed files, .MP3 audio files, and MS PowerPoint files (.PPT). This was verified upon opening the “ds2_hdr.txt” file with a text editor.

3.6.2 Analysis Results

File Signature Generator (FSG) was executed on ten different file types, five of which were listed in the “ds2_hdr.txt” and five that were not. Table 3-6 shows the file signatures that were added, and the file signatures generated that were already in the “ds2_hdr.txt” file signature list. Table 3-7 represents the comparison between the file signatures already created in the ds2_hdr.txt file and the file signatures created by DataLifter’s FSG component.

| File Type | File Signature |
|------------------------------|-------------------------------|
| Microsoft PowerPoint (*.PPT) | D0 CF 11 E0 A1 B1 1A E1 |
| MP3 Music File (*.MP3) | No valid signature created |
| Tagged Image Format (*.TIF) | 49 49 2A 00 08 00 |
| Photoshop Image (*.PSD) | 38 42 50 53 00 01 |
| RAR Compressed File (*.RAR) | 52 61 72 21 1A 07 00 CF 90 73 |

Table 3-6



| File Type | DataLifter Original | FSG Created |
|----------------------------------|-------------------------------|-------------------------------|
| Adobe Illustrator (*.AI) | 25 21 50 53 2D 41 64 6F 62 65 | 25 21 50 53 2D 41 64 6F 62 65 |
| WinZip (*.ZIP) | 50 4B 03 04 | 50 4B 03 04 |
| Rich Text Format (*.RTF) | 7B 5C 72 74 66 | 7B 5C 72 74 66 |
| Graphic Image Format (*.GIF) | 47 49 46 38 | 47 49 46 38 |
| Portable Network Graphic (*.PNG) | 89 50 4E 47 0D 0A 1A 0A | 89 50 4E 47 0D 0A 1A 0A |

Table 3-7

Results

DataLifter provides two lists of standard file headers, “ds2_hdr.txt” and “ds2_advhdr.txt.” The reason for this is that many files have complex file signatures. These signatures may have unique values in specific places that designate it as that type of file. When creating new file signatures that were not included with the DataLifter install, the MP3 file format was one file unable to produce a file signature. File Signature Generator is designed to find basic file signatures, not more complex ones. The vendor states that MP3 files have a complex file signature that FSG would not be able to discover. File Extractor Pro, release date scheduled for April of 2005, will be able to discover the MP3 format. FSG was able to verify that all five file types that were already included with DataLifter have the same file signature that the FSG component returned.

3.7 File Extractor

3.7.1 Analysis of File Extractor

During this analysis, File Extractor was executed one time on both the NTFS file system and the FAT 32 file system.. The File Extractor component of DataLifter states the ability to scan unallocated space clusters for files. These clusters were 650 MB in size and created by FTK Imager. The DataLifter suite contains a program known as DS2DUMP, which duplicates all of the unallocated space, also commonly referred to as free space, from a digital evidence device to a new location. DataLifter no longer supports this program, and instead supplies the user, at the user’s request, with FTK Imager v2.0b.

DataLifter’s File Extractor scans the unallocated space for designated file signatures supplied from the vendor in the files “ds2_hdr.txt” and “ds2_advhdr.txt”. The program then extracts the data from unallocated space, and places it into the folder specified by the user.

A minimum of three files of each specific type listed in the aforementioned text files were placed into unallocated space on the hard drive. This was done by placing the files onto a forensically wiped hard drive. These files were then deleted from the hard drive, in effect placing them into unallocated space. When a file is deleted, the operating system marks the space that file occupied as unallocated space. FTK Imager was then executed to create a forensic image of the hard drive’s unallocated space. File Examiner was then executed on the FTK disk image. The resulting extracted files were then compared to the list of files placed into unallocated space and compared for consistency. Consistency is obtained



when File Extractor’s resulting list is the same as the list of files placed into unallocated space.

3.7.2 Analysis Results

A compilation of five files of each file type included in both the “ds2_hdr.txt” and “ds2_advhdr.txt” text files were collected and copied onto a forensically wiped hard drive. The files were then deleted off the hard drive in order to make those files appear in unallocated space. FTK Imager was then used to create a forensic disk image of the hard drive. File Extractor was executed against the resulting disk image. Table 3-8 represents the results of the File Extractor analysis.

| | Recovered | Recovered with Errors | Not Recovered |
|-----------------------|--|---|---------------|
| Ds2_hdr.txt | AI ART (version 1) ART (version 2) CPE DAT DCI SXW DRW EML(Netscape) EML(Eudora) EML(generic) GIF PDF (1.2) PDF(Adobe) PNG RTF WKS WPC RAR TIF PSD | JPG (type 1) JPG (type 2) JPG (Kodak) PPT ZIP DOC (MS generic version) DOC (star writer 6) SDW | MP3 |
| Ds2_advhdr.txt | AVI DBX XLS (type 1) XLS (type 2) WAV DAT (all versions) DOC (MS Word 8) DOC (MS Word 10) | BMP (generic) BMP (type 1) BMP (type 2) BMP (type 3) | EMF PST |

Table 3-8

Results



File Extractor was able to correctly recover 21 out of 30 of the file types listed in “ds2_hdr.txt.” File extractor was able to recover all three JPEG versions, but in five different cases duplicate images were returned. This happened because the Kodak JPEG header starts off with the same four hex values as the JPEG generic version 1. The generic JPEG header is FF D8 FF E1 whereas the Kodak JPEG header is FF D8 FF E1 4E D8 45 78 69 66 00 00 49 49. Due to this, DataLifter returned duplicate images for those versions. Similar problems occurred with the PPT, SDW, and DOC (MS generic version) files. These three files share similar file headers, and therefore were recovered multiple times. ZIP and DOC (Star Writer V6.0) encountered the same problem as well. The MP3 file format did not recover correctly because the file signature is more complex than the File Signature Generator could create.

File Extractor was able to correct recover 17 out of 23 of the file types listed in “ds2_advhadr.txt.” While testing the BMP image type, File Extractor returned either duplicate or triplicate images. For the test, 100 BMPs were gathered, and File Extractor returned 385 out of unallocated space. Also, File Extractor was unable to extract the Outlook PST file or the EMF file, which is a Windows Metadata file format.

3.8 Email Retriever

3.8.1 Analysis of Email Retriever

DataLifter’s Email Retriever is designed to provide the user with an easy way to view Microsoft Outlook, Microsoft Outlook Express, Eudora, Pegasus, and Netscape email without using any specific email client. DataLifter does this by importing the email database from these clients into its own version of an email client designed to handle the specific email formats.

During this analysis, email was compiled within each of the five software email clients. The email databases from these programs were then manually collected, copied from their original locations, and placed into a separate folder. DataLifter was subsequently executed to determine whether or not it is capable of importing each individual email database. If an email database is successfully imported, DataLifter is capable of exporting individual emails.

Email Retriever claims the ability to export email in four different ways:

- **Export Only Highlighted Email:** Exports only the message(s) that are currently highlighted.
- **Export Checked Email:** Exports only the messages that are checked.
- **Export Email With Attachments:** Exports only messages that have attachments.
- **Export All Email In Selected Folder:** Exports all messages in the selected folder. You can only have one folder selected at a time.

DataLifter was tested to determine the ability to perform these four functions. Along with that, Email Retriever has the ability to search through the imported email based on keywords provided by the user.



3.8.2 Analysis Results

Two of each of the email databases from Microsoft Outlook (*.PST), Microsoft Outlook Express (*.DBX), Pegasus (*.PMM and *.PMI), Eudora (*.MBX), and Netscape (*.DBX) were all gathered into a folder. Once this was completed, DataLifter's Email Retriever component was executed against this folder. The analysis was conducted to determine if DataLifter could successfully import the specific email databases and to determine the ability of DataLifter to search through the email, and correctly display the email contents. Table 3-9 represents the ability of Email Retriever to successfully import email databases and manipulate them from within DataLifter.

| | Import Email Database | Display Email Contents | Export Email Functions | Perform Search |
|------------------------|-----------------------|------------------------|------------------------|----------------|
| Microsoft Outlook PST | Successful | Successful | Successful | Successful |
| MS Outlook Express DBX | Successful | Successful | Successful | Successful |
| Netscape MBX | Successful | Successful | Successful | Successful |
| Eudora MBX | Successful | Successful | Successful | Successful |
| Pegasus PMM | Unsuccessful | N/A | N/A | N/A |

Table 3-9

Results

Email Retriever achieved all expected results with every email version except for the Pegasus mail database. The Pegasus email database was a PMM file; no MBX or DBX file could be discovered. Earlier versions of Pegasus may have used these formats. Since the import of the email database was unsuccessful, the other tests could not be performed. DataLifter was able to display the email contents, complete all the export options, open attachments, and search the emails for keywords defined by the user.

3.9 Ping/Trace Route/Whois

3.9.1 Analysis of Ping/Trace Route/Whois

During this analysis, five different websites were used to test DataLifter's ability to Ping, Trace Route, and perform a whois query. In order to verify the results of these tests, the MS-DOS versions of Ping and Trace Route were used along with the website <http://www.SamSpade.org> to test the WhoIs search queries. The five websites tested consisted of <http://www.google.com>; <http://www.yahoo.com>; <http://www.cnn.com>; <http://www.nbc.com>; and <http://www.abc.com>.



3.9.2 Analysis Results

DataLifter's ping component was tested on five different websites. These same five websites were pinged by the Windows 2000 command shell ping protocol. Table 3-10 represents the ability of both DataLifter's ping component and the Win2K command shell ping component to correctly ping the target website.

| Website URL | DataLifter Ping | MSDOS Ping |
|-----------------------|-----------------|-----------------|
| http://www.google.com | Ping Successful | Ping Successful |
| http://www.yahoo.com | Ping Successful | Ping Successful |
| http://www.cnn.com | Ping Successful | Ping Successful |
| http://www.nbc.com | Ping Successful | Ping Successful |
| http://www.abc.com | Ping Successful | Ping Successful |

Table 3-10

DataLifter's trace route component was tested on five different websites. The Windows 2000 command shell trace route component was then tested on the same five websites. Table 3-11 represents the ability of both DataLifter's trace route component and the Win2K command shell trace route component to correctly trace the path to the target website.

| Website URL | DataLifter Trace Route | MSDOS Trace Route |
|-----------------------|------------------------|-------------------|
| http://www.google.com | Trace Successful | Trace Successful |
| http://www.yahoo.com | Trace Successful | Trace Successful |
| http://www.cnn.com | Trace Successful | Trace Successful |
| http://www.nbc.com | Trace Successful | Trace Successful |
| http://www.abc.com | Trace Successful | Trace Successful |

Table 3-11

DataLifter's Whois component was tested on five different websites. SamSpade.org's version of Whois was then tested on the same five websites. Table 3-12 represents the ability of both DataLifter's Whois component and the SamSpade Whois query to correctly ascertain information about the target website.

| Website URL | DataLifter Whois | SamSpade Whois |
|-----------------------|--------------------|------------------|
| http://www.google.com | Query Unsuccessful | Query Successful |
| http://www.yahoo.com | Query Unsuccessful | Query Successful |
| http://www.cnn.com | Query Successful | Query Successful |
| http://www.nbc.com | Query Successful | Query Successful |
| http://www.abc.com | Query Successful | Query Successful |

Table 3-12



Results

In both the DataLifter Ping and Trace Route tests, DataLifter achieved comparable results to that of the Windows 2000 command shell versions of Ping and Trace Route in that both were capable of pinging and tracing the path to the target websites. The Trace Route results were within 3 total hops difference of each other in all cases. DataLifter's Whois query was not as capable as the SamSpade.org Whois query in retrieving information about the target websites. DataLifter was unable to return any results for either the Google or Yahoo websites. DataLifter offers a variety of Whois search engines. Each site that was queried was done so with all of the offered Whois search engines. These engines do not all contain the same information. SamSpade.org employs a more extensive Whois capability and was able to find information on Yahoo and Google's websites.



4 CONCLUSION

The DataLifter tool suite is comprised of 10 different tools that are designed to assist a computer forensic investigator in completing a thorough examination. The tools included in this suite include Active Reports, a report-auditing tool; Recycle Bin History, a tool designed to allow the user to view INFO2 recycle bin files; Internet History, a tool designed to review index.dat internet history files; Disk2File, a disk cataloguing tool; Image Linker which scans the hard drive or folder for images and places them into an HTML file; File Signature Generator, which compares two files of the same extension to determine the file signature; File Extractor, a tool used to parse data out of unallocated space. Other tools include the Email Retriever tool, which scans email databases and Ping/Trace Route/Whois query tool. Along with that, DataLifter provides a Screenshot capability and the ability to link an external graphics viewer to the DataLifter main screen.

DataLifter's Active Reports component was completely successful in logging all the activity from within DataLifter. DataLifter's Recycle Bin History component was also successful in the tests that were performed against it. DataLifter can accurately read the INFO2 file. Along with that, DataLifter's Image Linker, Disk2File, and File Signature Generator components all completed their individual test phases with expected results. These components met the functions stated by the vendor.

DataLifter's Internet History Viewer component was mostly capable of performing as the vendor stated it was able to. DataLifter was unable to read the Netscape 7.2 history.dat file. Other than that, all tests performed achieved expected results.

DataLifter's File Extractor Component was also largely successful in performing its stated capabilities. File Extractor was able to successfully recover 38 of 53 total file types. Out of the 15 files not recovered correctly, 13 were recovered, but often times in duplicate or triplicate because they share common file signatures. For example, the Kodak JPEG header's first four values are the same as the JPEG Type 1. This caused a several files to be recovered in both columns. File Extractor was unable to recover the MP3 file format because of its complex file header. Also, both the EMF file type and the PST file type were not recovered by the File Extractor scan.

The Email Retriever component of DataLifter was able to recover 4 out of 5 types of email it stated the ability to. It was unable to read the Pegasus Email database. The file in question has a PMM extension, and all other email versions had a DBX, MBX, or a PST extension. The Microsoft Outlook PST extension was imported correctly.

The Ping/Trace Route/Whois tests were largely successful as well. The only issues arose when doing the WHOIS query search. In these queries, only 3 of the 5 websites queried returned the expect results. When looking up www.google.com and www.yahoo.com, DataLifter was unable to return any information.



5 APPENDIX A – SAMPLE ACTIVE REPORTS OUTPUT

Investigator: CyberScience Lab Investigator
Subject/Client: John Doe
Case#: 00001
Date/Time: Thursday, December 02 2004

Audit Tracking Section

DISK2FILE

No Activity Recorded

FILE EXTRACTION

No Activity Recorded

IMAGE LINKER

No Activity Recorded

INTERNET HISTORY

No Activity Recorded

EMAIL RETRIEVER

No Activity Recorded

PING/TRACE ROUTE/WHOIS

No Activity Recorded

RECYCLE BIN HISTORY

No Activity Recorded

SCREEN CAPTURE/VIEWER

No Activity Recorded

Ping/Trace Route/Whois Section

Recycle Bin History Section

DataLifter v2.0 Settings

This is a summary of your current configuration.
After reviewing it for accuracy, select any of the tools
from the Buttons above or View menu.



Case/Exam #: 00001
Detective/Examiner: CyberScience Lab Investigator
Date/Time: Friday, December 10 2004
Subject: John Doe

Your examination source files are located at:
C:\ERTEST

Any data extracted from your source files will be saved
in the directory: C:\DOCUMENTS AND SETTINGS\PATRICK\DESKTOP\

