

ATC-NY

*A subsidiary of
Architecture
Technology
Corporation*

Dr. Rob Joyce

rob@atc-nycorp.com

Dr. Frank Adelstein

fadelstein@atc-nycorp.com

DFRWS 2007

Pittsburgh, PA

August 14, 2007



Problem

- Often peer-to-peer (P2P) software present on seized disks
- **Lots** of different types of P2P software, each with different file locations, formats, logs, etc.
- Investigator must look up specific details for each instance of P2P software encountered
- Time consuming, tedious process



Solution

Develop File Marshal, a tool to automate the process!

- ◆ Extract downloaded files
- ◆ Extract log files
- ◆ Parse log files, translate to standard format
- ◆ Extract any useful data present, e.g., servers, user IDs, passwords
- ◆ Perform tasks in a forensically sound way
- ◆ Make system extensible
 - Investigator can add new types of P2P software to config file
 - Investigator only needs to do this once (per P2P software)
- ◆ Generate report in a clear, usable format

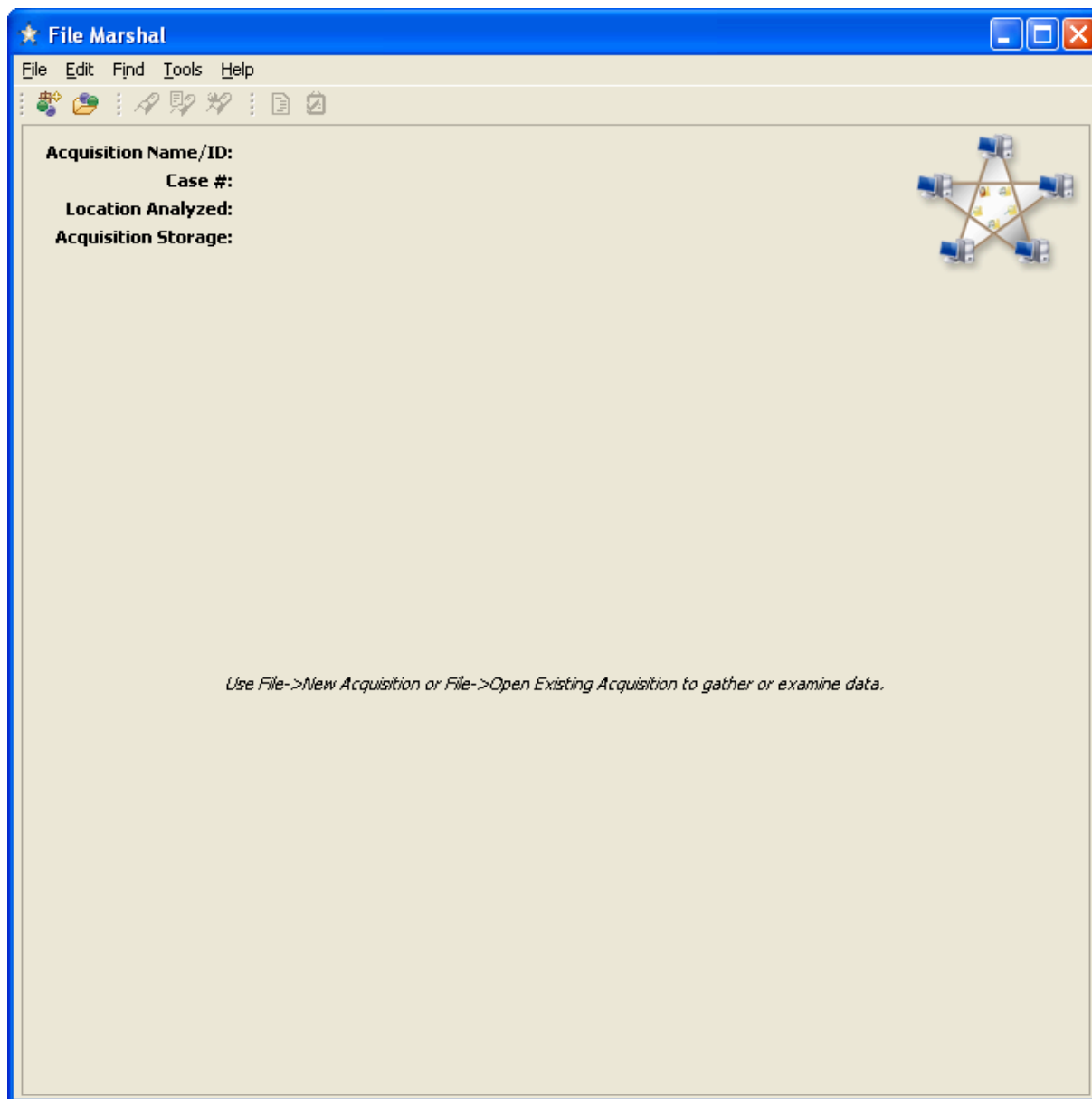


Benefits

- Reduce investigator workload
- Reduce turnaround time
- Standardize processing of data and reporting
- Log all steps performed by File Marshal



Starting File Marshal





File Marshal Acquisition: Selecting the Evidence Source

New Acquisition

Location to be Analyzed
Select the image, partition, or directory to gather data from

Examine a mounted disk partition

Pa...	Name	Type	File System	Size
C:\		Fixed	NTFS	148.9 GB (65.2 GB free)
O:\	rob	Remote	NTFS	253.9 GB (84 GB free)
P:\	TechStaff	Remote	NTFS	253.9 GB (84 GB free)
Q:\	Transfer	Remote	NTFS	253.9 GB (84 GB free)
S:\	SourceSafe	Remote	NTFS	253.9 GB (84 GB free)
T:\	Programs	Remote	NTFS	253.9 GB (84 GB free)

Examine a directory

Path:

Examine a disk image file (not yet supported)

Image file:



File Marshal Main Window

File Marshal

File Edit Find Tools Help

Acquisition Name/ID: sdfsd
Case #: s
Directory Analyzed: C:\Documents and Settings\rob\Desktop\FileMarshalTest
Acquisition Storage: C:\Documents and Settings\rob\My Documents\New Folder (5)

LimeWire Kazaa

Installation Information
Software: [LimeWire](#) Version: 4.12.11
Location: Program Files\LimeWire Installation Status: Full

Usage Information
Usage by: All Users Combined

Peer Servers:

Address	Type	Last Contact
82.38.136.154	node	Sun Jan 08 23:58:16 EST 2006
81.76.82.243	node	Sun Jan 08 23:58:16 EST 2006
68.115.86.196	node	Sun Jan 08 23:58:09 EST 2006
83.24.168.24	node	Sun Jan 08 23:58:09 EST 2006

Shared/Downloaded Files:

Name	Shared	Size	Modification Time
2007-jeep-wrangler-4dr.jpg	yes	91.9 KB	Sun Jan 08 03:54:32 EST 2006
2007_jeep_wrangler_suv[1].jpg	yes	3.2 KB	Sun Jan 08 03:58:45 EST 2006
AOLBrandingQ4_Clouds_160x600_Bnr_120806[1].jpg	yes	19.8 KB	Sun Jan 08 03:38:33 EST 2006
Att_Window.gif	yes	21.3 KB	Fri Jan 06 06:43:33 EST 2006

Usage Log:

Time	Entry
Thu Jul 19 15:34:14 EDT 2007	test log entry 1
Thu Jul 19 15:34:14 EDT 2007	test log entry 2



File Marshal Search Window

FileMarshal Search

Search Close

Find files whose

filename

contains .gif

Case Sensitive
 Regular Expression

AND size

is at least 10000

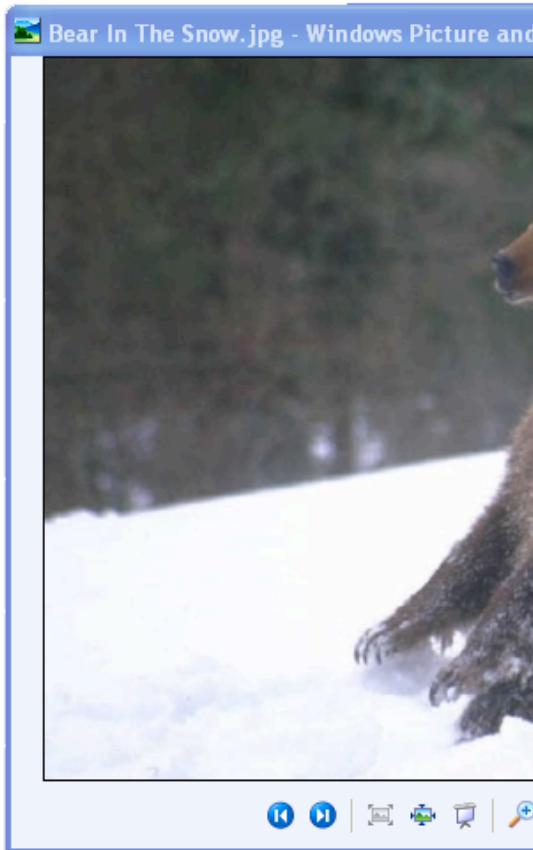
Shared/Downloaded Files:

Name	Shared	Size	Modification Time
Att_Window.gif	yes	21.3 KB	Fri Jan 06 06:43:33 EST 2006
CHRISTMAS TREE.gif	yes	241.4 KB	Fri Jan 06 07:18:23 EST 2006
CLOUD.GIF	yes	11 KB	Fri Jan 06 07:19:42 EST 2006
Cloud 1.gif	yes	17.7 KB	Fri Jan 06 07:25:51 EST 2006
Cloud-01-june.gif	yes	43.5 KB	Mon Jan 09 01:06:23 EST 2006
Cloud_Rain_Showers[1].gif	yes	10.2 KB	Fri Jan 06 07:28:40 EST 2006
cloudmoon.gif	yes	40.2 KB	Fri Jan 06 07:27:41 EST 2006
clouds[1].gif	yes	11.1 KB	Mon Jan 09 01:04:56 EST 2006
firewall_database.gif	yes	10.4 KB	Sat Jan 14 02:33:21 EST 2006
lightning.gif	yes	16.9 KB	Sat Jan 14 02:43:46 EST 2006
snow-frame.gif	yes	12.1 KB	Mon Jan 09 00:57:11 EST 2006
snowflakev.gif	yes	15 KB	Mon Jan 09 00:55:32 EST 2006
snowman.gif	yes	15.6 KB	Mon Jan 09 00:58:18 EST 2006



File Marshal Investigation Audit Log

```
File Marshal: Audit Log
[2007-07-09T17:34:15.234-04:00] CREATE: New File Marshal acquisition
(created on host ATC-53.inside.oracorp.com)
[2007-07-09T17:34:15.781-04:00] DATA_ACQUIRE: Performed discovery,
saved to C:\Documents and Settings\rob\My Documents\New Folder (5)\clientsfound.xml;
size=1236,
MD5 hash=0ff487104376d08442114a57ee9e013d,
SHA-1 hash=4904f6ca37cac4810fd4433f149965c3449a7881
[command: C:\eclipse-3.2-workspace\com.atc_nycorp.filemarshal.ui.win32\bin\ctools\findp2p.exe --discover --status
--config=C:\eclipse-3.2-workspace\com.atc_nycorp.filemarshal.module.limewire\fmacquire_config.xml -
-config=C:\eclipse-3.2-workspace\com.atc_nycorp.filemarshal.module.kazaa\fmacquire_config.xml "-
-topdir=C:\Documents and Settings\rob\Desktop\FileMarshalTest"]
[2007-07-09T17:34:16.093-04:00] DATA_ACQUIRE: Gathered usage data for LimeWire installed at Program
Files\LimeWire,
saved to C:\Documents and Settings\rob\My Documents\New Folder (5)\limewireresults.xml;
size=1443,
MD5 hash=669e7056f4f1c324eb2b4f32d13e6a47,
SHA-1 hash=85b99f1c9d6b172c09ac512ac69dcac846d93bf0
[command: C:\eclipse-3.2-workspace\com.atc_nycorp.filemarshal.ui.win32\bin\ctools\findp2p.exe --acquire "-
-instdir=Program Files\LimeWire" --status "--userdir=Documents and Settings" --config=C:\eclipse-3.2
-workspace\com.atc_nycorp.filemarshal.module.limewire\fmacquire_config.xml "--topdir=C:\Documents and
Settings\rob\Desktop\FileMarshalTest"]
[2007-07-09T17:34:16.156-04:00] DATA_ACQUIRE: Gathered usage data for Kazaa installed at Program Files\Kazaa,
saved to C:\Documents and Settings\rob\My Documents\New Folder (5)\kazaaresults.xml;
size=1377,
SHA-1 hash=daceaa79b79303272785ceee6635d6441e79760a,
MD5 hash=ded765f562b3dddab0f1b958b8a18257
[command: C:\eclipse-3.2-workspace\com.atc_nycorp.filemarshal.ui.win32\bin\ctools\findp2p.exe --acquire "-
-instdir=Program Files\Kazaa" --status "--userdir=Documents and Settings" --config=C:\eclipse-3.2
-workspace\com.atc_nycorp.filemarshal.module.kazaa\fmacquire_config.xml "--topdir=C:\Documents and
```



File Marshal

File Edit Find Tools Help

Acquisition Name/ID: sdfsd
 Case #: s
 Directory Analyzed: C:\Documents and Settings\rob\Desktop\FileMarshalTest
 Acquisition Storage: C:\Documents and Settings\rob\My Documents\New Folder (5)

LimeWire Kazaa

Installation Information
 Software: LimeWire Version: 4.12.11
 Location: Program Files\LimeWire Installation Status: Full

Usage Information
 Usage by: All Users Combined

Peer Servers:

Address	Type	Last Contact
12.110.180.16	node	
12.14.225.48	node	
12.14.225.48	node	
12.145.232.160	node	Sun Jan 08 23:58:08 EST 2006

Shared/Downloaded Files:

Name	Shared	Size	Modification Time
Att_Window.gif	yes	21.3 KB	Fri Jan 06 06:43:33 EST 2006
Bear In The Snow.jpg	yes	43.8 KB	Mon Jan 09 00:57:59 EST 2006
Blue Clouds tile purple left.gif	yes	921 bytes	Sun Jan 08 03:38:30 EST 2006
Browser_Window_Base.PNG	yes	1.8 KB	Fri Jan 06 06:48:23 EST 2006

Usage Log:

Time	Entry
Thu Jul 19 16:04:33 EDT 2007	test log entry 1
Thu Jul 19 16:04:33 EDT 2007	test log entry 2

File Marshal: Audit Log

```
[2007-07-09T17:34:15.234-04:00] CREATE: New File Marshal
(created on host ATC-53.inside.oracorp.com)
[2007-07-09T17:34:15.781-04:00] DATA_ACQUIRE: Performe
saved to C:\Documents and Settings\rob\My Documents\New
size=1236,
MD5 hash=0ff487104376d08442114a57ee9e013d,
SHA-1 hash=4904f6ca37cac4810fd4433f149965c3449a788
[command: C:\eclipse-3.2-workspace\com.atc_nycorp.filemarshal.ui.win32\bin\ctools\findp2p.exe --discover --status
--config=C:\eclipse-3.2-workspace\com.atc_nycorp.filemarshal.module.limewire\fmacquire_config.xml -
--config=C:\eclipse-3.2-workspace\com.atc_nycorp.filemarshal.module.kazaa\fmacquire_config.xml "-
-topdir=C:\Documents and Settings\rob\Desktop\FileMarshalTest"]
[2007-07-09T17:34:16.093-04:00] DATA_ACQUIRE: Gathered usage data for LimeWire installed at Program
Files\LimeWire,
saved to C:\Documents and Settings\rob\My Documents\New Folder (5)\limwireresults.xml;
```



Future Plans

- Enhance interface
 - ◆ Searching options
 - ◆ Report generation
 - ◆ Other features based on beta tester feedback
- Add support for additional clients
 - ◆ BitTorrent (Azureus, BitTorrent, μ Torrent)
 - ◆ Ares
 - ◆ Hello (Google)
- Beta release at end of summer to law enforcement partners for testing and feedback
 - ◆ Working with James Thompson, director of the Broome County (NY) Computer Analysis and Technical Services (CATS) Unit
- ***Version 1 release available to law enforcement at no cost by end of the year***
- Potential follow-on: more features, clients, functionality, etc.