



REPORT OF EXAMINATION OF DIGITAL EVIDENCE

Report prepared by: Dennis J. Browning

Case number: 07FTK0814

Date of report: 9 February 2008

Reference Case: n/a

This report describes the forensic examination and data recovery that was performed for Det. Melodie Woodward, Vermont State Police.

I) INTRODUCTION

On 5 February 2008, Det. Woodward provided me with a computer image of a computer that had been seized from the home of Charles Messier, Burlington, VT. Mr. Messier is suspected to have images of child pornography on his computer.

In addition, it is suspected that Mr. Messier has been in contact with a Mr. Galileo Galilei, talking about other forms of child pornography.

Pursuant to a search warrant, Det. Woodward has asked that the computer be examined and analyzed to determine whether there is any evidence of child pornography.

II) COMMENTS & RESULTS

The computer was searched for information pertinent to the search warrant, including in normal files, temporary files, deleted files, and file fragments in unallocated space. The examination employed software called the Forensic Toolkit (FTK).

There is evidence that suggest that Mr. Messier has images of child pornography on his harddrive. Also that he has been in contact with a Mr. Galilei. It appears that Mr. Messier has roughly 550 images on his drive.

13 E-mails were recovered of conversations between Mr. Messier and Mr. Galilei.

III) CONCLUSIONS & OPINIONS

The information on the supplied hard drive validates Mr. Messier's does indeed possess images of child pornography. And that he has been in contact with Mr. Galilei.

IV) MEDIA EXAMINATION & DATA ACQUISTION STEPS

This section will detail the specific steps taken to preserve the integrity of the original evidence, prove the integrity of the media that was actually examined, and the procedures used to acquire and recover the data from the media. The steps outlined here are consistent with the practices of the Vermont Internet Crimes Task Force

and the Champlain College Center for Digital Investigation. All software utilized in this examination is licensed to, or authorized for use by, the examiner.

1. Det. Woodward provided the examiner with a forensic copy of Mr. Messier's hard drive; evidence tag 07FTK0814-001; only the image was provided (i.e. no peripherals) via DVD. A written chain-of-custody record was started in order to document the evidentiary chain (see file *chain_of_custody_07FTK0814.rtf* in the case ZIP file).
2. The image files were imported into FTK (AccessData) for analysis and reporting.
3. The image was examined and was found to contain a **three** logical partitions:
 - a. **Partition 1:** aFAT-32 partitioned named FAT32. The partition contains in excess of 2,500 files including emails, pictures, general files.
 - b. **Partition 2:** a NTFS partitioned named NTFS. The partition contains in excess of 600 files including pictures, email, operating system files.
 - c. **Partition 3:** a NTFS partitioned named NTFS Compressed. This partition contains in excess of 300 files including program files.
 - d. **Un-partitioned Space:** Files were recovered from this space and visual examination confirms that there is data in the area of the drive.
4. The *slack space* of all areas on the disk was searched for potentially relevant lost or hidden data. The *unallocated space* on the disk was also examined; this is called *Drive Free Space* by FTK. No files were found.
5. A listing of all the files on the medium can be found in the FTK report in the List by File Path, All Items section.

V) ANALYSIS AND EXHIBITS

The FTK report can be accessed by unzipping the messier case #07FTK0814.zip file and pointing a Web browser to index.html. The items contained in the report, as categorized by the navigation menu on the left side of the screen are listed below:

1. Case Summary

1.1 **Case Information** – Identifying information about the case and examiner

1.2 **File Overview** – A high-level overview of the number of files found on the medium.

There were 4 primary evidence items: three formatted disk partitions plus the unpartitioned space. In total, the media help approximately 3,619 files including 309 documents, 1,199 graphics, 5 multimedia, 43 e-mail messages.

1.3 **Evidence List** – The name of the disk images used to create this case report.

2. Supplementary Files

2.1 **Glossary of Terms**- Glossary of technical terms used in this report.

2.2 **Case Log** - The file provides an audit trail of actions taken while running the FTK program.

3. List by File Path

3.1 **All Items** – A diagram of the tree structure of all files on the medium image.

4. Bookmarks

4.1 **Contents** – A list of all the bookmarks below with a brief description.

4.2 **Activities Weekend 13SEPT02** – Appointments on Mr. Messier's Outlook Calendar from 12SEPT02 through 14SEPT02

4.3 **Bios** – Documents that were sent via e-mail on child pornography leads.

4.4 **Debate** – Documents that reference a debate.

4.5 **Deleted Folders** – Reference to the possible deleted folder.

4.6 **Galileo** – E-mails between Mr. Messier and Mr. Galilei and any attachments connected to each message.

4.7 **Multiwave** – Files that were recovered from the deleted folder Multiwavelength Messier 45 – The Pleiades Cluster_files.

4.8 **Photos** – Images of child Pornography.

4.9 **Picture of the Day** – Items that referenced Picture of the Day.

V) TECHNICAL BACKGROUND TOPICS

This section provides information about additional technical issues associated with this examination and analysis:

- The Use of Automated Tools in Computer Forensics Examinations

The Use of Automated Tools in Computer Forensics Examinations

A discussion about the use of automated tools in compute forensics exams can be found in the article "The 'Tools Proven in Court' Question" by Steve Hailey, available from <http://www.cybersecurityinstitute.biz/TPICQ.pdf>. Access Data's FTK software, this exam, and this examiner can pass all of the tests brought up in this article:

1. Was the evidence gathered and verified in a sound manner?
2. Was a chain of custody maintained?
3. Is the ownership and licensing appropriate for the tools used?
4. Was the proper examination environment being maintained?
5. Can the results of the technical analysis be duplicated using other tools?
6. Does the Analyst understand what the tools they use are actually doing, or are they merely taking for granted what an automated process is reporting?
7. Do other professionals use the same techniques and methodology?
8. Is the Analyst technically capable of defending/supporting their interpretation of the evidence?

The Tests:

- Has or can the expert's technique or theory been/be tested?
- Has the technique or theory has been subject to peer review and publication?
- Is the potential rate of error of the technique or theory known, and accepted?
- Are standards controlling the technique's operation in existence and are they maintained?
- Has the theory or method been generally accepted by the scientific community?

CONFIDENTIAL