

iPod Forensics Update

Matthew Kiley

Tim Shinbara

Marcus Rogers

Purdue University Cyber Forensics Laboratory
Department of Computer and Information Technology
Purdue University

Abstract

From student to business worker, the popularity and ubiquity of mobile devices is exploding. As these devices saturate modern culture, they continue to grow in functionality. Such devices can now play music, store photos, contacts, and files or even play full-length movies. Apple's iPod has taken mobile entertainment to the next level by incorporating all of this into a single device. In fact, the iPod has become so popular that sales have topped nearly sixty seven million units (Apple, 2006). With increased popularity however, criminals have found ways to exploit an otherwise altruistic device. The challenge that lies before law enforcement now becomes identifying the evidence an iPod may contain. Since there has been minimal research in portable music players within the digital forensics community, law enforcement may be fighting blind during their investigations. This paper is an update to previous research by Marsico and Rogers (2005) that presents new procedures and methodologies for law enforcement to obtain digital evidence from the new generations of iPods. As software and hardware revisions have changed, this research analyzes what effect this has on the extraction of evidence.

Introduction

The iPod, though initially a device to store and play music files, has evolved to become a mobile device that allows users to watch video, listen to music and store a wide variety of data. In fact, the market may soon see another large increase in portable music device storage (Toshiba, 2006). Along with these changes however, the digital forensic community must continually keep pace. Software updates made in iTunes, Apple Software Updater, and forensic tools make a re-evaluation of previous research necessary (Marsico & Rogers, 2005). This paper is meant to update law enforcement, incident response team members and other forensic first responders regarding the newest generation of Apple's iPod and its forensic value. Another goal of this paper is to increase awareness of this unusual source of digital evidence and assist in the recovery of data for law enforcement. It should be noted that the findings of this research are valid regardless of the investigative model used to collect it. Legal admissibility should always be foremost in consideration whenever collecting and analyzing evidence, and proper forensic procedures should be followed (Daubert, 1993).

iPod Forensics

iPod Design

In its default mode the iPod can accept audio, video, and photo based files. However, in *disk mode* the iPod acts as an external hard drive to the host computer. Disk mode allows for any type of file to be transferred through Windows Explorer. While text files can be created and transferred to the *Notes* folder on the iPod, thus showing up on the device itself, files transferred directly from Windows Explorer will not appear on the iPod while browsing the device through the integrated screen.

Thus, files transferred through Windows Explorer cannot be seen directly on the device. Instead they will be displayed in the iPod's file system during a physical analysis. Therefore, the iPod will only display data on its screen if it is imported through iTunes. This is important to note because all data seen on the iPod screen is a direct result of user interaction through iTunes.

Even with the upgrades in capacity, the "five-point five generation" (5.5g) generation iPods still utilize HFS+ (for iPods initialized on an Apple system) or FAT32 (for iPods initialized on a Windows system). It is important to note however, that iPods initialized on a Windows machine will not be re-initialized upon connection to a Mac, as OS X can read and write to FAT32 volumes. Identifying which file system currently resides on a suspect iPod should be paramount to ensure that the proper analysis tools are utilized. This can be quickly accomplished by browsing the device under the Settings => About menu. If the screen states that it is a "Windows" format, the device has a FAT32 file system. If anything else is displayed the device is using HFS+.

Legal Considerations

Generally speaking, the iPod should be treated as though it were a suspect hard drive. This is not only because there could be important data within the iPod, but there could also be malicious programs prepared to destroy the iPod or any attached system. Items such as iPods should be covered within the details of a warrant ensure, as some judges may not consider iPods (or other digital devices) under the scope of the warrant. If the investigator believes there may be malicious programs installed on the device, a physical removal of the hard drive may be necessary.

Testing

Methodology

Four forensic tools were included in this test: Access Data's Forensic Tool Kit (FTK), FTK Asia, EnCase, and Subrosasoft's Macintosh Forensic Software (MFS). FTK Asia was added for its support of the HFS+ file system. It should be noted that the latest updates of these forensic tools were incorporated as well as the inclusion of a Tableau

T8 Forensic USB write-blocker to eliminate any possibility of data contamination during analysis.

Methods similar to the previous paper were followed to eliminate both errors and to replicate results. The iPod was first initialized under iTunes on a Windows XP SP2 based computer, thus creating the FAT32 file system. Music files and other data were then copied or imported onto the iPod via iTunes or Windows Explorer. After verifying the USB write blocker, each forensic tool imaged and indexed the iPod's file system, creating a baseline for the remainder of the study. Software write-blocking methods were not utilized in this study, as they are generally unreliable, can be subverted and more forensically sound methods are now available (Lyle & Black, 2005). It should also be noted that the internal hard drive of the iPod was not removed during our tests.

This testing occurred on 3rd, 4th and 5.5 generations of the Apple iPod.

High-Level Testing Protocol

- Perform one time zero-out of iPod using *dd* and */dev/zero* as input
- Verify overwrite using forensic tools
- Initialize using iTunes 7.0.1
- Copy files in (2) ways
 - Windows Explorer (or Finder)
 - iTunes
 - Import
 - Synchronize
- Employ USB write blocker
- Image & Analyze with:
 - FTK – Version 1.62.1 - Build 06.07.27
 - FTK Asia – Version 1.0
- Image & Analyze with
 - EnCase – Version 5.05
- Image & Analyze with
 - Subrosasoft's Macintosh Forensic Software – Version 1.6
- Erase predetermined files
 - Delete two of each file type: music, video, document, picture
 - Of these, delete one from iTunes
 - Delete other through Explorer or Finder
 - Hide file in Windows/Mac
 - Mark as hidden in Windows
 - Rename file to ".filename" in Mac
- Attempt to recover using same forensic tools
- Restore using iTunes and re-image and analyze

Testing on Windows XP

- Connect iPod and zero out device using *dd*
- Install iTunes and Apple Software Update
- Connect iPod and initialize using iTunes
- Upload and sync files through Explorer and iTunes
 - Calendar, Contacts
 - Picture and Video
 - Music files
- Connect & verify USB write-blocker
- Image & analyze with forensic tools
- Disconnect write-blocker
- Delete predetermined files
- Re-connect & verify write-blocker
- Re-image and analyze
- Disconnect write-blocker and restore device using iTunes
- Reconnect write-blocker and re-image and analyze

Testing on Mac OS X 10.3.9

- Install iTunes and Apple Software Update
- Connect iPod and initialize using iTunes
- Upload and sync files through Finder and iTunes
 - Calendar, Contacts
 - Picture and Video
 - Music files
- Connect & verify USB write-blocker
- Image with Macintosh Forensic Software
- Mount acquired image and analyze
- Disconnect write-blocker
- Delete predetermined files
- Re-connect & verify write-blocker
- Re-image and analyze
- Disconnect write-blocker and restore device using iTunes
- Reconnect write-blocker and re-image and analyze

Results

Testing performed on three generations of iPods produced interesting results. One such result was the inability of the forensic tools to analyze the HFS+ file system. Once files were deleted in HFS+, the only way to retrieve them was to perform data carving. This often produced odd results, as data carving is simply a “best guess” at determining file types and sizes. Restoring the device under Mac iTunes produced the same results. It appears that “restoring” a device under iTunes simply rewrites the partition tables and

creates a new directory structure. The old data still remains, but file carving must be used to recover it. While file carving was generally successful for images, almost every forensic tool had difficulty carving video files.

Marsico and Rogers (2005) mentioned the ability to find the username and computer that initialized the iPod during their analysis. This is no longer the case. In fact, the DeviceInfo file no longer appears anywhere on the iPod. While this may be a function of iTunes 7.0.1 or even firmware updates to the iPod, it should be noted that the information is no longer contained on the iPod. There are still ways to link the iPod to an individual, however. The unique USB identifier on every iPod can be found on the host computer and the iPod itself by performing a string search for "GUID." Another way to link the suspect to the computer is by looking at their "full-resolution photos" directory path. If the suspect is using an iPod with photo capabilities, they may choose an option under iTunes to store the full-resolution photos on the device as well (rather than just a thumbnail image). The path may be found performing a string search against "frpd." Other information, such as contact information and calendar entries, was easily grabbed by performing string searches such as "VCARD" and "VCAL."

The "five point five" generation iPods (5.5g) proved to be extremely difficult to analyze. This may be due to the fact that the Master Boot Record (MBR) appears almost identical to the Volume Boot Record (VBR). When the Master Boot Record is read as a FAT32 Volume Boot Record, the FAT is interpreted as zero sectors long. According to AccessData, this is the cause of FTK's failure to interpret the 5.5g's file system (M. Hodnett, personal communication, January 22, 2007). Essentially, the only way to analyze the 5.5g iPod was a "live analysis" on a logical drive. This puts a serious constraint on analysis, as unrecognized partitions will be hidden from the forensic tool and the investigator. Both the third and fourth generations of iPods were imaged and analyzed with FAT32 correctly, but again had trouble with the HFS+ file system.

Table 1: Overview of forensic tool success

iPod Version	Forensic Tool	FAT32		HFS+	
		Image	Exam	Image	Exam
3g	FTK Asia	Yes	No	Yes	No
	FTK	Yes	Yes	No	No
	EnCase	Yes ¹	Yes	Yes	No
	MFS	Yes ¹	No	No	No
4g	FTK Asia	Yes	No	Yes	No
	FTK	Yes	Yes	No	No
	EnCase	Yes ¹	Yes	Yes	No
	MFS	Yes ¹	No	No	No
5.5g	FTK Asia	No ³	Yes ²	Yes	No
	FTK	No ³	Yes ²	No	No
	EnCase	Yes ¹	Yes ²	Yes	No
	MFS	No ³	No	No	No

1 - Firmware partition not detected

2 - Only possible with "live" analysis

3 - No file system detected

Windows Version

The Windows version proved much easier to analyze than its Mac counterpart. With the exception of Subrosasoft's MFS, the third and fourth generation iPods were imaged and analyzed successfully with FTK and EnCase. As mentioned, the 5.5g iPod was more difficult to analyze. EnCase performed the best under the FAT32 file system, earning "yes" in every category. However, even EnCase did not successfully capture the firmware partition. Although EnCase performed well, file carving video files was still difficult and produced anomalous results. If it is possible to modify this partition to include arbitrary user data, the tools would not pick this up because of MBR and VBR peculiarities.

Table 2: Tool overview for Windows formatted iPods

iPod Version	Forensic Tool	FAT32					
		File Structure	String Search	Deleted	After Restore	Hidden Files	File Carving
3g	FTK Asia	Yes	Yes	No	Yes	No	Yes
	FTK	Yes	Yes	Yes	Yes	Yes	Yes
	EnCase	Yes	Yes	Yes	Yes	Yes	Yes
	MFS	No	Yes	No	No	No	Yes
4g	FTK Asia	Yes	Yes	No	Yes	No	Yes
	FTK	Yes	Yes	Yes	Yes	Yes	Yes
	EnCase	Yes	Yes	Yes	Yes	Yes	Yes
	MFS	No	Yes	No	No	No	Yes
5.5g	FTK Asia	No	Yes	No	No	No	Yes
	FTK	No	Yes	No	No	No	Yes
	EnCase	Yes	Yes	Yes	Yes	Yes	Yes
	MFS	No	Yes	No	No	No	Yes

Macintosh Version

The HFS+ file system was much more difficult to analyze, but the file system is only placed on the iPod under certain conditions. If the device is initialized under Windows, the file system will remain FAT32, as Mac OS X is able to read and write to FAT32 volumes. However, if the device is first initialized under Mac, or a FAT32 device is “restored” under iTunes using a Mac, then HFS+ will be placed on the iPod. FTK Asia, EnCase, and MFS performed the best under this file system.

MFS requires that the image acquired of the device be mounted as a volume. After it is mounted, hidden files can be displayed, but the software is limited. It cannot report a file as deleted by the user, and file carving (“salvaging” in MFS) produces mixed results. It was, however, the only tool that correctly “salvaged” video files. FTK Asia was able to interpret the file structure correctly, but analysis and reporting utilities with this software were not as robust as its counterpart FTK. FTK was unsuccessful with the 5.5g, except as a “live analysis,” which potentially can exclude large amounts of data. All of the forensic tools may have difficulty because of the 5.5g’s Master Boot Record.

Table 3: Overview of Macintosh formatted iPods

iPod Version	Forensic Tool	HFS+					
		File Structure	String Search	Deleted	After Restore	Hidden Files	File Carving
3g	FTK Asia	Yes	Yes	No	No	Yes	Yes
	FTK	No	Yes	No	No	No	Yes
	EnCase	Yes	Yes	No	No	Yes	Yes
	MFS	Yes	Yes	No	No	Yes	Yes
4g	FTK Asia	Yes	Yes	No	No	Yes	Yes
	FTK	No	Yes	No	No	No	Yes
	EnCase	Yes	Yes	No	No	Yes	Yes
	MFS	Yes	Yes	No	No	Yes	Yes
5.5g	FTK Asia	Yes	Yes	No	No	Yes	Yes
	FTK	No	Yes	No	No	No	Yes
	EnCase	Yes ¹	Yes	No	No	No	Yes
	MFS	Yes	Yes	No	No	Yes	Yes

1 - Firmware partition not detected

Conclusion

The newest generation of iPod, the "5.5g," is capable of storing vast amounts of data. With technology improving, the forensic community will only see the size and complexity of such devices continue to grow. This complexity is revealed through the analysis of current forensic tools on the market. The tools have an extremely difficult time analyzing the newer iPods, along with the HFS+ file system. In addition, software and hardware changes have eliminated the user name and initializing computer on the iPod, one valuable piece of evidence found by Marsico & Rogers (2005). However, valuable forensic evidence can still be found. Calendar entries, contact info, deleted images, and documents can be found using string searches and file carving. The potential evidence contained on an iPod cannot be ignored by the investigator, especially as more and more criminals turn to these devices to obscure their data. From child pornography to stolen information, the iPod is no longer a simple music device. Investigators must know the importance of these devices, and what tools can be used to extract the evidence they require.

© Copyright 2007 International Journal of Digital Evidence

About the Authors

Matthew Kiley is a graduate student pursuing a Masters degree in technology with a specialization in information security from the College of Technology at Purdue University. He is involved with the CERIAS research center and has research interests

in computer forensics, network security, and cryptography. Prior to receiving his masters, he earned an undergraduate degree in telecommunications and networking from Purdue University.

Tim Shinbara received a Masters degree in technology in December of 2006 from the College of Technology at Purdue University. Prior to receiving his masters, he earned an undergraduate degree in telecommunications and networking also from Purdue University. He was involved with Northrop Grumman during his graduate studies, and is currently employed with them.

Marc Rogers, Ph.D., CISSP, CCCI is the Chair of the Cyber Forensics Program in the Dept. of Computer and Information Technology at Purdue University. He is an Associate Professor and also a research faculty member at the Center for Education and Research in Information Assurance and Security (CERIAS).

References

- Apple. (2007). *Apple Reports First Quarter Results*. Retrieved January 19, 2007 from <http://www.apple.com/pr/library/2007/01/17results.html>.
- Carrier, B. (2002). *Open source digital forensics tools: The legal argument* (Research Report): @stake. Retrieved November 19, 2006, from www.digital-evidence.org/papers/opensrc_legal.pdf.
- Daubert v. Merrell Dow Pharmaceuticals (509 US 579 1993).
- Kruse, W. G., & Heiser, J. G. (2002). *Computer forensics: Incident response essential*. Boston: Addison-Wesley.
- Lyle, J. R. & Black, P. E. (2005). *Testing BIOS Interrupt 0x13 Based Software Write Blockers*. Retrieved January 28, 2007 from http://hissa.nist.gov/~black/Papers/testSWB_ECCE05.html.
- Marsico, C & Rogers, M. (2005). iPod Forensics. *International Journal of Digital Evidence, Volume 4 (2)*. Retrieved January 15, 2007 from <http://www.utica.edu/academic/institutes/ecii/publications/articles/B4A8B3F3-94D2-F7E5-D32D97CF1539EBB4.pdf>.
- National Institute of Standards and Technology. (2001). General test methodology for computer forensic tools. In U.S. Department of Commerce (Ed.) (Version 1.9).
- Toshiba Storage Device Division. (2006). *Toshiba Breaks 100GB Threshold For 1.8-Inch Hard Disk Drives*. Retrieved January 21, 2007, from <http://sdd.toshiba.com/localcache/82000000303F0000C88000000010000000.pdf>.