

CA-FCE - iPod Forensics - Matthew Kiley - SAE



CERLAS

the center for education and research in information assurance and security

iPod Forensics Update

Department of Computer & Information Technology Matthew Kiley, Tim Shinbara & Marcus K. Rogers

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, or files and even play full-length movies. Apple's iPod has incorporated all of this into a single device. 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, and which forensic tools are able to acquire this evidence.

erview Explore	Graphics	E-Mail	Search	Bookmark							
Case	· · · · · ·			- m . N		ଚା 🔊					
🗄 🗐 Disk1			- (em.)								
Part_1 Part_1											-
	1										
P I NEPTUNE-FAT32											
Calendars											
Contacts											
DriveFreeSpac	e0001				alasta .						
						I					
Notes					· · · · · ·	I					
🖻 💼 Photos			III .								
E Eul Resolu	ition					I					
⊡ <u> </u>						I					
	18					I					
Thumbs											
onpartopace											
at all descendants											
t all descendants	GFF Unfiltered		All Columns	•	DTZ						
et all descendants	Full Path		All Columns	<u>•</u>	DTZ Recycle Bi Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date
et all descendants	GFF Unfiltered Full Path Disk1\Part_2\NEPTU	INE-FAT32\Pho	All Columns	√2006\10\1	ртz Recycle Bi Ext bmp	File Type Bitmap File	Category Graphic	Subject	Cr Date 10/18/2006 11:26:52	Mod Date 10/9/2006 9:10:04 PM	Acc Date
et all descendants	Full Path Disk1\Part_2\NEPTU	INE-FAT32\Pho INE-FAT32\Pho	All Columns	▼ 1\2006\10\1 1\2006\10\1	Recycle Bi Ext bmp	File Type Bitmap File Bitmap File	Category Graphic Graphic	Subject	Cr Date 10/18/2006 11:26:52 10/18/2006 11:26:50	Mod Date 10/9/2006 9:10:04 PM 10/9/2006 9:09:40 PM	Acc Date 11/8/2006 12:00:00 11/8/2006 12:00:00
t all descendants	 OFF Unfiltered Full Path Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU 	JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho	All Columns	▼ \\2006\10\1 \\2006\10\1 \\2006\10\1	Recycle Bi Ext bmp bmp jpg	File Type Bitmap File Bitmap File JPEG/JFIF File	Category Graphic Graphic Graphic	Subject	Cr Date 10/18/2006 11:26:52 10/18/2006 11:26:50 10/18/2006 11:29:02	Mod Date 10/9/2006 9:10:04 PM 10/9/2006 9:09:40 PM 10/17/2006 7:25:02	Acc Date 11/8/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00 10/80/2006 12:00:00
aqibx. 400x400.bmp	Full Path Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU	JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho	All Columns	▼ \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1	Recycle Bi Ext bmp jpg png	File Type Bitmap File Bitmap File JPEG/JFIF File PiNG File (Po	Category Graphic Graphic Graphic Graphic Graphic	Subject	Cr Date 10/18/2006 11:26:52 10/18/2006 11:26:50 10/18/2006 11:29:02 10/18/2006 11:26:50 10/18/2006 11:26:50 10/18/2006 11:26:50	Mod Date 10/9/2006 9:10:04 PM 10/9/2006 9:09:40 PM 10/17/2006 7:25:02 10/9/2006 9:07:50 PM 10/9/2006 9:07:50 PM	Acc Date 11/8/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00 10/18/2006 12:00:00 10/18/2006 12:00:0
t all descendants	Full Path Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU Disk1\Part_2\NEPTU	JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho	All Columns Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution	▼ \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1	DTZ Recycle Bi Ext bmp bmp ipg png ipg	File Type Bitmap File Bitmap File JPEG/JFIF File PiNG File (Po JPEG/JFIF File JPEG/JFIF File	Category Graphic Graphic Graphic Graphic Graphic Graphic	Subject	Cr Date 10/18/2006 11:26:52 10/18/2006 11:26:50 10/18/2006 11:29:02 10/18/2006 11:26:50 10/18/2006 11:26:50 11/8/2006 3:37:54 PM	Mod Date 10/9/2006 9:10:04 PM 10/9/2006 9:09:40 PM 10/17/2006 7:25:02 10/9/2006 9:07:50 PM 10/9/2006 9:02:16 PM 10/9/2006 9:01:30 PM	Acc Date 11/8/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00 10/18/2006 12:00:0 10/18/2006 12:00:0 11/8/2006 12:00:0 11/8/2006 12:00:0
t all descendants		INE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho	All Columns Dotos\Full Resolution Dotos\Full Resolution Dotos\Full Resolution Dotos\Full Resolution Dotos\Full Resolution Dotos\Full Resolution Dotos\Full Resolution	▼ \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1	Recycle Bi Ext bmp bmp ipg png ipg ipg ipg	File Type Bitmap File Bitmap File JPEG/JFIF File PiNG File (Po JPEG/JFIF File JPEG/JFIF File JPEG/File JPEG/File	Category Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	Cr Date 10/18/2006 11:26:52 10/18/2006 11:26:50 10/18/2006 11:29:02 10/18/2006 11:26:50 10/18/2006 11:26:50 11/8/2006 3:37:54 PM 10/18/2006 11:26:52	Mod Date 10/9/2006 9:10:04 PM 10/9/2006 9:09:40 PM 10/17/2006 7:25:02 10/9/2006 9:07:50 PM 10/9/2006 9:02:16 PM 10/9/2006 9:02:16 PM 10/9/2006 9:02:54 PM	Acc Date 11/8/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00 10/18/2006 12:00:0 10/18/2006 12:00:0 11/8/2006 12:00:0 10/18/2006 12:00:0 10/18/2006 12:00:0
t all descendants	OFF Unfiltered	JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho	All Columns Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution	✓ \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1 \2006\10\1	DTZ Recycle Bi Ext bmp bmp jpg jpg ipg ipg	File Type Bitmap File Bitmap File JPEG/JFIF File PiNG File (Po JPEG/JFIF File JPEG/JFIF File JPEG/Exif file GIF File	Category Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	Cr Date 10/18/2006 11:26:52 10/18/2006 11:26:50 10/18/2006 11:29:02 10/18/2006 11:26:50 10/18/2006 11:26:50 11/8/2006 3:37:54 PM 10/18/2006 11:26:52 10/18/2006 11:26:52	Mod Date 10/9/2006 9:10:04 PM 10/9/2006 9:09:40 PM 10/17/2006 7:25:02 10/9/2006 9:07:50 PM 10/9/2006 9:02:16 PM 10/9/2006 9:02:54 PM 10/9/2006 9:05:04 PM	Acc Date 11/8/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00 10/18/2006 12:00:00 10/18/2006 12:00:00 10/18/2006 12:00:00 10/18/2006 12:00:00 11/8/2006 12:00:00
t all descendants		INE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho	All Columns Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution Dtos\Full Resolution	▼ 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1	Recycle Bi Ext bmp bmp ipg png ipg ipg ipg ipg gif	File Type Bitmap File Bitmap File JPEG/JFIF File PiNG File (Po JPEG/JFIF File JPEG/Exif file GIF File PiNG File (Po	Category Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	Cr Date 10/18/2006 11:26:52 10/18/2006 11:26:50 10/18/2006 11:29:02 10/18/2006 11:26:50 10/18/2006 11:26:50 11/8/2006 11:26:52 10/18/2006 11:26:52 10/18/2006 11:26:52	Mod Date 10/9/2006 9:10:04 PM 10/9/2006 9:09:40 PM 10/17/2006 7:25:02 10/9/2006 9:07:50 PM 10/9/2006 9:02:16 PM 10/9/2006 9:02:54 PM 10/9/2006 9:02:54 PM 10/9/2006 9:05:04 PM	Acc Date 11/8/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00 10/18/2006 12:00:00 10/18/2006 12:00:00 11/8/2006 12:00:00 10/18/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00
t all descendants t all descendants lunny2.bmp aqibx.400x400.bmp blah.ipg C64 Funny Writer 3.0.png elks_portable_football.ipg football.ipg footb	 OFF Unfiltered Full Path Disk1\Part_2\NEPTU 	INE-FAT32\Pho INE-FAT32\Pho INE-FAT32\Pho INE-FAT32\Pho INE-FAT32\Pho INE-FAT32\Pho INE-FAT32\Pho INE-FAT32\Pho INE-FAT32\Pho INE-FAT32\Pho	All Columns Dtos\Full Resolution Dtos\Full Resolution	<pre></pre>	DTZ Recycle Bi Ext bmp bmp ipg png ipg ipg ipg ipg gif pg gif png	File Type Bitmap File Bitmap File JPEG/JFIF File PiNG File (Po JPEG/JFIF File JPEG/Exif file GIF File PiNG File (Po PiNG File (Po	Category Graphic Graphic e Graphic e Graphic e Graphic e Graphic graphic Graphic Graphic Graphic	Subject	Cr Date 10/18/2006 11:26:52 10/18/2006 11:26:50 10/18/2006 11:29:02 10/18/2006 11:26:50 10/18/2006 11:26:50 11/8/2006 11:26:52 10/18/2006 11:26:52 10/18/2006 11:26:52	Mod Date 10/9/2006 9:10:04 PM 10/9/2006 9:09:40 PM 10/17/2006 7:25:02 10/9/2006 9:07:50 PM 10/9/2006 9:02:16 PM 10/9/2006 9:02:54 PM 10/9/2006 9:05:04 PM 10/9/2006 9:07:30 PM 10/9/2006 9:06:32 PM	Acc Date 11/8/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00 10/18/2006 12:00:00 10/18/2006 12:00:00 10/18/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00
t all descendants		INE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho	All Columns Dotos\Full Resolution Dotos\Full Resolution	▼ 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1 1/2006/10/1	Recycle Bi Ext bmp bmp ipg ipg ipg ipg ipg ipg gif png gif	File Type Bitmap File Bitmap File JPEG/JFIF File PiNG File (Po JPEG/JFIF File JPEG/Exif file GIF File PiNG File (Po GIF File	Category Graphic Graphic e Graphic e Graphic e Graphic e Graphic Graphic Graphic Graphic Graphic Graphic	Subject	Cr Date 10/18/2006 11:26:52 10/18/2006 11:26:50 10/18/2006 11:26:50 10/18/2006 11:26:50 10/18/2006 11:26:50 11/8/2006 11:26:52 10/18/2006 11:26:52 10/18/2006 11:26:52 10/18/2006 11:26:52	Mod Date 10/9/2006 9:10:04 PM 10/9/2006 9:09:40 PM 10/17/2006 7:25:02 10/9/2006 9:07:50 PM 10/9/2006 9:02:16 PM 10/9/2006 9:02:54 PM 10/9/2006 9:02:54 PM 10/9/2006 9:05:04 PM 10/9/2006 9:06:32 PM 10/9/2006 9:06:32 PM	Acc Date 11/8/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00 10/18/2006 12:00:0 10/18/2006 12:00:0 10/18/2006 12:00:0 10/18/2006 12:00:0 11/8/2006 12:00:0 11/8/2006 12:00:00 11/8/20000 11/8/20000 11/8/20000 11/8/200000 11/8/200000 11/8/
t all descendants		INE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho JNE-FAT32\Pho	All Columns Dtos\Full Resolution Dtos\Full Resolution	✓ 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1 1/2006\10\1	DTZ Recycle Bi Ext bmp bmp ipg png ipg ipg ipg ipg gif png gif ipg gif ipg	File Type Bitmap File Bitmap File JPEG/JFIF File PiNG File (Po JPEG/JFIF File JPEG/Exif file GIF File PiNG File (Po GIF File Bitmap File	Category Graphic Graphic e Graphic e Graphic e Graphic graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	Cr Date 10/18/2006 11:26:52 10/18/2006 11:26:50 10/18/2006 11:26:50 10/18/2006 11:26:50 10/18/2006 11:26:50 11/8/2006 11:26:52 10/18/2006 11:26:52 10/18/2006 11:26:52 10/18/2006 11:26:52 10/18/2006 11:26:52	Mod Date 10/9/2006 9:10:04 PM 10/9/2006 9:09:40 PM 10/17/2006 7:25:02 10/9/2006 9:07:50 PM 10/9/2006 9:07:50 PM 10/9/2006 9:02:16 PM 10/9/2006 9:02:54 PM 10/9/2006 9:02:54 PM 10/9/2006 9:05:04 PM 10/9/2006 9:05:04 PM 10/9/2006 9:05:04 PM 10/9/2006 9:05:32 PM 10/9/2006 9:04:04 PM 10/9/2006 9:04:04 PM 10/9/2006 9:04:04 PM	Acc Date 11/8/2006 12:00:00 11/8/2006 12:00:00 11/8/2006 12:00:00 10/18/2006 12:00:0 10/18/2006 12:00:0 10/18/2006 12:00:0 11/8/2006 12:00:0 11/8/2006 12:00:00 11/8/20000 11/8/200000 11/8/2000000 11/8/20000000000000 11/8/20000000000000000000000000000000000

PROBLEM

Software, firmware and forensic tool revisions have made updates to previous research necessary. These revisions create unknown effects during forensic Locating evidence deleted from iTunes and Explorer

		FA	T32	HF	S+
iPod Version	Forensic Tool	Image	Exam	Image	Exam
Зg	FTK Asia	Yes	No	Yes	No
	FTK	Yes	Yes	No	No
	EnCase	Yes ¹	Yes	Yes	No
	MFS	Yes	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

examinations and may change what data can be extracted from a device. These changes must also be recognized for law enforcement and other organizations in order to be effective against criminals that are utilizing iPods in unintended ways.

RESULTS

Data such as pictures, documents, and calendar entries could be easily found using data carving or string searches. Almost every tool however had difficulty carving video files, which could pose a problem for investigators. The tools were also incapable of analyzing the HFS+ file system found on Macintosh formatted iPods. In addition, the analysis of 'five point five' generation iPods, which have nearly identical Master Boot Records and Master Volume Records, proved challenging with current forensic tools. Finally, the user name and computer name used to initialize the iPod can no longer be found under the iPod_Control directory. 1 - Firmware partition not detected

2 - Only possible with "live" analysis

3 - No file system detected

Forensic Tool Overview

FUTURE WORK

The resulting interaction between the iPod operating system and the internal hard drive on forensic tools is unknown. Future analysis could include physical removal of the hard drive to determine these effects. In addition, other portable devices and technologies have yet to be analyzed such as:

- Solid state devices (iPod Nano)
- Apple iPhone
- Microsoft Zune





