CERIAS

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

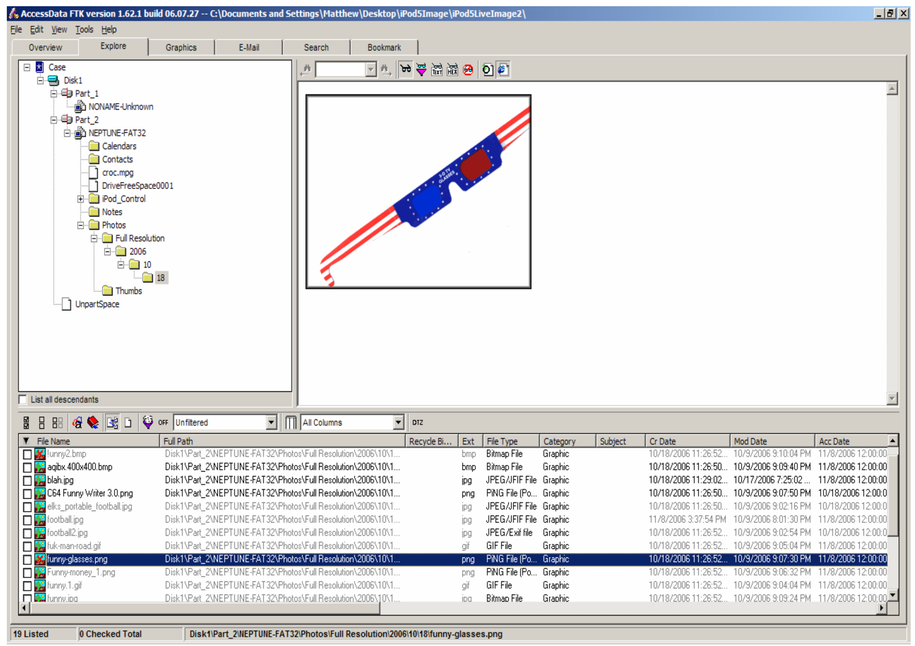
From student to business worker, the popularity and ubiquity of mobile devices is exploding. As these devices saturate modern culture, they continue to grow in functionality. Such devices can now play music, store photos, contacts, or files and even play full-length movies. Apple's iPod has incorporated 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.

PROBLEM

Software, firmware and forensic tool revisions have made updates to previous research necessary. These revisions create unknown effects during forensic 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.



Locating evidence deleted from iTunes and Explorer

		FAT32		HFS+	
iPod Version	Forensic Tool	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

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

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center