CERIAS

iPod Forensics

Christopher V. Marsico & Marcus K. Rogers
Purdue University
Dept. of Computer Technology
Cyber Forensics Lab
CERIAS

Abstract

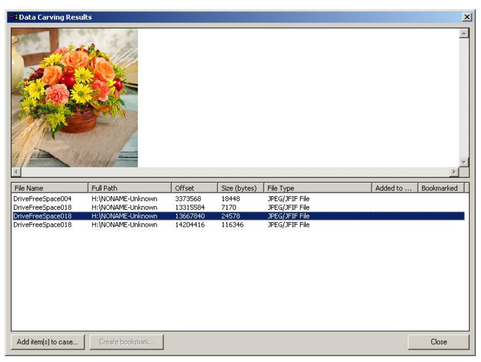
The iPod is the most popular digital music device. The newest versions of the iPod have become more PDA like then ever before. With this new functionality the iPod has recently found its way into the criminal world. With the continued growth of the digital music device market, the iPod's use in criminal activity will only continue to increase. This research discusses some of the features of the iPod and how a criminal could use them. Literature review found little or no documentation or discussion on the forensic analysis of the iPod or similar devices. Therefore, this research outlined what should be considered when an iPod is found at the crime scene, and offers a critical analysis of some common forensic tools and their ability to collect and analyze data from an iPod.

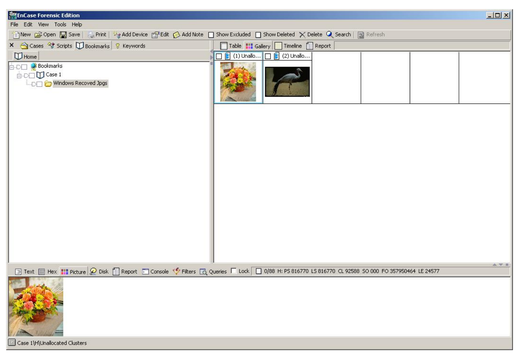
The Problem

The iPod is a digital device that can hold any type of file. They are not simply just for music. This unique device is something that should be of interest to a forensic examiner. Recently, the proliferation of the iPod has advanced it into the criminal world. These devices are simply portable hard drives of which the largest versions can store up to 60 GB. Apple has branched out and included additional applications. The iPod now has contact book, calendar and other features. The newest version can even display photos on a color screen. These types of devices are only going to become more popular and 10 million+ have already been sold. A first responder is currently not prepared for these types of devices and there is no documentation on how well the common tools, used by cyber forensic practitioners of today, work with the iPod. There are two versions of the iPod; the Macintosh version which uses the HFS+ file system and the Windows version that uses the FAT file system. These two versions each have unique requirements for the recovery of information from them.

Testing

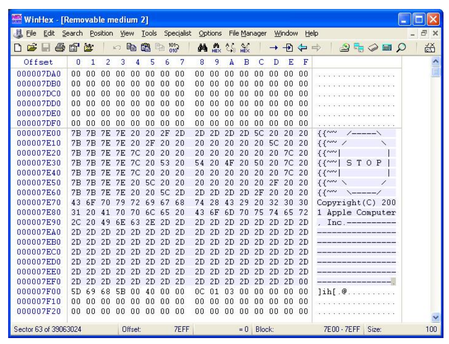
This research tested EnCase, Forensic Tool Kit (FTK) and Blackbag's Mac Forensic Software (MFS). These common forensic tools were tested for the latten file recovery from the iPod. The iPod was loaded with picture files, documents, contacts, and calendar entries. These files were then viewed using the forensic tools. The files were deleted and then recovered. Also the iPod underwent the "restore" feature of the iPod updater software. Finally the iPod was switched several times from the HFS+ to FAT file system and vise versa.





Results

The information found on the iPod could be seen as a wealth of information to a law enforcement officer or a privacy concern. The forensic tools tested in this research were successful at the extraction of latent deleted files from the iPod. Files were able to be recovered even after the device had been put though the "restore" function of the iPod updater. The forensic tools were also able to recover data from the iPod after the device was reformatted once or several times between files systems. The tools are much more capable with the FAT version of the iPod then with the HFS+ version. The iPod also records the computer and username of the computer it is first connected to. EnCase proved to be the most successful at data recovery for both versions of the iPod.



PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center