iPod Forensics

Christopher V. Marsico
Marcus K. Rogers
Purdue University Cyber Forensics Lab
Department of Computer Technology
Purdue University

Abstract

The iPod is one of the most popular digital music devices in today’s marketplace. The newest versions of the iPod have become more PDA/storage like than 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 paper discusses some of the features of the iPod and how a criminal could use them. A literature review found little or no documentation or discussion on the forensic analysis of the iPod or similar devices. Therefore, this research outlines 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. Suggestions for future research are also provided.

iPod Forensics

The Apple iPod is the most common digital music player on the planet. Having sold over four million units, the iPod has become a household name and has skyrocketed Apple computer back to mainstream success (Thomas, 2004). The combination of Apple’s iTunes and the iPod has been a “tremendous knock out punch” in the digital music market and a driving force for the digital music revolution. Similar to the way the personal computer became common in the home in the 80s and 90s, the iPod is becoming common today.

An example of the proliferation of the iPod is Duke University’s iPod project. In 2004, all freshmen at Duke were given an iPod as part of a research project to study the use of the device to enhance learning ("Duke iPod first-year experience FAQs," 2004). The students were encouraged to use the device to store their files, academic calendars, contacts, and input their homework assignments as tasks (Menzies, 2004).

While most users see the iPod as a device for entertainment and enjoyment, others have found ways to use the iPod for more devious endeavors. This has allowed a criminal element to find “alternative” uses for a seemingly harmless device, and the

Apple iPod is finding its way into the criminal's bag of tricks. As more features are added to the iPod, to make life more convenient for its users, some decide to use these conveniences to further their criminal trade craft.

Those who have chosen a different path, one of enforcing the laws of society, now must come to understand that the iPod and similar devices are used for these criminal purposes. Investigators must be prepared to encounter these devices in the crime scenes of today and stay one-step ahead of the criminal element. This paper discusses the importance of understanding what type of evidence the Apple iPod can contain and how this evidence can be collected – one of the first steps in the digital forensic process. This paper outlines some of the features of the iPod that may be used by criminals in facilitation of their crimes, offers recommendations for best practices when encountering the iPod in today's crime scene, and critically analyzes several forensic tools that can be used to collect evidence from the iPod[1].

iPod Design

In disk mode, the iPod can store other types of files, such as documents or pictures. Apple's digital music player has a capacity of up to 60GB. With this much storage space, Apple has branched out and included features like calendar and contacts ("Apple iPod - music and more", 2004). The latest versions include photo viewing and a color screen. Additionally with proper configuration, an iPod can run Linux and even contain all the necessary information for a computer system to run effectively (Knaster, 2004). This would allow an individual to carry their entire computer around with them and boot it via their iPod attached to any computer. With the iPod taking on more PDA and storage like characteristics, investigators must understand how to deal with iPods; similar to the work done by the National Institute of Standards and Technology (NIST) in developing guidelines for PDA forensics (Jansen & Ayers, 2004).

The iPod uses the Apple HFS+ file system when the device is run with an Apple system and uses the FAT32 file system when used with a Windows PC. The differences in these file systems make each version of the iPod a little different. Therefore, an individual who wishes to forensically analyze an iPod must be aware of the type of device with which they are dealing. The iPod can be configured with a variety of capacities. They include 20, 40 and now 60 GB versions. All iPods run similar software, though there are four different generations and now there is an iPod photo with additional features.

The iPod uses the standard vCard file format for storing contact information. Calendar entries are stored in the industry standard vCalendar format. Music is stored in a range

[1] This paper is an academic contribution to the cyber forensic community. This is by no means a legal document and no guarantees are made by the authors that in following the guidelines of this paper, the evidence collected will be admissible to a court. As always consult with a knowledgeable attorney before attempting to collect evidence from an unknown situation.

of folders on the device and can be played in AAC, MP3 and other file formats. These main types of files are the majority of information on the iPod. However, users can store any file they wish on the device including encrypted or hidden files. Commercial accessories will allow an iPod to be used for a variety of functions including voice recording and digital camera photo storage.

A criminal can use the iPod and all its features in a variety of ways. Calendar entries may contain dates of crimes or other events that could be related to a crime. The contact information of conspirators or victims, along with photos or other documentation, could all be transferred and stored on the iPod. Any of the files on the device may be of relevance to the case. As an example, recently in the UK a gang of car thieves was captured and evidence that will be useful to their prosecution was found on an Apple iPod (BBC News, 2004). The iPod was used to store and pass information between the members of the gang about the cars they stole.

Legal Considerations

When evidence is being prepared for possible submission to court proceedings, it is important for it to be collected in a forensically sound manner (Kruse & Heiser, 2002). The case of *Daubert v. Merrell* outlines the rules necessary for scientific evidence admissibility ("Daubert v. Merrell Dow Pharmaceuticals," 1993). Additionally, the case of *Kumho Tire Co. Ltd. v. Carmichael* extended these criteria to technological and engineering evidence ("Kumho Tire Co. Ltd. v. Carmichael," 1999). Carrier (2002), in *Open source digital forensics tools: The legal argument,* discusses the fact that well documented and commonly accepted tools and techniques are necessary for admissibility under the Daubert criteria. Care must be taken to ensure that evidence collected from an iPod meets these criteria.

Because of the iPod’s large capacities and increased functionality, the cyber forensic and law enforcement community should treat it in a similar manner to how they treat a suspect’s hard drive. As discussed, suspects could potentially store key evidence on the iPod, and thus, a proper method for handling this type of evidence must be developed. This poses an interesting challenge for the forensic examiner, especially in terms of collection and analysis.

Crime Scene Considerations

It is now necessary to search a physical crime scene and a suspect’s personal effects for iPods or other digital music devices. Some considerations when an iPod is found at a crime scene include:

- The first responder should wait for the advice of a forensics specialist before any evidence is collected.
- Documentation of where the device is in the scene should be taken by photographing its location and anything around it.

- The device should be left in its current state, as it is possible that the device could be booby trapped with a delete command set to execute if the device is disconnected from a charger or computer.

Some axioms for the collection process are as follows. When collecting the device, note its state when at the scene. If the device is connected to a computer at the scene, check to see if the device is mounted. Determining whether a device is mounted can be done by looking at the screen of the iPod, if it says “Do Not Disconnect” it is then necessary to unmount the device before disconnecting it from the computer. Dragging the icon of the iPod to the trashcan on the Macintosh desktop will do this. It is important to note the name of the iPod on the desktop before unmounting it. It is not a good idea to simply disconnect or unplug the computer, because the iPod’s disk could be damaged if not disconnected properly. If the iPod is connected to a Windows machine, it is recommended that it also be unmounted by clicking the “Unplug or eject hardware” icon on the task bar on the bottom right of the screen. The type of machine the device is connected to will give the forensic analyst a better ideal of what type of tools to use when analyzing the device. This information should be recorded and kept with the documentation of the iPod.

The iPod should be stored in the same manner as a hard drive -- in a static free bag -- and marked as evidence. It should not be stored near anything, such as a magnet, that could damage evidence on the device. Traditional good evidence procedures should be followed and the chain of custody should be thoroughly documented.

Unlike some PDAs, the iPod does not need to be connected to a power supply while in storage. The contents of the device’s hard drive will not be lost if the device loses power. It is important to note however that it is possible for the battery to drain to a point where it may not be possible to charge it again and will need to be replaced. While this is unlikely, it is possible in cases where an iPod may remain in storage for several years.

When the iPod is taken to the lab for analysis, it is important to report the type of computer or computers that were found on the scene. The name of the computer with which the iPod t was initialized is stored on its drive. This information will be very useful in linking any evidence found on the device to the computers at the scene and then to the suspect.

Finally, determining if an iPod is formatted for Macintosh or Windows can be done on the device itself by selecting: “Settings >” then “About >”. When scrolling down in the “About” display, “Format: Windows” will show at the bottom of the screen if it is formatted for Windows. If that phrase is not there, it is safe to assume that it is an HFS+ formatted Macintosh iPod.

Testing

Methodology

Once the iPod has been identified as containing potential evidence, it needs to be examined and analyzed. This is problematic, as no standard protocol has yet been published. In order to assist law enforcement, several tests were conducted to identify any problems or issues. The testing methodology used the National Institute of Standards testing methodology for forensic tools as a guideline. The NIST testing methodology is based on ISO 17025 (National Institute of Standards and Technology, 2001).

Three forensic tools were included in the test, Access Data's Forensic Tool Kit (FTK), EnCase Forensic Edition, and Blackbag Technologies' Macintosh Forensic Software (MFS). FTK and EnCase are two of the most prominent tools available today. Blackbag's MFS is a forensic tool exclusive to Apple Macintosh platform. The Sleuthkit/Autopsy browser was not used in this testing due to the fact that it does not support HFS+.

The method for assessing the collection of evidence from the iPod consisted of testing the iPod with each tool to determine if data could be collected from the device with the tool and if deleted entries could be retrieved. This was done for both the Macintosh format of the iPod and the Windows format. It was hypothesized that the tools would work properly even through the firewire interface. However, it may also be necessary to disassemble the iPod and remove the hard drive for true forensic analysis. At the time of the study, no hardware write block devices were available for the standard firewire or USB interfaces. A means of software write blocking was later discovered and can be accomplished through the modification of the Windows XP Service Pack 2 registry. This software write block capability was not tested in this research. Finally testing was conducted on different platforms to determine if cross platform forensics can be done on the device or if analysis must be done in the device's native environment.

This testing occurred on a new fourth generation 20 GB Apple iPod. (http://docs.info.apple.com/article.html?artnum=61688#clickwheel). Apple's iTunes version 4.7 and iPod Updater 2004-08-06 were also used for this testing.

Testing Protocol

- **<u>Remove device from packaging</u>**
  - Photo and Document Everything
  - Charge Device's Battery
  - Start Device
    - Select English and note any other settings

Testing Mac Version:

- Connect to Mac
- Record information found on device.
- Connect to a Windows Machine via firewire (Without iTunes)
    - Explore media via forensic tools
- Connect to Mac
    - Explore use with Mac and iTunes
    - Add contacts
    - Add calendar
    - Upload files (Microsoft Word, JPEG image and text file)
- Use MFS tool via firewire
    - Explore media
- Connect to a Windows Machine via firewire (Without iTunes)
    - Explore media via forensic tools
- Connect to Mac and delete all information
- Use MFS tool via firewire
    - Explore media
    - Attempt to recover deleted information
- Connect to a Windows Machine via firewire (Without iTunes)
    - Explore media via forensic tools
    - Attempt to recover deleted information

Full system restore as described in the users manual.

- Examine with Forensics tools in
    - Mac
        - Attempt to recover deleted information
    - Windows
        - Attempt to recover deleted information

Testing of Windows Version:

- Connect to windows system
    - Install iTunes and iPod Updater
    - Reformat
    - Documents changes to the device
    - Explore features in Windows
- Run forensic software (Mac & Windows) to recover old files on device before reformat
- On Windows system
    - Upload Files (Microsoft Word, JPEG image and text file)
- Use Windows forensic tools
    - Find files
- Connect to Mac and use MFS
    - Find files
- Delete files from Windows machine
- Use Windows forensic tools

Recover Deleted Files
Connect to Mac and use MFS
Recover Deleted Files

<u>Full system restore</u>

Results

The results indicated that EnCase was the most suitable forensic tool for collection of information from both versions of the iPod, given the testing protocol used. All of the research questions above were answered. It was shown that information could be recovered after it was deleted from both versions of the iPod and tools on both platforms were able to recover deleted information no matter how the iPod was formatted (Mac or Windows). This demonstrates cross platform compatibility. It was found that information could be recovered even after a full restore. Apple claims that the full restore function, “completely erases your iPod.” This is only partially true, as residual information and files can be recovered even after multiple restores. It was also observed that after the device was reformatted from the HFS+ Mac version to Windows FAT32 version, data could still be recovered even after switching the file system several times.

An interesting discovery was that the iPod keeps a persistent record of the computer with which it is initialized; the username of the computer user and the computer’s name are saved. This information is located just underneath the iPod device name in several locations on the drive. An analyst using a string search for the iPod’s name can easily find these other two entries. The username is directly underneath the iPod name and the computer name is underneath the username in the DeviceInfo file in the iTunes folder under the iPod_Control folder and in other places on the drive. This information can be potentially useful in cases that hinge on connecting the device to a particular user, account, or computer system. If the username stored on the iPod is the same as the username of the Mac computer that it was attached to, the iPod can be linked to the suspect’s computer and to the suspect’s account.

The calendar and contact entries are also easily found on the iPod by doing a string search. The standard vCard and vCalendar formats store the entries on the hard drive in plain text and the information can be found by searching the hard drive for the strings in the header of the file. A calendar entry is stored with the file header of “BEGIN:VCALENDAR.” The contacts can be found with the file header “BEGIN:VCARD.” These file headers note the beginning of each vCalendar or vCard entry and remain even after a file is deleted.

The iPod also has another investigation friendly characteristic. It appears that the iPod stores information using the entire disk from beginning to end before returning to the beginning to store information again in areas that may have been deleted. It is possible the iPod is using a technique similar to “wear leveling,” which helps prevent one area of the disk from being used more often then the rest and possibly getting worn out (The PC Guide, 2001; Wong, 2005). This has implications for the forensic investigator because old entries do not become over written as quickly.

Macintosh Version

The HFS+ Mac formatted version of the iPod was more difficult to analyze than the Windows version. The Mac version nonetheless had a major difference that could make it more lucrative to the forensic examiner. All of the forensic tools were able to read some information off of the HFS+ iPod, though some were better then others.

The Forensic Tool Kit from Access Data, was unable to interpret the HFS+ file structure, but did allow an examiner to see the hard drive with disk viewer in HEX format and index strings on the drive. FTK did not interpret any of the files on the HFS+ formatted disk including the documents or pictures. The entire drive appeared as free space and had to be indexed. From this, images and word documents could be carved. Text files could only be found though a string search for known words in the file. Searches for vCard and vCalendar entries easily produced results.

Blackbag's MFS was able to read the iPod, but some of its tools are designed to only analyze an image of the device. When an image was created using Apple's Disk Utility software, MFS could recover deleted pictures and old contacts out of the disk image. Creating a disk image is not a true bit by bit image and is not considered a forensically sound approach. MFS was only useful at bringing out deleted pictures from the image file. The image created by the Apple Disk Utility was a .dmg file and was not readable by EnCase or FTK. It should be noted that the use of DD to create a true bit by bit image on the Macintosh failed. The DD program run from a terminal window reported that the "Device is busy" and was unable to create an image.

EnCase was the most efficient and user friendly for recovering data from the HFS+ file system. The tool was able to display the file structure of the HFS+ formatted device, including hidden folders. It was not, however, able to automatically display deleted files. For this, the Find File script had to be used to carve out deleted files including images and word documents. These searches were easily, but not as quickly, done using the scripting option. String searches were also successful for vCard and vCalendar entries.

It was also noted that deleting files on the iPod actually moved the files to the trash, but did not delete them. The iPod has a folder named ".Trashes" that can be viewed using the forensic tools. When files are deleted or moved to the trash and the trash is not emptied, the files are simply moved to the ".Trashes\501" folder. The files are easily accessible in the ".Trashes\501" folder from a file viewer that can recognize hidden files or a forensic tool. Once the trash is emptied, the files are deleted, but can still be found by using the deleted file recovery process of the forensic tool on the ".Trashes\501" folder. This makes locating deleted files easier and lessens the places that must be searched. It is recommended that the entire device be searched for deleted files, because in some instances files can be removed without being moved to the ".Trashes" folder first.

Contact and calendar entries that are deleted are also moved to ".Trashes". Entries that are not deleted are stored in their corresponding folders. Calendar entries are stored in an .ics file in the Calendars folder. Contact entries are stored in .vcf files in the Contacts folder.

Overall, the results indicated that with the HFS+ formatted device the forensic tools tested were useful for conducting a forensic examination. Cross platform compatibility when using a forensic tool was shown and a Windows machine did not need to have iTunes installed to register the iPod as a device. The iPod will mount as a drive without iTunes installed.

Windows Version

The Windows version of the iPod is formatted with the FAT32 file system and can be easily read by a Windows machine. The FAT32 formatted device was easily analyzed by the Windows forensics tools used in this study. Both EnCase and FTK were able to effectively recognize the device and show file structures and files that had been deleted since the conversion to a FAT32 file system. One of the interesting differences was the lack of a ".Trashes" folder on the FAT32 formatted devices. In testing when files were deleted on the iPod, it was found that they were actually deleted and not simply moved to a ".Trashes" folder. However, these files could be easily recovered by the forensics tools in the Windows environment. All the tools were able to use string searches to find vCard and vCalendar entries. The results confirmed that it was much easier to recover information and find files relevant to possible criminal activity on a FAT32 formatted device.

FTK was the fastest at recovering information for the Windows iPod. The indexing allowed fast string searches, which allowed the quick carving of images and document files. The file structure was completely interpreted, including file slack and free space. Files that were added to the Windows version and then deleted, were quickly shown directly in the file tree structure. To recover files from before the restore and reformat operations the carving function had to be used. This function was successful at recovering all the images ever placed on the device.

EnCase also worked well with the FAT32 formatted iPod. EnCase correctly displayed the file structure and files deleted in the FAT32 format. The File Find script in EnCase was also able to recognize these deleted files, as well as images and word documents deleted and on the device prior to both restore and reformat operations.

Mac Forensic Software was also able to locate the files and directories on the FAT32 iPod. The Mac Carver image software could not be used because it requires an image and an image of the iPod was not created for the Windows version. When connecting a FAT32 iPod to the Macintosh, a ".Trashes" folder is automatically added to the device.

In an investigation, this would corrupt the evidence and probably result in loss of admissibility. This being the case, it is again important to know what type of iPod is being examined before conducting an analysis; without proper write protection, a Macintosh OS X system should not be used to analyze a Windows iPod.

Conclusion

The Apple iPod should be identified as a possible source of evidence in any crime scene investigation. As a digital device, it takes on two different yet related functions – music player and storage media. In the collection and analysis of the iPod, some of the popular computer forensics tools of today proved to be sufficient in accessing and recovering information and deleted entries.

Although the current study was exploratory and limited by the testing of only three computer forensics tools, the results have serious implications for the computer forensics field. Investigators and analysts need to be aware of the type of file system with which the device has been formatted, as this affects the ability of the various tools to correctly interpret and display the file and directory structure. The finding that data is stored in a manner that increases the likelihood of recovering deleted files, while decreasing the probability of data being overwritten, is significant. This should allow for easier reconstruction of events and timelines.

Another important finding is that the iPod can be linked to the computer system and user account that originally initialized it. In cases where an iPod is seized in the absence of a computer system, it is possible to determine what system it was connected to, and which user had accessed the device – at least initially.

Further research needs to be done on imaging an iPod and development of a forensically sound acquisition protocol using both software write blockers and USB or Firewire write blockers. With the continued proliferation of the iPod, it is important that forensic tools be written with better support for the HFS+ file system and the Apple Macintosh.

The cyber forensic practitioners of tomorrow will not only find the iPod in their crime scenes, but a diverse array of unique devices that have not been thought of yet. The cyber forensic community must be ready to accept the continued evolution of technology and respond with scientifically sound theories, tools, methods, and practices, to account for the ever-changing technology world.

“When you have eliminated all which is impossible, then whatever remains, however improbable, must be the truth.” (Sir Arthur Conan Doyle – Sherlock Holmes- The Adventure of the Blanched Soldier)

About the Authors

Christopher Marsico received a Masters degree in technology with a specialization in information security and assurance in May of 2005 from the College of Technology at Purdue University. He was involved with the CERIAS research center and has research interests in computer forensics, especially mobile devices such as digital music devices, biometrics and network security. Prior to receiving his masters, he earned an undergraduate degree in telecommunications and networking also from Purdue University. Christopher is currently pursuing other opportunities.

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

Daubert v. Merrell Dow Pharmaceuticals (509 US 579 1993).

Kumho Tire CO. Ltd. v. Carmichael (526 US 137 1999).

Apple iPod - Music and More. (2004). Retrieved September 3, 2004, from www.apple.com/ipod/musicandmore.html

Duke iPod first-year experience FAQs. (2004). Retrieved September 3, 2004, from http://www.duke.edu/ipod/help/faq.html

BBC News. (2004). iPod car theft ringleader jailed. Retrieved September 3, 2004, from http://news.bbc.co.uk/1/hi/england/london/3932847.stm

Carrier, B. (2002). *Open source digital forensics tools: The legal argument* (Research Report): @stake. Retrieved September 10, 2004, from http://www.atstake.com/research/reports/acrobat/atstake_opensource_forensics.pdf

Jansen, W., & Ayers, R. (2004). Guidelines on PDA forensics (Draft Special Publication 800-72 ed.): National Institute of Standards and Technology.

Knaster, S. (2004). *Hacking iPod and iTunes*. Indianapolis, IN: John Wiley & Sons.

Kruse, W. G., & Heiser, J. G. (2002). *Computer forensics: Incident response essential.* Boston: Addison-Wesley.

Menzies, D. (2004). Duke to give Apple iPods to first-year students for educational use. Retrieved September 3, 2004, from http://www.dukenews.duke.edu/news/ipods_0704.html

National Institute of Standards and Technology. (2001). General test methodology for computer forensic tools. In U.S. Department of Commerce (Ed.) (Vol. 1.9).

The PC Guide. (2001). Wear leveling. Retrieved December 1, 2004, from http://www.pcguide.com/ref/hdd/perf/qual/featuresLeveling-c.html

Thomas, D. (2004). Mobile threat to company data exposed by security experts. Retrieved September 9, 2004, from http://www.personneltoday.com/pt_news/news_daily_det.asp?liArticleID=25477

Wong, W. (2005). Mobile storage: Chips served with hard-disk salsa. Retrieved, April 29, 2005, from http://www.elecdesign.com/Articles/Print.cfm?ArticleID=10184