CERIAS Tech Report 2005-13

IPOD FORENSICS

by Christopher V. Marsico & Marcus K. Rogers

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Running head: iPod Forensics

iPod Forensics

Christopher V. Marsico
marsicoc@purdue.edu
&
Marcus K. Rogers
rogersmk@exchange.purdue.edu

Purdue University Cyber Forensics Lab
Department of Computer Technology
1421 Knoy Hall, Room 225
Purdue University
West Lafayette, IN, USA, 47907

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 paper 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 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 given.

Keywords: iPod, iPod forensics, digital music device, cyber forensics, tool testing, collection, analysis

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. 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. Similar to the way the personal computer became common in the home in the 80s and 90s, the iPod is becoming common today. 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 in their profession. Sometimes this profession just happens to be the world of crime.

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 being 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 preparation involves gaining an understanding of what type of evidence the Apple iPod can contain and how this evidence can be collected. This paper outlines some of the features of the iPod that maybe used by the criminal 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

The problem of this study is to determine if data can be collected in a forensic manner from an Apple iPod digital music device. In recent years, there has been a proliferation of iPods. iPods are simply a portable hard drive and have the ability to store more then just music files that can be replayed by the user.

As a hard dive, 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. With the iPod taking on more PDA like characteristics, it necessary for work to be done similar to the work done by the National Institute of Standards and Technology (NIST) in developing guidelines for PDA forensics (Jansen & Ayers, 2004). 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.

---

[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.

An example of the proliferation of the iPod is Duke University's iPod project. This year 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).

The iPod uses the Apple HFS+ file system when the device is run with the Mac and uses the FAT32 file system when used with a Windows PC. The differences in these file systems makes each version of the iPod a little different and 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 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 though users can store any file they wish on the device including encrypted or hidden files. 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 on the cars they stole.

Legal Considerations

It is important for evidence to be collected in a forensically sound manner when it is being prepared for possible submission to court proceedings (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 as well ("Kumho Tire Co. Ltd. v. Carmichael", 1999). Carrier (2002) discusses the fact that well documented and commonly accepted tools and techniques are necessary for admissibility under the Daubert criteria. These requirements are not currently met for the collection of evidence from an Apple iPod.

With its large capacities and increased functionality, the cyber forensic and law enforcement communities should treat the iPod as they would treat a suspect's hard drive. As discussed, suspects could potentially store key evidence on them and there must be a method developed for it to be recovered. This poses an interesting challenge for the forensic examiner, especially in terms of collection and analysis. It is now necessary to search a physical crime scene and a suspect's personal effects for iPods or other digital music devices. When encountering an iPod in a crime scene, it is important not to overlook the device.

Crime Scene Considerations

Some considerations when an iPod is found at a crime scene include the following, as always the first responder should wait for the advice of a forensics specialist before any evidence

is collected. Document where the device is in the scene. This should be done by photographing its location and anything around it. Leave the device in its current state. 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.

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. This 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 should also be unmounted by clicking the “Unplug or eject hardware” icon on the task bar on the bottom right of the screen, though this step is not necessary in the Windows environment. The type of machine it 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 like 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 event is unlikely, it is possible in cases where an iPod may remain in storage for more than 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 iPod will store the computer name of the machine it was initialized with 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 >”. If the device is formatted for Windows, by scrolling down in the “About” display it will say “Format: Windows” on the bottom of the screen. If there is not mention of Windows, it is safe to assume that it is an HFS+ formatted Macintosh iPod.

Testing

Testing Methodology

The tool testing methodology of the National Institute of Standards program to test forensic tools was used as a guideline for the development of the testing method used in this research. NIST uses their own test methodology based on ISO 17025 (National Institute of Standards and Technology, 2001). The authors of this paper have created the method for testing collection from the iPod while keeping the standard NIST methodology in mind. Basing this method loosely on the NIST method adds construct validity to this research. Forensics experts reviewed the method to obtain face validity.

The problem of iPod forensics was addressed through the use of three forensic tools for the collection and analysis of information from the Apple iPod. The tools used in this research were limited to several of those available at the Purdue University Cyber Forensics Lab. They

were 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 for the Apple Macintosh.

The method for assessing the collection of evidence from the iPod was determined by testing of 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 will work well through the firewire interface, but it is possible that it may be necessary to disassemble the iPod and remove the hard drive for true forensic analysis because no hardware write block tools are available for the standard firewire or USB interfaces. A means of software write block 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. (Detailed device information and photographs are available upon request.) Apple's iTunes version 4.7 and iPod Updater 2004-08-06 were also used for this testing. The testing steps are outlined below:

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

Testing of 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

Full system restore

Results

EnCase proved to be the best forensic tool for collection of information from both versions of the iPod. 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 shows cross platform compatibility. It was shown that information could be recovered even after a full restore. The restore function Apple claims, "Completely erases your iPod," this is true but information and files could be recovered even after multiple restores. After the device was reformatted from the HFS+ Mac version to Windows FAT32 version, information could still be recovered, even after the device was switched several times between the two file systems.

An interesting piece of information that was found during the study was that the iPod keeps a 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 can use a string search for the iPod's name, and 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 iTune folder under the iPod_Control folder and in other places on the drive. This could be very useful in linking the iPod to the suspect in the case. 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.

The calendar and contact entries can be easily found on the iPod by doing a string search. The standard vCard and vCalendar formats store the entries on the hard drive in plaintext 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. The iPod uses the whole disk before returning to the beginning to store new information. The researcher believes that when the iPod stores information it automatically uses 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 hypothesized that 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). This is very nice 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.

FTK 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 pull any of the files off the Macintosh 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 though 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. This necessity to create a disk image was not foreseen and it was not a true bit by bit image. MFS was only useful at bringing out deleted pictures from the image file. This image created by the Apple Disk Utility was a .dmg file and was not readable by EnCase or FTK. 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 proved to be the best at recovering data. The software was able to display the file structure of the Macintosh device including hidden folders. It was not however able to automatically pull out 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. String searches were also successful for vCard and vCalendar entries.

It was shown that the forensic tools used in this study could read information off the HFS+ version of the iPod. All were able to recover deleted information. 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.

Another aspect that was found during the testing of the Mac version of the iPod was that deleting files on the iPod actually only moved the files to the trash and did not delete them. The iPod has a folder named ".Trashes" that can be seen 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 however, 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.

Windows Version

The Windows version of the iPod is formatted with the FAT32 file system and can be easily read by a Windows machine. This version of the iPod was easily analyzed by both of the Windows forensics tools used in this study. Both EnCase and FTK were able to quickly 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. In testing when files were deleted on the iPod, they were actually deleted and not simply moved to a ".Trashes" folder. These files could be easily recovered by the forensics tools in the Windows environment. All the tools were able to string search to find vCard and vCalendar entries. Overall with the Windows version it was much easier to recover information and find files relevant to possible criminal activity.

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 shown including file slack and free space. Files that were added to

the Windows version and then deleted, where 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 easily 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 though 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 Windows 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 collected before conducting an analysis because without proper write protection, a Macintosh should not be used to analyze a Windows iPod.

Conclusion

The Apple iPod has become a device that should be looked for in the diverse crime scene of today. As a digital device, it takes on two different yet connected forms. It is a real world physical device that contains possibly a wealth of evidence in a digital crime scene. In the collection and analysis of the iPod, some of the popular tools of today proved to be sufficient in accessing and recovering information and deleted entries.

Further research needs to be done on imaging of the iPod and a device or software for USB or Firewire write block needs to be tested. A true first responder's guide for unique digital

devices, including the iPod, would be useful when encountering these technologies in the field. The newest version of the iPod includes photo capabilities and the specifics of this are likely to be of interest in future criminal cases. This research focused on collection and tools, but additionally the theories of cyber forensics should be examined to determine if they are sufficient for use with the iPod and similar devices. 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 also a diverse array of unique devices that have not been thought of yet. The cyber forensic community must be ready to accept this continued evolution of technology and respond with theories, tools, methods, and practices, to account for the ever-changing technology world.

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.

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*: John Wiley & Sons.

Kruse, W. G., & Heiser, J. G. (2002). *Computer forensics: Incident response essentials*: 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