Chapter 4

PDA, Blackberry, and iPod Forensic Analysis

By Kevin Cardwell
and Craig Wright

Solutions in this chapter:

- PDA Forensics
- Investigative Methods of PDA Forensics
- PDA Investigative Tips
- Deploying PDA Forensic Tools
- Introduction to the Blackberry
- Operating System of the Blackberry
- Blackberry Operation and Security Capabilities
- Forensic Examination of a Blackberry
- Attacking the Blackberry
- Securing the Blackberry

Introduction

In this chapter we will discuss the concept of conducting a forensic investigation on data that has been read, stored or manipulated on some type of mobile device. The techniques for investigating a mobile device are similar to that of our more traditional storage devices; however, there are some notable differences that we need to be aware of while collecting potential evidence. Chapter 9 also provides more detail on iPod forensics.

PDA Background Information

A PDA is a handheld computing device that combines a multitude of functions and features. These features include things like computing, telephone, fax and Internet. Additionally, the PDA can and most often does contain some form of networking or other form of connectivity capabilities. Today a PDA is a powerful device it can function as a cellular phone, fax sender, web browser and a personal organizer. These devices have reached such a level of power, and functionality they are in essence a mini-computer.

Components of a PDA

The PDA device has several components that we will discuss now. There are many components that can be part of the PDA. Our intent here is to just discuss some of the more common ones. The first component of the PDA is the Micro-Processor; all PDA devices have to have some form of a Micro-Processor. This is similar to any micro-processor, the only difference is the processor has a restriction on the size it can be. Another component of the PDA is some form of input device, one of the most common means of input is the touch screen. In addition to these components, an essential component is the operating system that is running the software for the PDA device.

PDA Forensics

As discussed previously the concept of PDA forensics is very similar to the procedures and methodologies that are used with any form of forensics. When we discuss PDA forensics there are investigative methods that you should use when it comes to performing a forensic investigation of a PDA.

Investigative Methods

There are four main steps when it comes to performing a forensic investigation of a PDA. These four steps are identified as follows:

1. Examination
2. Identification
3. Collection
4. Documentation

We start off be securing the evidence. It is essential that we follow a process that has been approved by some form of legal counsel to secure the PDA. When we seize the PDA we have to ensure we take the PDA, docking cradle and external memory cards. This is probably one of the most difficult things to control and requires that you conduct a thorough search for any and all memory cards. With the size of memory cards today there is an extensive amount of evidence that you would be missing if you miss just one memory card. Once you secure the evidence the next step is to acquire the evidence as with any collection of evidence you will have to create an exact image to preserve the crime scene. Once we have acquired the image it is time for us to examine the evidence. This is where we can apply our tools on the evidence and look for potential evidence for our investigation. Once we have examined the evidence then we have to present the evidence, this step is usually completed by compiling an extensive report based on our investigation thus far. Our job as a forensic examiner is not over, because it is your responsibility as the examiner to maintain the evidence, this consists of keeping it in a secure location, and unlike other devices, you have to ensure the PDA remains charged so that data and information is maintained in a constant state. Now let's discuss the four main steps in more detail.

Step 1: Examination

In the examination step of PDA forensics we first need to understand the potential sources of the evidence, with a PDA these sources can be the device, the device cradle, power supply and any other peripherals or media that the device being examined has came into contact with. In addition to these sources you should also investigate any device that has synchronized with the PDA you are examining.

Step 2: Identification

In the identification step of PDA forensics we start the process by identifying the type of device we are investigating. Once we have identified the device we then have to identify the operating system that the device is using. It is critical to our investigative process that we determine the operating system; furthermore, once we have identified the operating system it is important to note that it is possible, that the device could be running two operating systems. During the identification process there are several interfaces that can assist us; these are the cradle interface, the manufacturer serial number, the cradle type and the power supply itself.

Step 3: Collection

During this part of our forensic investigation it is imperative that we collect data and potential evidence from the memory devices that are part of or suspected to be part of the PDA we are investigating. There are a multitude of these types of devices, so we will limit our discussion to just a few. The SD, MMC semiconductor cards, micro-drives and universal serial bus (USB) tokens. These SD cards range in size from a few Megabytes (MB) all the way up to several Gigabytes (GB). Today, the USB tokens can range from a few MBs themselves all the way up to multiple GBs. In addition to seizing and collecting the memory devices we also have to collect the power leads, cables and any cradles that exist for the PDA. Extending our investigation process further it is imperative that we collect all the types of information. This information consists of both volatile and dynamic information; consequently, it is imperative we give the volatile information priority while we collect evidence. The reason for giving this information priority is because anything that is classified as volatile information will not survive if the machine is powered off or reset. Once the information has been captured it is imperative that the PDA be placed into an evidence bag, and maintained at stable power support throughout.

Step 4: Documentation

As with any component in the forensic process, it is critical that we maintain our documentation and "chain of custody." As we collect our information and potential evidence, we need to record all visible data. Our records must document the case number, and the date and time it was collected. Additionally the entire investigation area needs to be photographed. This includes any devices that can be connected to the PDA, or currently are connected to the PDA. Another part of the documentation

process is to generate a report that consists of the detailed information that describes the entire forensic process that you are performing. Within this report you need to annotate the state and status of the device in question during your collection process. The final step of the collection process consists of accumulating all of the information and storing it in a secure and safe location.

PDA Investigative Tips

When it comes to the PDA device, there are several things we need to consider while carrying out an investigation. These devices can be managed and maintained by your suspect at all times. Adding further complications is the fact that with PDA devices they have immediate access 24 hours a day, and 7 days a week. Another thing that makes your job as an investigator more challenging is PDAs are immediate boot cycle devices. Having said that, it is important to remember these devices typically contain a plethora of information for the examiner, and are a vault of evidence for the forensic examiner.

Device Switched On

When you are beginning your investigation process, and discover that the PDA that you are wanting to process for evidence is in the "on" mode, it is imperative that you act immediately, and get power to the PDA, so that it will not lose the volatile information that could quite possibly be essential to our evidence collection process.

Device Switched Off

If the device is in the off state, you leave the device in this state then switch the device on and take a picture of the device. Additionally you need to note and record the current battery charge.

Device in its Cradle

Avoid any further communication activities with the device. Remove any connection from the PC device. It is important to note that there is a possibility that a sophisticated suspect might have a "tripwire" device and once you disconnect the PC this could activate the device which in turn could run a script that might erase potential evidence. Despite this possibility, you have to disconnect the device to continue the investigation.

Device not in its Cradle

If the device is not in the cradle our investigative requirements are made much simpler, because there is no danger of a "tripwire" being triggered. With the device being out of its cradle, we simply seize the cradle and any cords associated with it.

Wireless Connection

Avoid any further communication activities if at all possible. Eliminate any wireless activity by placing the device into an envelope that can isolate the device. This envelope needs to also provide anti-static protection, so that the device is not damaged.

Expansion Card in Slot

Do not initiate any contact that requires taking components off of the device, or requires you to open the device in any way. This includes any and all peripheral devices and/or media types of cards.

Expansion Sleeve Removed

The first thing to accomplish is you have to seize the sleeve itself, additionally, seize any and all related peripherals and media cards.

Notes from the Underground...

Impact of Mishandling PDA Devices

While conducting an investigation of a potential crime scene, our team encountered several PDA devices, and one of the team members was investigating one of the Blackberry (RIM) devices, and the surrounding area near the device when they discovered a sticky note with a password written on it. The team member entered the password, and it did not work, so he thought maybe the case was wrong or something else, but no matter what they did, they could not get access, and after the tenth attempt the Blackberry did a complete data wipe, and whatever information was on that device was lost. This is because there is software that will log the attempts at entry and do a complete wipe after a certain amount of invalid login attempts.

Deploying PDA Forensic Tools

When we are conducting a forensic investigation, there is no shortage of tools available for us. Investigating handheld, or PDA devices do not offer as many tool choices as a typical forensic investigator will have.

PDA Secure

Our first tool to discuss is the tool PDA Secure. This tool offers enhanced password protection, along with encryption, device locking and data wiping. The PDA secure tool allows administrators greater control over how handheld devices are used on networks. Additional features of the tool are it allows you to set a time and date range to monitor information such as; network login traffic, infrared transmissions and any applications being used.

PDA Seizure

PDA Seizure is a comprehensive tool that assists us in seizing the PDA. It allows the data to be acquired viewed and reported on. The tool works only within a Windows environment. This tool can extract the random access memory (RAM,) and read only memory (ROM). The tool has an easy to use graphical user interface (GUI), and includes the tools that are needed to investigate the files that are contained within the PDA.

PDA Seizure provides multi-platform support, and the forensic examiner can acquire and examine information on PDAs for both the Pocket PC and Palm OS platforms. The PDA Seizure tool has a significant amount of features, this includes forensic imaging tools, searches on data within acquired files, hashing for integrity protection of acquired files and book-marking capability to assist the examiner in the organization of information.

EnCase

EnCase is one of the most popular commercial forensic tools available, and this tool can be used to acquire information and evidence from a PDA. The EnCase tool can acquire images, and also consists of tools that allow for us to conduct complex investigations efficiently and accurately.

Introduction to the Blackberry

The Blackberry is also known as a RIM device. The device is equipped with the RIM software implementation of proprietary wireless-oriented protocols; furthermore, the device is supported by the RIM Blackberry Message Center. The Blackberry (RIM) device shares similarities to the PDA devices we discussed earlier; however, the Blackberry (RIM) device is always-on, and participating in some form of wireless push technology. As a result of this the Blackberry (RIM) does not require some form of desktop synchronization like the PDA does. This unique component of the Blackberry (RIM) device adds a different dimension to the process of forensic examination, and in essence this portability can be the examiners greatest ally.

Operating System of the Blackberry

The current version of the Blackberry OS has numerous capabilities and features. These features include; over the air activation, ability to synchronize contracts and appointments with Microsoft Outlook, a password keeper program to store sensitive information and the ability to customize your blackberry display data.

Blackberry Operation and Security

The Blackberry (RIM) device has an integrated wireless modem; this allows the device to communicate over the BellSouth Intelligent Wireless Network. The Blackberry (RIM) device uses the Blackberry Serial Protocol. This protocol is used to backup, restore and synchronize the data that is communicated between the Blackberry (RIM) handheld unit and the desktop software. This protocol comprises simple packets and single byte return codes. The device uses a strong encryption scheme that safeguards confidentiality, and authenticity of data. It keeps data encrypted while in transit between the enterprise server and the device itself.

Wireless Security

The Blackberry (RIM) has a couple of transport encryption options. These options are the Triple Des (Data Encryption Standard) or AES (Advanced Encryption Standard. Those who want to implement the most secure method will elect to encrypt with the AES algorithm. The Blackberry has another feature that is referred to as the Password Keeper, this feature offers the capability of securely storing password entries on the devices, these could consist of banking passwords, PINs, etc. This critical and important information is protected by AES encryption.

Security for Stored Data

There are several capabilities available on the Blackberry device when it comes to securing the data that is stored there. The first option we will discuss is the capability to make password authentication mandatory through the customizable IT policies on the Blackberry Enterprise Server. An additional method of protection from unauthorized parties is the fact that there is no staging of data between the server and Blackberry device where data is decrypted.

Forensic Examination of a Blackberry

Since the Blackberry (RIM) is an always-on, push messaging device information can be pushed to it at anytime. It is important to note that this information that is pushed does have the potential of overwriting any data that possibly was previously deleted. The problem is compounded by the fact that without warning there are a multitude of applications that may receive information, and make the attempts by the forensic investigator to recover information and an unaltered file system much more difficult. The first step in preserving the information is to eliminate the ability of the device to receive this data push. If possible you could turn the radio off, or a better solution is to take the device to an area where the signal cannot be received, this possibly can be achieved by putting the device inside of a filing cabinet drawer, but your mileage will vary here. One might think, "I'll just turn it off." This would be a serious mistake! The Blackberry (RIM) device is not really "off" unless power is removed for an extended period, or the unit is placed in storage mode; furthermore, once the unit is powered back on any items that were in the queue waiting to be pushed to the device could possibly be pushed before you could stop them. As mentioned previously, and we will reiterate it here, it is quite possible that a change to state such as a power off of the Blackberry could result in a program being run on the unit that will allow the device to accept remote commands via email.

Acquisition of Information Considerations

The considerations for the Blackberry (RIM) device are similar in some ways to the PDA devices, but there are some differences, so let's take a look at the considerations you have to make when acquiring evidence from the Blackberry (RIM) device.

Device is in the "off" State

If the unit is off at the time of acquisition, the investigator needs to take the unit to a shielded location before attempting to switch the unit on. If a shielded location is not readily available, you might have success using a safe or other room that can block the signal well enough to prevent the data push. One thing to consider is having a unit available that you can use to walk the network and area to test the coverage, and look for weak coverage areas to use.

Device is in the "on" State

If the device you are examining is in the "on" state then as outlined and detailed above, you need to take the device to a secure location and disable or turnoff the radio before beginning the examination.

Password Protected

One thing that has to be considered when it comes to password protection is the fact that the password itself is not stored on the device, the only thing that is stored on the device is a hashing of the plain text password. This storage is similar to the storage used by the majority of operating systems out there.

Evidence Collection

To collect evidence from the Blackberry we have to violate the traditional forensic methods by requiring the investigator to record logs kept on the unit that will be wiped after an image is taken. There are several different log files that we want to collect evidence from; Radio Status, this log lets us enumerate the state of the devices radio functions; Roam and Radio, thus log has a buffer of up to 16 entries usually, records information concerning the tower, channel etc, and will not survive a reset; Transmit/Receive, records gateway information, and type and size of data transmitted; Profile String, this contains the negotiation with the last utilized radio tower. Once the log information is extracted and enumerated then the image will be taken. If you do not require or need the log information then the image can be acquired immediately.

Unit Control Functions

The logs are reviewed by using the unit control functions; there are several functions we will discuss. The first function is the Mobitex2 Radio Status, this provides information on the Radio Status, Roam and Radio Transmit or Receive and Profile String. The second control function is the Device Status; it provides information on memory allocation, port status, file system allocation and CPU WatchPuppy. The third control function is the Battery Status, and as the name implies it provides information on battery type, load, status and temperature. The last control function we will discuss is the Free Mem, this provides information on memory allocation, Common Port File System, WatchPuppy, OTA status, Halt and Reset.

Imaging and Profiling

When you are conducting a forensic examination of a Blackberry (RIM) device we need to conduct imaging and profiling. This is accomplished by extracting the logs from a developed image; acquiring an image of a bit-by-bit backup using the Blackberry (RIM) Software Development Kit (SDK). The SDK is available from www.blackberry.com and is essential for the forensic examiner when investigating a Blackberry (RIM) device. The SDK utility dumps the contents of the Flash RAM into a file. Once the Flash RAM is dumped it can be examined and reviewed using traditional methods with your favorite hex editor or other tool. In addition to reviewing the evidence with traditional methods, you can use the Simulator from the SDK to match the network and model of the investigated unit.

Attacking The Blackberry

We have several tools and methods available that allow us to attack the Blackberry, The first tool is the Blackberry Attack Toolkit, and this toolkit along with the BBProxy software can be used to exploit website vulnerabilities. The second tool is the Attack Vector, this tool links and tricks users by downloading malicious software to the Blackberry. The last method we will discuss is the method of hijacks, or as it is sometimes referred to blackjacks. As the name implies this allows someone to hijack a legal users Blackberry (RIM) and replace them on the network with potentially harmful devices.

Securing the Blackberry (RIM)

We have several things we can do to secure the information on the Blackberry (RIM) device. The first thing we can do is clean the Blackberry (RIM) device memory, and we can protect stored messages on the messaging server. You can encrypt the application password as well as the storage of if it on the Blackberry (RIM) device; furthermore, you can protect storage of user data on a locked Blackberry device by limiting the password authentication attempts. It is possible to set a maximum of 10 attempts to gain access to the device. Additionally, you can use AES technology to secure the storage of the password keeper and password entries on the Blackberry device.

Information Hiding in the Blackberry (RIM)

When it comes to hiding information in the Blackberry (RIM) device we have several places we can hide information. You can create hidden databases; you can hide information in partition gaps. Data can be hidden in the gap between the Operating System/Application and file partitions.

Blackberry (RIM) Signing Authority Tool

This tool helps the developers protect their data and intellectual property. It enables the developers to handle access to their sensitive Application Program Interfaces (APIs). The tool provides this protection by using public and private signature keys. It does this by using asymmetric cryptography to validate the authenticity of the request; furthermore, the signing tool allows developers to exchange API information in a secure manner and environment.

iPod Forensics

Apple computers produce three separate digital media players all bearing the iPod brand. Whether the original iPod, the iPod Nano or an iPod shuffle, all of these devices have the capability not only to play music but also to act as a storage device. The capability to store digital data coupled with the iPods popularity will result in the forensic analysis of these devices becoming more common. (Also, see Chapter 9 for more on iPod forensic analysis.)

Consequently, ,the National Institute of Standards and Technology (NIST) have developed guidelines for PDA forensics (Jansen & Ayers, 2004) to address this issue.

The secret is to treat the iPod as you would treat any other suspect hard drive being analyzed. Treat it with the respect and care it deserves and remember it is evidence.

The iPod

The Apple iPod family currently comprises five generations of devices for the primary units and two generations of ancillary models. These are listed below.

- First Generation iPod October 2001 saw the first release of the Apple iPod. This device connected using a FireWire jack and introduced the Apple physical scroll wheel. This device used the original form factor and is the classic iPod design.
- Second Generation iPod Implemented the large hard drive (10 Gb and 20 Gb), introduced the touch sensitive wheel and put a cover on the FireWire port but was otherwise physically the same as the first generation iPod.
- Third Generation iPod The third generation introduced a central row of touch sensitive buttons and a dock connector port. The primary connection was still FireWire but USB was introduced for data syncing.
- Fourth Generation iPod The fourth generation of the iPod introduced the photo viewer. The color the display was introduced at this stage. Either FireWire or USB could be used.
- Fifth Generation iPod The next generation introduced a video function and lyrics support. This version has no AC adapter universal block or A/V included and must be purchased separately. The latest edition (generation 5.5) features a brighter display, the ability to search and the longer video battery. Fifth generation iPods use only USB with FireWire connections relegated to charging only.

The ancillary iPods include the following models:

- iPod mini The iPod mini is a slimmer version of its original cousin. These devices use either USB or FireWire connections using either a 4 or 6 GB hard drive. This device implements a scroll wheel with integrated buttons. There are two generations of iPod minis. iPod mini connections are made using either USB or FireWire.
- iPod Nano The iPod nano implements a flash memory storage system. These devices are otherwise similar to the fifth generation iPod in many

respects. The iPod nano uses USB connections with FireWire for charging only.

- iPod shuffle Again there are two generations with the iPod shuffle. All these devices implement flash memory instead of hard drive storage. The iPod shuffle uses USB connections and the later models implement USB through the docking function alone.

iPod Features

The iPod supports a variety of file formats including Protected AAC, AIFF, MP3, WAV, M4A/AAC LC and Apple Lossless audio file formats. From the introduction of the fifth-generation iPod a number of video formats are also supported. These include the .m4v and .mp4 MPEG-4 (H.264/MPEG-4 AVC) file formats. Additionally, iTunes has the capability to translate Windows WMA formatted files to an iPod format as long as they are not copy protected.

The iPod is not currently able to play copy protected WMA files. Additionally, the iPod is unable to play MIDI, Ogg Vorbis and FLAC multimedia formats. It is however possible to translate MIDI files to another format using iTunes. iTunes will not transfer songs from the iPod to a computer because of perceived Copyright and other legal issues. A number of third-party products have been created to circumvent the iPod's copy protection.

Current iPod's have the inclusion of a limited PDA functionality. Macintosh users have been altered synchronise schedules and contacts in their address book and iCal using iSync. From the release of iTunes version 5.0, Apple has integrated the ability to synchronise contacts and schedules from iTunes to the iPod. Contact maintained in either Microsoft Outlook or Outlook express may be synchronise with the iPod in this manner. Mozilla calendar files use the same format as the iPod. So although there is no automated method to synchronise Mozilla data, these files may be copied to the iPod manually.

In with this functionality however, the inability to add or update entries on the iPod itself limits the functionality of the iPod as a PDA. From a forensic perspective, this does not diminish the ability to capture data (including calendar entries and schedules) from the device.

Damage & Defense...

Mac vs. Windows

The debate comparing Windows to Macintosh has become something of a holy war. For the most part it comes down to personal preference. In the case of an analysis of the iPod, the Mac is definitely preferred over Windows. This is not a comparison of the operating systems, but rather relates to the interaction of the iPod and the host machine.

Simply put, Apple HFS+ is superior to Windows FAT 32 from the perspective of a forensic analysis. When iPod is initially connected to a Mac it is formatted using Apple HFS+. When it is initialized using a Windows machine, it is formatted with FAT 32. Unfortunately the iPod doesn't come configured to support NTFS.

The Apple HFS+ format provides more detailed meta-data which supplies the forensic analyst with far greater detail than is supplied by a FAT 32 format. So it is a question of whether the Mac is better than Windows or vice versa, simply that in iPod connected to a Mac supplies more Meta-data for analysis.

The iPod as Operating System

The iPod can run as a small portable computer system. iPodLinux is a μClinux-based Linux distribution (see http://ipodlinux.org/Main_Page for details). iPodLinux is a specifically designed kernel capable of running on a number of the iPod devices. Wikipedia (http://en.wikipedia.org/wiki/IPodLinux) details a list of compatible devices and known issues.

One of the primary components of iPodLinux is podzilla and podzilla 2. The podzilla applications provide iPodLinux with an iPod like interface, video playback with sound and the support for a large number of music file extensions. Using iPodLinux, the iPod can play AAC, MP3 and basic OGG sound file formats. Depending on the hardware capability of the specific iPod, the audio recording capabilities under iPodLinux said to be at much higher quality than Apple's firmware.

IPodLinux also supports the ability to play a number of games such as Doom and Doom II and many games for the Nintendo Game Boy (with the appropriate add-on software such as iBoy).

μClinux stands for "MicroController Linux", and is pronounced "you-see-Linux". μClinux supports up to the version 2.6 kernel. μClinux (http://uclinux.org/) has support of a number of compiler programs such as the standard C++ library rich run correctly under podzilla. As such, an attacker could create and compile middleware or other code of interest to the forensic analyst which can be stored on the iPod.

Drive Formats - Apple HFS+ Or FAT32

The drive format used by the iPod hard drive is dependent on the computer system to which the iPod is initially synchronised. If the iPod is initially synchronised with a Mac machine, the iPod will be formatted using the Apple HFS+ file system. Where the iPod is initially connected to a Windows host, the iPod drive will be formatted with the FAT32 file system.

When conducting a forensic analysis of the iPod is important to know which type of system the iPod has been synchronised with. This information also provides the analyst with some background information as to the use and history of the device. Knowledge of the format used will generally make it easier to match the iPod device to the host and has been synchronising with. It is important to remember that just because the output has initially synchronised with either a Windows or Mac host, but it may also have been used on other machines.

The iPod writes data from the beginning to the end of the drive before returning to the beginning. This is a valuable feature for the forensic analyst as the use of this wear- levelling technique makes the overwriting of files less likely.

Being that the FAT32 file system does not maintain records of file ownership, the HFS+ file system (which maintains ownership metadata) is the preferred format from a forensic perspective. Unfortunately, the HFS+ file system is somewhat less common than the FAT32 file system.

The iPod System Partition

The System Partitions of either the Windows or Macintosh format iPod demonstrate that there is no user identifiable data stored in this partition. The data contained in this partition is associated with the running of iPod and includes:

- The iPod embedded Operating System.
- The images used during the operation of the device such as the Apple logo and the "Do Not Disconnect" screen image.

- The system fonts used for the display of the text on the device.
- Games and other applications copied to the device

Where iPodLinux has been installed user data may exist in the system partition. Installing iPodLinux will change the hash value for the System Partition. This is because iPodLinux modifies the boot loader in the System Partition. The boot loader allows the iPod user to select either the official Apple embedded operating system or the iPodLinux operating system. The system files for iPodLinux are maintained in the iPod Data Partition. However, the changes to the boot loader require the System Partition to be modified changing the hash value of the system partition.

Notes from the Underground...

Hiding the Hidden Functions

With iPodLinux it is possible to create a dual booted iPod that runs both the standard embedded Apple operating system and Linux. A clever attacker could partition their iPod so that the Linux partition is hidden when connected using the default embedded system. In this manner they could create a device that on a basic inspection would appear as an iPod with nothing to hide.

The Linux partition could be configured to be visible when booted into iPodLinux mode. A clever attacker could use this partition to smuggle data into and out of an organization or even introduce code into a secured system. A preliminary investigation and search of the device would find only the "clean" iPod partition. Most people investigating iPod would not expect a separate Linux partition and it would be common for this to go unnoticed.

Application Formats

Music and other file formats are stored on a variety of locations within the iPod. Accessories exist little alley iPod to be used for a variety of functions. Applications and accessories may be loaded using either the native iPod operating system or iPodLinux. These applications allow for the storage of a variety of files including voice recordings, digital camera photo storage and electronic games.

These files can be easily found by searching the drive for the text strings BEGIN:VCARD and BEGIN:VCALENDAR. This entry indicates the beginning of the respected file types. The data remains after the entries are deleted.

Misuse of an iPod

Like any other digital storage device, the iPod may hold incriminating evidence. In its native format the iPod may contain calendar entries related to a crime or other event of interest. Additionally, contact information stored on the device may be relevant to an investigation. The iPod is also capable of creating voice recordings. As such, recordings of meetings may be recovered. Coupled with photographs or other substantiation the iPod could be a rich source of evidence to the investigator.

With its large hard drive, the iPod is the ideal storage location for music that violates Copyright, and with the newer devices pornographic pictures.

iPod Investigation

When an iPod is found at a crime scene, the first respondent should wait for the advice of a forensic specialist. This is essential to ensure that the site of the evidence is documented correctly. Either explicitly document the location of the iPod and anything around it or preferably photograph the site. Leave the device in its current state until it is thoroughly investigated. It is possible that the point could be booby-trapped with a delete command or wipe function. This is particularly relevant when the device has been configured with iPodLinux. There are tools under iPodLinux that can be set to wipe the hard drive of the iPod if it is disconnected from the charger or computer without a special code being entered.

Note the state of the iPod. If it is connected to another system, check whether it is mounted. If it is, the screen of the iPod will display message saying "Do Not Disconnect". In this case it is necessary to unmount the device prior to disconnecting the computer. On a Mac this may be achieved by dragging the icon of the iPod to the trash can on the Mac desk top. Note the name of the iPod as it is displayed on the desktop before unmounting it.

Simply disconnecting or on plugging the computer could damage disk sectors on the iPod. For this reason this should be avoided. If the iPod is connected to a Windows machine, it may be mounted by clicking the "Unplug or eject hardware" icon generally located on the task bar on the bottom right of the screen. On a

Windows machine the chances of the corruption resulting from disconnecting the iPod are less than on a Mac.

When collecting the iPod specify the connections and cabling as well as all the details of machine connected to (if it was connected). Ensure that this information is kept with the device. The iPod should be stored like a hard drive. This is it should be stored in an antistatic bag in an environment where both temperature and humidity are controlled. It should also not be exposed to excessive vibration. Never store the iPod near a magnetic source such as a speaker. It is important to maintain a strong chain of custody throughout the process.

The iPod is unlike some other embedded devices in that it does not need to be connected to a power supply while in storage. If the battery drains over time, the information will not be lost from the hard drive. With hard drive models, it may be more effective to extract the hard drive from the iPod for processing. This will allow the use of an external hardware write blocker. The difficulty is that imaging the hard drive correctly requires both a high level of technical skill and specialised hardware.

An iPod stores the name of the computer which it initialised with on the drive. This information may be used to link the device to other computers and consequently suspects.

Although it is recommended that the iPod is imaged before doing any other tests, it is possible to determine the format of the drive from the iPod itself. This is achieved by selecting: "Settings >", "About >". If the iPod is formatted for a Windows system scrolling down in the "About" display will state "Format: Windows" towards the lower section of the screen. If this is not displayed, it is likely that the device has been formatted using the HFS+ format and that the iPod was initially connected to a Mac.

Timeline Generation

The iPod is designed to only be linked to one system at a time. As a result, a series of likely connection times to a system can be established. The identified times associated with connection events may also be discovered on the linked system. The times will reflect the system time of the linked system (not that as displayed on the iPod).

Time entries of primary concern to the forensic analyst may be found in the following files:

- \iPod_Control\Device\SysInfo – the modified time of the file records when the iPod was last restored.

- \iPod_Control\iTunes\iTunesControl - the creation time of the file records when the iPod was initialised using iTunes.
- \iPod_Control\iTunes\DeviceInfo ? the modified time of the file records when the iPod was last connected to iTunes.
- All music files located under \iPod_Control\Music\ - the creation times of the files records when these files were copied from the linked system to the iPod. The modification times for these files provides further evidence linking the iPod and the Windows system and helps to create a timeline of actions/activity.

These times provide evidence of connection times to the linked system. If the Windows host is available, it may be possible to correlate these times to events on this computer as well.

Tools & Traps...

Have You Captured All the Data?

Always check the size of the iPod's physical disk against the size of the partition. As an example it is possible that a clever suspect could re-partition their iPod making it appear smaller than it actually is. For instance, an 80Gb iPod could be formatted to appear to be a 60Gb device. This would leave 20Gb worth of data available. This hidden section of the disk could either be formatted using Ext2 or another format not natively available to a Windows host or data could be copied to the raw partition.

Using a tool such as DD, it is possible to stream data to the physical partition. In this manner it would be possible to hide a small disk image on the physical drive. This image would be invisible to any normal scan as no file partition would have ever been created in the disk MFT. However, an analysis of the physical disk would reveal this data.

For this reason the forensic analyst must never assuming everything is at face value. Always check and ensure that everything is as it seems.

Lab Analysis

When analysing the iPod, it is important to be familiar with the tools used in the analysis. A variety of tools such as Access Data's Forensic tool kit (FTK), the Sleuthkit/Autopsy browser, Blackbag Technologies' Macintosh forensic software (MFS) or Encase forensic edition are more than adequate for this task. , it must be noted, however, that the tool must be matched to the device. For instance, Blackbag MFS is designed exclusively for the Mac environment and the Sleuthkit/Autopsy browser requires specialist consideration to work with the Apple file system.

It is also necessary to ensure that the necessary connectors are in place. Depending on the type of iPod, either FireWire or USB connections may be required. Ideally the forensic analyst will disassemble the iPod and remove the hard drive for analysis. Disassembly allows for the use of a hardware write blocker.

It is generally considered best practice to disassemble the device. By activating the device it is possible to either alter the drive thus damaging the evidence or to set off a booby trap. It is not difficult to configure a wipe program to run on the system boot-up using iPodLinux. Such a tool could destroy valuable evidence before the forensic investigator could get to it.

Remove Device from Packaging

When receiving an iPod for forensic imaging is important to document every step. First, remove the iPod from the packaging. Carefully note with the state of the machine, the model and the interfaces. Photograph and document everything to ensure the chain of custody records are complete.

Depending on the actions that the investigator intends to take there are two possible courses:

1 Work on the iPod as is (not recommended for hard drive models), or

2 Disassemble the device and extract the hard drive.

It is always possible to reassemble the device after the drive has been imaged. For this reason it is better to duplicate the hard drive first. This is a little more difficult in the non-hard drive models such as the iPod nano. In this case it may be more practical to copy the device assembled.

When working on assembled device (including when the device has already been imaged and reassembled) the following steps are recommended:

1 Ensure that the battery is charged. Leave the iPod on the charger until the battery is fully charged,

2 Turn on the iPod,

3 Note any device settings and document these,

4 Based on whether the iPod has been connected to a Windows or Mac host, the subsequent stages will differ.

NOTE

It is important to remember that the iPod is in effect an external storage device. Although it has extra functionality (such as a limited PDA function) than a simple external hard drive, it does have the capability to act as a hard drive. Everything that applies to the forensic analysis of a hard drive also applies to an iPod.

The iPod restore process

The iPod restore process does not clear the hard drive of the iPod. Using a restore process copies new data to the iPod which makes it appear as if it was erased and reloaded. However, only the file pointers are erased. Unless data was specifically over-written by the restore process it will still be available for recovery.

The Microsoft restore process is detailed in the following stages:

1. An unformatted, corrupted, or Mac HFS+ formatted iPod is connected to the Windows computer and Windows automatically loads the drivers.
2. The iPod Updater software loads then prompts the user to format the iPod. On selecting "Restore" the following occurs:
   a. New Partition tables are written to the iPod hard drive
   b. A replacement System Partition is created on the iPod and loaded with required data
   c. A new Data Partition and File Allocation Table for the FAT32 Data Partition is created
   d. \iPod_Control and \iPod_Control\Device directories are created on the iPod hard drive

e. The \iPod_Control\Device\Preferences file is created containing binary data

f. The \iPod_Control\Device\SysInfo file is created. This file contains technical data about the iPod in text format

3. When the iPod is connected to the Power Adapter the operating memory is reloaded.
4. The iPod is now re-connected to the host system and either iTunes automatically loads, or it is manually run.
5. The iTunes iPod Setup Assistant will prompt the user allowing them to set the name on the iPod. If a name is set and "Next" is selected then the name will be entered in the DeviceInfo file. If the cancel is selected, the iPod Setup Assistant will then set the device name to the default, "IPOD". The file will thus contain either the name entered by the user or "IPOD". If the name is stored it is recorded with the username and computer name used in configuring the iPod within iTunes. The following procedure then occurs:

   a. The \iPod_Control\iTunes directory is made and the files DeviceInfo, iTunesControl, iTunesEQPresets, iTunesPrefs, and winPrefs are produced in this directory.

   b. The \iPod_Control\Music directory is created with subdirectories named sequentially from F00 through to F49.

These entries are reflected in the \Windows\setupapi.log file on the Windows host used to configure the iPod with a second entry from the iPodService.exe program which also records the USB serial number of the iPod. The creation time of the \iPod_Control\iTunes\DeviceInfo on the iPod reflects the time value in the \Windows\setupapi.log file on the Windows host used to configure the iPod.

Configuring & Implementing...

Encase and the IPod

Use the EnCase Program with an iPod

- Install EnCase Academic Edition.
- Connect the iPod to your computer. It is always best to ensure that you have configured read-only mode within Windows XP (SP2) by changing the registry key: HKEY_LOCAL_MACHINE\System\CurrentControlset\Control\StorageDevicePolicies to the hex value of 0x00000001 and restarting the computer.
- Take an image of the iPod drive.
- Explore various features of this program based on the EnCase information in the courseware.

The iPod and Windows

It is possible to set iPod to read-only mode within Windows XP (SP2) by changing the registry key: HKEY_LOCAL_MACHINE\System\CurrentControlset\Control\StorageDevicePolicies.

Setting this key to the hex value of 0x00000001 and restarting the computer will stop write access to any USB storage devices effectively rendering them as read only. Setting the value to 0x00000000 and restarting the computer enables write access (Andersen & Abella 2004).

The Registry

The Windows registry contains significant amounts of information to the forensic analyst. Of primary concern in investigating iPods are:

1. The keys created by the connection of the iPod to the Windows computer, and
2. The last write times indicating the last time the registry keys were changed.

An iPod creates a series of registry keys when it is connected to the Windows computer. These can be found under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\ in the registry. Located under USBSTOR will be found a key that identifies a disk device presenting the vendor identifier "Apple", the product identifier "iPod", and a revision code. This information can be used to match the host computer and iPod being investigated.

The last write time for this key indicates the first time that the iPod connected to the Windows host. Under this in the registry is a further key corresponding to the serial number of the iPod USB connection, followed by "&0". This value will match the value of FirewireGuid on the iPod contained in the \iPod_Control\Device\SysInfo file. The last write time associated with this key is the last time that the iPod connected to the Windows host.

NOTE

Remember that the iPod does not update file times and that these will reflect the create and modify time stamps of the computer to which the iPod is paired.

setupapi.log

The Windows file, setupapi.log (in the Windows installation directory) records all driver installations that after the system has booted. On the first time that an iPod is connected to a Windows system, the connection event will be recorded in this file. The information in this file will match with the last write times of a series of registry keys related to the iPod.

This file is also useful in reconstructing the sequence of connection events the iPod and the host system. This is as this file lists the driver installations. If iTunes is also installed, each occasion that an iPod connection occurs after boot will be recorded. If however iTunes is not installed, than only the driver installation will be recorded. Also, if the iPod has been connect to the host prior to its being booted, the drivers will load during boot-up and will not be recorded even if iTunes is installed. In any event, this file provides a means to reconstruct events that have occurred on the host and also associated a particular iPod with a particular computer at a given time.

The iPod and Linux

The following procedure may be used to mount the iPod under Linux (Ubuntu used for this example):

1 Disable auto-mounting of removable media devices by selecting the "System" menu from the top of the screen, then "Preferences", then "Removable Drives and Media".

2 When the following window opens up click to remove the check marks by each item then select "OK".

3 Locate the iPod within the Linux device tree as follows:

   a. Right click in a clear area of the Linux desktop to open up a menu and select "Open New Terminal",

   b. Enter "ls /dev/sd*" to list of all the SCSI drives on the system.

   c. Connect the iPod to the computer.

   d. Wait 20 seconds for the computer to recognise the iPod.

   e. Retype "ls /dev/sd*" to get an updated list of all SCSI drives on the system and note the new listings which belong to the iPod.

4 Depending on the application you can now mount the iPod in read only mode.

Note: The apple file system is required to be loaded into the Linux kernel in order to mount an iPod initialized using a Mac.

User Accounts

When an iPod has been setup using iTunes, a file \iPod_Control\iTunes\DeviceInfo is created which contains user name and computer information. This information may be used to identify the user and computer which initialised the iPod. If this file contains the word "IPOD" then the software was restored to the iPod without having been connected to iTunes.

Deleted Files

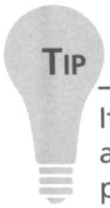
The iPod deletes file pointers rather than actually erasing the file. Coupled with the iPod's sequential file writing technique that starts from the beginning of the drive

and adds data to the end before returning to the beginning, recovery on an iPod can be a simple process.

iPod Time Issues

The manner in which the device records time is one of the most crucial aspects of any digital forensic analysis. To be able to link the deletion, access or alteration of the file to a particular user is necessary to be able to determine the time when the event occurred. The iPod has an internal clock but unfortunately the standard embedded operating system does not update file times.

On iPodLinux however, the system clock updates file access times. It is important to remember this differentiation in times. The native iPod operating system will record the time is associated with the computer it is connecting to. Where an alternative operating system such as iPodLinux is involved, however, the time will be set through the iPod's internal clock.



It is important to remember that the file create and modify times as they appear on the iPod reflect the timestamp associated with the pared computer. Although the iPod has an internal clock it does not use this to update or modify the time stamps associated with a file which it stores. This can be useful in proving that a particular iPod was connected to a host machine.

Registry Key Containing the iPod's USB/Firewire Serial Number

The file: \iPod_Control\Device\SysInfo file is created on the iPod when system software is restored or the iPod is initialised. This file contains valuable data about the iPod. Another significant file: \iPod_Control\iTunes\DeviceInfo is created after iTunes has linked the iPod with a computer. The name of the user and computer involved in linking the iPod and iTunes will be stored in this file.

Where iTunes is running on Windows, a record will be created in both the registry and setupapi.log file with a reference to the USB / Firewire serial number presented in the SysInfo file on the iPod.

iPod Tools

In addition to the standard drive imaging tools, several products specifically designed for use with the iPod had been produced. Two of the more common tools include "Music Recovery" from DiskInternals and "Recover My iPod" by GetData.

DiskInternals Music Recovery

"Music Recovery" from DiskInternals is designed to recover any type of music files from a hard drive, iPod, USB-flash drive or CD/DVD. It is available in shareware format from: http://www.diskinternals.com/music-recovery/. Music Recovery comes with an integrated media player to preview the files prior to recovery. DiskInternals provides native support for the iPod but does not run on Mac or Linux.

The software works to recover lost files and data from damaged disks, inaccessible drives and also works with corrupt or damaged partition tables. Although Music Recovery only runs on Windows hosts, it has support for several file systems including:

- NTFS 4 & 5,
- Linux Ext2 & Ext3,
- MacOs & Apple HFS,
- Iso9660, and
- UDF.

Recover My iPod

"Recover My iPod" allows the user to recover lost or deleted music, video and photos including .m4a, .mp3, .mov, quicktime and jpeg file formats. The product is available from GetData at http://www.recovermyipod.com/. The software supports all versions of the iPod including the iPod, iPod shuffle, iPod Mini and iPod Nano. The product recovers data after an iPod Reset or Restore. It is important to remember that Recover My iPod will not run on a MAC.

This software will recover data and files from iPod even when a "Drive Not Formatted" message appears or if the iPod is not recognized by the computer. In this case it is necessary to connect to the "Physical Drive". Although not as effective as a hardware write blocker, "Recover My iPod" mounts the iPod drive in read only format.

"Recover My Files" is a more complete recovery tool from GetData. This tool allows for the searching of Computer drives and also iPods. Both products support a "deep scan" and "fast search" mode.

DD and the iPod

To image in iPod which is mounted under Linux type "dd if=/dev/sda of=/mnt/hdb1/iPod.image" (where the iPod is connected as device /dev/sda). This command will duplicate the entire iPod drive to the image file. If you only require a section of the drive then substitute sda with the section you need. Change iPod.image to the filename of the image that you wish to use as evidence. The entire process may take some time. Do not assume that nothing is occurring as imaging often takes a long time.

Type "md5sum /dev/sda" to generate a checksum for the entire drive and record this value.

Summary

The chapter started with an introduction to the Personal Digital Assistant device, and how the technology of today has pretty much provided us with a handheld computer. We continued the discussion with a look at the concept of PDA forensics. And how many of the same things that have to be considered in forensics on normal systems; however, we discussed some of the difference that had to be considered when performing forensics on PDA devices.

Once we had covered the considerations you have to make when it comes to PDA forensics we moved on and discussed the methods of investigating a PDA. We talked about securing the evidence, and how the PDA, docking cradle and any external memory cards should be seized. The next method we discussed was the acquiring of the evidence, we covered how we have to create an exact image of the evidence, and once we have secured and acquired the evidence we need to go on and examine the evidence we have acquired.

We continued in the chapter talking about the forensic examination considerations when confronted with a Blackberry (RIM) device. We concentrated on how the Blackberry (RIM) has similarities to the PDA, but one way that they do differ is the Blackberry (RIM) does not require synchronization to receive a significant amount of information. The Blackberry (RIM) is always on, and to make our task a little more difficult it is in a state where it is susceptible to receiving push technology updates at any time; therefore, we discussed how it is imperative that we take this into account when preparing to examine the Blackberry (RIM). We also discussed in this chapter the software that is available to assist us when we are examining the Blackberry (RIM), an excellent package of software is the Software Development Kit (SDK) from Blackberry themselves. We also discussed some of the ways and tools available to attack the Blackberry (RIM), we discussed the Blackberry Attack Toolkit, the Attack Vector, and the forms of hijacking or blackjacking as it is called. Finally, we wrapped up this chapter by discussing the methods of securing the Blackberry (RIM), we did this by discussing the Blackberry Signing Authority Toolkit that provides tools to help developers protect their data and intellectual property, and uses asymmetric cryptography to authenticate information.

Notes

Andersen, S & Abella, V (2004)," Changes to functionality in Microsoft Windows XP service

pack two"
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2otech.mspx

Knaster, S. (2004) "Hacking iPod and iTunes" John Wiley & Sons.

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

Solutions Fast Track

PDA Forensics

- ☑ PDA Forensics is very similar to forensics of any system.
- ☑ With the PDA being a handheld type of computer, you process data and information the same as you do when investigating a PC.

Investigative Methods of PDA Forensics

- ☑ Prior to investigating the PDA we have to secure and acquire the evidence.
- ☑ There are four steps to investigating a PDA:
  - Examination
  - Identification
  - Collection
  - Documentation

PDA Investigative Tips

- ☑ If the device is in the "on" state you have to preserve the state by supplying adequate power.
- ☑ If the device is in the "off" state, leave it in that state, switch on the device, not battery and photograph the device.
- ☑ If device is in the cradle avoid any communication activities.

- ☑ If wireless is "on" eliminate any activity by placing the device in an envelope, anti-static and isolation bag.

Deploying PDA Forensic Tools

- ☑ PDA Secure is a tool that provides enhanced password protection, encryption and data wiping.
- ☑ PDA Seizure allows PDA data to be acquired, viewed and reported on.
- ☑ EnCase provides many tools that allow investigators to conduct complex investigations efficiently?

Introdution to Blackberry

- ☑ The Blackberry device is similar to the PDA when it comes to forensics.
- ☑ The Blackberry device is a push technology device that does not require synchronization with a PC

Operating Systems of the Blackberry

- ☑ The operating system of the Blackberry (RIM) device has multiple features such as:
  - Over the Air Activation
  - Ability to Syncronize Contacts and Information
  - Password Keeper
  - Customized Display

Blackberry Operations and Security Capabilities

- ☑ The Blackberry device uses the Blackberry Serial Protocol to backup, restore and synchronize data between the Blackberry and the desktop software.
- ☑ The protocol comprises simple packets and single byte return codes.
- ☑ The Blackberry offers two encryption algorithms for protecting dat:

- Triple DES
- AES

Forensic Examination of a Blackberry

☑ The Blackberry device is an always-on and information can be pushed at any time.

☑ The first step in conducting an examination of a Blackberry is to isolate the device. This can be achieved by placing the Blackberry in an area where it cannot receive the push signal.

Attacking the Blackberry

☑ The "attack vector" links and tricks the users by downloading the malicious software.

☑ "Blackjacks" or "hijacks" programs will takeover a Blackberry device, and replace them with malicious devices.

Securing the Blackberry

☑ Clean the Blackberry memory.

☑ Limit password authentication.

☑ Use AES to protect information

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: When conducting a forensic investigation of a PDA, what is the first step in the process?

A: As with any forensic examination, the first step is to have permission to seize the evidence that is required for your investigation.

Q: What sort of tools do I use to conduct a forensic examination of a PDA?

A: Most of the forensic tools that work with images will create an image of a PDA file system, the commercial software product EnCase has this capability as does many others.

Q: If I am preparing to conduct an investigation of a PDA, why must I maintain the charge to the device?

A: Similar to our regular PC, the PDA device has both volatile and non-volatile information, and if the power is not maintained, there is a possibility you could lose information.

Q: Isn't a PDA and a Blackberry the same thing?

A: It is not uncommon to make this assumption, and there are similarities, but there are also many differences. The Blackberry is an always-on device that can be pushed information at any time, and unlike the PDA, the Blackberry does not require synchronization with a PC;

Q: How would I get access to log files on the Blackberry?

A: Some of the best tools for conducting an investigation of a Blackberry come from Blackberry themselves. There is a Software Development Toolkit (SDK) that can access and collect log files and other information.